EC-Council

Building A Culture Of Security



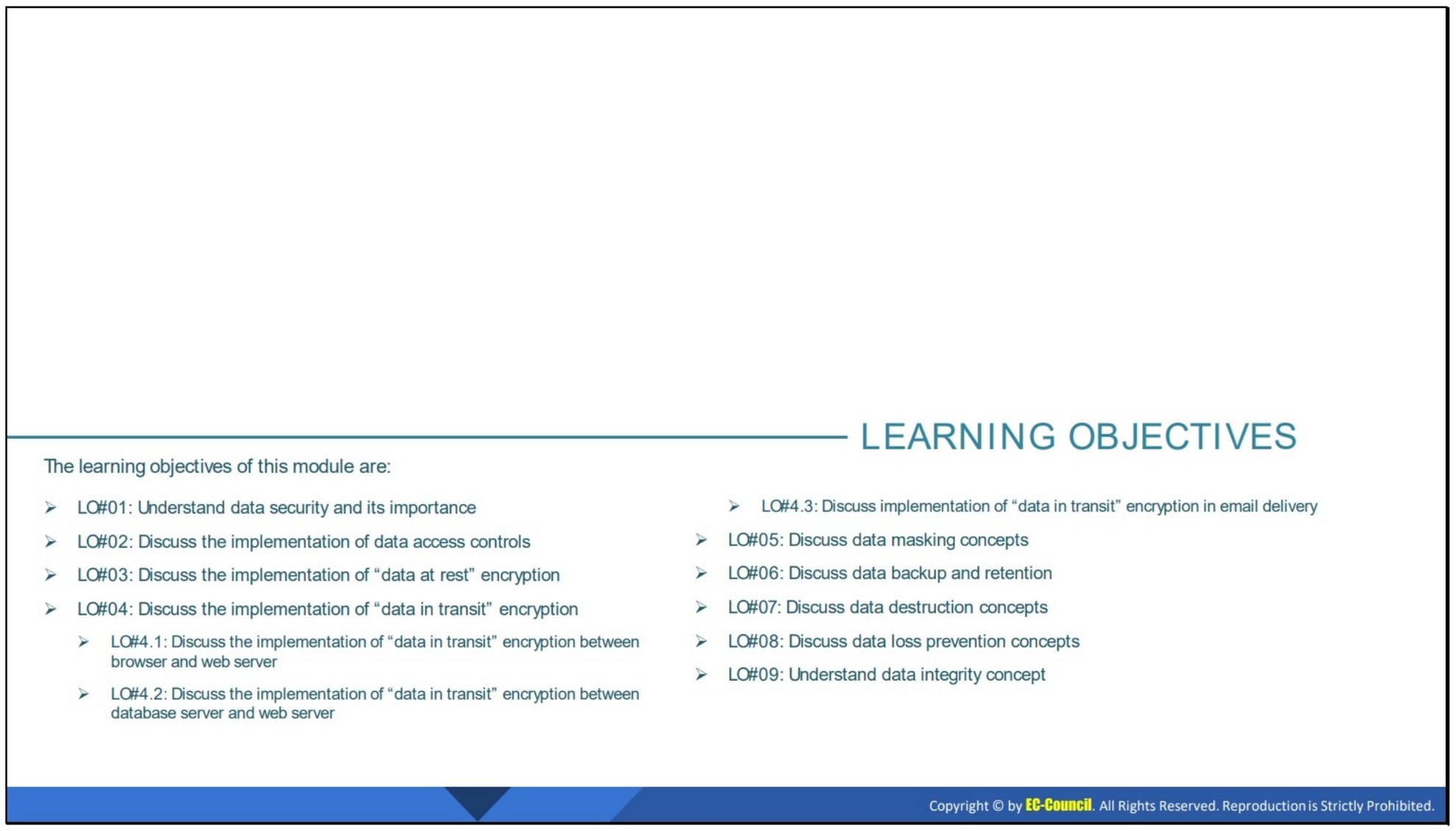
C|ND
Certified Network Defender

Certified Network Defender v3

MODULE 10
DATA SECURITY

EC-Council Official Curricula

This page is intentionally left blank.

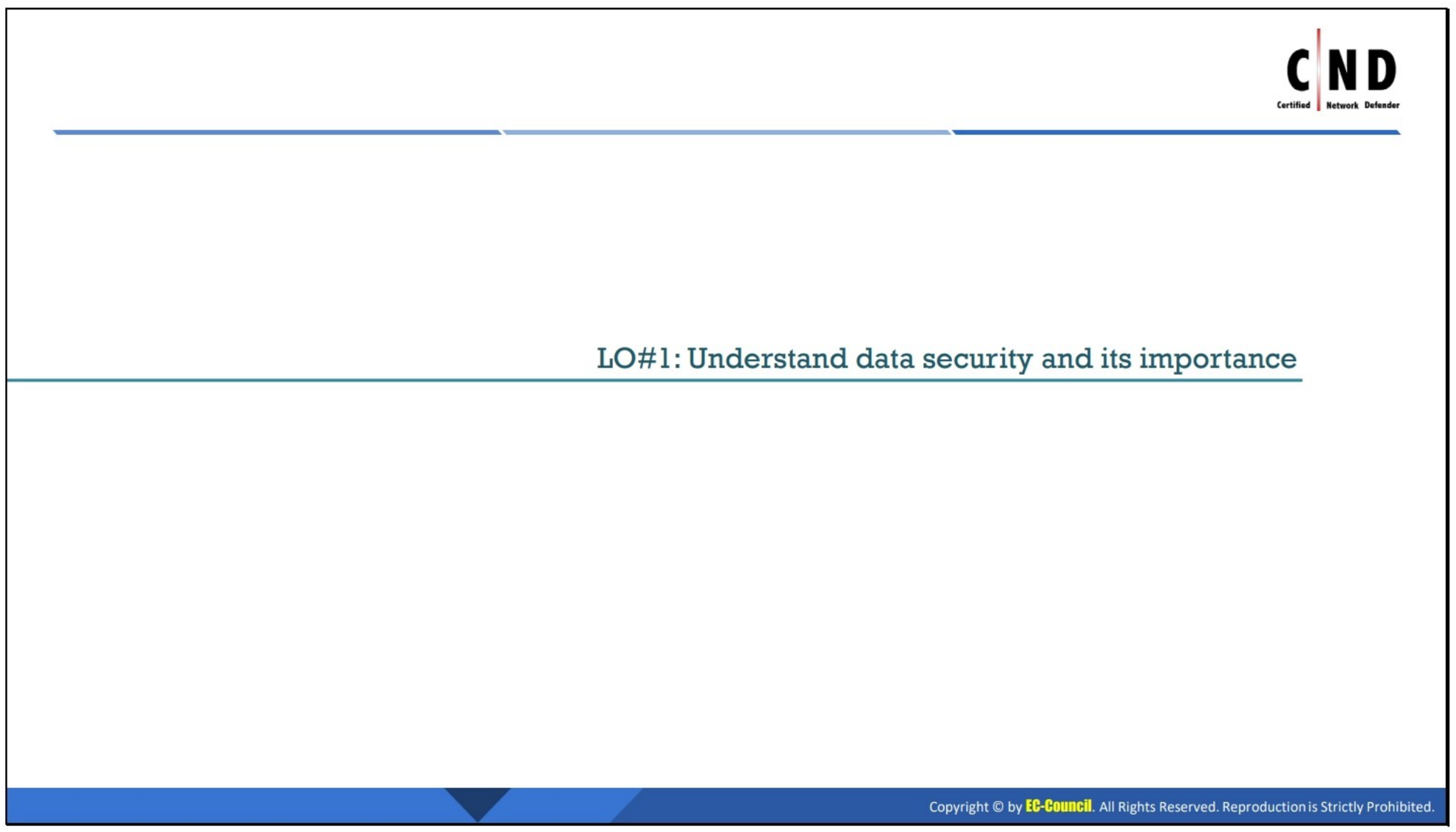


Learning Objectives

Data breaches can be costly for organizations. Therefore, it is important to keep organization data safe from prying eyes. This module explains the importance of data, and various techniques to protect data. The learning objectives of this module are:

- Understand data security and its importance
- Discuss the implementation of data access controls
- Discuss the implementation of "data at rest" encryption
- Discuss the implementation of "data in transit" encryption
  - Discuss the implementation of "data in transit" encryption between browser and web server
  - Discuss the implementation of "data in transit" encryption between database server and web server
  - Discuss implementation of "data in transit" encryption in email delivery
- Discuss data masking concepts
- Discuss data backup and retention
- Discuss data destruction concepts
- Discuss data loss prevention concepts
- Understand data integrity and its importance

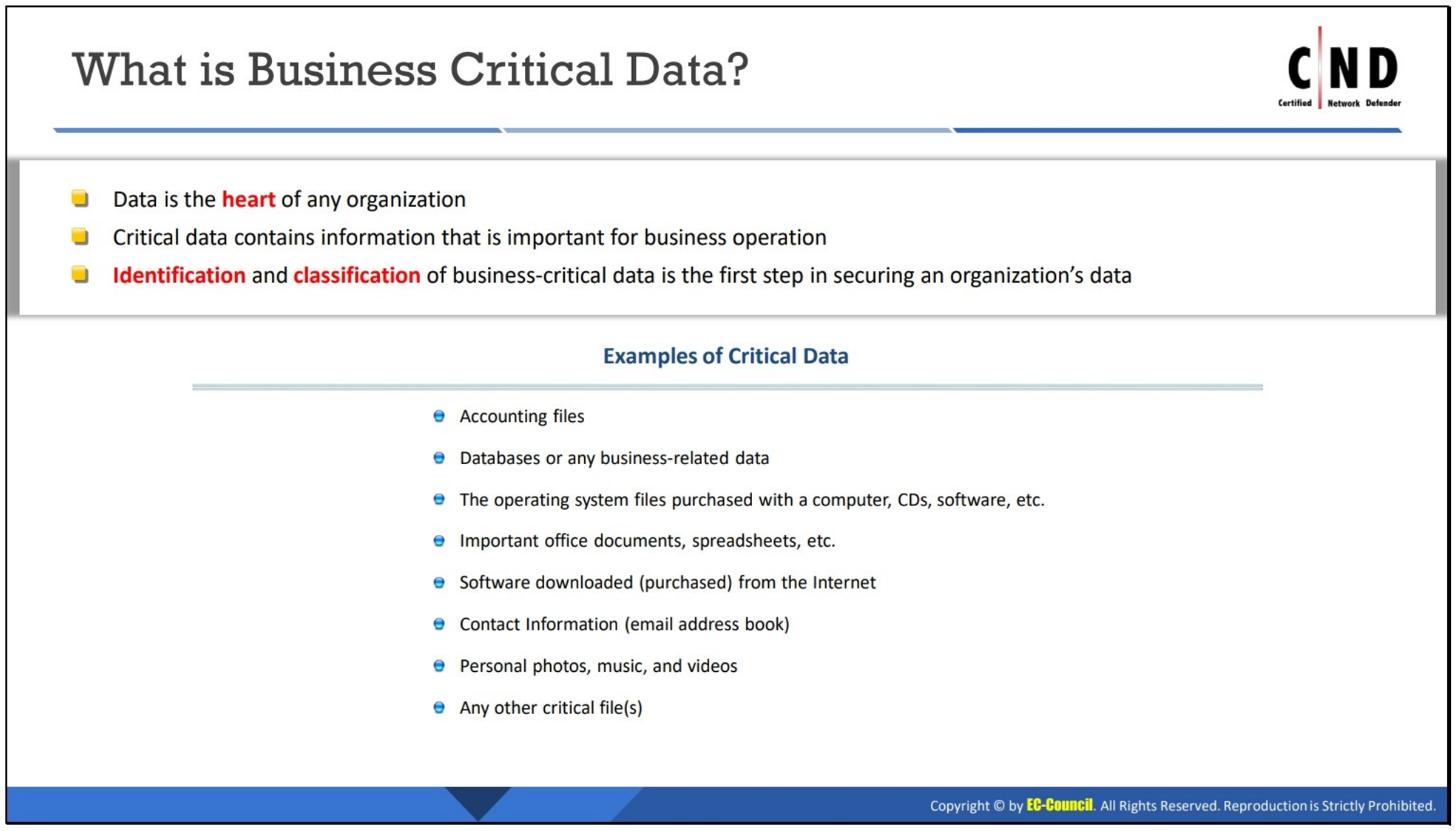
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



LO#01: Data Security and Its Importance

The objective of this section is to explain the importance of data security. The module also explains the three states of data, i.e., data at rest, data in use, and data in transit, and introduces various data security technologies.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



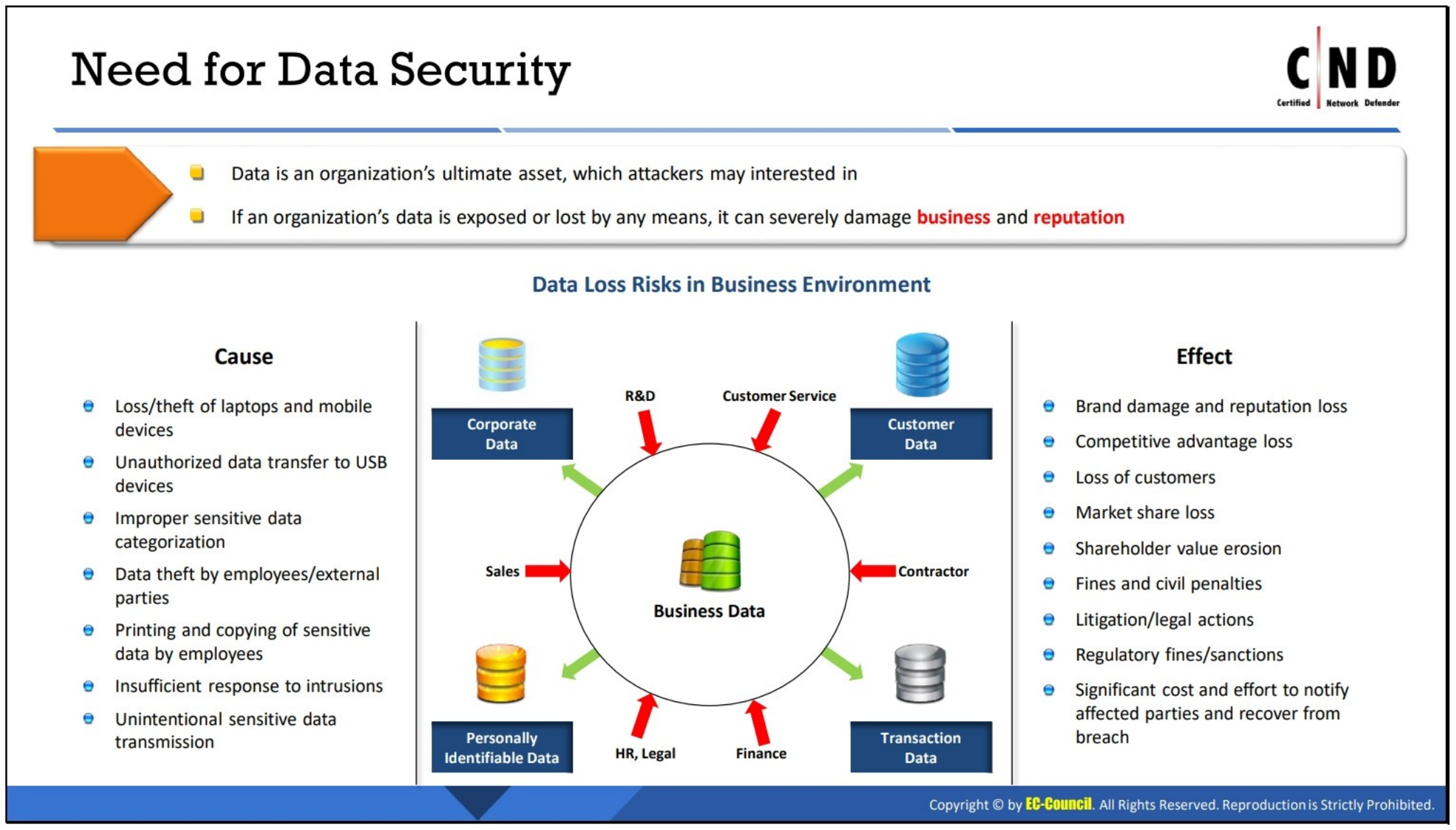
What is Business Critical Data?

Every organization has an abundance of data. An organization should identify their critical data or files. The criticality of data is based on its importance to the organization. This requires analyzing and deciding which information is more important for the organization to function properly. Critical data may consist of revenue, emerging trends, market plans, database, files including documents, spreadsheet, emails, etc. Loss of such critical data can significantly affect the organization.

How Can Critical Data Be Identified?

- Conduct a business impact analysis to determine the critical functions and data in an organization. Identify processes and functions that depend on and co-exist with the critical data.
- Evaluate the impact of data damage on the business.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



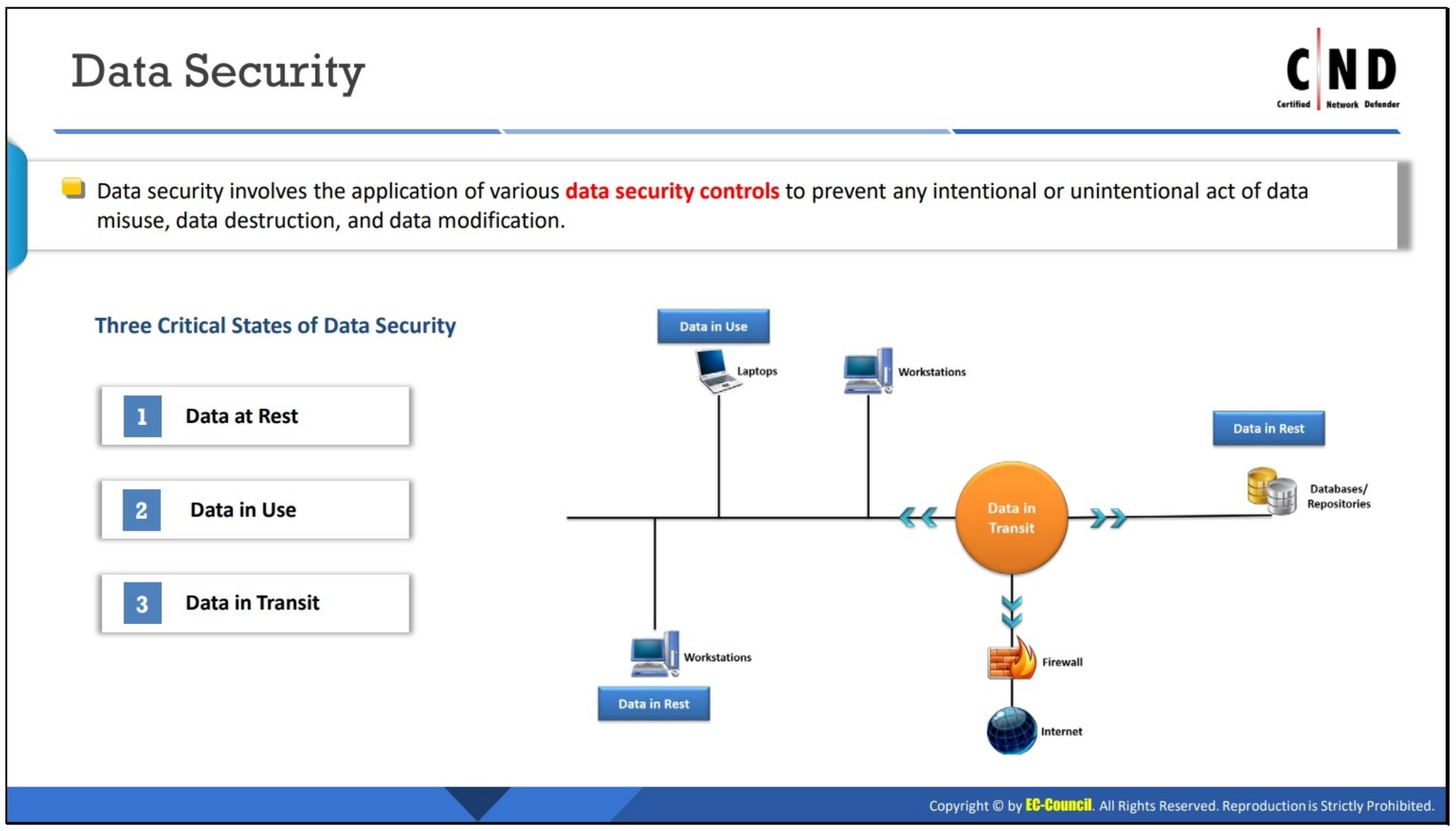
Need for Data Security

Data is an important asset for an organization, and it is essential to safeguard it from cybercriminals. If an organization's data is exposed or lost by any means, it can damage the organization's business and reputation to a great extent.

There are numerous causes for data loss, such as device loss or theft, unofficial transfer of data to USB devices, printing or copying of sensitive data by employees, unknowingly transferring sensitive data, inadequate response to intrusion, etc. The resulting data loss leads to loss of brand loyalty and trust, decreases the number of customers, and affects market share and shareholder value, regulatory fines, legal proceedings, etc.

Data breaches and cyberattacks have increased because of the expansion of computer networks; hence, data security is necessary to protect the data in an organization.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Data Security

Data security involves the application of various data security controls to prevent any intentional or unintentional act of data misuse, data destruction, and data modification.

An organization's data is considered to be secured when they have sufficient provisions for:

- Restricting data from intentional or accidental destruction, modification, or disclosure
- Recovering lost or modified data following incidents
- appropriate data retention and destruction policies

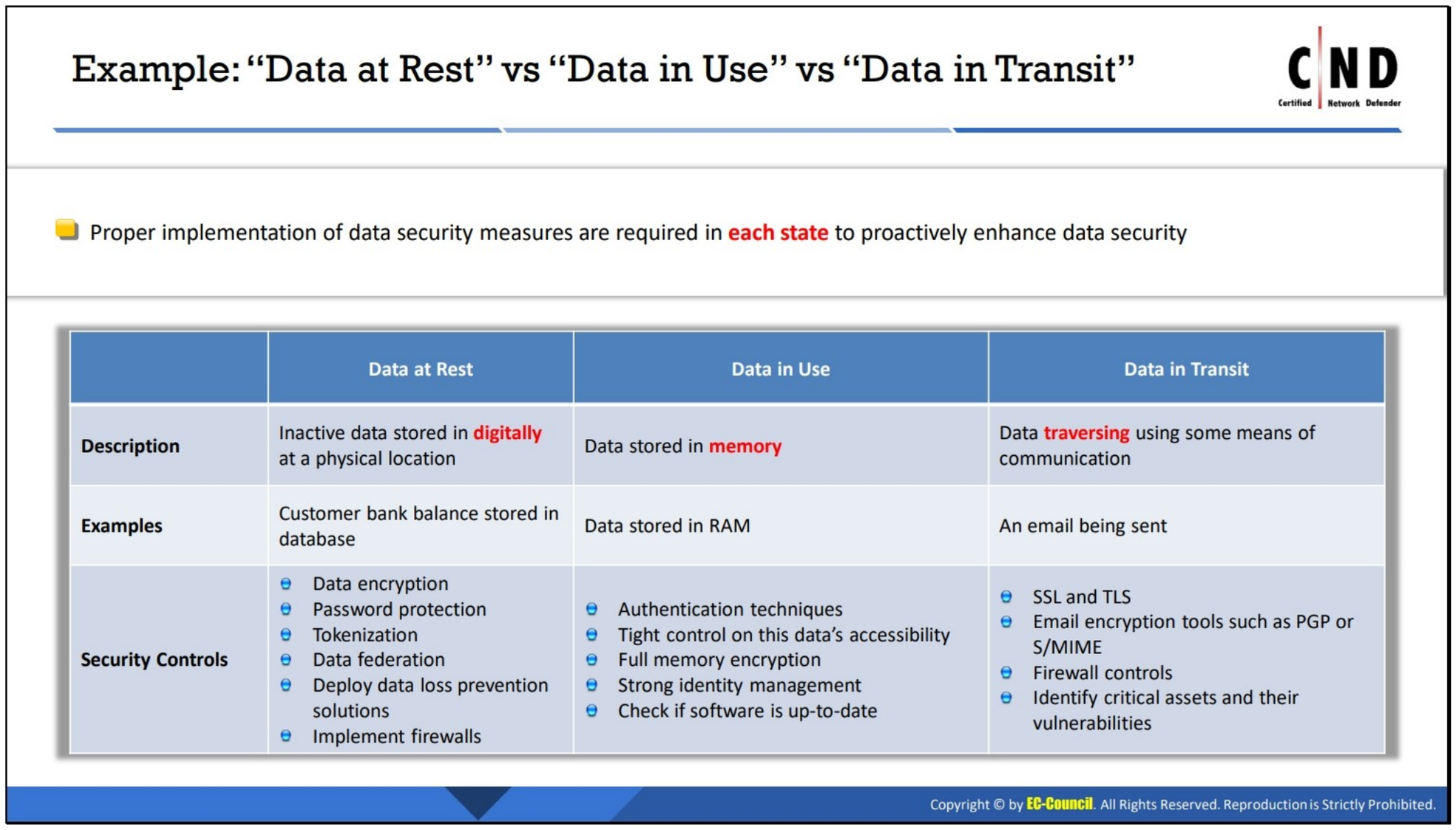
Three Basic States of Data

Data at rest: This data is inactive and is stored on a device or a backup medium such as hard drives, laptops, backup tapes, mobile devices, or at the offsite cloud backup. Data at rest remains in a stable state. The data at rest will not move actively in a system or network, and cannot be accessed by an application or program.

Data in transit: This data actively moves from one location to another across the network, or is encrypted before moving and/or being transmitted through encrypted connections such as HTTPS, SSL, transport layer security (TLS), FTPS, etc.

Data in use: This data is stored or processed by RAM, CPUs, or databases. It is not passively stored on the system, but actively moves across IT infrastructure. It is updated, erased, processed, accessed, and/or read by the system.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Example: "Data at Rest" vs "Data in Use" vs "Data in Transit"

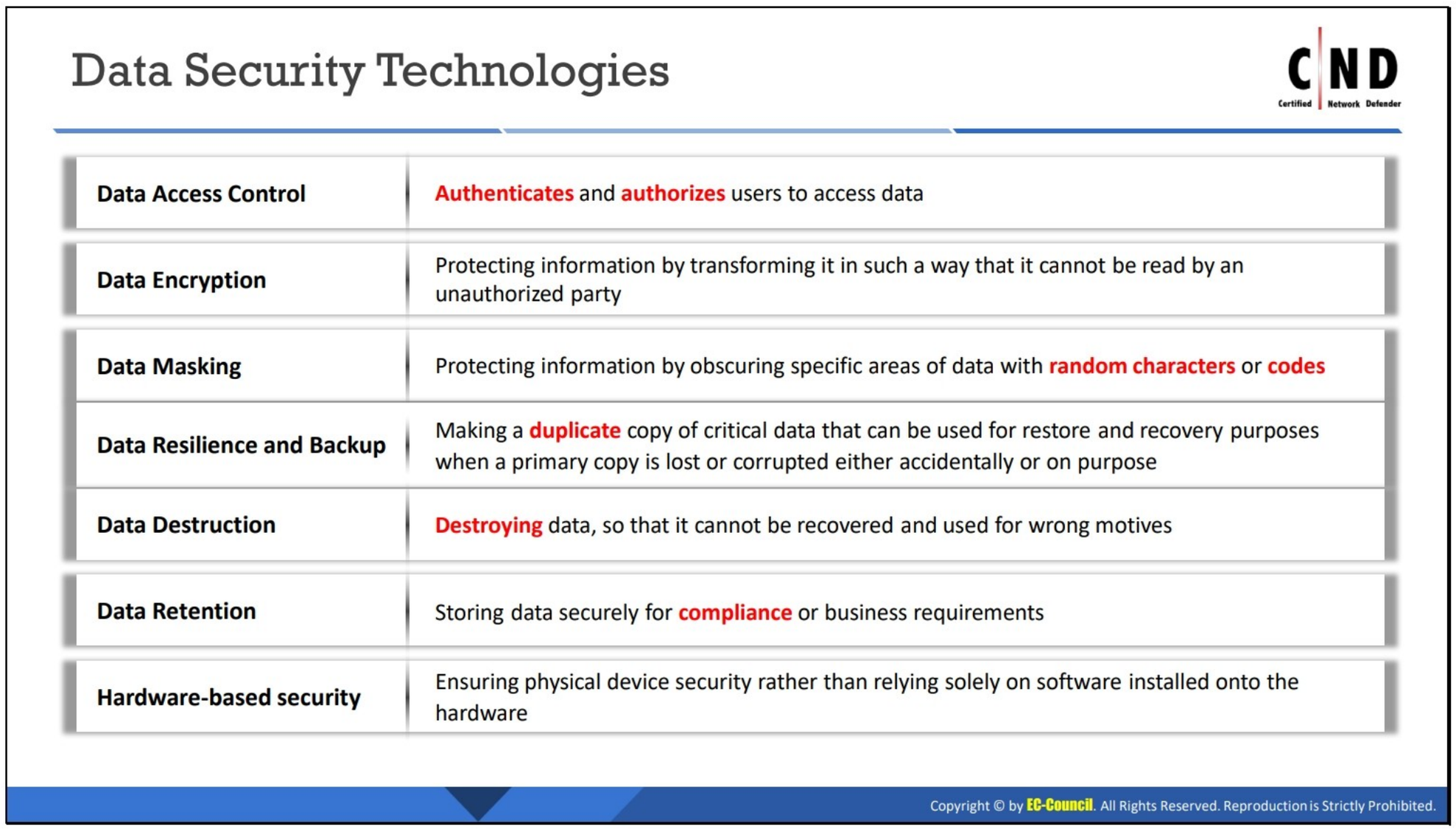
A proper implementation of security measures is required in each state to proactively enhance data security.

Various states of data, their specific examples, and security controls to protect against attacks are as follows.

	Data at Rest	Data in Use	Data in Transit
Description	Inactive data stored in digitally at a physical location	Data stored in memory	Data traversing using some means of communication
Examples	Customer bank balance stored in database	Data stored in RAM	An email being sent
Security Controls	• Data encryption • Password protection • Tokenization • Data federation • Deploy data loss prevention solutions • Implement firewalls	• Authentication techniques • Tight control on this data's accessibility • Full memory encryption • Strong identity management • Check if software is up-to-date	• SSL and TLS • Email encryption tools such as PGP or S/MIME • Firewall controls • Identify critical assets and their vulnerabilities

Table 10.1: Data at Rest vs Data in Use vs Data in Transit

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Data Security Technologies

Data Access Control

Data access controls enable authentication and authorization of users to access the data. It is an important component of security compliance programs that protect unauthorized access to confidential information.

Data Encryption

Protecting information by transforming it so that it becomes unreadable for an unauthorized party. It safeguards corporate secrets, classified information, and personal information. The encrypted data cannot be read by any unauthorized persons or entities.

Data Masking

Protecting information by obscuring specific areas of data with random characters or codes. Data masking protects sensitive data such as personally identifiable information, protected health information, payment card information, intellectual property, etc. Apart from this, data masking also protects against an insider threat. Implementing data masking will bolster the security strategies of an organization.

Data Resilience and Backup

Making a duplicate copy of critical data to be used for restoring and recovery purposes when the primary copy is lost or corrupted, either accidentally or on purpose. Data resilience allows the data to remain available to the applications if there is any failure in the hosted data. Retaining multiple copies of a data backup help in restoring the data with ease, and mitigate the risks of data corruption or malicious attacks.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Data Destruction

It involves destroying the data so that it cannot be recovered and used for a wrong motive. The destruction of old hard drives or electronic devices should be done securely and safely. Data destruction helps in physically destroying the old information of customers and employees.

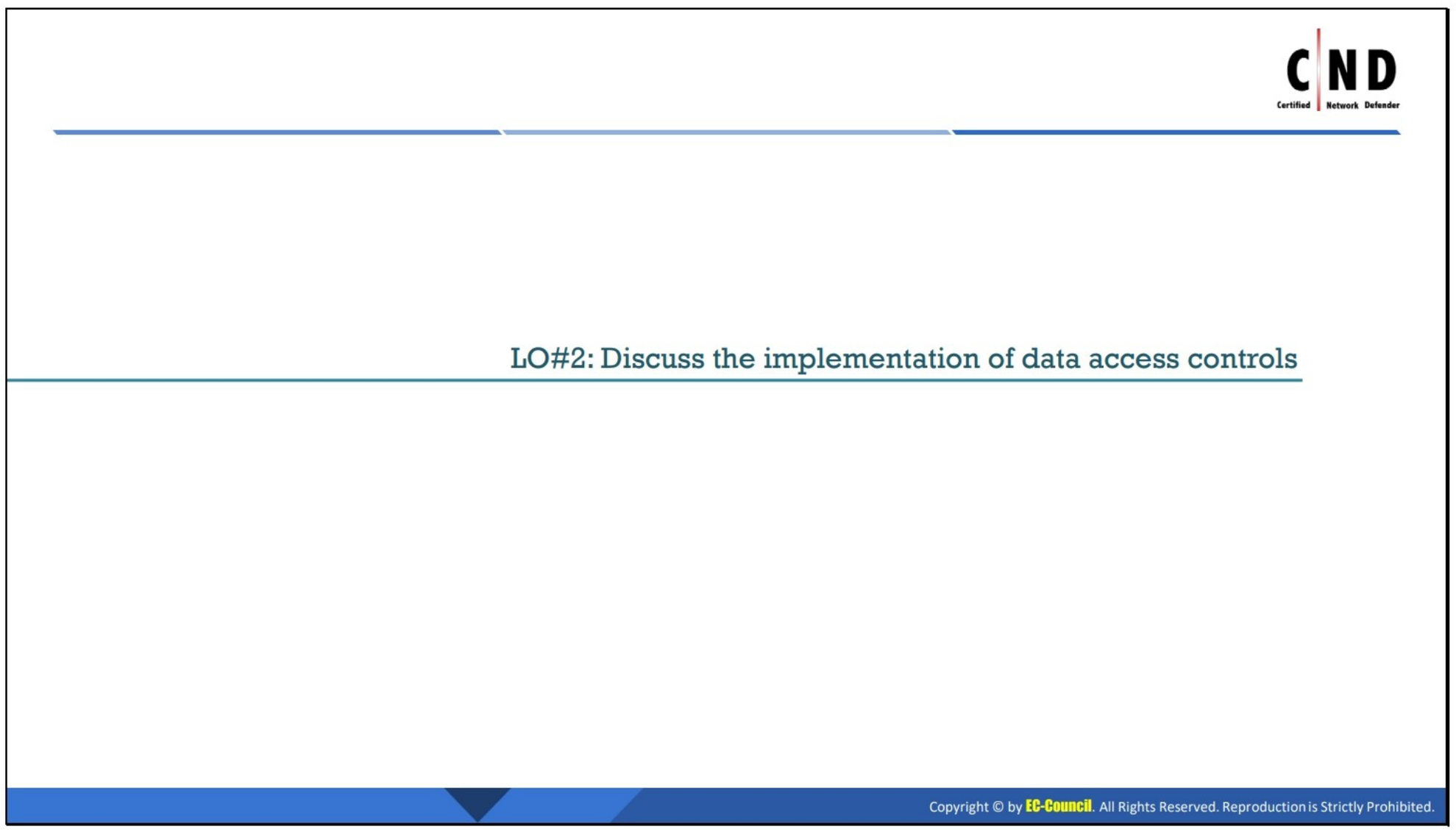
Data Retention

Storing data securely for compliance or business requirements. An organization should have policies and processes for retention and removal of data. Data retention programs have a tremendous impact on data security, and can meet the expectations of customers and governments in safeguarding privacy.

Hardware-based security

Hardware-based security refers to the physical security of a device, rather than relying exclusively on software installed on the hardware. As attackers target all layers of the IT infrastructure, companies require hardware-based protection to ensure hardened devices.

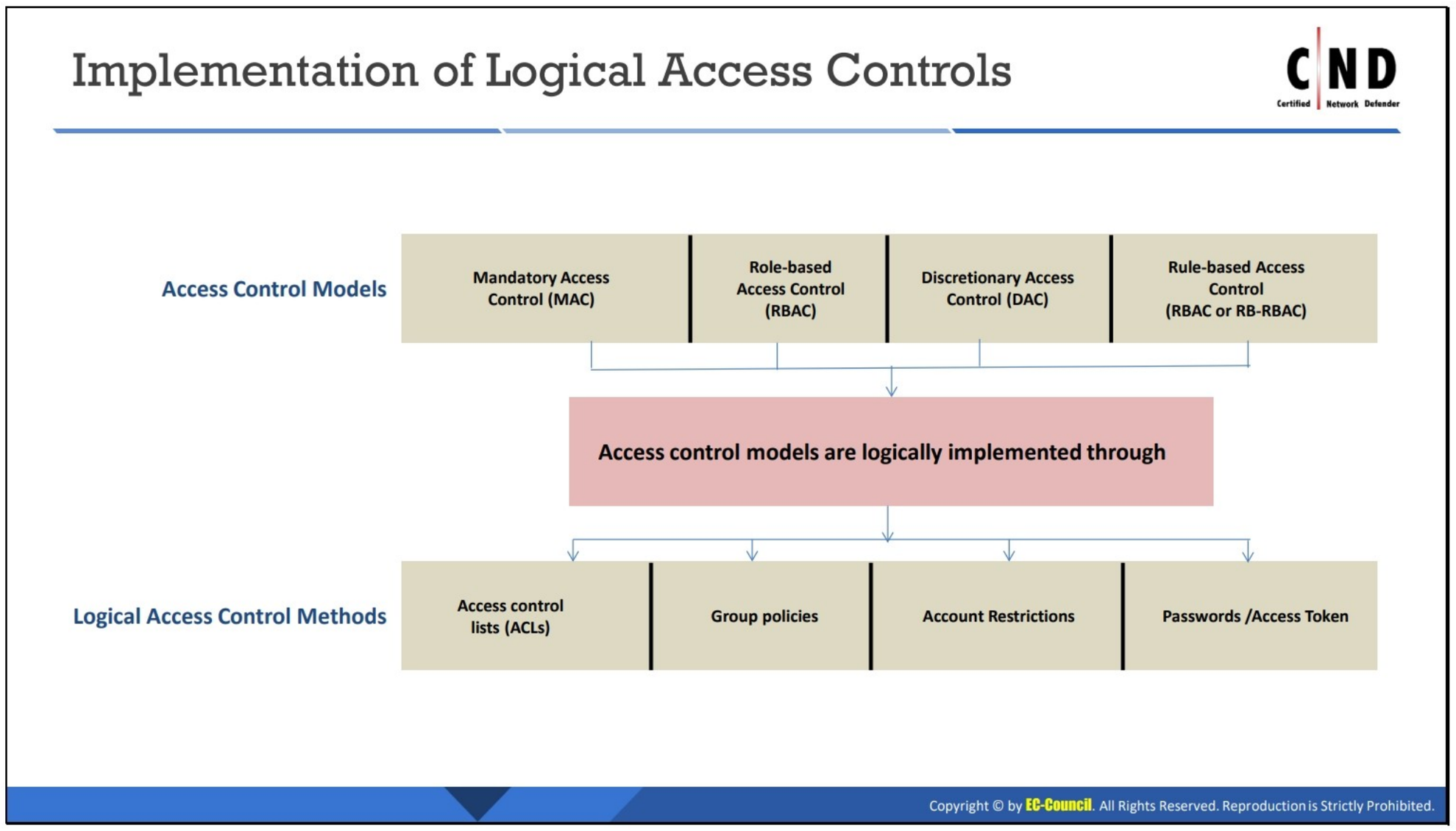
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



LO#02: Implementation of Data Access Controls

The objective of this section is to explain data access controls that is, who can access what type of information, and also discuss the implementation logical data access controls.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Implementation of Logical Access Controls

Logical access control helps in IT security by limiting the users' access to information. Depending on the type and sensitivity of data processed by an organization, an access control model can be determined. Various access control models are logically implemented through

- Access control lists (ACLs)
- Group policies
- Account restrictions
- Password/access tokens

These methods are not mutually exclusive, and many systems implement a combination of these methods.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

ACL: Setting Access Controls and Permissions to Files and Folders in Windows

Applying NTFS permissions

- Typical **file permissions** allowed on the NTFS file system are:
  - Full Control
  - Modify
  - Read and Execute
  - Read
  - Write
- Each of these permissions includes a **logical group** of special permissions

Special Permissions associated with each NTFS File Permission:

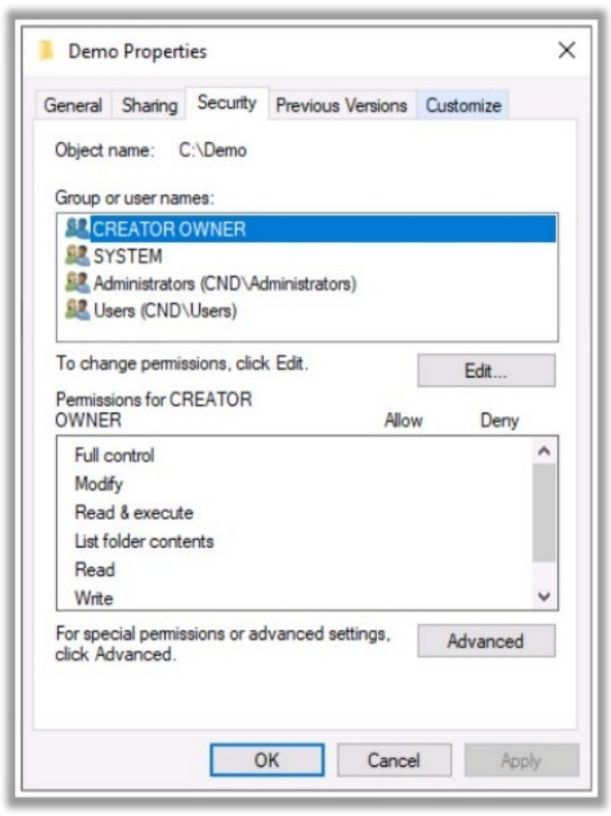
Special Permissions	Full Control	Modify	Read and Execute	Read	Write
Traverse Folder/ Execute File	✓	✓	✓		
List Folder/ Read Data	✓	✓	✓	✓	
Read Attributes	✓	✓	✓	✓	
Read Extended Attributes	✓	✓	✓	✓	
Create Files/Write Data	✓	✓			✓
Create Folders/ Append Data	✓	✓			✓
Write Attributes	✓	✓			✓
Write Extended Attributes	✓	✓			✓
Delete Subfolders and Files	✓				
Delete	✓	✓			
Read Permission	✓	✓	✓	✓	✓
Change Permission	✓				
Take Ownership	✓				
Synchronise	✓	✓	✓	✓	✓

https://technet.microsoft.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

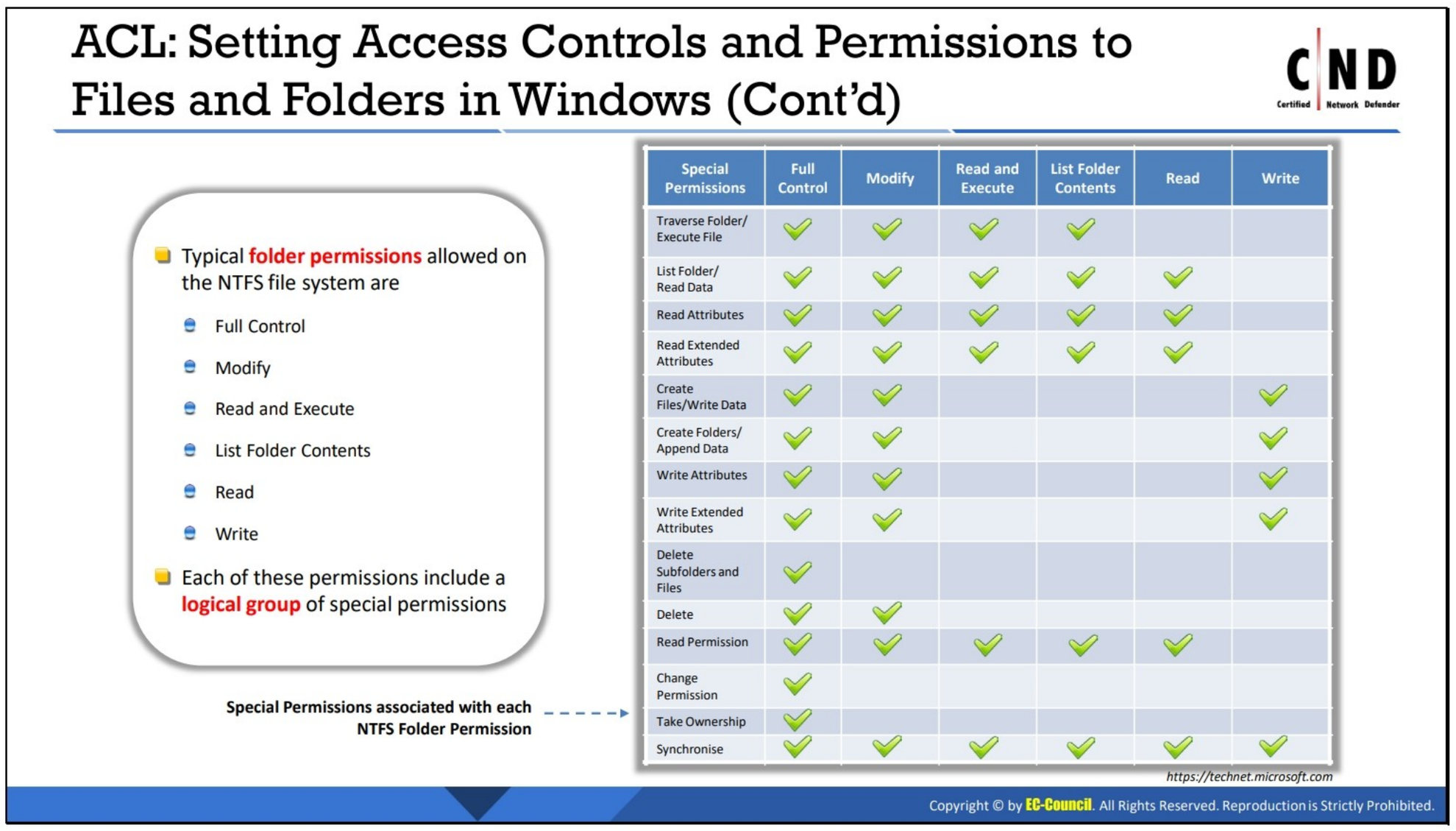
ACL: Setting Access Controls and Permissions to Files and Folders in Windows (Cont'd)

- To set, view, edit, or remove **special permissions**:
  1. Go to the specific file or folder on which you want to set a special permission
  2. Right-click on the file or folder, click **Properties**, and then click the **Security** tab
  3. Click **Advanced**
  4. Click **Add** to set special permissions for a new group or user in Permission Entry Window



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



ACL: Setting Access Controls and Permissions to Files and Folders in Windows

Access controls can authorize users, groups, and computers to access files and folders in a computer. When a user or an application requests for an access to the operating system resources, they need to submit their credentials to the operating system. Credentials are access tokens created every time a user or an application tries to log in. The operating system verifies whether the access token is created as a permission to access the objects before allowing the user or application to access them. Here, the OS compares the details contained in the access tokens with the access control entries (ACEs) for verification. The ACEs can block or permit the services depending on object type. For example, the ACEs for a Printer are print, manage printing, and manage documents. The ACLs contain a combination of an object's ACEs.

- **ACEs**: An ACL can have zero or more ACEs, wherein each ACE has the access to an object. Overall, there are six types of ACEs, out of which securable objects support three (generic types), and the other three are directory service objects (object-specified types).
- The three **generic types of ACEs** are:
  - Access denied ACE: Used in a discretionary ACL to prevent access to any user.
  - Access allowed ACE: Used in a discretionary ACL to allow access to any user.
  - System audit ACE: Used in a system ACL to create an audit log for each attempt by a user while accessing the objects.
- The three **object-specified types** of ACEs are:
  - Access denied, object-specific ACEs: Used in the discretionary access control list to block access to a property or property set. It can even stop the inheritance level of a specified type of child object.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Access allowed, object-specific ACEs: Used in a discretionary ACL to permit access to a property or property set. It can even stop the inheritance level of a specified type of child object.
- System audit, object-specific ACEs: Used in a system ACL to create an audit log when a user attempts to access the child object.

The object-specific types and generic types differ only in the design of the inheritance level.

- **ACLs**: An ACL is a table that provides a detailed description of the access rights of the users for accessing objects. Every object has an ACL that contains the details of the user rights and privileges for accessing that object. Each OS system has specific ACLs. The ACLs have one or more ACEs that contains the user details.
- **Permissions**: Each container or object has a security descriptor attached to itself. This security descriptor contains a detailed description of the user access rights. The security descriptor is created along with the container or object. An ACE represents the permission to users or user groups, and the entire list or set of permissions is contained in an ACL. There are two types of permissions:
  - Explicit permissions: Permissions that are set by default upon creation.
  - Inherited permissions: Permissions inherited from the parent object to the child object.

For example, any files and folders in a folder can inherit the permissions applicable to that particular parent folder. Here, the parent folder has an explicit permission, whereas the files and folders have inherited permissions.

- There are two sets of permission entries for accessing a folder on a file server:
  - Share permission on a folder: Used for files and folders shared across the network or many user accounts. The permissions can be either denied or granted depending on the users or user accounts. The most commonly used shared permissions are full control, change, and read.
  - NTFS permissions on a folder: Control the permissions over a network and local computers. The most commonly used NTFS permissions are full control, modify, read and execute, and read and write.

Applying NTFS Permissions to Files and Folders

Access controls for files and folders can specify which users and user groups can have the access permissions. NTFS files and folder permissions allow users to access files stored on a local computer and also files stored in a shared folder over a network. NTFS also allows the sharing of permissions on shared folders in accordance with file and folder permissions.

- **NTFS permissions for files**:
  - Full control: Specifies whether the user has all permissions to access files. Users with full control have the complete access rights to any file even if permission is denied to them.
  - Modify: Allows the user to read, write, execute, and traverse.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Read and execute: Allows the user to go through each directory and read all files.
- Read: Allows the user to list folders, read files, read attributes, and read permissions.
- Write: Allows the user to create files, write data, create folders, and set attributes.

- **NTFS permissions for folders**:
  - Full control: Specifies whether the user has complete access to folders.
  - Modify: This allows the user to read, write, execute, and traverse.
  - Read and execute: This allows the user to list folders, read files, read attributes, and read permissions.
  - List folder contents: Specifies if the user can access the folders and sub-folders.
  - Read: This allows the user to list folders, read files, read attributes, and read permissions.
  - Write: Allows a user to create files, write data, create folders, and set attributes.

List folder contents permissions can be set only when they are inherited by folders and not files, whereas read and execute can only be set for files and folders.

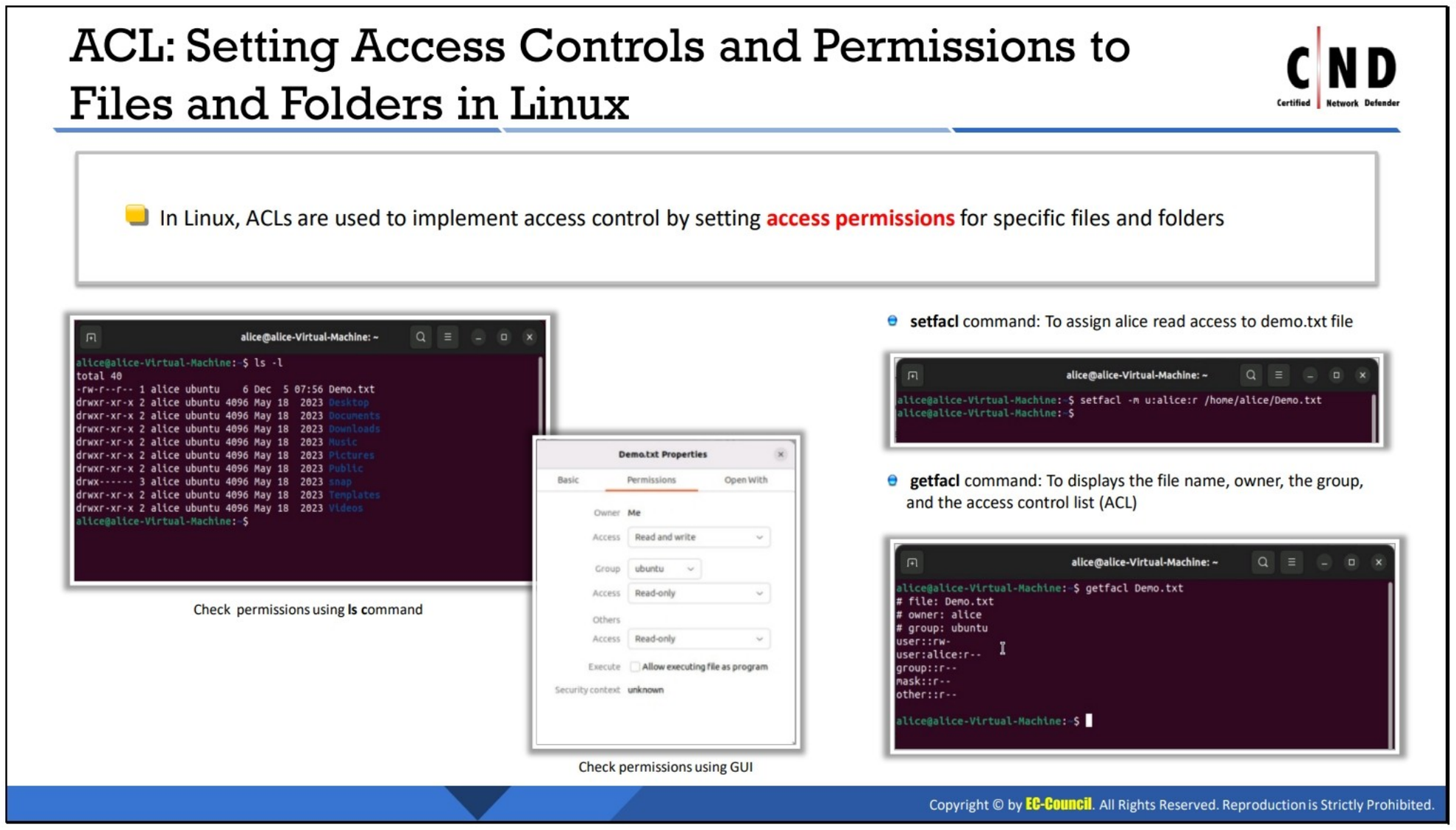
It is possible to back up and restore data on NTFS files. However, it is not possible to set permissions to individual files and folders for FAT files.

To set, view, change, or remove special permissions for files and folders, go to a specific file or folder on which you want to set the special permission.

1. **Right-click** the file or folder, click **Properties**, and then click the **Security** tab
2. Click **Advanced**
3. Click **Add** to set special permissions for the user or new group in the **Permission Entry** window

In Linux, ACLs are used to implement access control by setting access permissions to a specific file or folder.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



ACL: Setting Access Controls and Permissions to Files and Folders in Linux

In Linux, a user can use commands such as chmod, chown, chgrp, etc. to set the permissions on files or folders. ACL provides detailed access control features. It can precisely configure permissions on files or folders.

Steps to Configure ACLs to Set File and Folder Permissions

Step 1: Install ACL Package

Install the acl package to use ACLs. You can use the below statement to install acl package:

 # yum install acl

Step 2: Configure ACL Support on a File System

The file system consisting of the files or directories should be supported. Use the following statement to mount a local ext3 file system with ACL support:

 # mount -t ext3 -o acl [device-name] [mount-point]

For example,

 # mount -t ext3 -o acl /dev/mapper/VolGroup00-LogVol00 /data

If /etc/fstab contains a partition, include the acl options:

 # vi /etc/fstab

LABEL=/data /data ext3 acl 0 0

Step 3: ACL Rules

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

ACL rules define how a specific user or group can access the file or directory. There are two types of ACL rules:

- **Access ACLs**: It specifies user and group access permissions for a specific file or directory
- **Default ACLs**: It is applied only to a directory. It specifies the access permissions that a directory inherits from its parent directory.

Commands for Setting up Access ACL Permission for Files

To set or modify one or more ACL rules on any file or directory, use setfacl command as follows:

 # setfacl -m [rules] [files]

where the **rules** are:

- **u:name:permissions**: It configures access ACL for a specific user [r, w, and x for read, write, and execute, respectively]
- **g:name: permissions**: It configures access ACL for a specific group
- **m:permissions**: It configures the effective rights mask. It is a combination of permissions for user / group.
- **o:permissions**: It configures access ACL for everyone

  For example,

  To set read and write permission in the ACL of file test for a guest user, use the following statement:

  # setfacl -m u:user1:rwx test

  To remove all access ACL rules of the file test for a guest user, use the following statement:

  # setfacl –x u:guest test

  To remove all ACL rules of the file test for a guest user, use the following statement:

  # setfacl –b u:guest test

Command for Setting the Default ACLs

By adding d: before the access rule and defining a directory name in place of a file name, you can configure the default ACL.

 # setfacl -m d:o:rx /[directory]

For example,

To set default ACL for test directory, use the following statement:

 # setfacl -m d:o:rx /Testdir

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

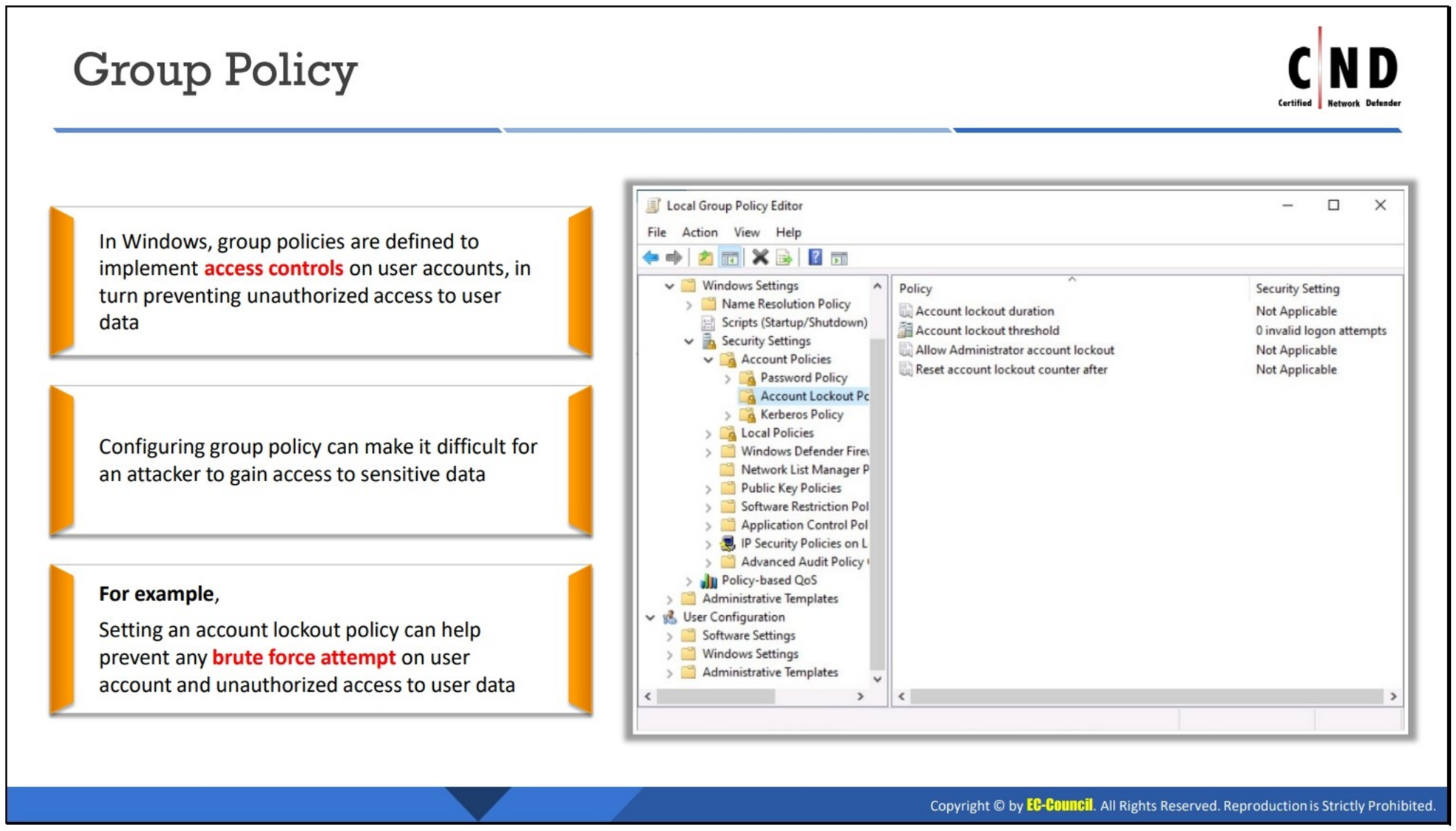
Command to Display ACLs Rules on Files

To display ACL on any file or directory, you can use the **getfacl** command, as shown below.

#getfacl [file/directory]

For example, **#getfacl test** will display the ACL for the test file

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

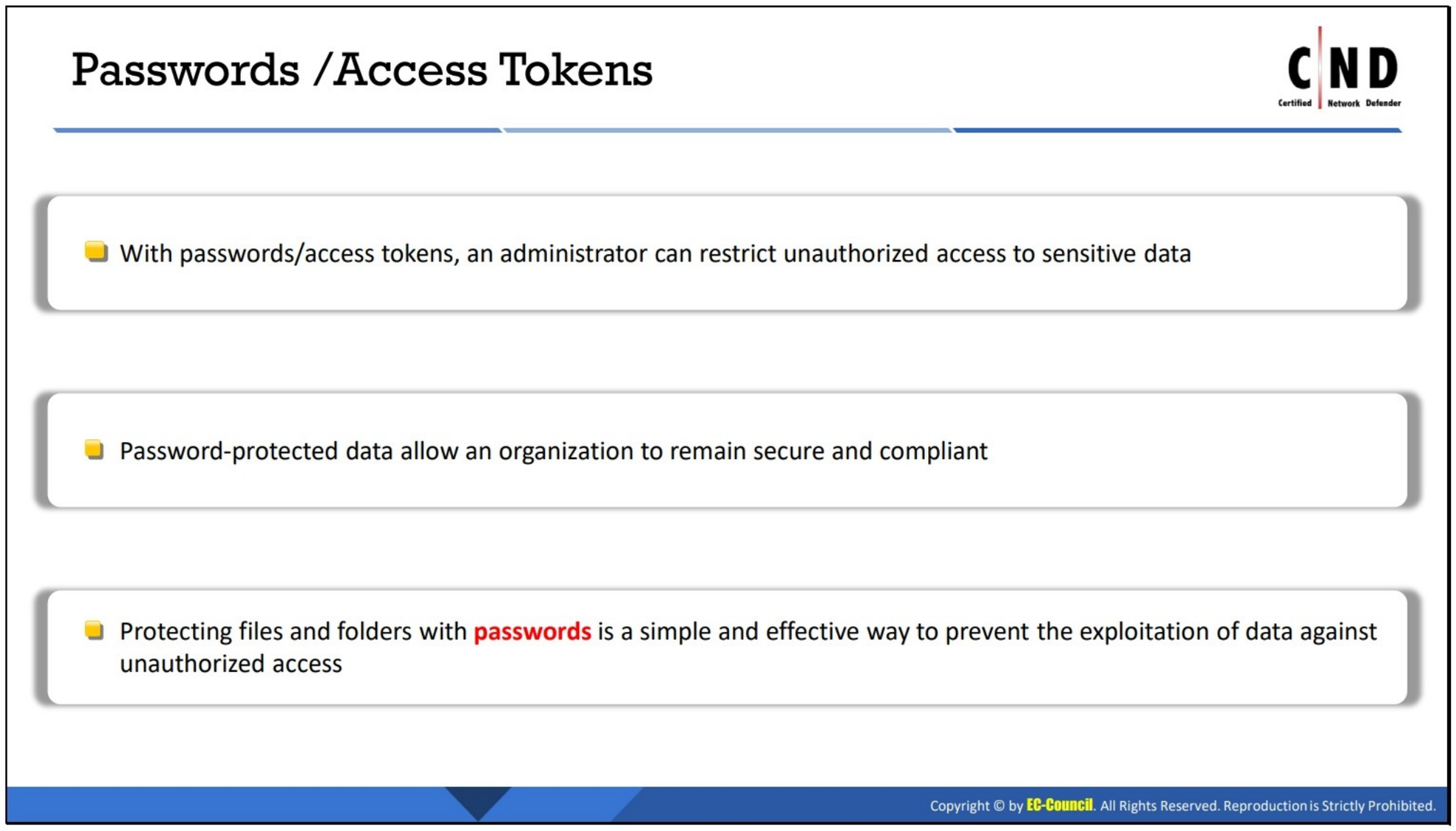


Group Policy

With a group policy, network defender can implement fine-grained access control to restrict users from accessing data. A group policy allows the network administrator to configure security settings for users/computer accounts, which in turn help administrators in restricting unauthorized data access.

Users or groups that have permissions can access the data. A group policy manages user permissions and enhances data security based on the principle of least privilege to multiple users. It safeguards data by preventing access to unauthorized users. Configuring group policy settings protects the device against data breach and make it difficult for an attacker to gain access to sensitive data. For example, account lockout policies are defined to prevent brute force attempts by limiting the number of incorrect logins allowed to a user. This user account restriction can prevent unauthorized data access from a user account on which a brute-force technique is attempted.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Passwords /Access Tokens

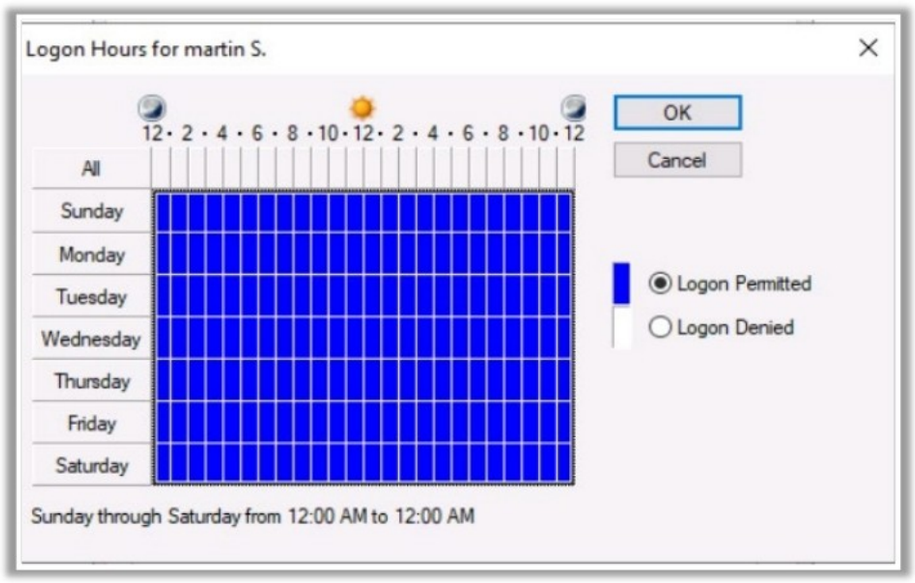
With password/access tokens, the network defender can restrict unauthorized access to sensitive data. Password protection allows only an authorized user to gain access to certain information. Protecting files and folders with passwords is a simple and effective way to prevent the exploitation of data against unauthorized access. For example, password protection on data is enabled when two users use the same account, to prevent one user from accessing the other user's data. Password-protected folders allow an organization to remain secure and compliant.

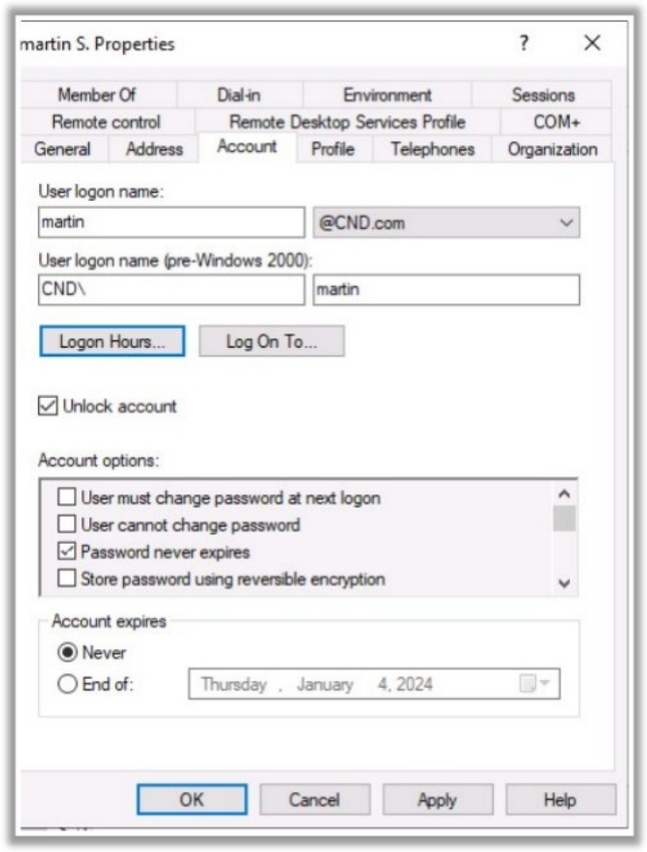
You can either apply an inbuilt password protection mechanism to password-protect your data, or use third-party tools such as Folder Guard, Folder Lock, Protected Folder, etc. to password-protect the folder or directory.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Account Restrictions

- Access controls are implemented by **restricting the users accounts** from accessing data
- **Example**: Enabling time of day restrictions and account expiration



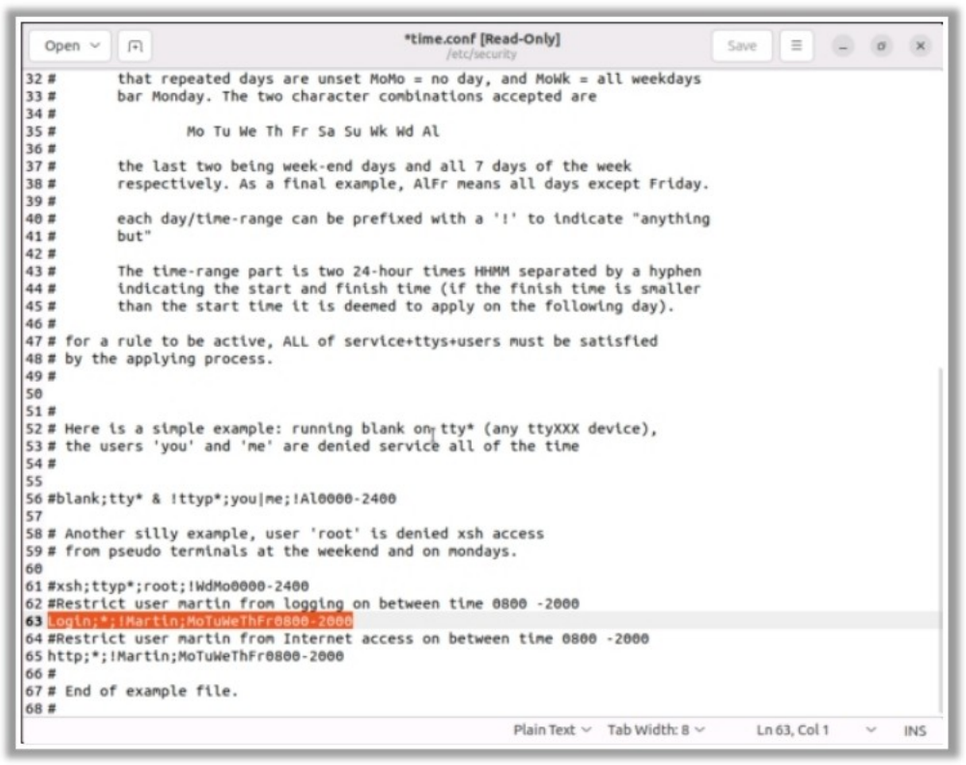


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Account Restrictions (Cont'd)

Restricting Logon Hours for Linux Users

1. To restrict login hours for users in Linux, configure the **pam_time** subsystem module in the PAM module
2. Edit the **'/etc/security/time.conf'** file in the pam_time module



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Account Restrictions

Account restrictions safeguard an account against unauthorized access by temporarily invalidating the account. The number of concurrent logins to a user set through account restrictions mitigates the attack. It prevents the accidental exposure of data and intentional privilege misuse and abuse.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Two types of restrictions can be implemented on an account.

- **Time of day restrictions**: In time of day restrictions, the user can access certain records only up to a certain period of time.
- **Account expiration**: In account expiration, a specific account will expire after a specified date and time, so that attackers cannot exploit them.

Access controls are implemented by restricting the user accounts from accessing resources through time of day restrictions and account expiration.

To Enable Account Expiration

- Open the **Start menu**.
- Locate and select **Administrative Tools**.
- On the displayed window, select **Active Directory Users and Computers**.
- Locate and expand your user account (domain) name.
- Go under the **Users** tab, and right-click on the user name.
- On the list of options, select **Properties**.
- Navigate to the **Account** tab, and Uncheck **Never** under **Account Expires**.
- Click **Apply → OK** (at the bottom of the display window).
- Exit the window.

Logon Hours Restrictions

Logon hours restrictions are implemented by editing the user account as follows.

- Open the user object.
- Select **Account** in the tab.
- Click **Logon hours** button.

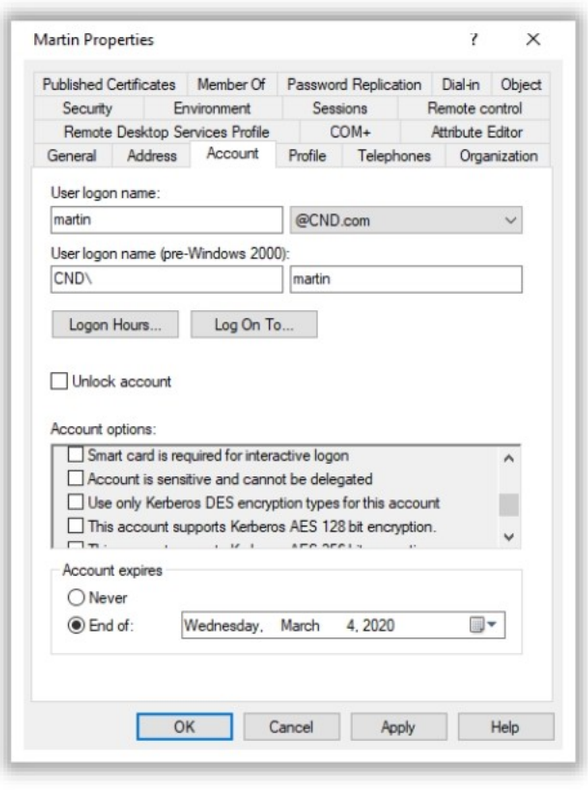


Figure 10.1: Screenshot of Logon Hours Restrictions

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- In the new window, set the restriction or logon time.

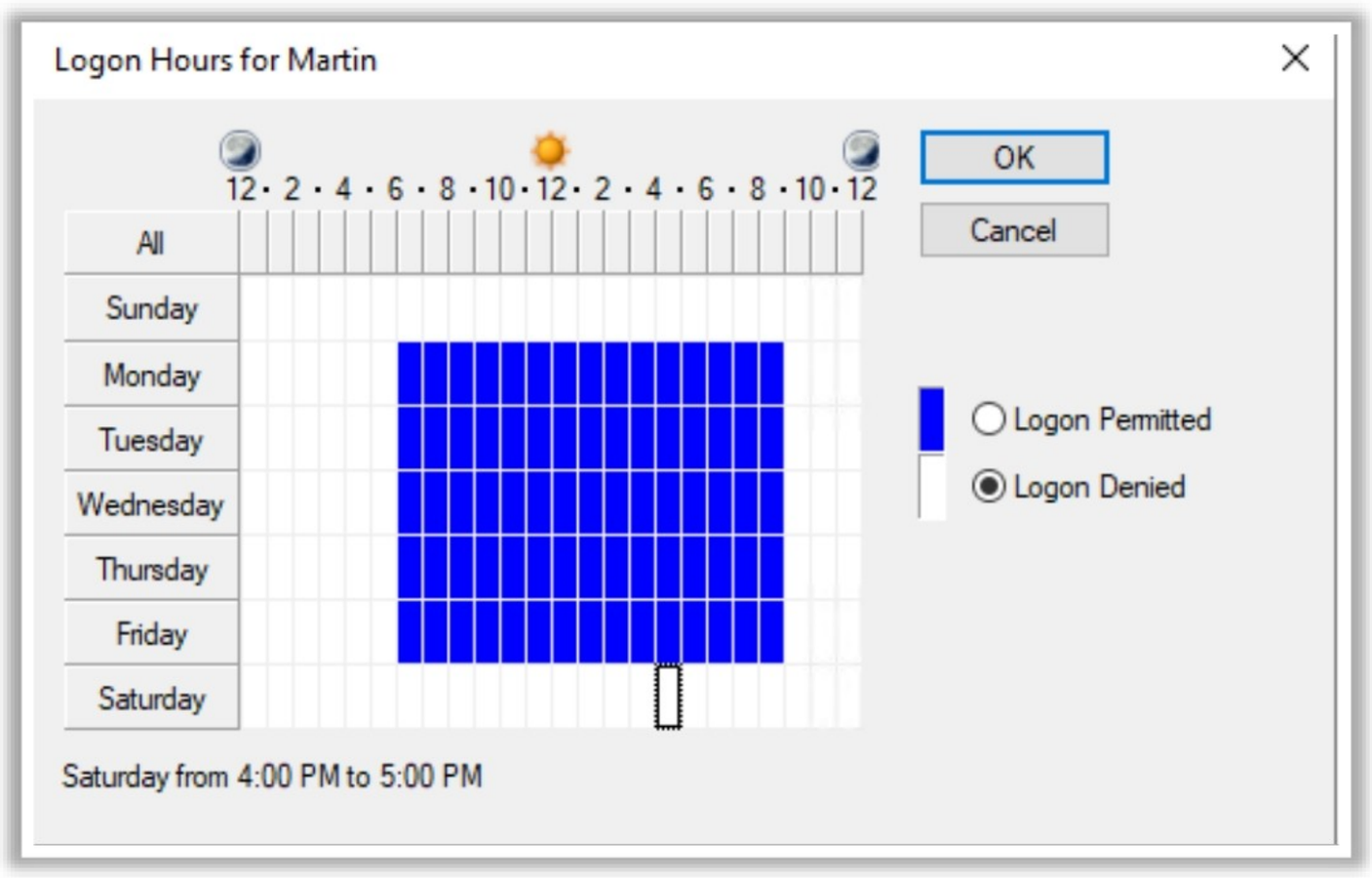


Figure 10.2: Screenshot of Logon Hours Restrictions

Restricting Logon Hours for Linux Users

To restrict login hours for users in Linux, configure the **pam_time PAM module**, which restricts access to a system or specific applications. This module denies access to users based on their name, the service they are applying for, time of the day/week, etc.

The configuration file that provides default rules for time/port access /etc./security/time.conf.

Example: The following figure defines a setting to restrict user Martin from logging on between the 0800 and 2000 hours.

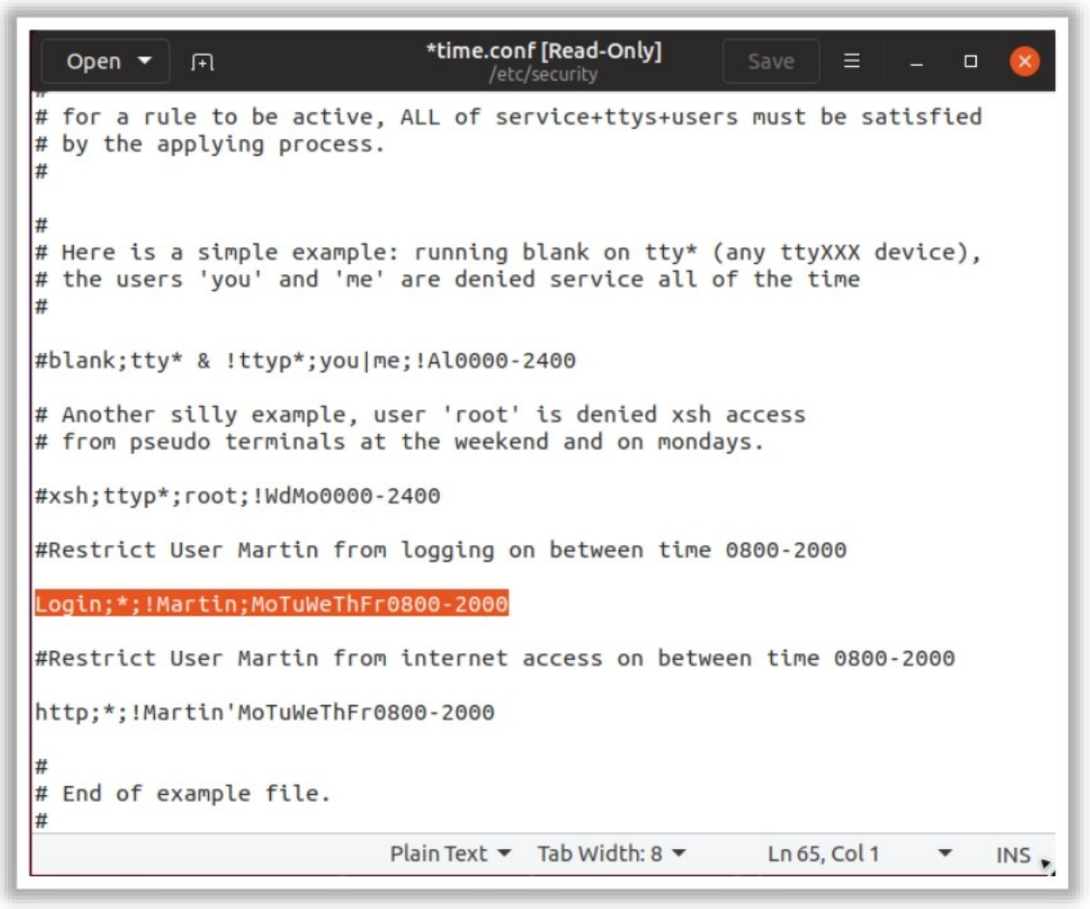
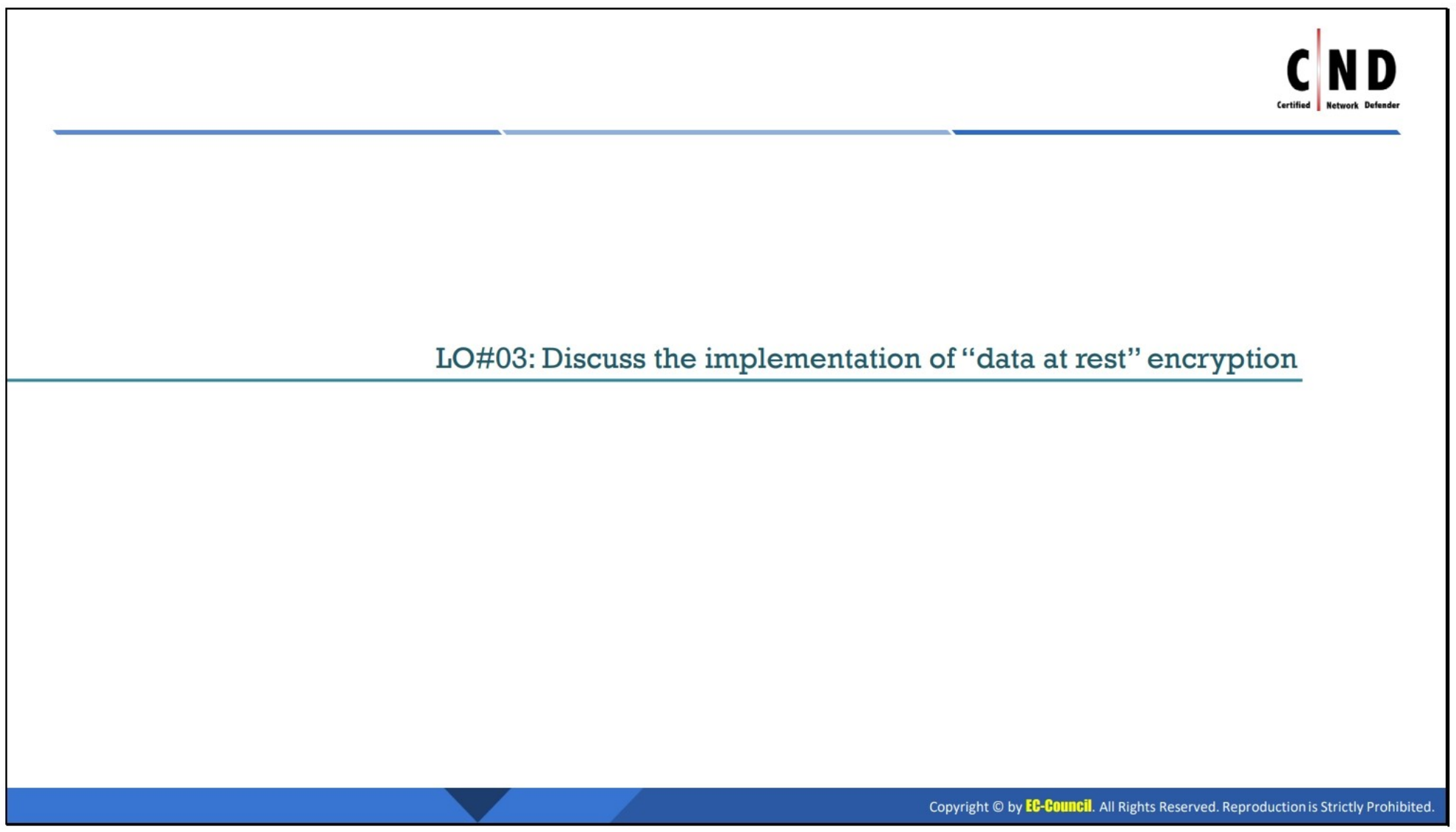


Figure 10.3: Screenshot of Restricting Logon Hours for Linux Users

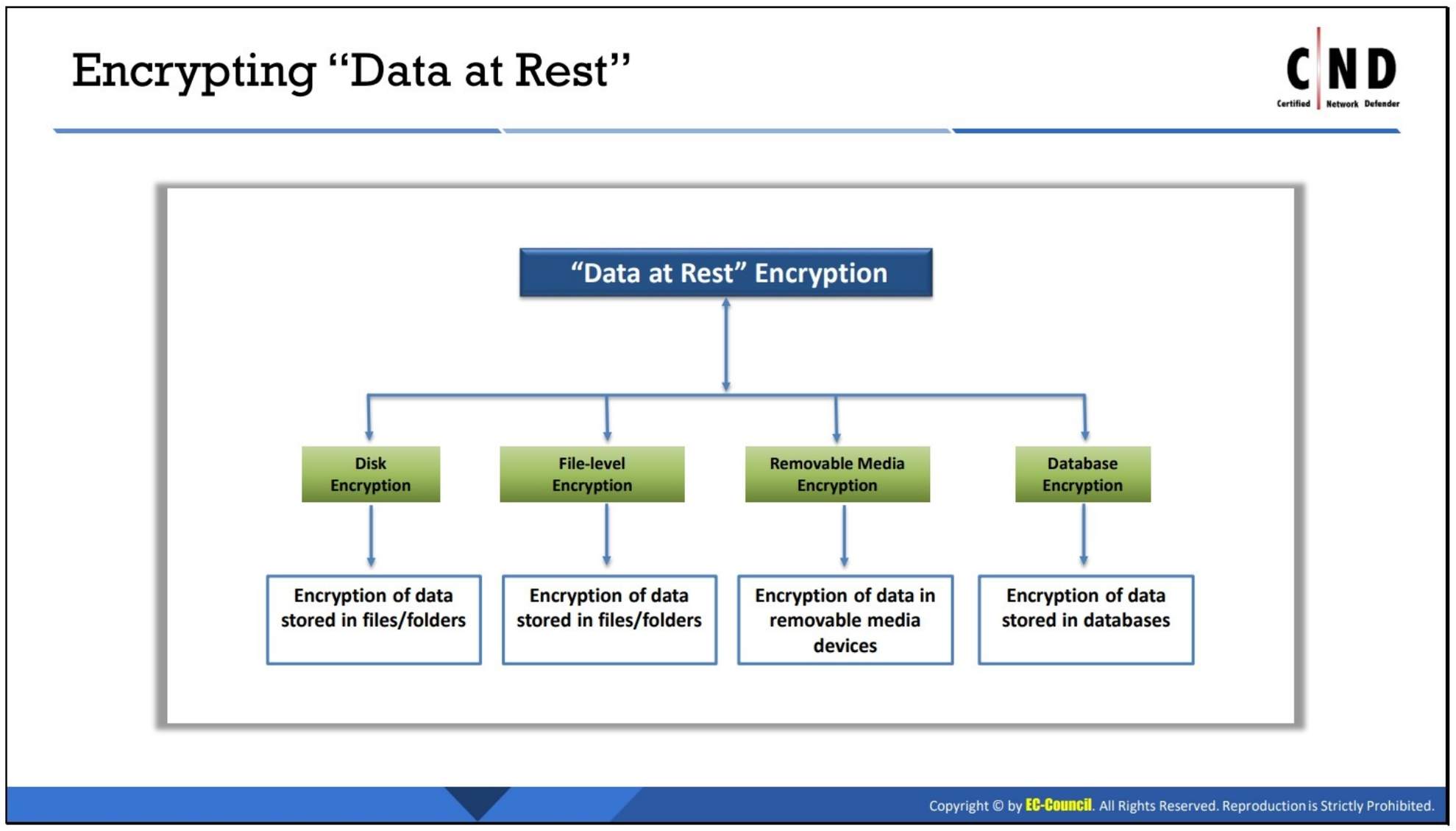
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



LO#03: Implementation of "Data at Rest" Encryption

The objective of this section is to explain the use of encryption technology to secure the data at rest.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Encrypting "Data at Rest"

Disk encryption: Encryption of data stored in a physical or logical disk. Full disk encryption is the encryption of all data in a disk except the master boot record (MBR). The data is automatically converted into a form which cannot be easily deciphered by an unauthorized user. In full disk encryption, the data is encrypted while being written on the disk, and decrypted when the user reads the data from the disk. The benefits of full disk encryption are

- It is a simple encryption method.
- The encryption method is clear and coherent to users, applications, and databases.
- It is a hardware-based encryption with high performance.

File-level encryption: Encryption of data stored in files/folders. In this type of encryption, the encryption occurs at a filesystem level, and in combination with a cryptographic algorithm, the encrypted data will be extremely secure. File-level encryption regulates the access of unauthorized users to files or folders on networks or shared computers. The advantages of file-level encryption are as follows:

- Each file is encrypted with a discrete encryption key.
- Access control is enforced using public key cryptography.
- Both structured and unstructured data are supported.

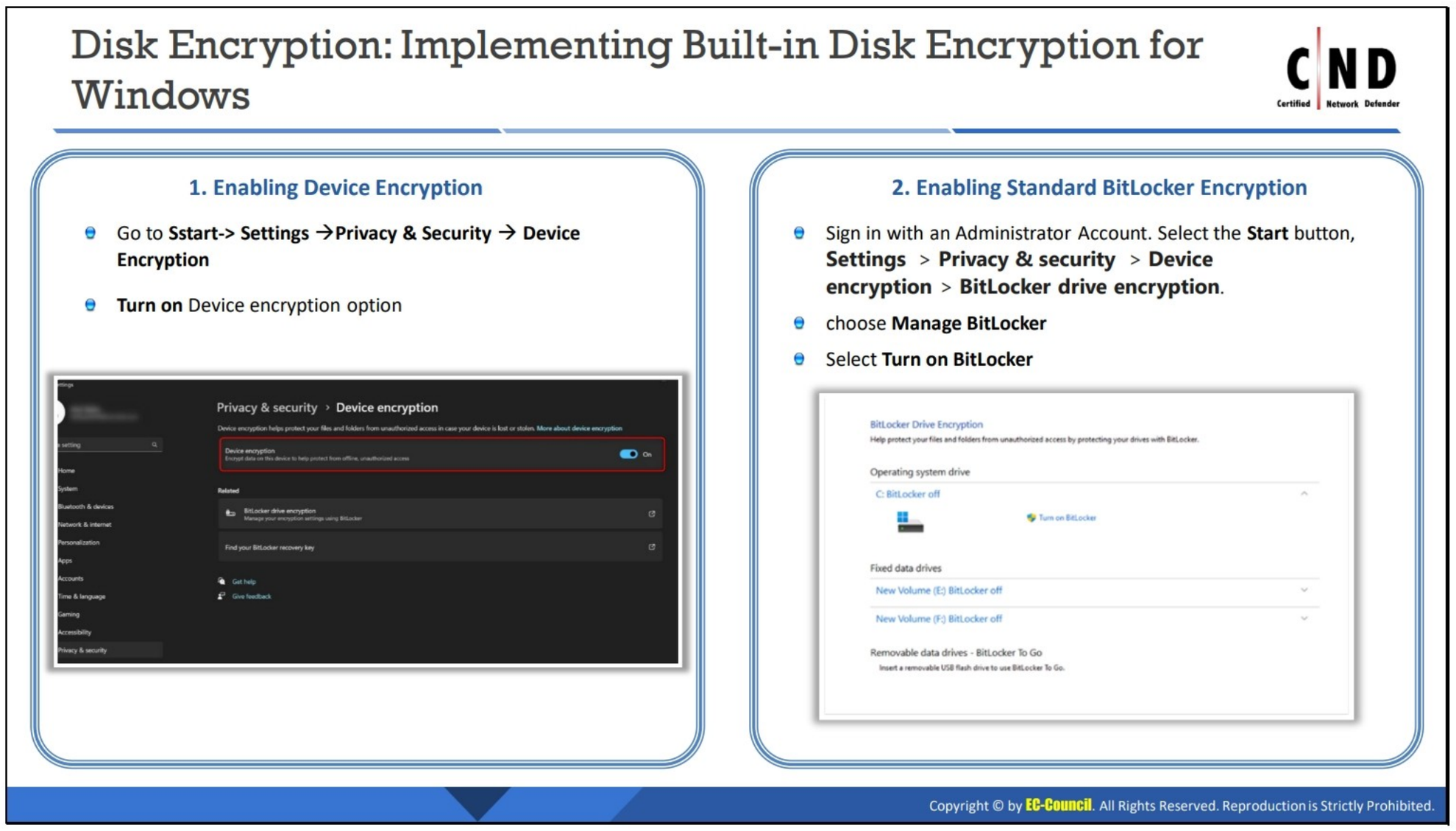
Removable media encryption: Removable media encryption prevents removable media devices such USB flash drives, portable hard disks, digital cameras, smartphones, tablets, etc. from unauthorized access.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Database encryption: Encryption of a specific subset of data or entire data stored in a database. The advantages of database encryption are as follows:

- It safeguards the data in a database.
- It protects against a wide range of threats, including malicious insiders.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Disk Encryption: Implementing Built-in Disk Encryption for Windows

Windows has built-in disk encryption methods to encrypt hard drives and safeguard user data. By default, disk encryption is enabled in all devices using Windows. There are two methods of disk encryption in Windows: device encryption and BitLocker. If the users do not have device encryption, they can enable standard BitLocker encryption.

Device encryption: It is the simplest encryption method and is available in all editions of Windows. If a user loses the device, device encryption can protect the data from unauthorized access. This feature scrambles the entire system drive and secondary drives connected to the device and allows only the user to access the device.

Prerequisites for Device Encryption

1. Trusted platform module (TPM).
2. Unified extensible firmware interface (UEFI).
3. Checking whether the device meets the device encryption requirements**.**

Steps to check whether the device meets the device encryption requirements

- Click the **Start** button**.**
- Search for **System Information**, right-click on the top result, and choose **Run as administrator**.
- Click **System Summary** on the left pane.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Search **Device Encryption Support**; the user device support device encryption if it reads **Meets prerequisites**.

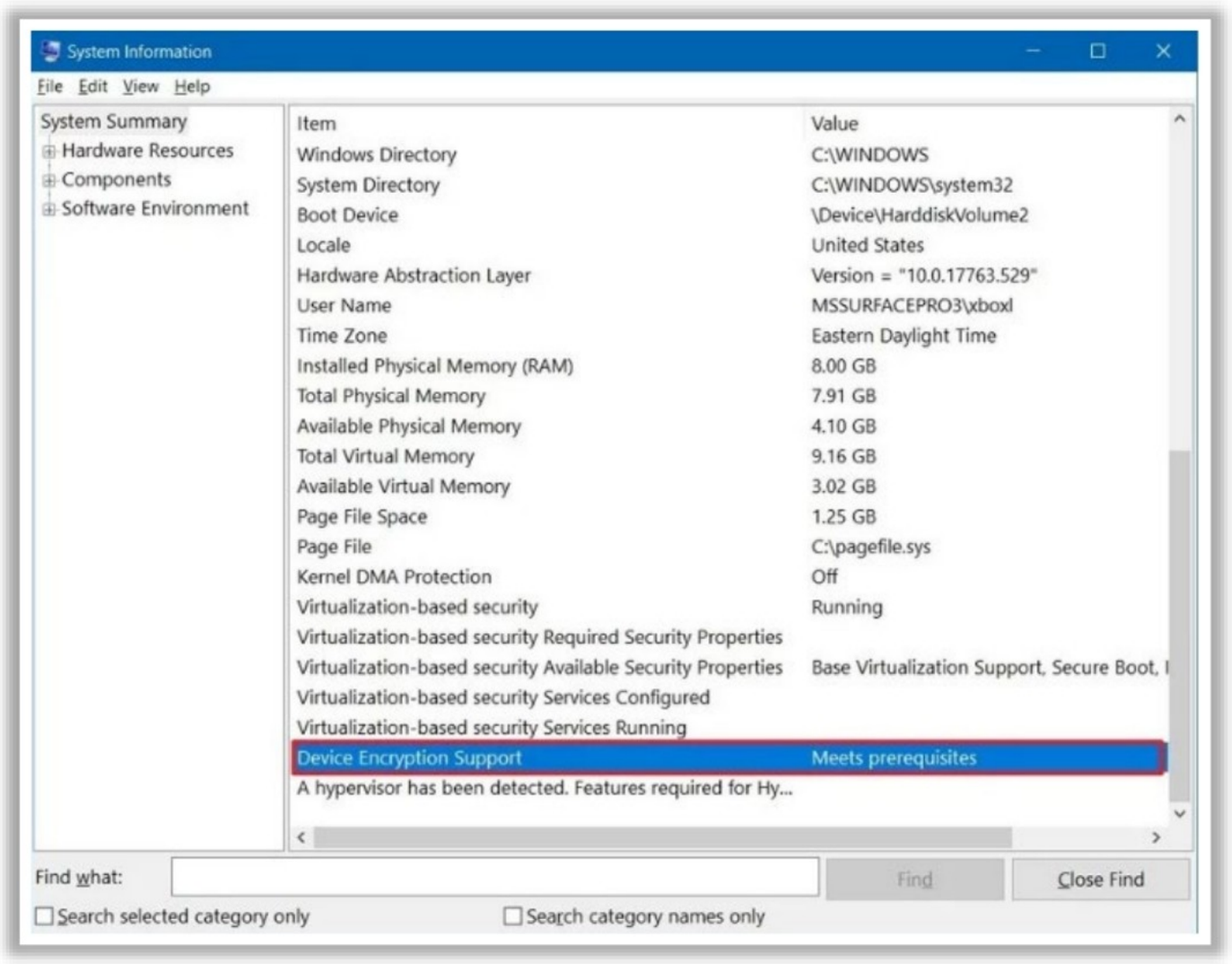


Figure 10.4: Checking Whether the Device is Meeting the Device Encryption Requirements

To Enable Device Encryption

- Open Settings.
- Select **Update & Security.**
- Choose **Device encryption.**
- In the **Device encryption** section, click the **Turn on** button.

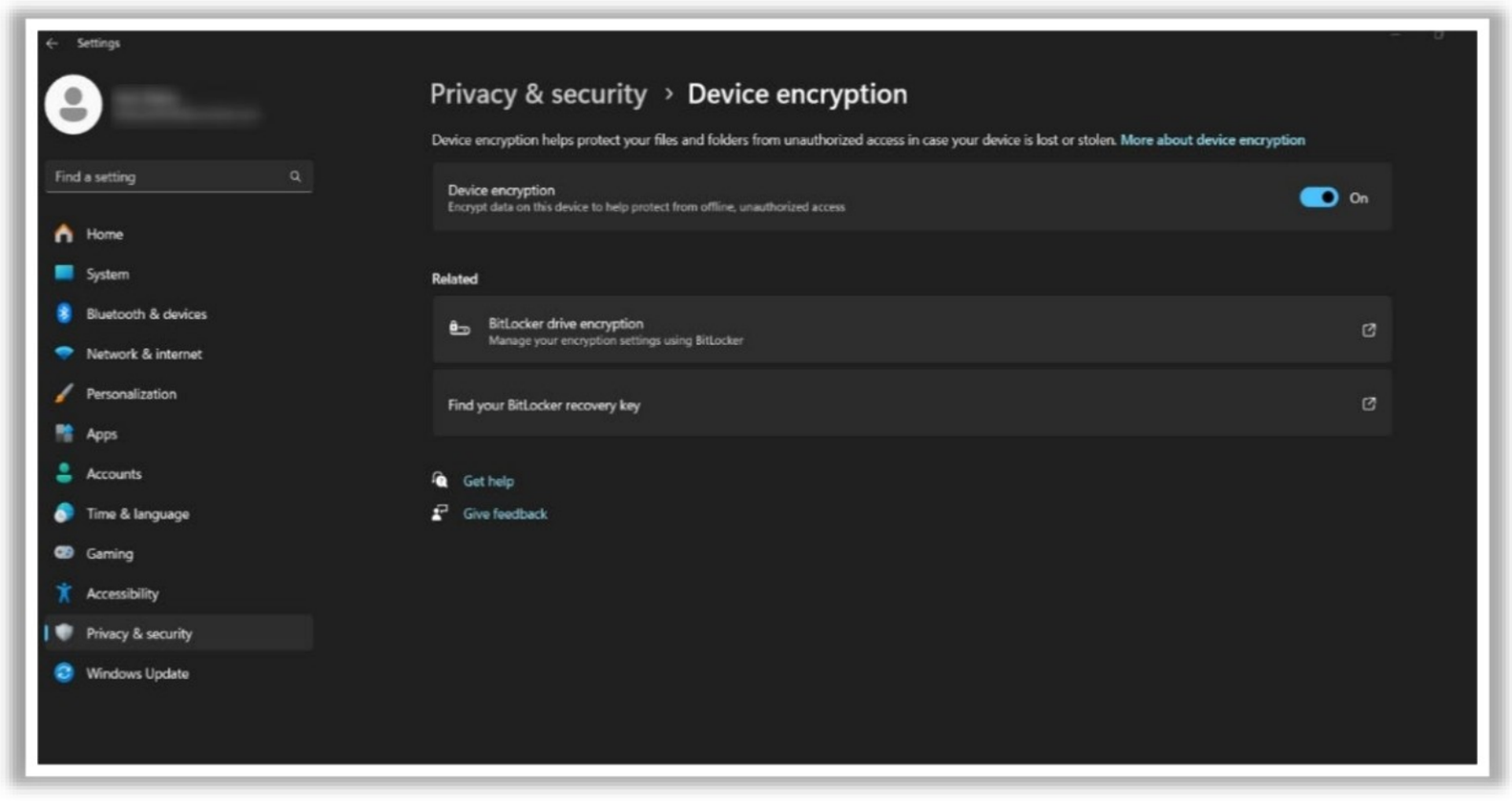


Figure 10.5: Enabling Device Encryption

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

To enable TPM on UEFI

Follow these steps to enable the TPM chip in the user device if it is in a disabled state.

- Open **Settings**.
- Select **Update & Security.**
- Select **Recovery.**
- Browse to **Advanced start up** section and click **Restart now** button.

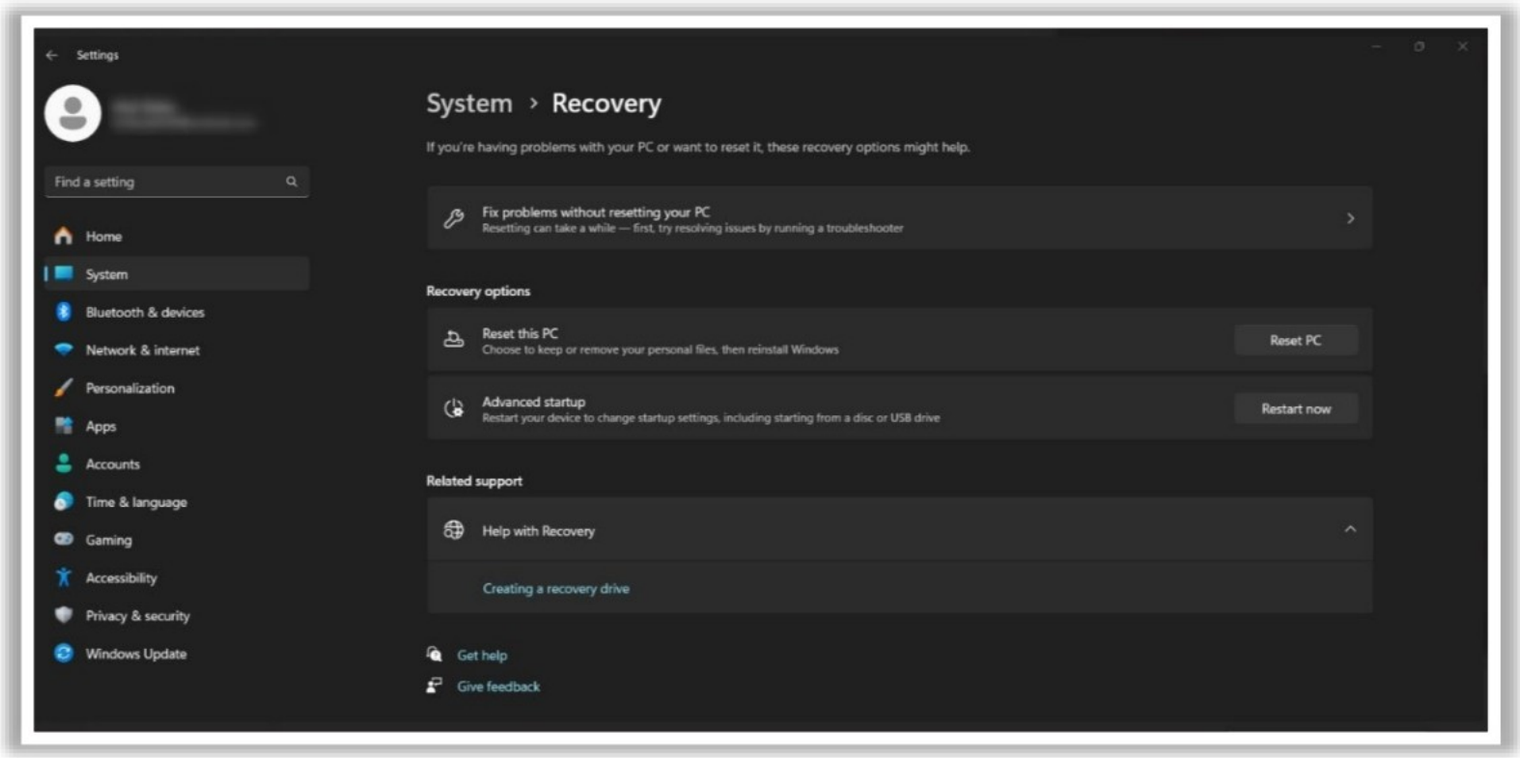


Figure 10.6: Enabling TPM on UEFI

- Click on **Troubleshoot**.

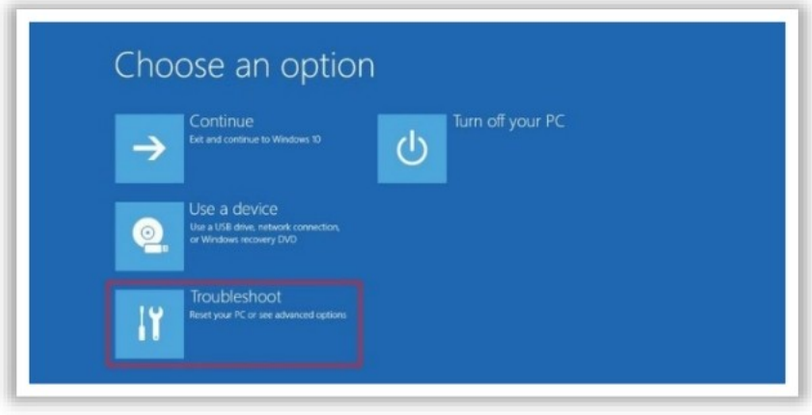


Figure 10.7: Choosing Troubleshoot Option

- Click on **Advanced Options**.

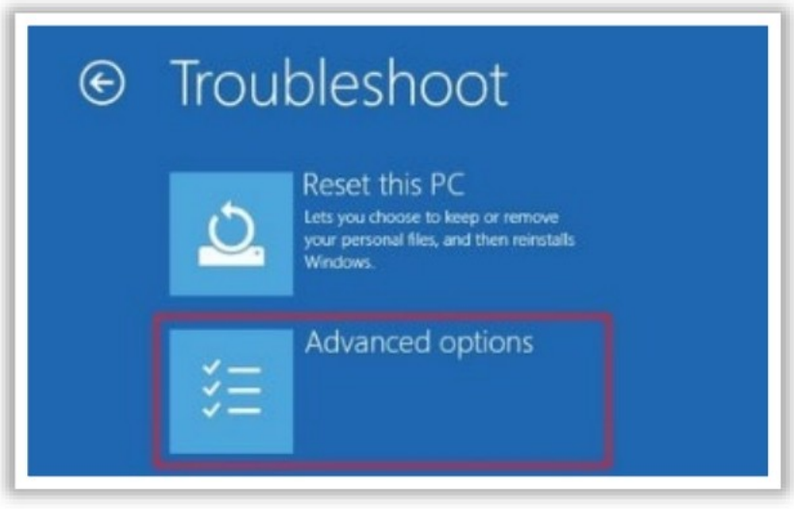


Figure 10.8: Clicking on Advanced Options

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Click on **UEFI Firmware Settings**.

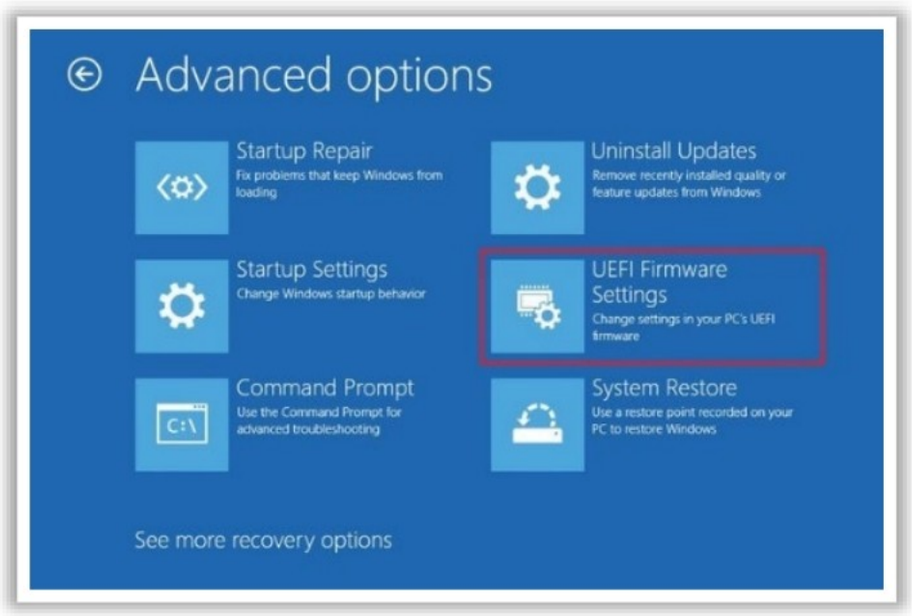


Figure 10.9: Selecting UEFI Firmware Settings

- Click **Restart.**



Figure 10.10: Restarting the System to change the UEFI Firmware Settings

- Navigate to security settings.
- Enable the TPM feature.

To Enable Device Encryption

- Go to **Start→Settings→Update & Security →Device Encryption**.
- **Turn on** the Device encryption option.



Figure 10.11: Enabling Device Encryption

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

BitLocker encryption: This protects the data by encrypting the entire volume of data using advanced encryption standard (AES) encryption algorithm in cipher block chaining (CBC) or XTS mode with a 128-bit or 256-bit key.

To Enable Standard BitLocker Encryption

- Sign in with an administrator account.
- Select the **Start** button.
- Choose **Control Panel,** then click on **System and Security.**
- Under **BitLocker Drive Encryption,** choose **Manage BitLocker.**



Figure 10.12: Selecting Manage BitLocker

- Select **Turn on BitLocker.**

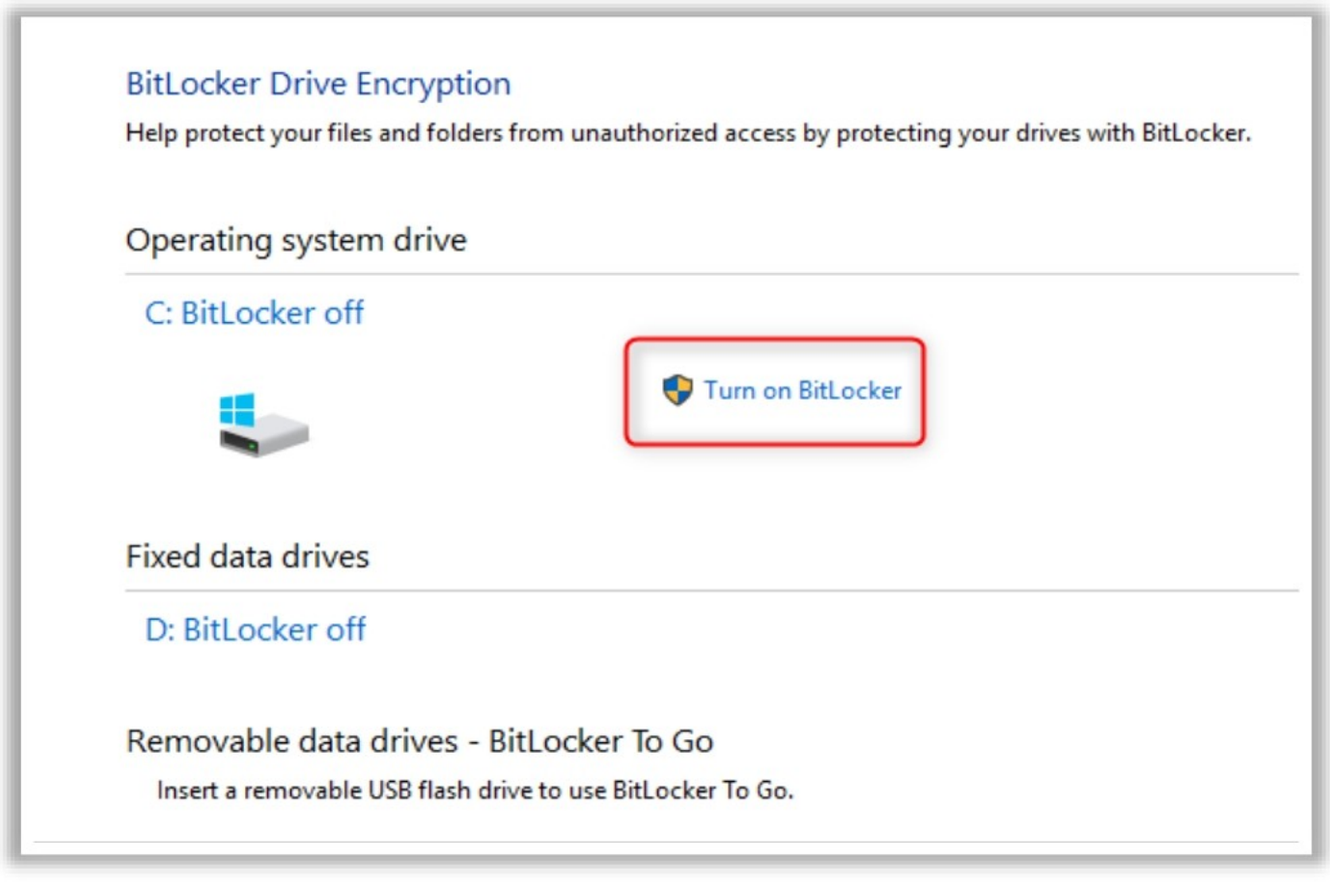
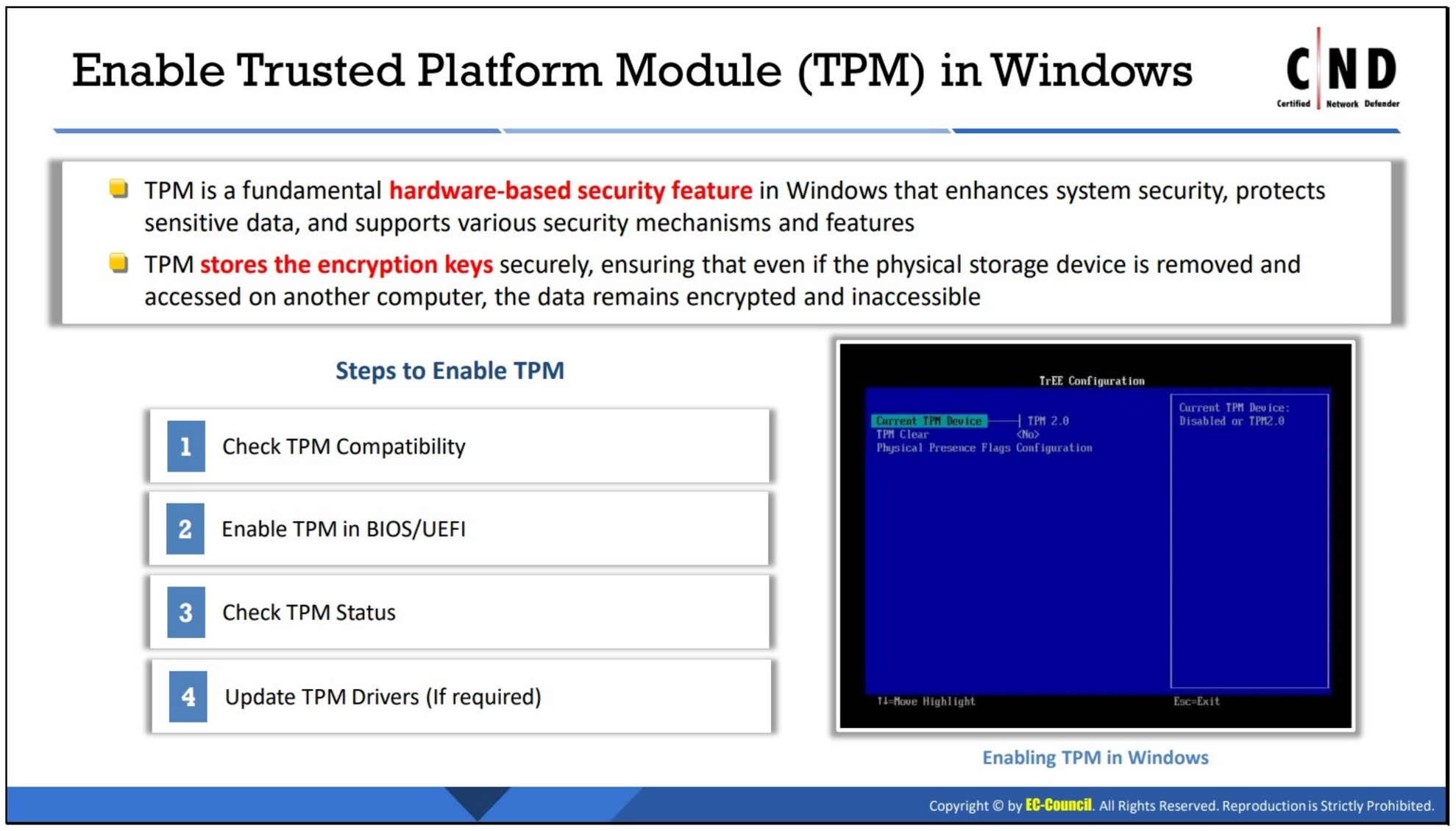


Figure 10.13: Enabling Standard BitLocker Encryption

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Enable TPM 2.0 on Windows

The Trusted Platform Module (TPM) version 2.0 is hardware integrated into the motherboard, providing a secure environment for storing and protecting encryption keys during hard drive encryption. To upgrade to Windows 11, the users must enable TPM 2.0. It supports the storage of cryptographic keys, ensures that the operating system remains untampered, and offers various security mechanisms and features to enhance protection.

Steps to Enable TPM

The steps to enable TPM are as follows:

- **Check TPM compatibility**

  If the TPM chip is not compatible, it shows "Compatible TPM not found" as status. If you see a message confirming TPM is ready to use, check the Specification Version under TPM Manufacturer Information to verify that it is 2.0 to meet Windows 11 requirements.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Enable TPM 2.0 on Windows 11**
  - Open **Settings -> Update & Security -> Recovery->** Click on **Restart now button.**

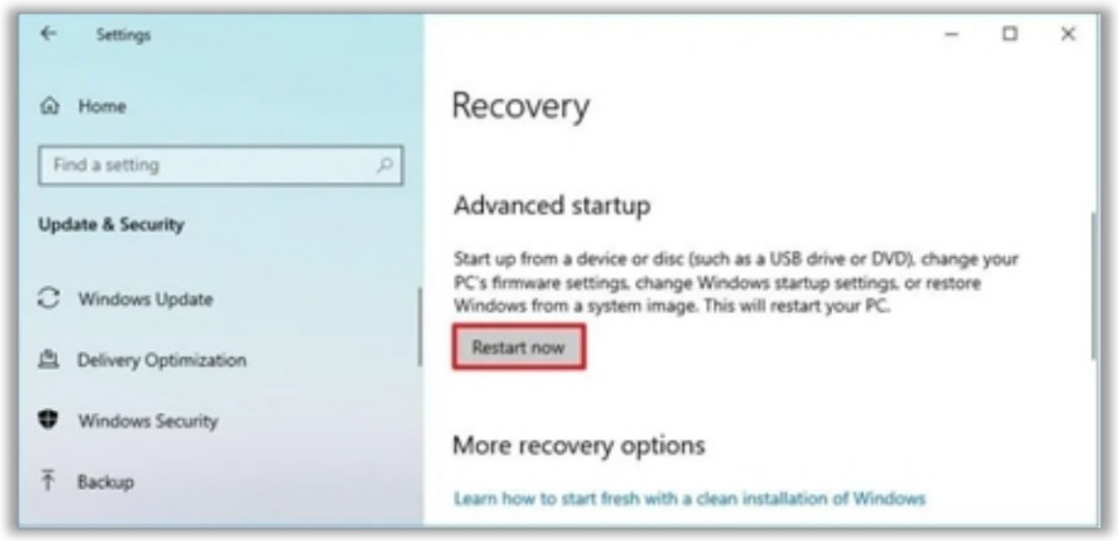


Figure 10.14: Settings Window

  - Click on **Troubleshoot.**

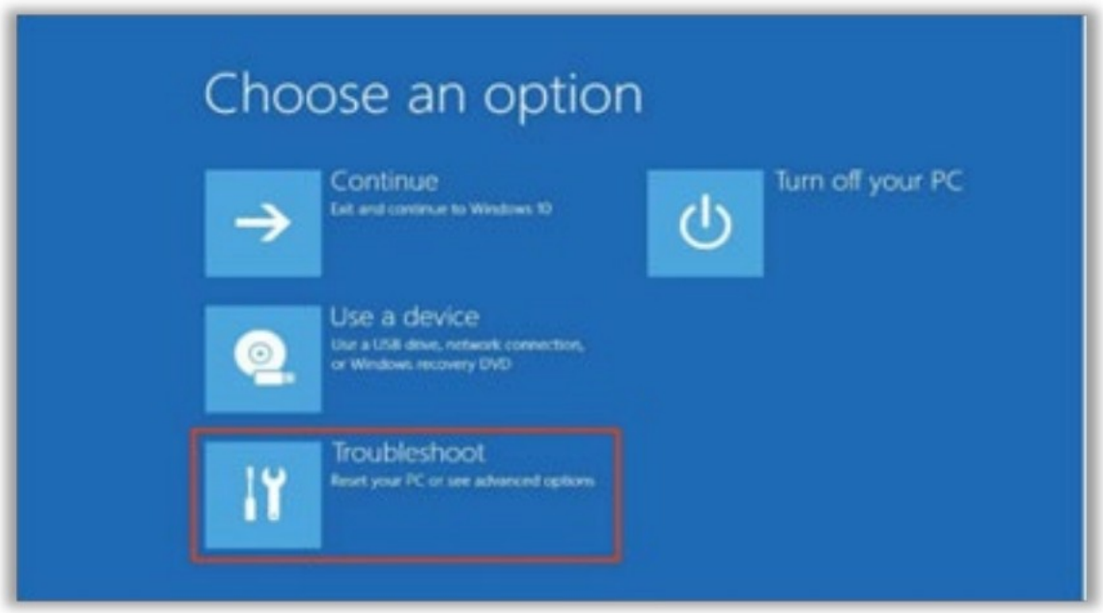


Figure 10.15: Select Troubleshoot

  - Click on **Advanced options** -> **UEFI Firmware Settings** option.

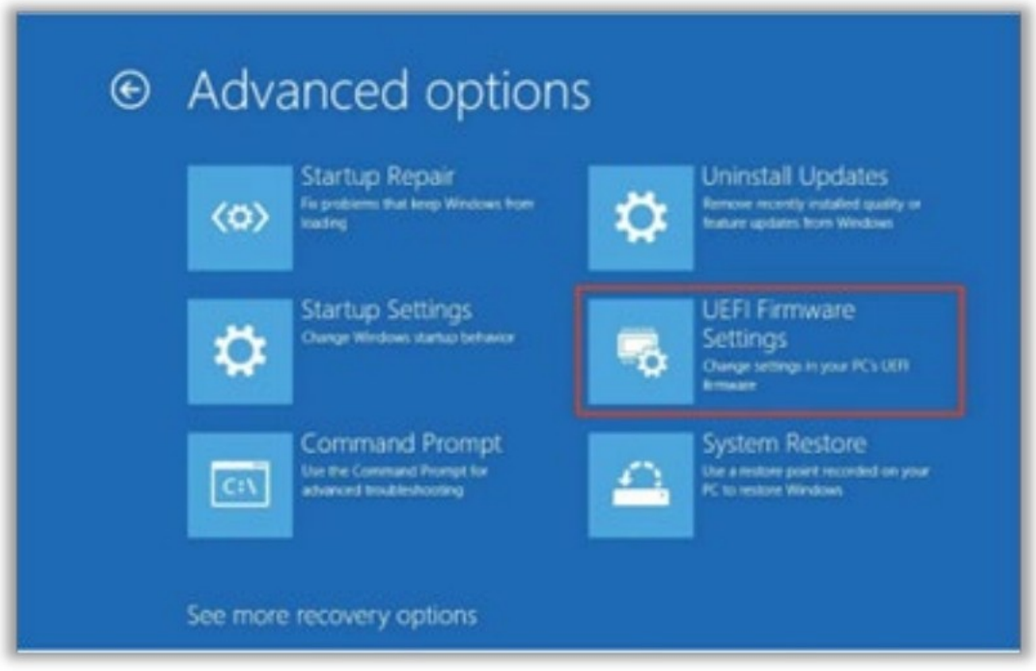


Figure 10.16: Advanced Options Window

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Click on the **Restart button-> advanced, security, or boot** settings page and select the **TPM2.0 option**; choose the **Enabled option**

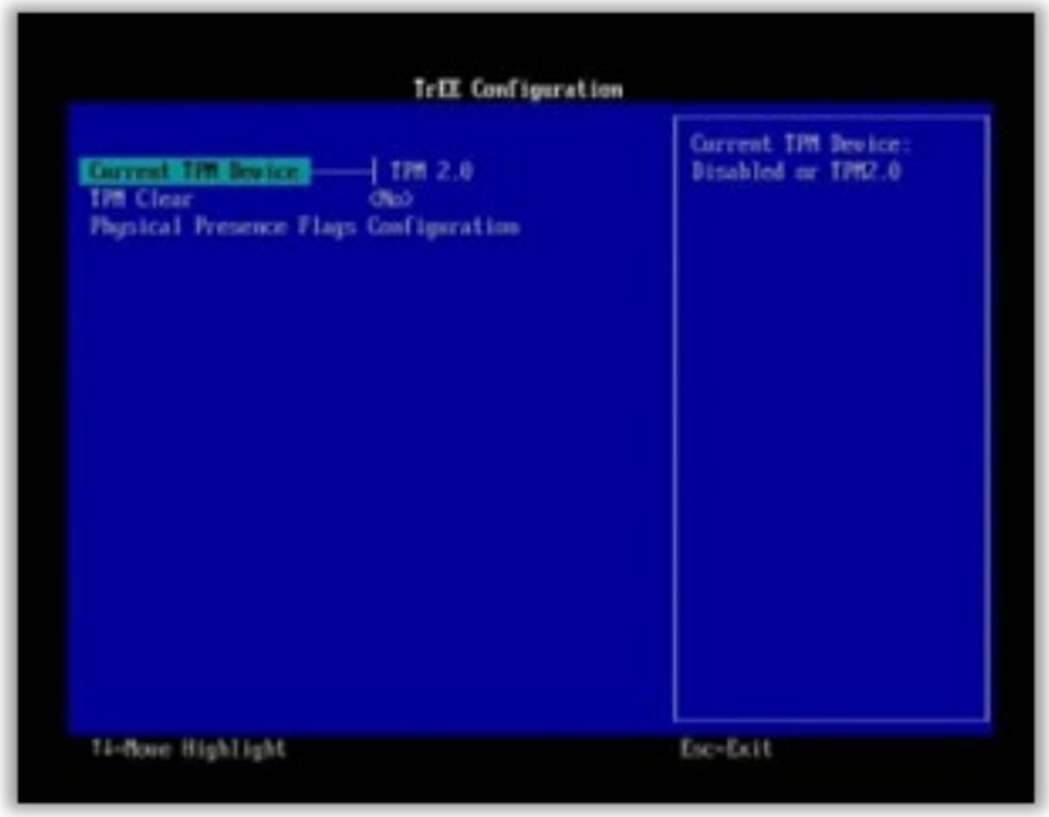


Figure 10.17: Advanced, Security, or Boot Settings Page

Check TPM Status

- Open **Start.**
- Search for **tpm.msc** and open the **Trusted Platform Module (TPM) Management tool**.
- In the **Status** and **TPM Manufacturer Information** sections, confirm TPM is present and version.

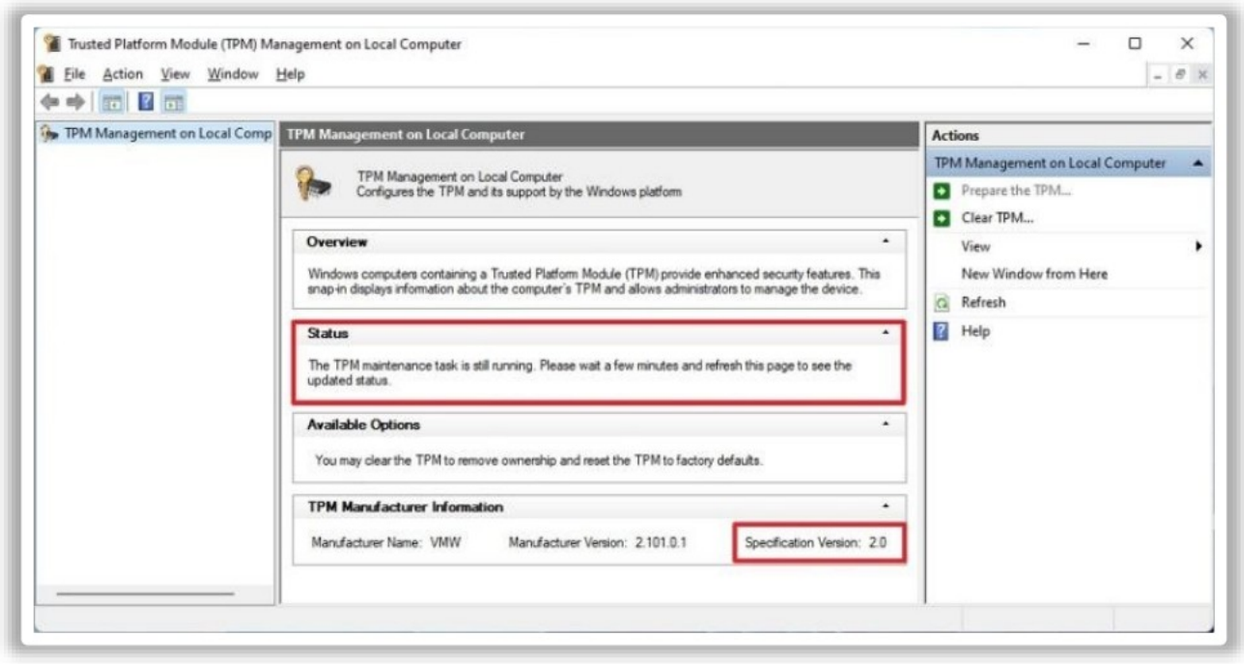


Figure 10.18: Status of TPM

Update TPM Drivers: Outdated TPM drivers become vulnerable, potentially compromising the security of the operating system. This requires the latest version of the security processor. Download and install the Windows OS updates from **Windows Update.** Find the device manufacturer of the TPM device, check for the corresponding link for updates, and apply the firmware update that is provided.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Disk Encryption: Implementing Built-in Disk Encryption for MacOS

MacOS comes with an inbuilt FileVault full disk encryption (FileVault 2) feature to encrypt the disk on a device for preventing unauthorized users from accessing the data on the startup disk. In Mac, the encryption occurs in the background, and if any new file is created, it is automatically encrypted and saved in the startup disk.

To Enable Disk Encryption in MacOS

- From **System Preferences** menu in MacOS, select **Security & Privacy.**
- Click the **FileVault** tab.
- Click the lock icon and enter the administrator details.
- Click **Turn On FileVault.**



Figure 10.19: Disk Encryption in MacOS

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Disk Encryption: Implementing Built-in Disk Encryption in Linux

- **dm-crypt** is a transparent disk encryption subsystem in Linux kernel versions 2.6 and later

dm-crypt in Plain Mode

Encrypts the device **sector-by-sector**, without adding any type of headers or metadata

Advantages

- More resistant to damage, as header cannot be destroyed
- Encryption algorithm details are difficult to understand

Disadvantages

- Accepts any passphrase, making it possible to overwrite useful data
- Difficult to change the password

dm-crypt with LUKS Extension

Sets up the **LUKS device header** and encrypts the master-key with the selected cryptographic options

Advantages

- Change password without re-encrypting the entire block device
- Supports multiple decryption keys it makes it easy to share the container without sharing the password
- Protect against brute-force attacks by strengthening the passphrases
- Stores encryption settings in a header and prevents re-encryption with a different password or different cryptographic parameters

Disadvantages

- Containers can be recognized as the header is not encrypted
- Accidental overwriting the master key present in the header cannot recover the data

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Disk Encryption: Implementing Built-in Disk Encryption in Linux (Cont'd)

A Partition Tree Viewed with lsblk Command

```
root@alice-Virtual-Machine: /home/alice
root@alice-Virtual-Machine:/home/alice# lsblk
NAME   MAJ:MIN RM   SIZE RO TYPE MOUNTPOINTS
fd0      2:0    1     4K  0 disk
loop0    7:0    0    62M  1 loop /snap/core20/1587
loop1    7:1    0     4K  1 loop /snap/bare/5
loop2    7:2    0  63.5M  1 loop /snap/core20/1891
loop3    7:3    0  73.1M  1 loop /snap/core22/634
loop4    7:4    0 163.3M  1 loop /snap/firefox/1635
loop5    7:5    0 400.8M  1 loop /snap/gnome-3-38-2004/112
loop6    7:6    0 349.7M  1 loop /snap/gnome-3-38-2004/140
loop7    7:7    0 460.6M  1 loop /snap/gnome-42-2204/102
loop8    7:8    0  91.7M  1 loop /snap/gtk-common-themes/1535
loop9    7:9    0  45.9M  1 loop /snap/snap-store/582
loop10   7:10   0  12.3M  1 loop /snap/snap-store/959
loop11   7:11   0    47M  1 loop /snap/snapd/16292
loop12   7:12   0   284K  1 loop /snap/snapd-desktop-integration/14
loop13   7:13   0   452K  1 loop /snap/snapd-desktop-integration/83
loop14   7:14   0  40.9M  1 loop /snap/snapd/20290
sda      8:0    0    80G  0 disk
├─sda1   8:1    0     1M  0 part
├─sda2   8:2    0   513M  0 part /boot/efi
└─sda3   8:3    0  79.5G  0 part /
sr0     11:0    1  1024M  0 rom
root@alice-Virtual-Machine:/home/alice#
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Disk Encryption: Implementing Built-in Disk Encryption in Linux

dm-crypt is a transparent disk encryption subsystem in Linux kernel versions 2.6 and later

dm-crypt in Plain Mode

This encrypts the device sector-by-sector without adding any type of headers or metadata. There is no master key, and the encryption options are used for a direct mapping between the encrypted disk and the named device.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

For creating a plain mode mapping with cryptsetup's default parameters:

cryptsetup <options> open --type plain <device> <dmname>

Advantages

- More resistant to damage as the header cannot be destroyed.
- Encryption algorithm details are difficult to understand.

Disadvantages

- Accepts any passphrase, making it possible to overwrite useful data.
- Difficult to change the password.

dm-crypt With Linux Unified Key Setup (LUKS) Extension

This sets up the LUKS device header and encrypts the master key with the selected cryptographic options. Since LUKS is the default encryption mode a new LUKS device with default parameters is created (-v is optional)

cryptsetup -v luksFormat *device*

Advantages

- Changes password without re-encrypting the entire block device.
- Supports multiple decryption keys and makes it easy to share the container without sharing the password.
- Protects against brute force attacks by strengthening the passphrases.
- Stores encryption settings in a header and prevents re-encryption with a different password or different cryptographic parameters.

Disadvantages

- Containers can be recognized as the header is not encrypted.
- Accidental overwriting the master key present in the header cannot recover the data.

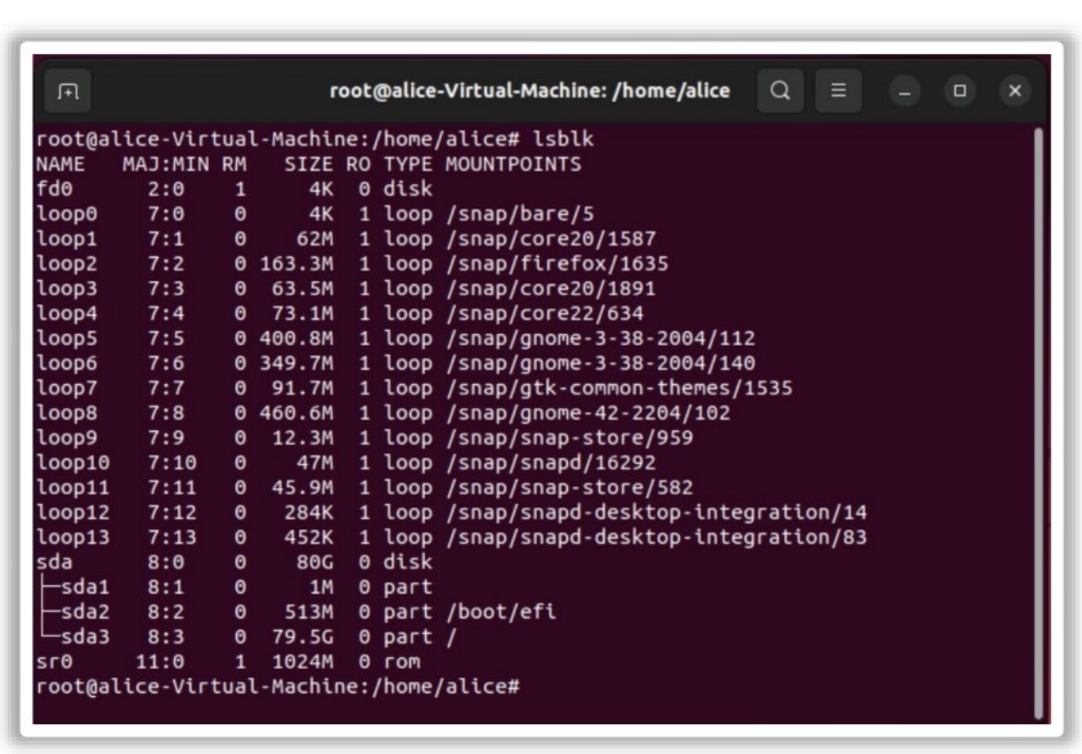
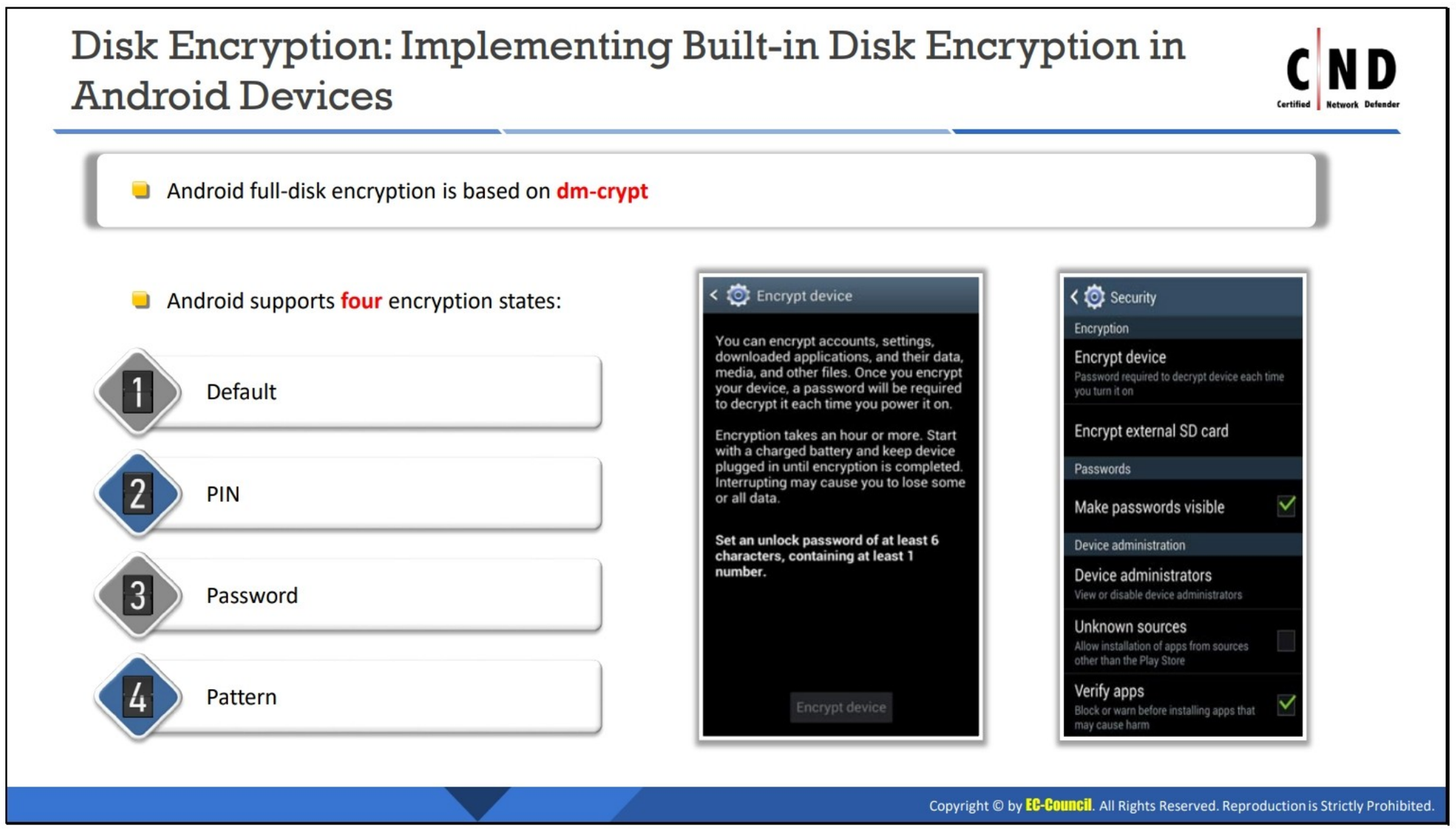


Figure 10.20: Viewing partition tree with the **lsblk** command

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Disk Encryption: Implementing Built-in Disk Encryption in Android Devices

In Android devices, the disk encryption is built on dm-crypt, which supports different ciphers.

The encryption algorithm is AES-128 with CBC. Android 5.0 supports four encryption states, which are as follows:

- Default
- PIN
- Password
- Pattern

To Enable Encryption on Android Devices

- From the Application screen, tap the **Settings icon.**
- Navigate to **More tab** and tap it.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Move down and tap the **Security icon.**



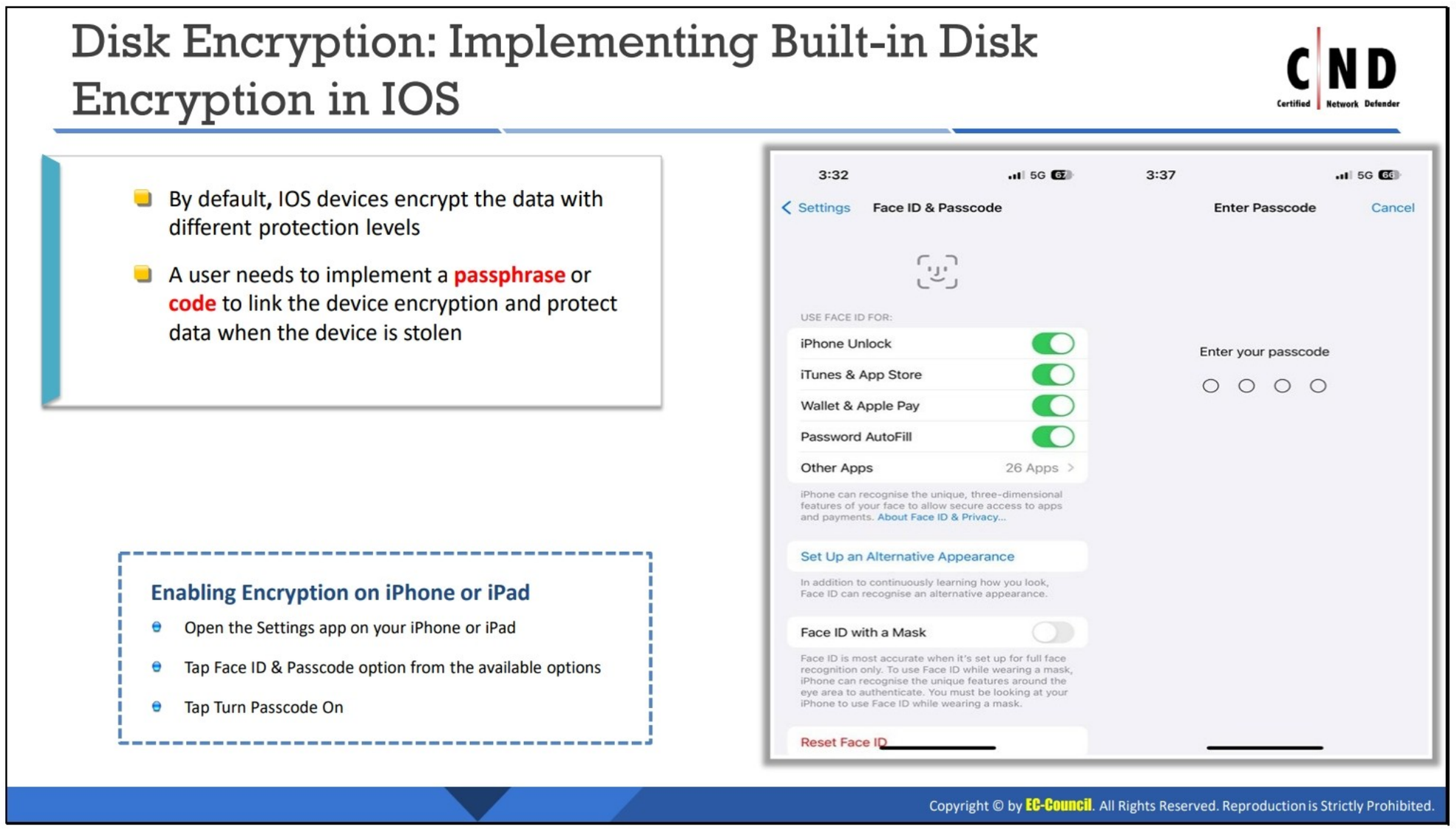
Figure 10.21: Selecting the Security Icon

- Tap the **Encrypt device** option



Figure 10.22: Enabling Encryption on Android Device

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Disk Encryption: Implementing Built-in Disk Encryption in IOS

By default, IOS devices encrypt the data with different protection levels. A user needs to implement a passphrase or code to link the device encryption and protect data when the device is stolen.

To Enable Encryption on iPhone or iPad

- Open the **Settings** app on your iPhone or iPad.
- Tap **Face ID & Passcode** option from the available options.

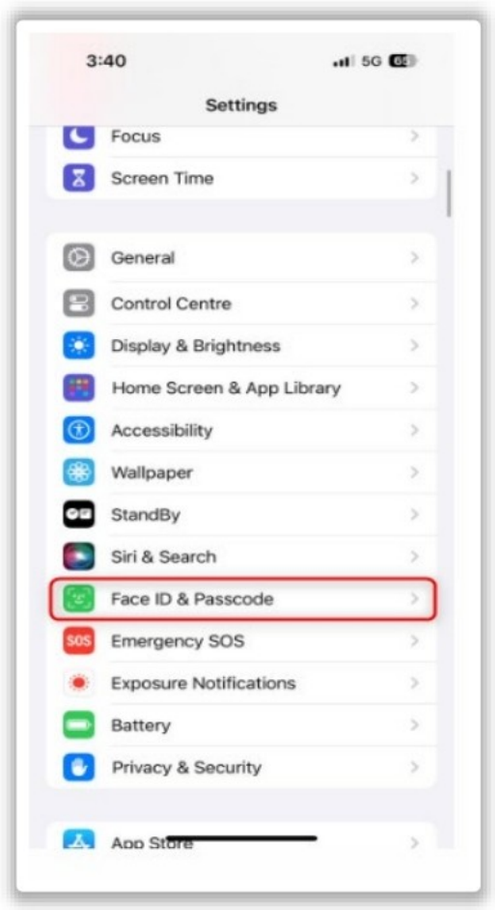


Figure 10.23: Tap Touch ID & Passcode option

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Tap **Turn Passcode On** if not enabled

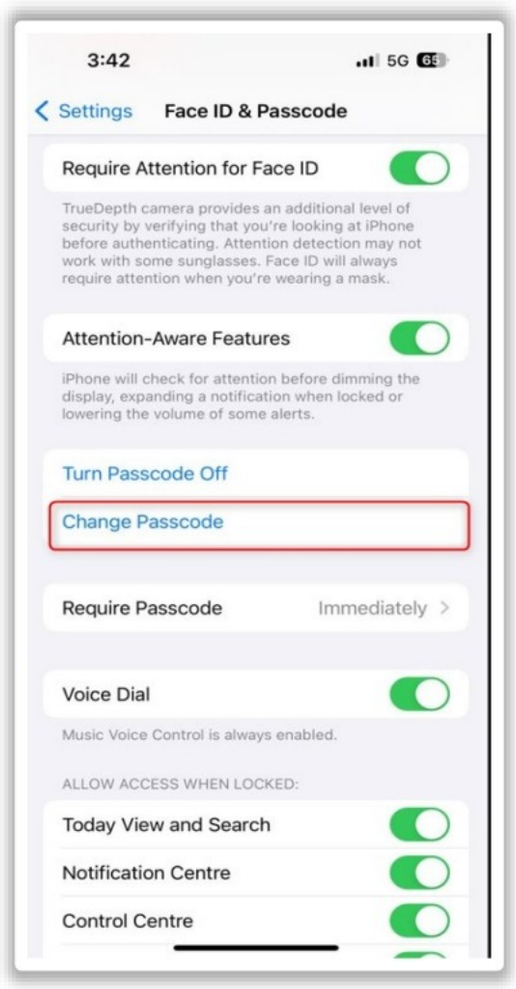


Figure 10.24: Screenshot of Change Passcode

- Tap **Passcode Options** to select a custom numeric or alphanumeric code.

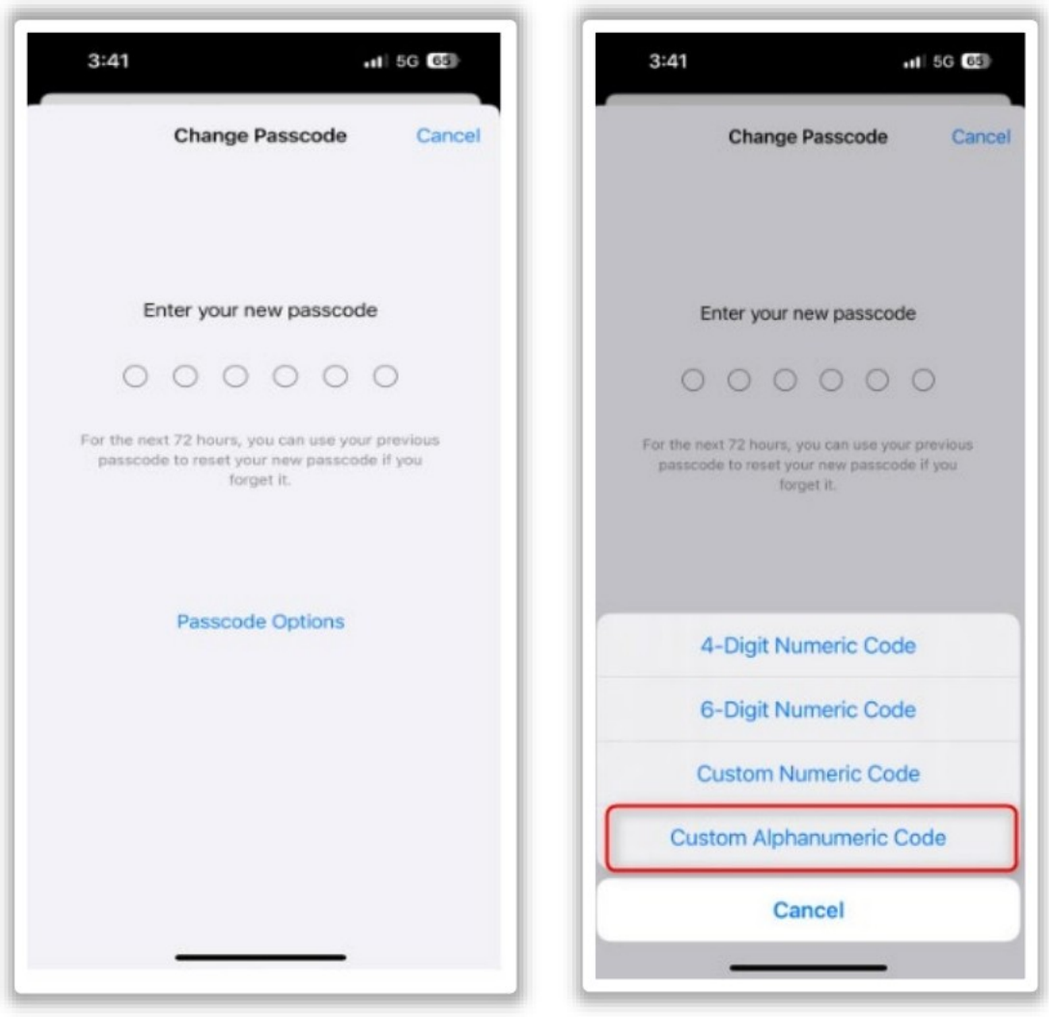
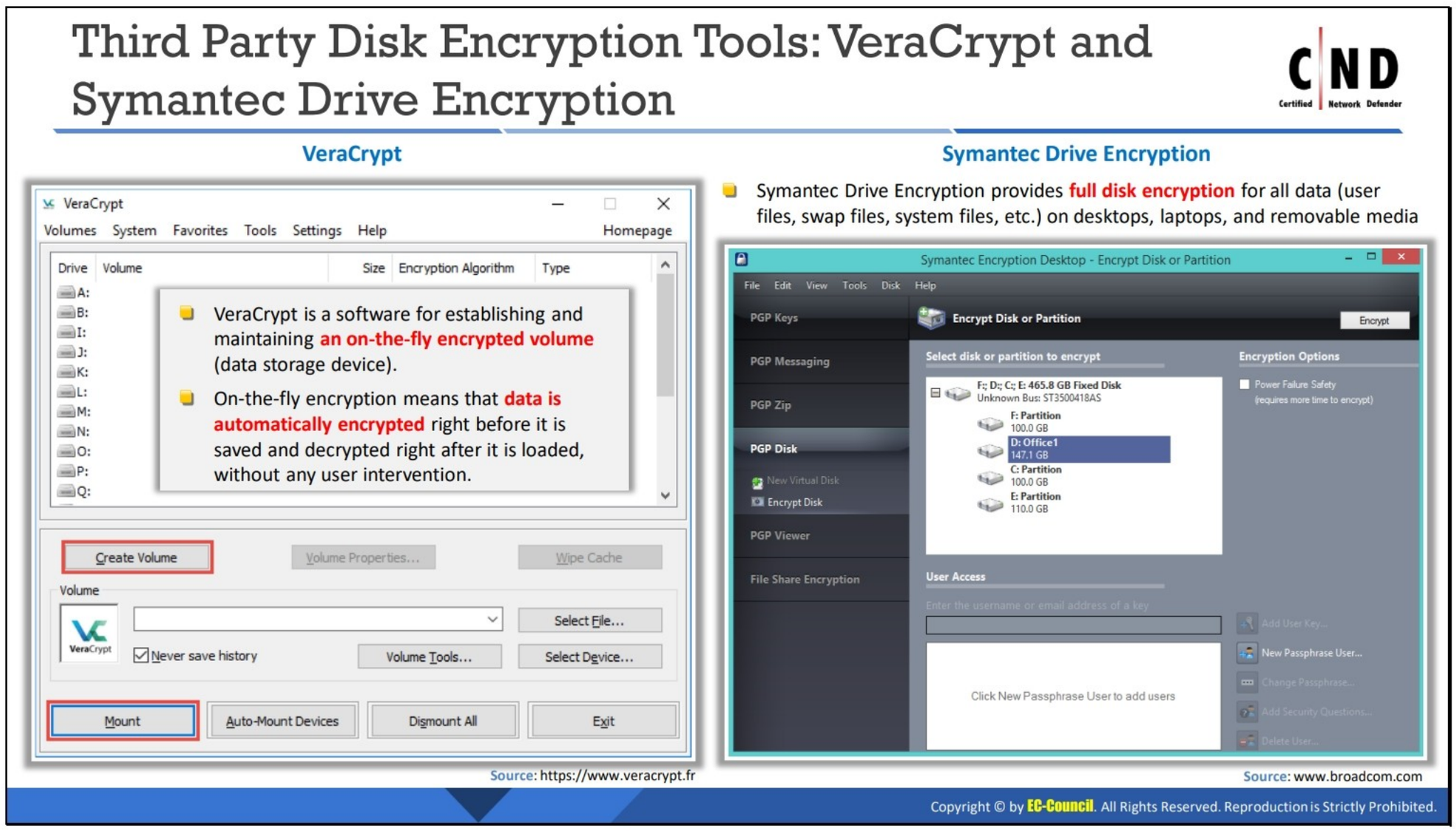


Figure 10.25: Selecting a Custom Numeric or Alphanumeric Code

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Third Party Disk Encryption Tools: VeraCrypt and Symantec Drive Encryption

Third-party disk encryption software can be used to encrypt everything on a device.

VeraCrypt

Source: www.veracrypt.fr

VeraCrypt is a free open-source disk encryption software by IDRIX for Windows, Mac OSX, and Linux, and is based on TrueCrypt 7.1a. This software establishes and maintains an on-the-fly encrypted volume (data storage device). On-the-fly encryption means that data is automatically encrypted right before it is saved and decrypted right after it is loaded, without any user intervention. No data stored on an encrypted volume can be read (decrypted) without the correct password/keyfile(s) or correct encryption keys. The entire file system is encrypted (e.g., file names, folder names, contents of each file, free space, metadata, etc).

Files can be copied to and from a mounted VeraCrypt volume just like they are copied to/from any normal disk (for example, with simple drag-and-drop operations). Files are automatically decrypted on-the-fly (in memory/RAM) while they are read or copied from an encrypted VeraCrypt volume. Similarly, files that are written or copied to the VeraCrypt volume are automatically encrypted on-the-fly (right before they are written to the disk) in RAM.

Symantec Drive Encryption

Source: www.symantec.com

Symantec Drive Encryption (formerly PGP Whole Disk Encryption) provides organizations with complete, transparent drive encryption for all data (user files, swap files, system files, hidden files, etc.) on laptops, desktops, and removable media. It protects data from unauthorized access, strongly securing intellectual property, along with customer and partner data. Symantec Encryption Management server can centrally manage the protected systems, as it simplifies deployment, policy creation, distribution, and reporting.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Additional Third-party Disk Encryption Tools

The following is a list of additional third-party disk encryption tools

GiliSoft Full Disk Encryption

Source: www.gilisoft.com

GiliSoft Full Disk Encryption is especially useful for laptops and other small computing devices that can be physically lost or stolen. It offers encryption of all disk partitions, including the system partition. By password-protecting a disk, disk partition, or operating system launch, the program disables any unauthorized read/write activity on a disk or PC, and restricts the access to and launch of specific disks and files. It provides automatic security for all information on endpoint hard drives, including user data, operating system files, and temporary and erased files. For maximum data protection, multifactor pre-boot authentication ensures user identity, while encryption prevents data loss from theft.

Endpoint Full Disk Encryption

Source: www.checkpoint.com

The CheckPoint Full Disk Encryption Software Blade provides automatic security for all information on endpoint hard drives, including user data, operating system files, and temporary and erased files. For maximum data protection, multifactor pre-boot authentication ensures user identity, while encryption prevents data loss from theft.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Dell Data Protection | Encryption

Source: www.dell.com

Dell Encryption detects data security risks on desktops, laptops, and external media. It protects data on these devices by enforcing access control policies, and authentication and encryption of sensitive data. It also manages data centrally with policies using collaborative tools that integrate into existing user directories. Moreover, it supports key and data recovery, automatic updates, and tracking for protected devices.

AxCrypt

Source: www.axcrypt.net

AxCrypt is a simple file encryption software for Windows, Mac, and mobiles. It integrates seamlessly with your workflow to encrypt, decrypt, store, send, and work.

Folder Lock

Source: https://www.newsoftwares.net

Folder Lock lets you password-protect files, folders, and drives; encrypt your important files on-the-fly; back them up in real-time; protect portable drives; shred files and drives; and clean history. It is the most downloaded file-security application, with more than 45 million users. It works on 32-bit and 64-bit Windows versions 10, 8, 7, Vista, and XP.

SecureDoc

Source: www.winmagic.com

SecureDoc is a comprehensive disk encryption product that secures data at rest. It has two main components: the client software is used to encrypt and decrypt data, and the server software is used to configure, deploy, and manage laptop encryption, desktop encryption, server encryption, and external device encryption for an entire organization.

Central Device Encryption

Source: www.sophos.com

Central Device Encryption encrypts content as soon as it is created. It facilitates synchronized encryption that proactively protects your data by continuously validating the user, application, and security integrity of a device before allowing access to encrypted data.

AlertSec

Source: ensure.alertsec.com

AlertSec educates, verifies, and enforces encryption on all third-party computers, smartphones, and tablets, regardless of what encryption types they use.

DriveCrypt

Source: www.securstar.biz

DriveCrypt securely and easily protects all proprietary data on notebooks and desktop computers. When data is read from a hard disk, DriveCrypt automatically decrypts the data

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

before it is loaded into memory. When data is written back to a hard disk, it is automatically re-encrypted. The disk encryption/decryption process is completely transparent to the user or any application program because the data is processed by an operating system extension on-the-fly as it moves back and forth between the hard disk and memory. Consequently, users do not need to remember to decrypt or re-encrypt their data, or change the normal operation of their PCs. In addition, only individual files are decrypted at any point in time, and not the whole hard disk.

ShareCrypt

Source: www.securstar.com

ShareCrypt store files encrypted on local disk, network shared folders, and file syncing cloud services. It provides user-based access rights to folders and their content. With ShareCrypt, you have full control over your sensitive data, ensuring that only you can access your data and lock out any unauthorized party. ShareCrypt is easy to use; it provides a virtual disk drive, under which all areas the user can access are visible. Files are encrypted individually with AES 256-bit keys, which are hashed with the user password using SHA-256. New user requests are encrypted with 2048-bit RSA public-private keys.

DriveCrypt Plus Pack

Source: www.securstar.com

DriveCrypt Plus Pack (DCPP) encrypts the entire operating system, partitions, or the entire hard disk using AES-256. DCPP file encryption software is automatic and completely transparent to the user. It not only decreases user involvement and training requirements but also creates the foundation for enforceable security. The careful integration of boot protection and automatic encryption provides a high degree of security with minimal impact on users.

Rohos Disk Encryption

Source: www.rohos.com

The Rohos Disk program creates hidden and protected partitions on a computer or USB flash drive and password protects/locks access to your Internet applications.

east-tec SafeBit

Source: www.east-tec.com

east-tec SafeBit is a disk encryption software, and the perfect solution for protecting your data against potential unauthorized access and information leaks. It features on-the-fly disk encryption, by creating virtual disk drives where you can hide files and folders, keep them encrypted all the time, but still work with them just as you work with normal files.

Cryptainer LE

Source: www.cypherix.com

Cryptainer LE creates an encrypted disk drive (volume) to store any type of data. It provides a 448-bit strong encryption and facilitates simple drag-and-drop operations. It works on all 32-bit as well as 64-bit versions of Windows. Cryptainer Mobile edition encrypts any data on any media (USB drives, CD-ROMs, and flash disks)

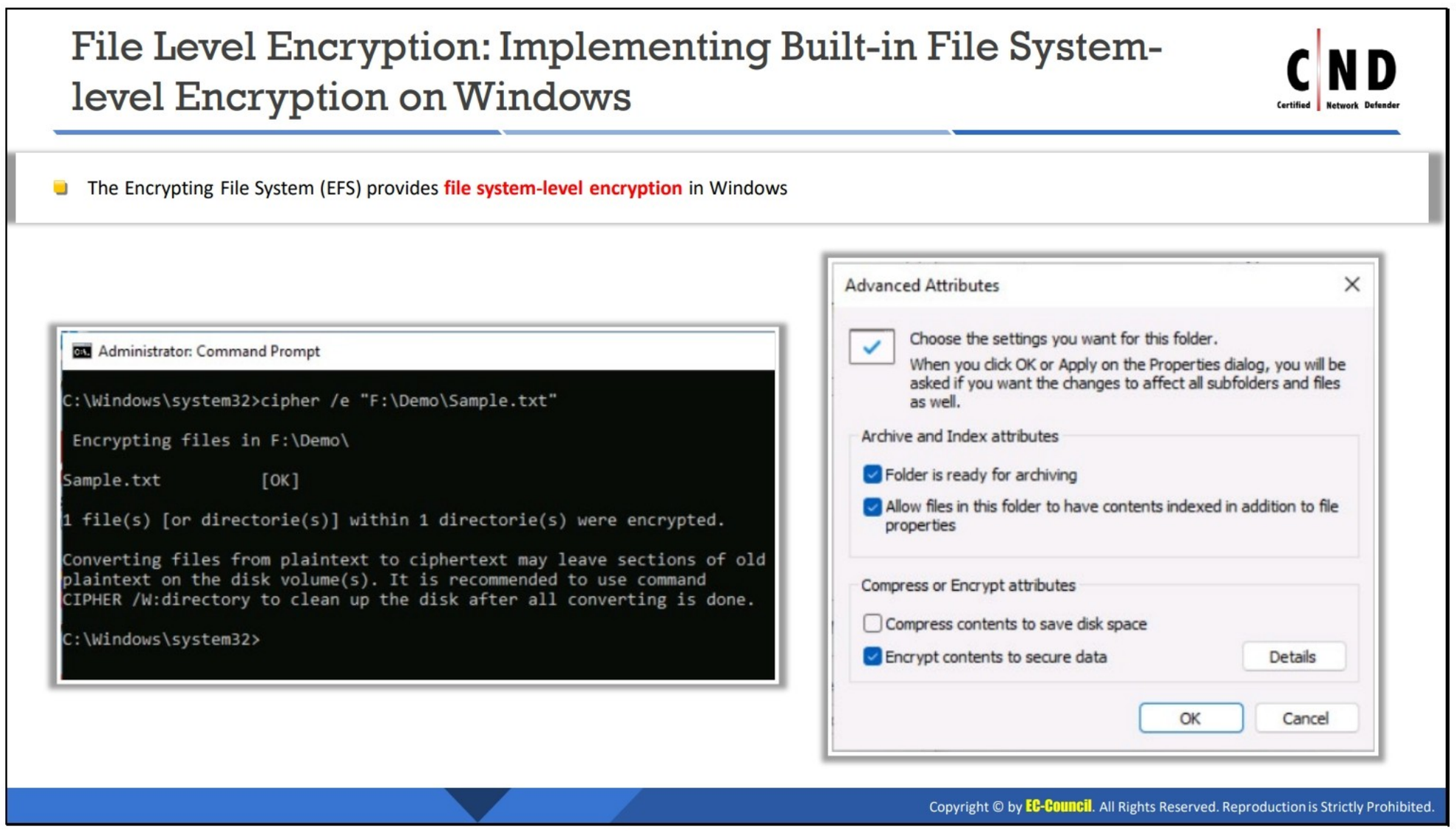
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

PocketCrypt

Source: www.securstar.org

PocketCrypt is a file encryption program that provides a virtually encrypted storage area for Windows systems. A container is created in the memory of the Windows Mobile device which is then protected by PocketCrypt Windows encryption software. This Pocket PC encryption software creates a "virtual directory" through which the data is accessed. Automatically any data written to the "virtual directory" is encrypted with the AES algorithm.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



File Level Encryption: Implementing Built-in File System-level Encryption on Windows

The Encrypting File System (EFS) provides file system-level encryption in Windows (starting from Windows 2000), except the home version. The user needs to enable this feature on a specific file, directory, or drive. EFS protects the confidential information from unauthorized users who have physical access to a computer.

File Encryption with EPS Using Command Prompt

- Right-click on the Start button and select **Command Prompt (Admin).**
- Type the following command:

  cipher /e “<PATH>”
- Enter the file path with extension and hit **Enter.**

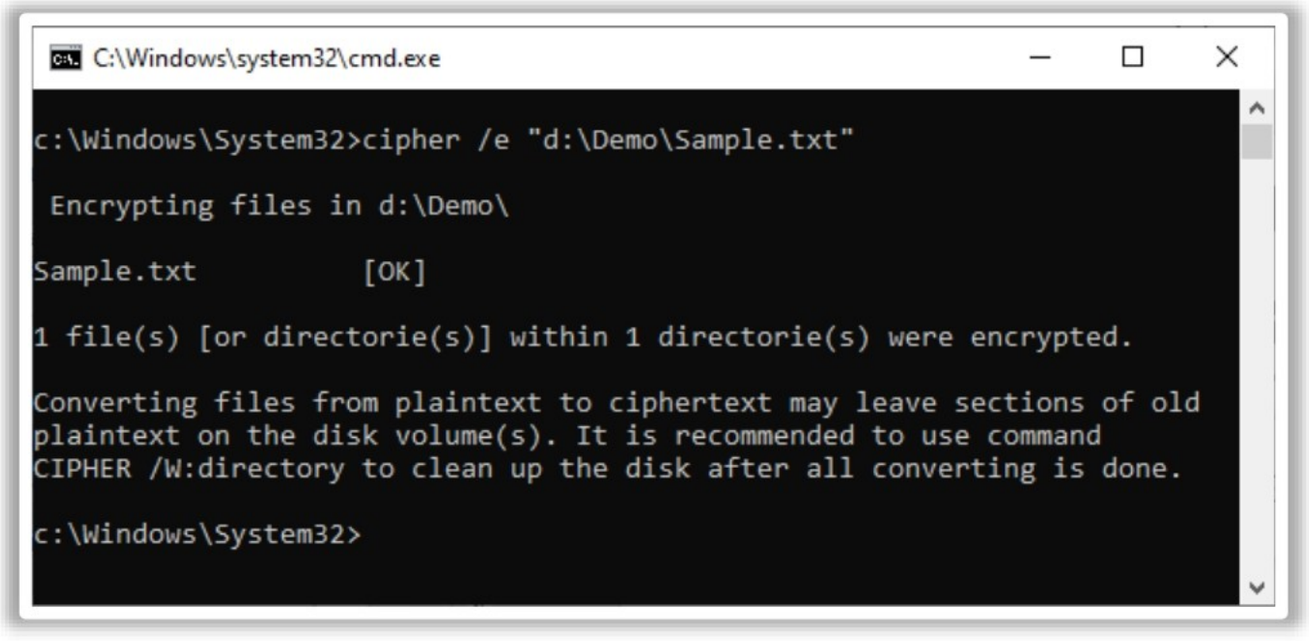


Figure 10.26: File encryption with EPS

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

To enable EPS Using Advanced Attributes in a Selected File/Folder

- Select the file for encryption using EFS.
- Right-click on the file and select **Properties**.

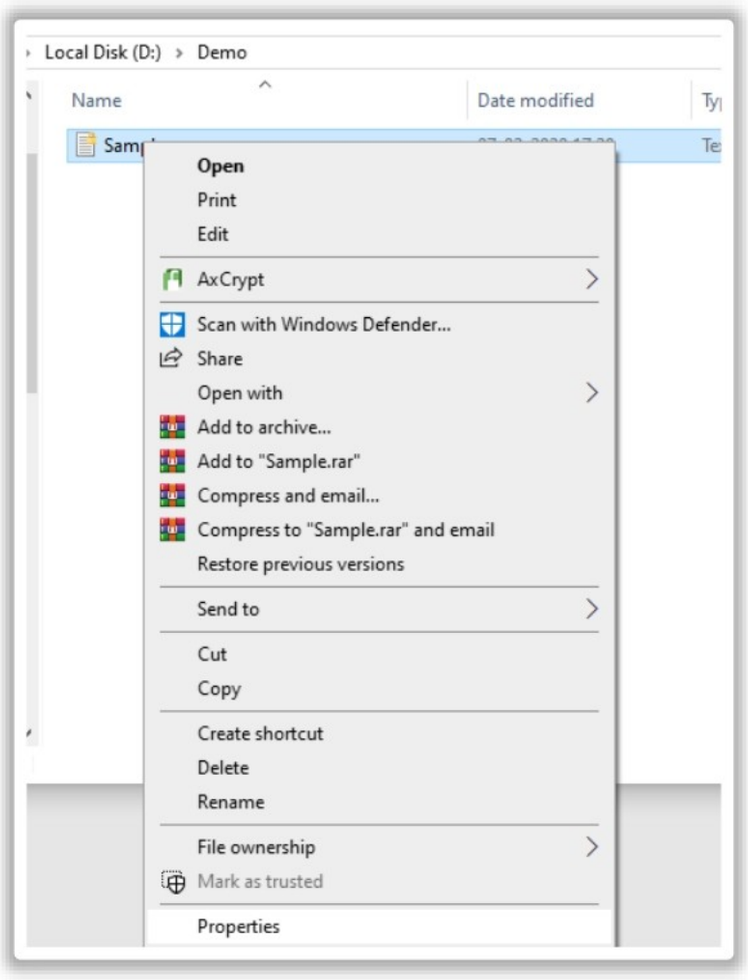


Figure 10.27: Screenshot of Selecting Properties

- Click **Advanced**

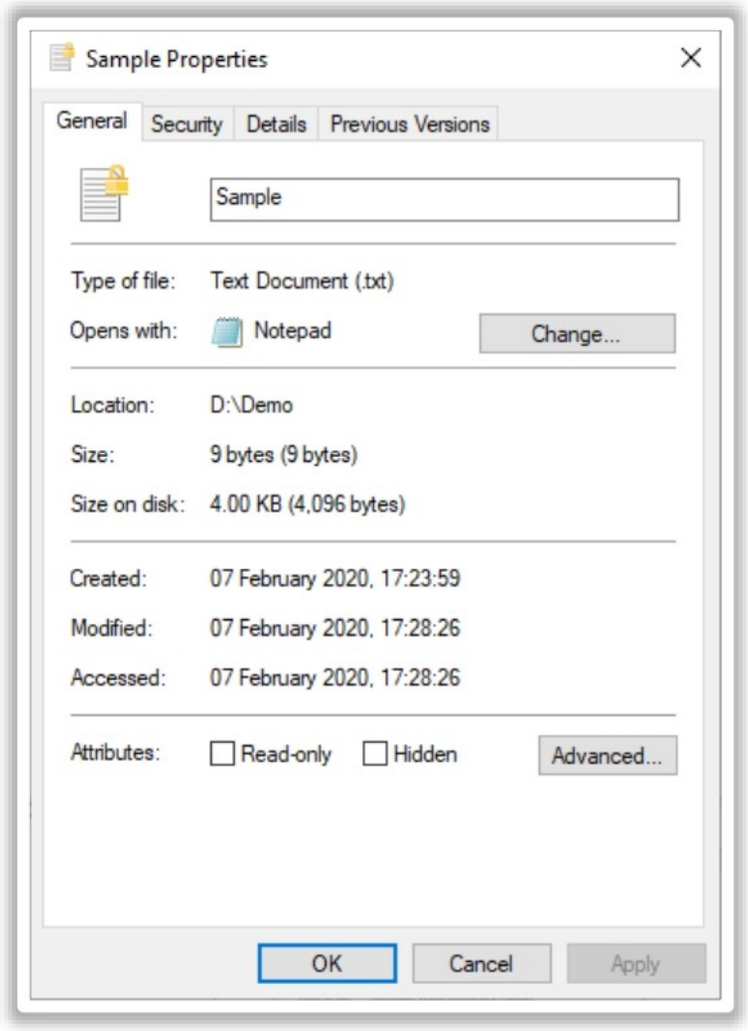


Figure 10.28: Choosing Advanced Option

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Check the box **Encrypt content to secure data** and click **OK**

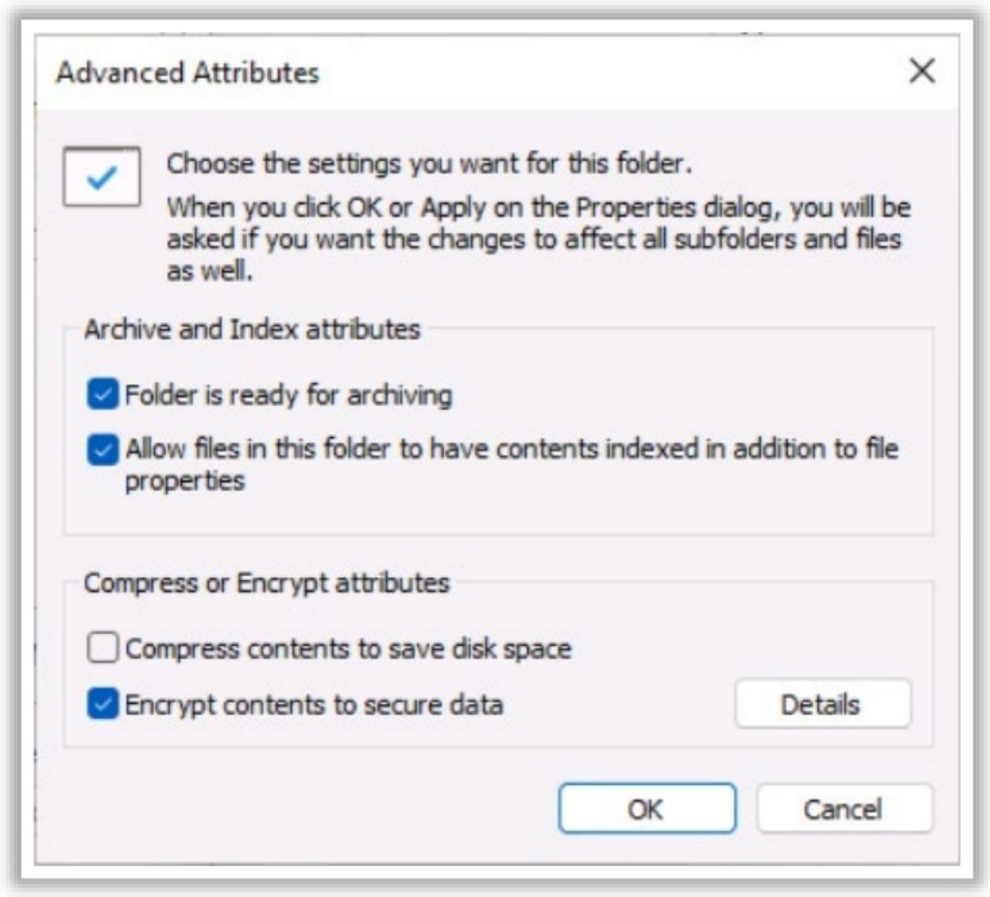


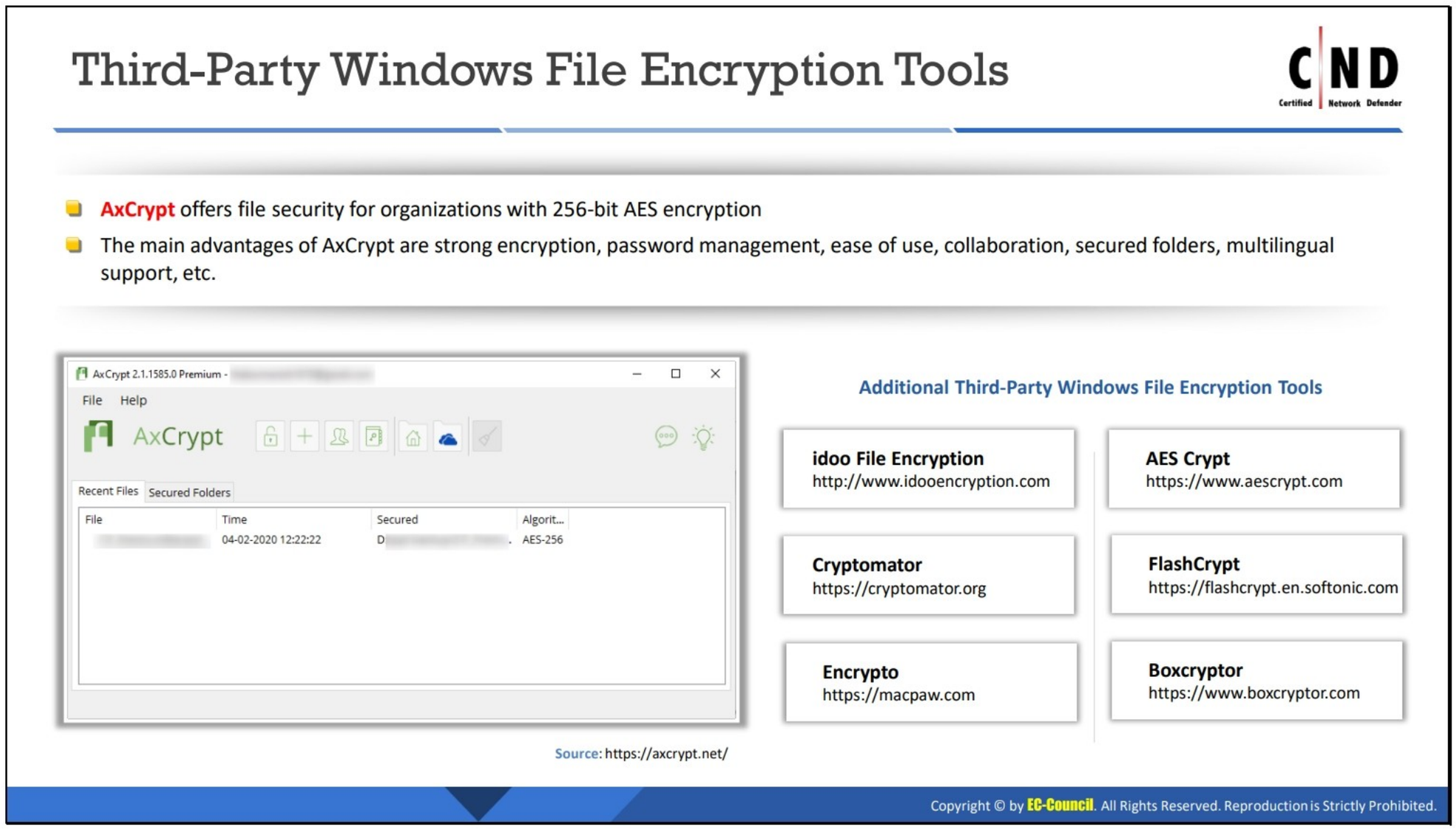
Figure 10.29: Selecting Encrypt Content to Secure Data

- Click **Apply**. A box will appear with the option to encrypt the file only or encrypt the file and its parent folder. Select as per requirements, and click **OK**



Figure 10.30: Encryption Warning

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Third-Party Windows File Encryption Tools

AxCrypt

Source: www.axcrypt.net

AxCrypt offers file security for companies and organizations with 256-bit AES encryption. Sharing files with the rest of the team is easy with the cloud storage awareness and key sharing feature for on-premise files. This allows users to comply with data protection regulations while protecting their files from costly data breaches. The main features of AxCrypt are strong encryption, password management, ease of use, collaboration, secured folders, multilingual support, etc.

Some Additional Third-party File Encryption Tools

idoo File Encryption

Source: www.idooencryption.com

idoo Secure Disc Creator is a CD/DVD encryption software for creating encrypted image files and virtual disks, and burning encrypted CD/DVDs. idoo DVD encryption can create a safe and public space on one disk. Using the military standard 256-bit AES on-the-fly encryption algorithm, idoo encryption software helps protect important files and folders by encrypting the safe space. The safe space can only be opened by a set password, while everyone can view the public space. Powerful functions along with easy operability makes idoo Secure Disc Creator the best choice for preventing the leakage of confidential information on a CD/DVD. Without installing any extra program on a computer, the user can open and read the data on a CD/DVD just by entering the correct password.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

AESCrypt

Source: www.aescrypt.com

AES Crypt is a free open-source software available on several operating systems that uses the industry-standard AES to encrypt files easily and securely. It is a tool for anyone who carries sensitive information with them while traveling, uploads sensitive files to servers on the Internet, or wishes to protect sensitive information from being stolen from their home or office.

Cryptomator

Source: https://cryptomator.org

Cryptomator is free and open-source software. It provides transparent, client-side encryption for your cloud. It protects your documents from unauthorized access. It encrypts file contents and names using AES. Your passphrase is protected against brute-force attempts using scrypt. Cryptomator is a so-called transparent encryption utility. This means that you do not have to learn new workflows. Just work with your files as you are used to.

Encrypto

Source: https://macpaw.com

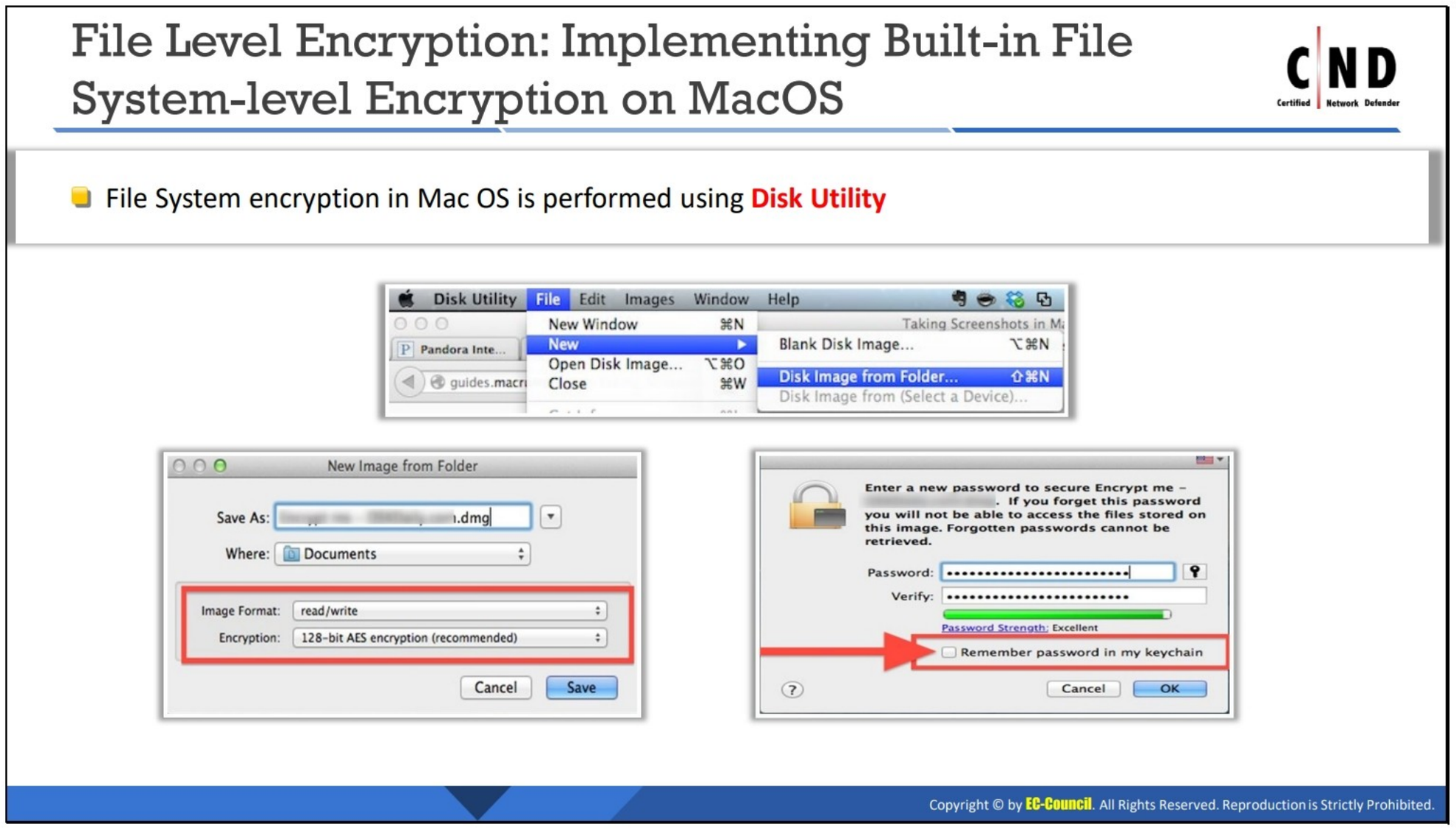
Encrypto lets you encrypt files before sending them to friends or coworkers. It takes any file or folder and adds an AES-256 encryption to it. With such an encryption, your file is incredibly secure and only the right person can access it.

Boxcryptor

Source: www.boxcryptor.com

Boxcryptor encrypts your sensitive files and folders in Dropbox, Google Drive, OneDrive, and many other cloud storage services. It combines the benefits of the most user-friendly cloud storage services with the highest security standards worldwide.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



File Level Encryption: Implementing Built-in File System-level Encryption on MacOS

File system encryption in Mac OS is performed using Disk Utility. Disk Utility is primarily used for disk repair and image utility; however, it can also be used to create disk images containing files and folders, which can be encrypted in MacOS.

To Enable File system-level Encryption on Mac OS

- Go to **Applications → Utilities → Disk Utility**.
- Click on the **File** menu, and select **New Image → Disk Image from Folder** from the drop-down list.
- Navigate to the folder you want to encrypt and click **Image**.
- Change the **Image Format** to **read/write** and the **Encryption** to **128-bit AES**. You can also use options other than **read/write** for **Image Format**.



Figure 10.31: Selecting Image Format and Encryption

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Enter a strong password. Ensure that you tick the box "**Remember password in my keychain**"
- Click **OK**.



Figure 10.32: Checking Password Strength

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Third-Party Linux File Encryption Tools

GnuPG

Source: https://gnupg.org

GnuPG allows a user to encrypt and sign their data and communications. It features a versatile key management system, along with access modules for all types of public key directories. GnuPG, also known as *GPG*, is a command-line tool with features for easy integration with other applications. A wealth of front-end applications and libraries are available. GnuPG also provides support for S/MIME and Secure Shell (ssh).

Some Additional Third-party Linux File Encryption Tools

dm-crypt

Source: www.kernel.org

dm-crypt encrypts the data and writes it onto the storage device using a storage format called LUKS. LUKS format is used on the drive itself, and is essentially used in place of a file system such as ext4. The dm-crypt system sits between the filesystem software; the filesystem software reads and writes ext4, and the ext4 data gets pushed through dm-crypt, resulting in the data being stored in LUKS format on the drive. Thus, a user can effectively have a file system such as ext4 or NTFS sitting “on top of” the encrypted LUKS format.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Cryptmount

Source: https://sourceforge.net

Cryptmount is a utility for GNU/Linux operating systems which allows an ordinary user to mount an encrypted filing system without requiring superuser privileges. It is aimed at Linux systems using the 2.6 kernel series or later.

CryFs

Source: www.cryfs.org

The goal of CryFS is not only to keep file contents but also file sizes, metadata, and directory structure confidential. To hide file sizes, CryFS splits the content of a file into same-sized blocks and encrypts these blocks individually. The blocks are encrypted using a block cipher chosen by the user. A random encryption key is generated when the filesystem is created. This key is stored in a configuration file, which is then encrypted using a password chosen by the user. Since it is encrypted, it can be stored together with the ciphertext blocks in the cloud, which is the default setting. If users want to use an insecure (e.g. empty) password or do not trust the scrypt algorithm used for encrypting the configuration file, they can also keep the configuration file locally.

VeraCrypt

Source: www.veracrypt.fr

VeraCrypt is a free open-source disk encryption software for Mac OS X. This software establishes and maintains an on-the-fly-encrypted volume (data storage device).

Tomb

Source: www.dyne.org

Tomb is a free and open-source system for file encryption on GNU/Linux, facilitating the backup of secret files. Tomb is written in code that is easy to review, and links commonly shared components. Tomb generates encrypted storage folders to be opened and closed using their associated key files, which are also protected with a password chosen by the user. A tomb is like a locked folder that can be safely transported and hidden in a filesystem; its keys can be kept separately, for instance, by keeping the tomb file on the user computer hard disk and the key files on a USB stick.

EncFSMP

Source: https://encfsmp.sourceforge.io

EncFSMP stores data in an encrypted folder. It is especially useful if you store your sensitive data in a cloud service like Dropbox or Google Drive. Since EncFS exists on many platforms, you can access your data from a Windows PC, an Apple computer, from Linux (using the built-in EncFS), or even from an Android device (using Cryptonite).

Although EncFSMP is an open-source project and its source code is released under the MIT license, it contains a closed-source component. Pismo File Mount, the file system component

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

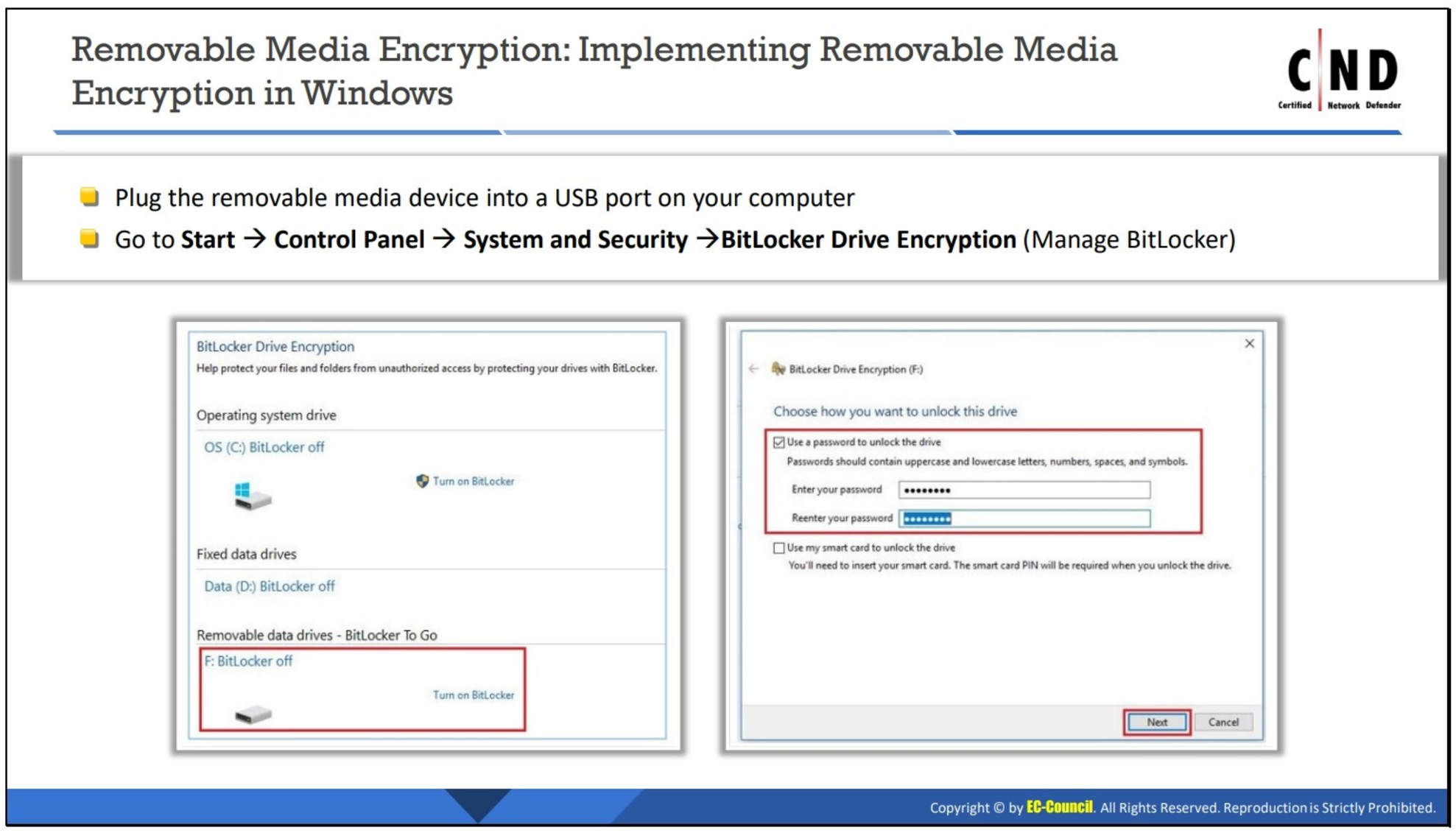
that allows EncFSMP volumes to be mounted, is developed by Pismo Technic Inc. Other than that, EncFSMP is 100% open-source.

7-zip

Source: www.7-zip.org

7-Zip is free open-source software. Most of the code is under the GNU LGPL license. Some parts of the code are under the 3-clause BSD license.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Removable Media Encryption: Implementing Removable Media Encryption in Windows

Removable media such as USB flash drives, iPods, smartphones, tablets, digital cameras, portable hard disks, etc. are prevalent in a workplace and pose a real threat to an organization. With these devices, the attackers can easily introduce a malicious code in a network or carry sensitive data out of an organization. Hence, encryption is the best way to protect sensitive data from being taken out of an organization.

Encryption can be applied to removable media to prevent it from unauthorized access in case of loss or theft. This will add an extra layer of security to confidential information. Various encryption solutions are available in the market with different features. Some encryption solutions encrypt the data stored on a local drive, but not on USB devices, whereas some encryption solutions automatically encrypt the data stored on removable media. While selecting a removable media encryption solution, it is important to verify how it is configured to restrict access to devices using an authorized list, personal devices, an authorized file copy, and encryption keys.

Operating systems such as Windows, Linux, and Mac use a couple of methods to encrypt removable media such as USB drives. They use either built-in features or third-party encryption solutions to encrypt removable media.

Implementing Removable Media Encryption in Windows: BitLocker

To Enable Removable Media Encryption in Windows 11

- Plug the removable media device into a USB port on the computer.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Go to **Start → Control Panel → BitLocker Drive Encryption.**

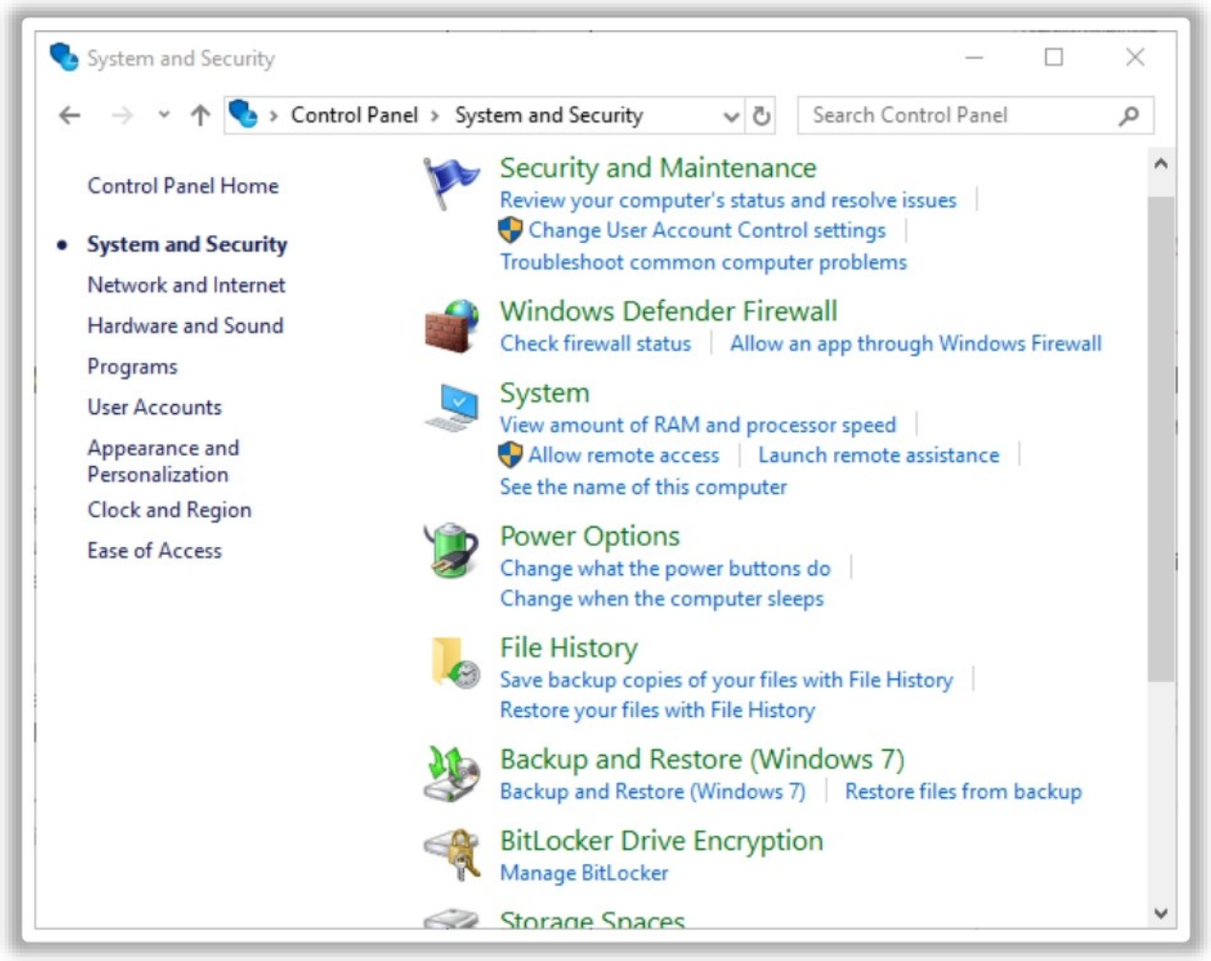


Figure 10.33: Choosing BitLocker Drive Encryption Option

- Select the removable media device to encrypt and click **Turn on BitLocker**.

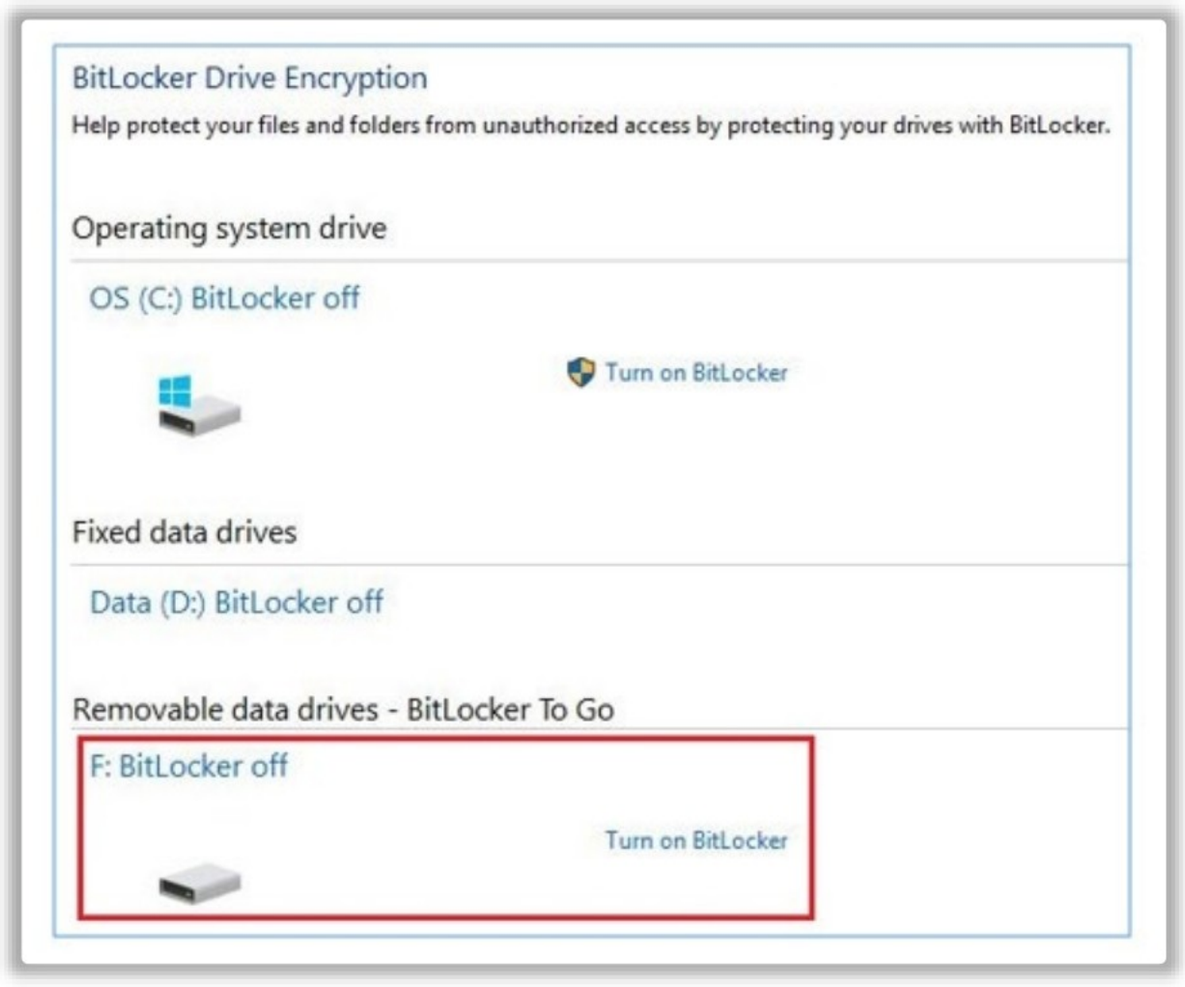


Figure 10.34: Turning on BitLocker

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- BitLocker initialization process will start. Wait for some time to finish the initialization process.

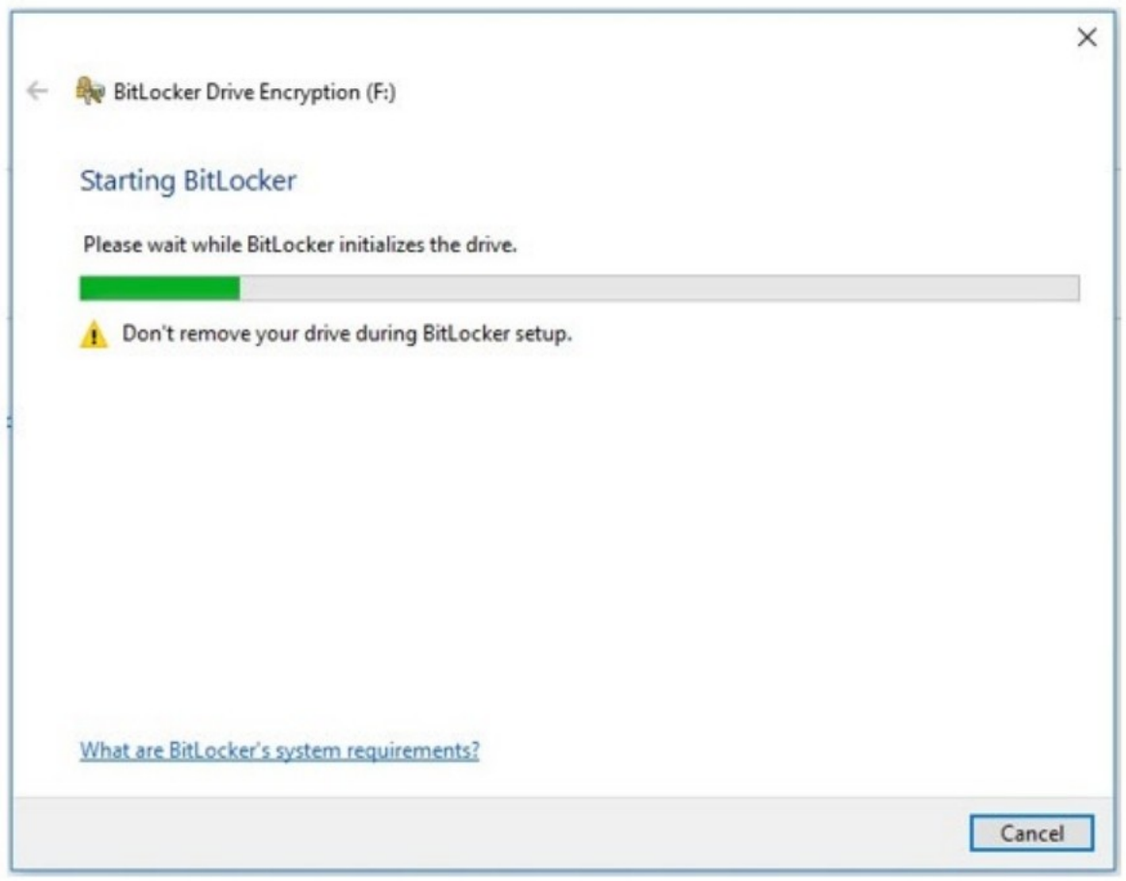


Figure 10.35: BitLocker Initiating the Drive

- In the **Choose how you want to unlock this drive** window**,** tick the **Use a password to unlock the drive** checkbox and enter a strong password, then click **Next**.

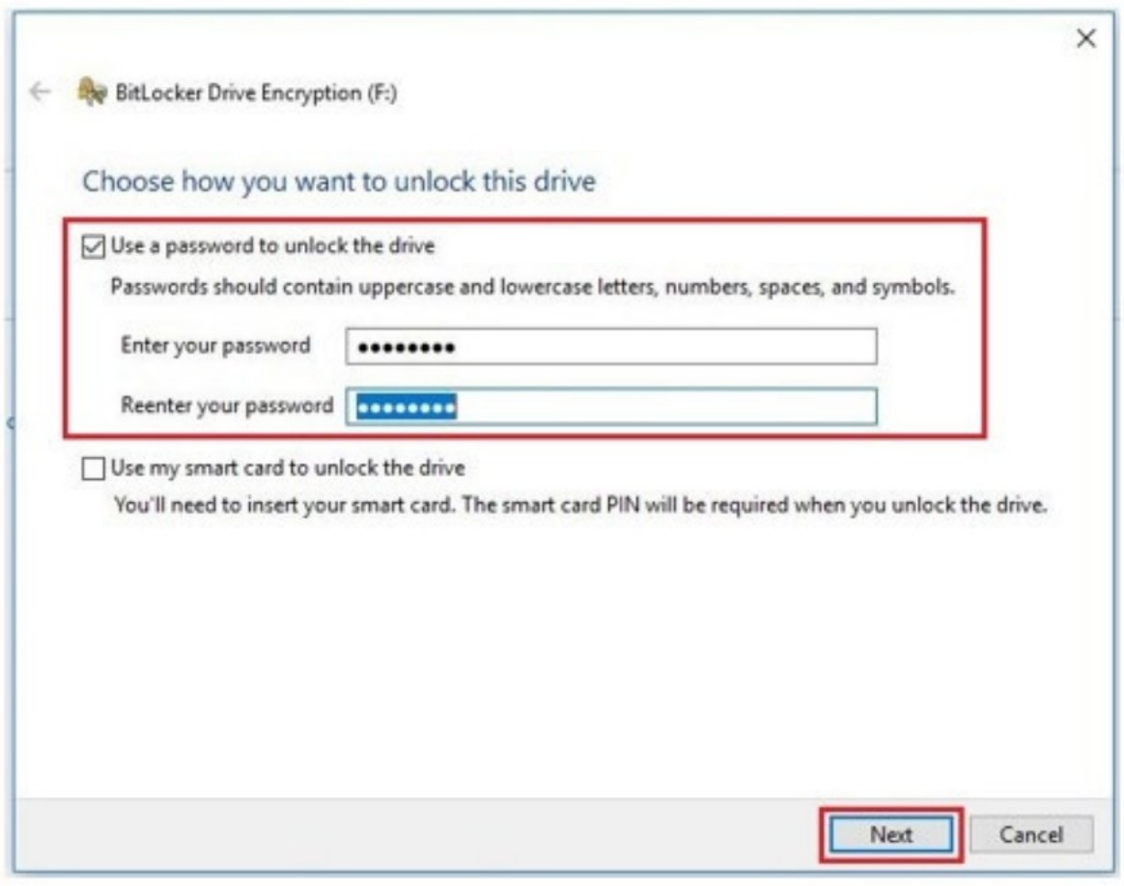


Figure 10.36: Unlocking the Drive

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- In **How do you want to back up your recovery key?** window, either choose **Save to a file** or **Print the recovery key**, then click **Next**.

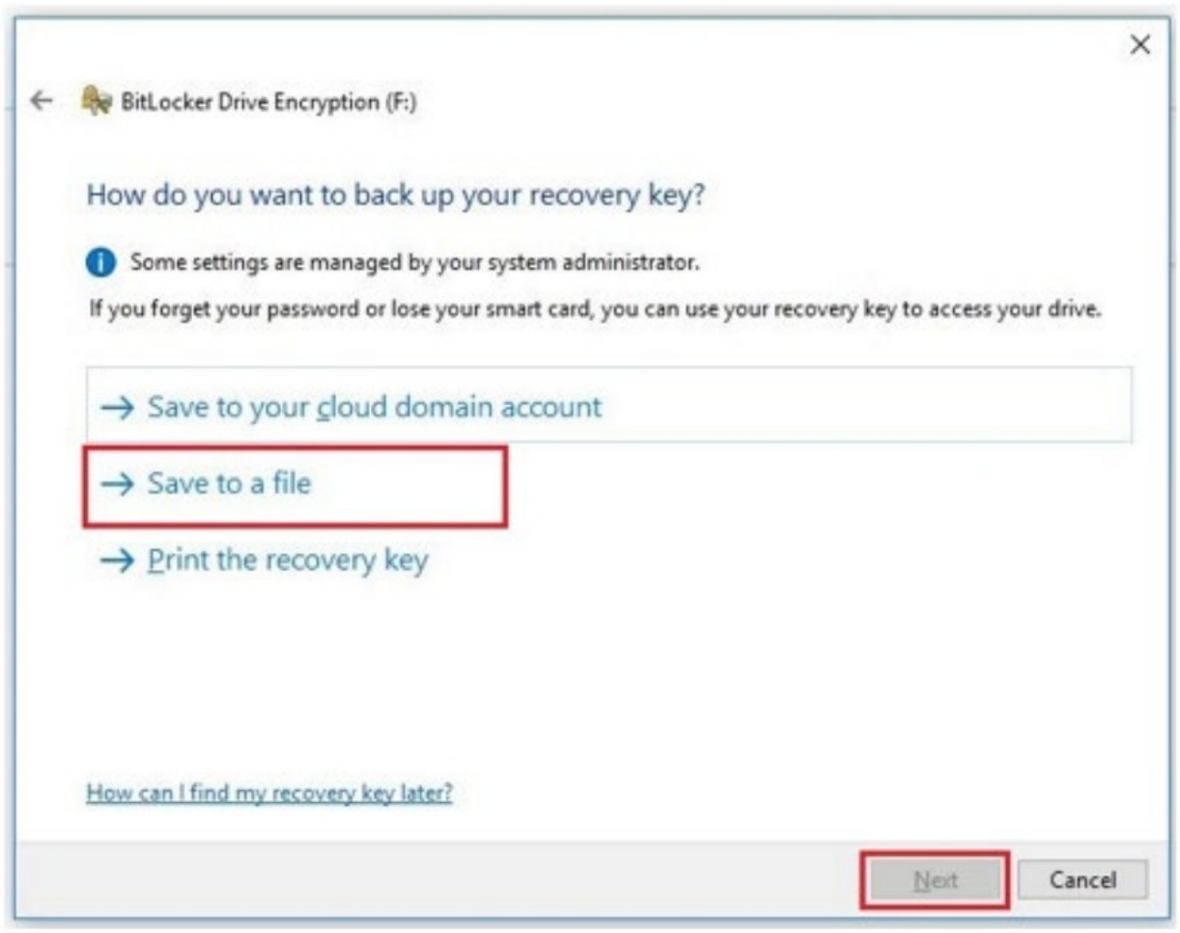


Figure 10.37: Saving to a File

- In the **Choose how much of your drive to encrypt** window, Select **Encrypt used disk space only** if the drive is new or select **Encrypt entire drive** if the drive contains data**,** then click **Next.**

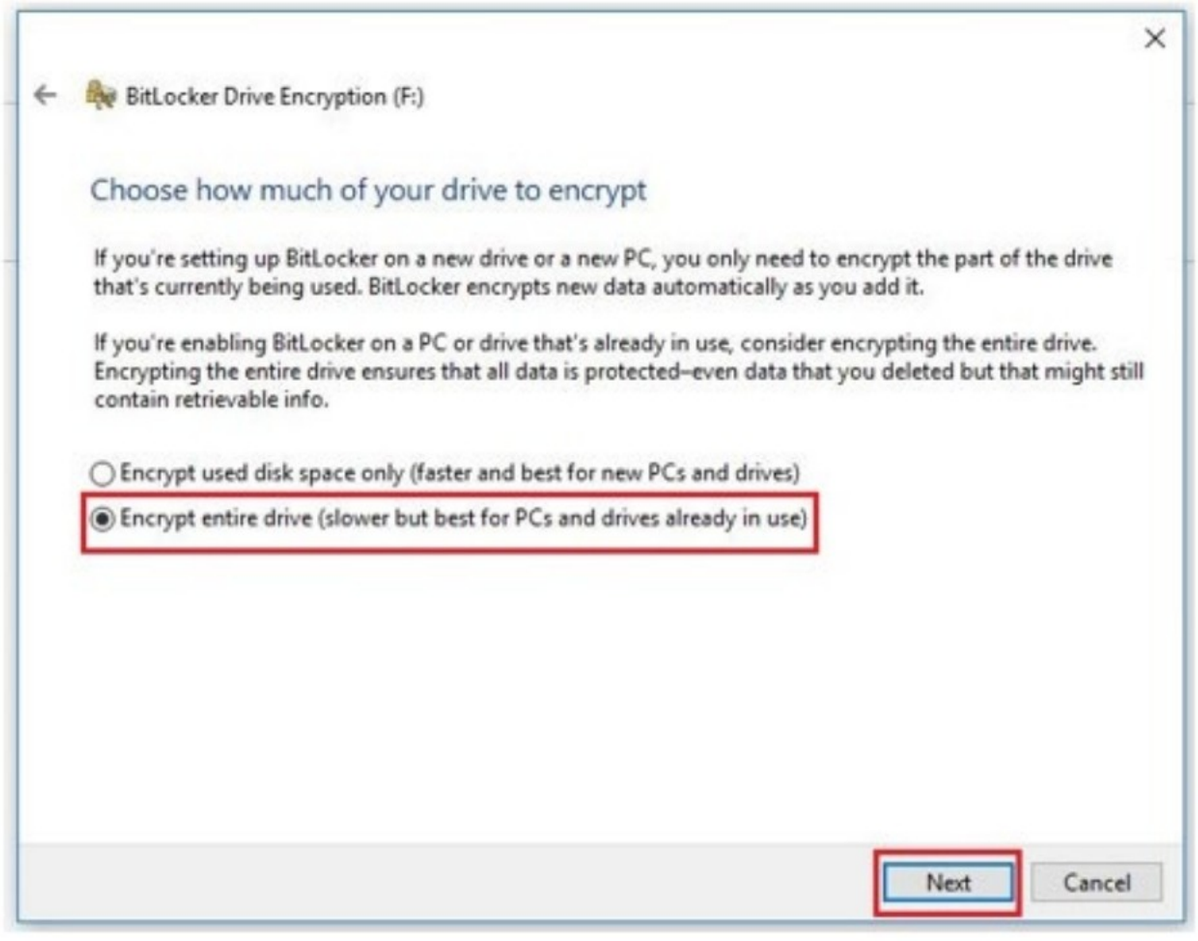


Figure 10.38: Choosing Encrypt Entire Drive Option

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- In the **Choose which encryption mode to use** window, select **Compatible mode** if the user wants to use the encrypted drive on older versions of Windows, or select **New encryption mode** if the user wants to use the encrypted drive on Windows 11 only. Then click **Next**.



Figure 10.39: Choosing Compatible Mode

- Click **Start encrypting**.

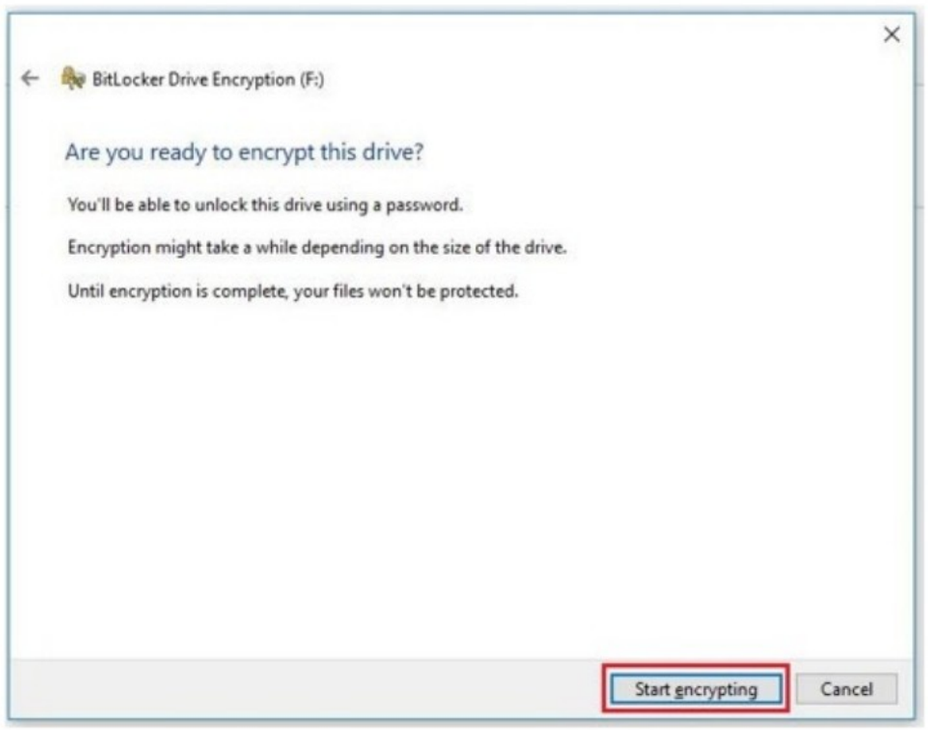


Figure 10.40: Starting the Encryption

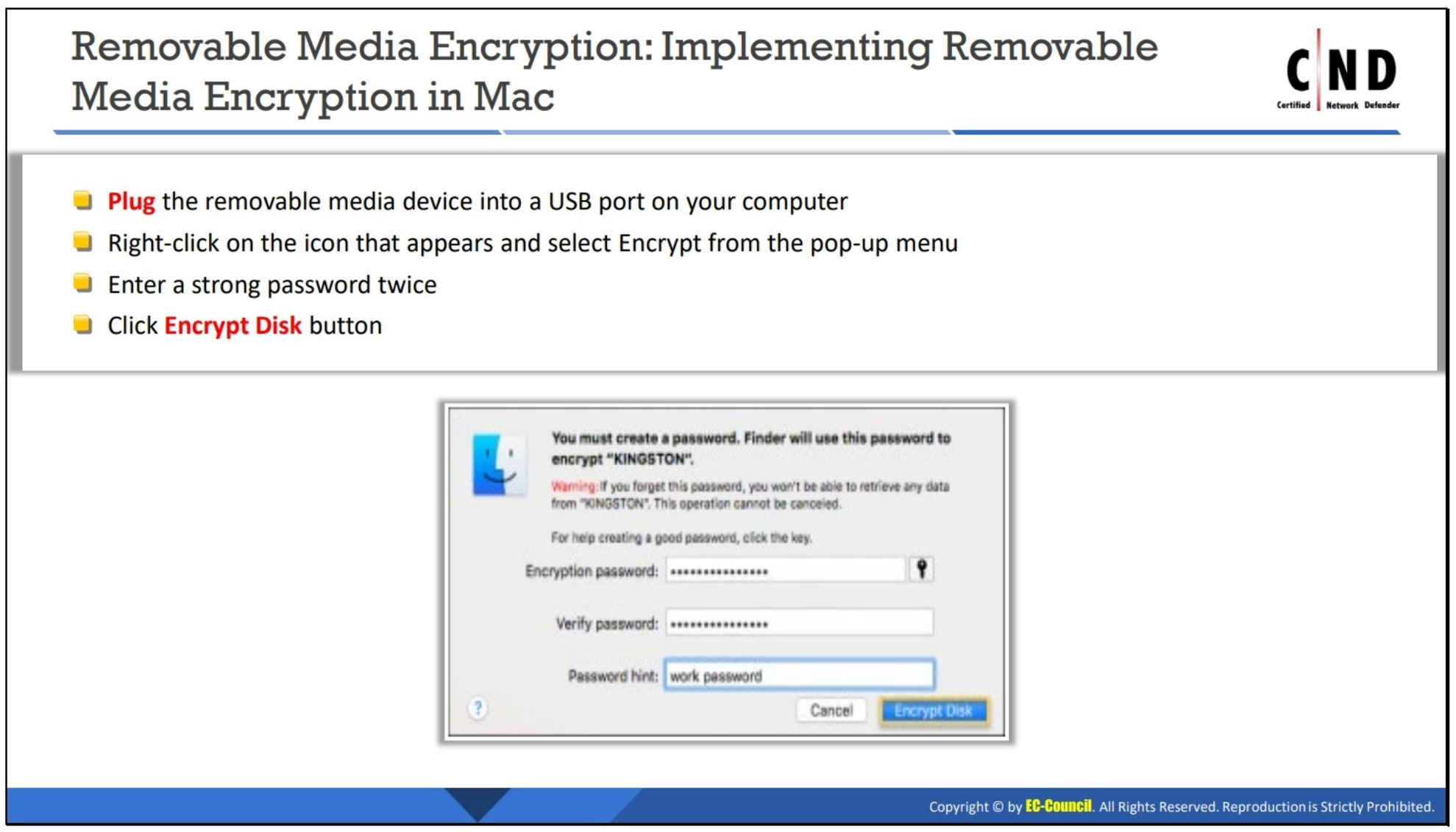
- Click **Close** when the encryption process is completed.



Figure 10.41: Completion of Encryption

Note: Whenever the user tries to connect the encrypted drive, they have to provide the password to unlock it.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Removable Media Encryption: Implementing Removable Media Encryption in Mac

To Enable Removable Media Encryption in Mac OS

- Plug the removable media device into a USB port on the computer.
- Right-click on the icon that appears and select **Encrypt** from the pop-up menu.



Figure 10.42: Removable Media Encryption in Mac OS

- The user will be asked to **create a password**. Enter **Encryption password**, re-enter the password in **Verify the password**, and provide a **Password hint**.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Click **Encrypt Disk**.



Figure 10.43: Selecting Encrypt Disk Option

- Most users receive a warning message regarding GUID Partition Table (GPT), as shown below. If no message is received, skip to step 16.

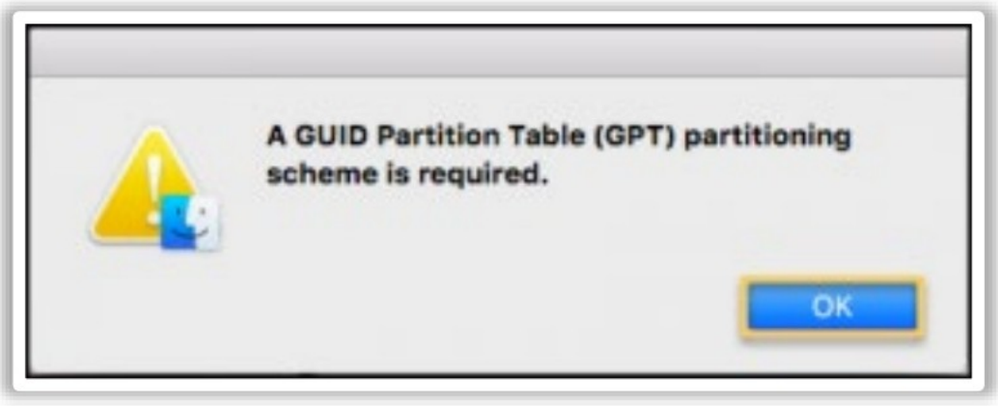


Figure 10.44: Warning Message of GUID Partition Table

- The GPT message means that it is necessary to format a removable media device properly for its encryption. Click **OK** to continue.
- Click on the magnifying glass icon located at the top right corner of the desktop to open **Spotlight Search**. **Spotlight Search** window will appear.

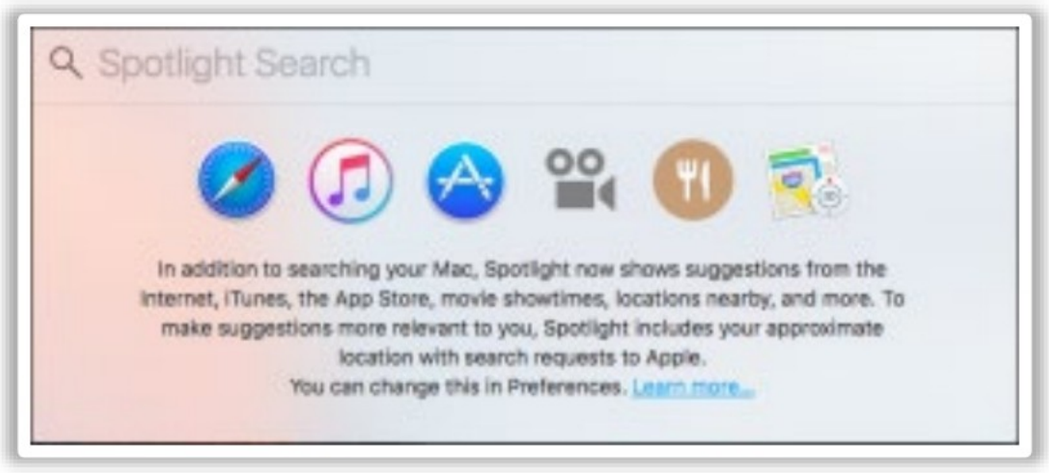


Figure 10.45: Spotlight Search Window

- In **Spotlight Search**, type **disk utility**. **Disk utility** screen will appear.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Select the removable media to encrypt from the left side of the Disk Utility screen and click on the **Erase** option.



Figure 10.46: Selecting Removable Media from Disk Utility Screen

- The **Erase** window will appear.



Figure 10.47: Appearance of Erase Window

- Give an appropriate name for the device in the Name field, for example, CND files. Select the **Journaled** option from the Format drop-down menu. Further, select the GUID Partition Map option from the Scheme drop-down menu.
- Once this is done, click the **Erase** button.
- Wait for some time to complete the process.
- A confirmation message will appear when the process is completed.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Click the **Done** button.



Figure 10.48: Clicking on Done Button

- Close all open screens and go back to the desktop.
- Right-click on the removable media icon and select the **Encrypt CND files** option.

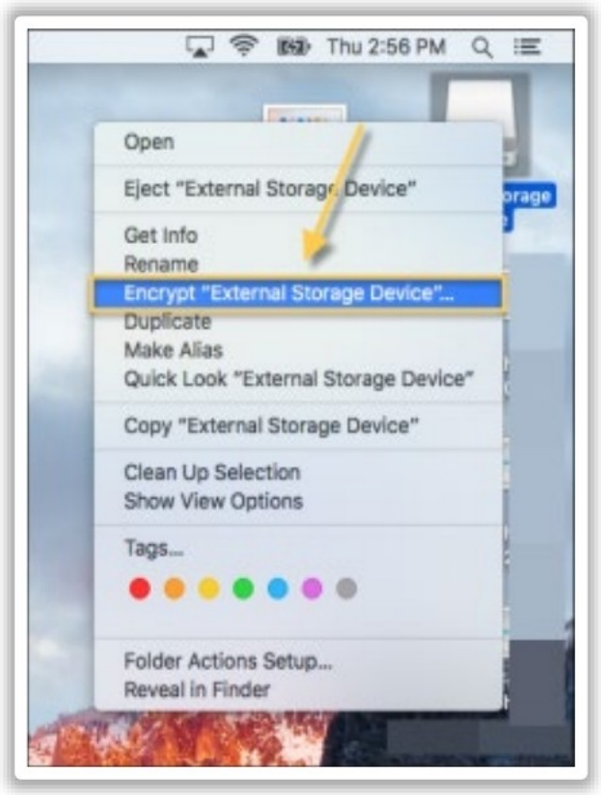


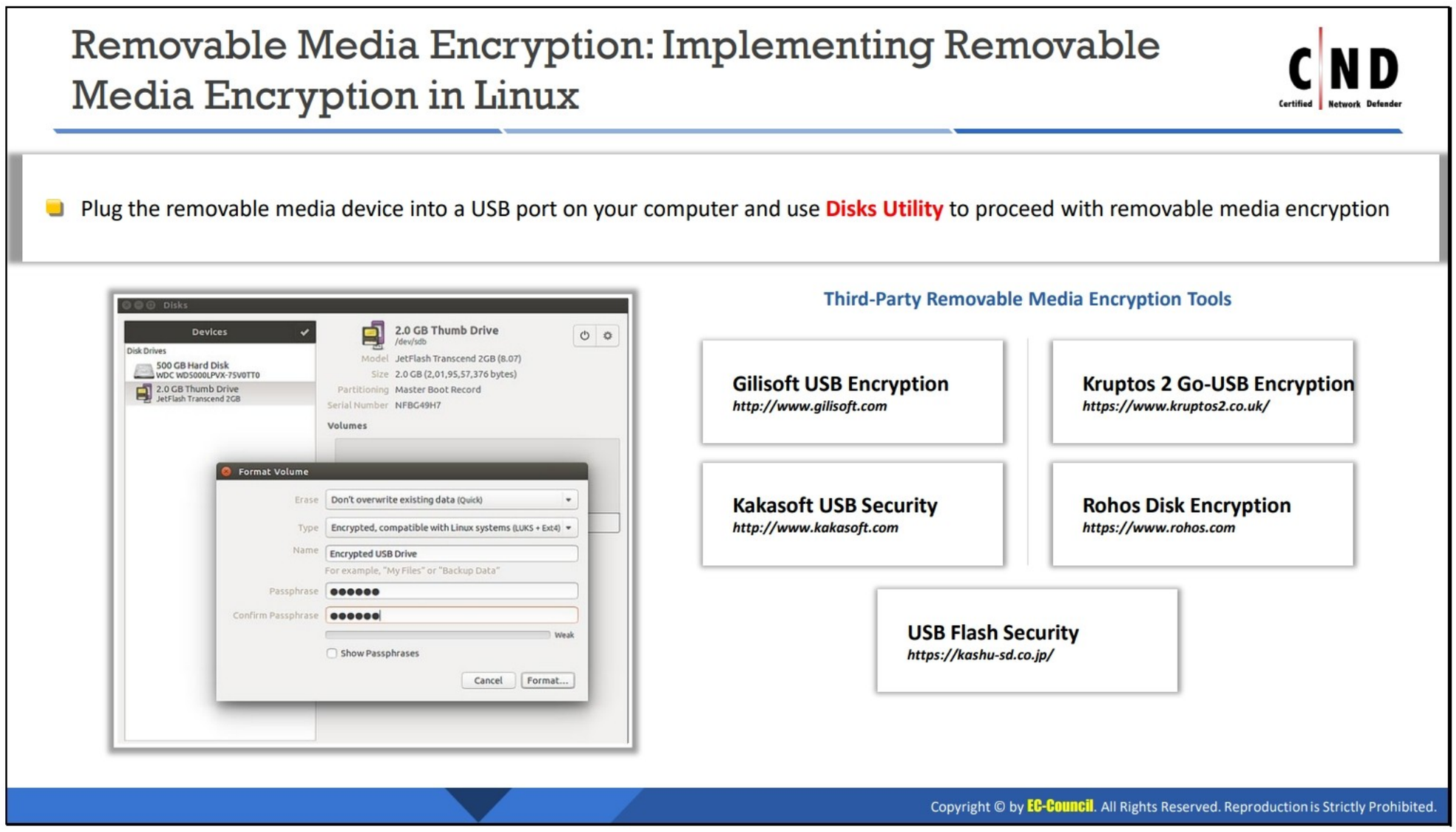
Figure 10.49: Selecting the Encrypt Option

- This will start the encryption process.
- Once the encryption process is completed, a no progress meter or other information is displayed.
- To verify the encryption process was successful, eject and disconnect the device from the computer, and reconnect it again. The encryption process is successful if the user is asked to enter the password while reconnecting it means.



Figure 10.50: Unlocking the Disk External Storage Device

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Removable Media Encryption: Implementing Removable Media Encryption in Linux

To enable removable media encryption in Linux

- Plug the removable media device into a USB port on the computer.
- Type Disks in Unity Dash to open the Disks utility.
- The Disks utility window will open, and the user will see a removable media device to the left.
- Unmount the filesystem by clicking Unmount Volumes as indicated below.
- Select the Format option
- Enter encryption type, partition name, and password.
- Click on the Format button to start the encryption process.
- The removable media is encrypted. To verify, unplug the removable media device and plug it again. The user will be asked to provide a password to access it.
- Enter the password and click on Connect button to access the removable media.

Third-party Removable Media Encryption Tools

GiliSoft USB Encryption

Source: www.gilisoft.com

GiliSoft USB Encryption is a solution for USB security that supports the encryption of portable storage devices (external drives), and can divide an external drive into two parts after encryption: a secure area and a public area. It converts a regular USB flash drive into a secured one in less

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

than a minute, and data on the protected area (secure area) is encrypted by a 256-bit AES on-the-fly encryption.

Kruptos 2 Go-USB Encryption

Source: www.kruptos2.co.uk

Kruptos 2 Go-USB Encryption is a password protection tool for your USB drive to protect your privacy and important data from data theft, loss, or leaks. Just drag and drop your files and folders into Kruptos 2 Go's encrypted "Vault" and they will be password-protected immediately, preventing your important data from being modified, read, or even accessed without the correct password.

Kakasoft USB Security

Source: www.kakasoft.com

Kakasoft USB Security protects your sensitive information in USB drives with the strongest encryption technique. This USB disk security program comprehensively secures your confidential data on USB flash drives, and protects them from unauthorized access with the adoption of marvelous cryptography and advanced encryption methods.

Rohos Disk Encryption

Source: www.rohos.com

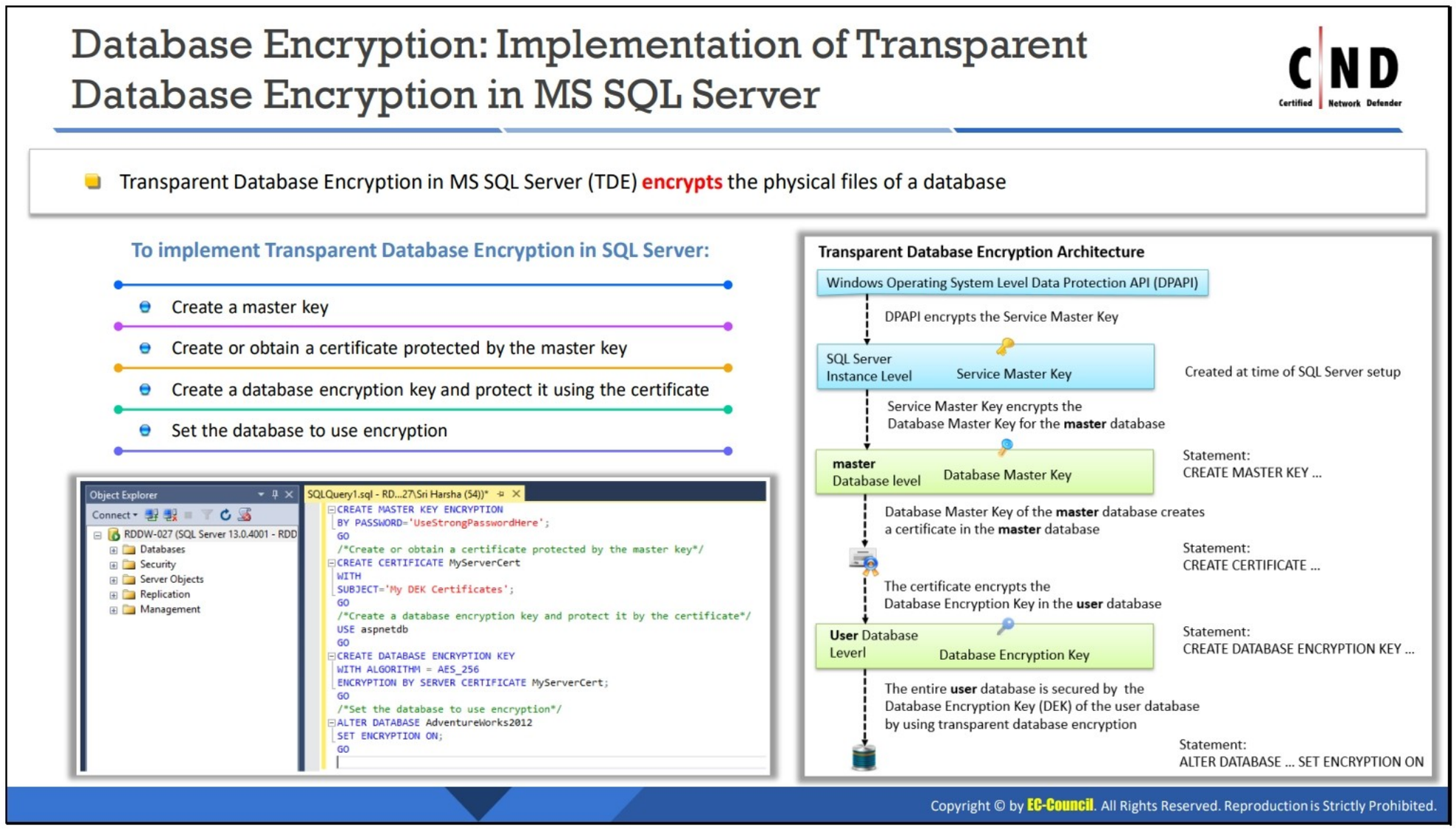
The Rohos Disk Encryption program creates hidden and protected partitions on a computer or USB flash drive, and password protects/locks access to your web applications.

USB Flash Security

Source: https://kashu-sd.co.jp/

USB Flash Security creates a password-protected USB drive that helps keep the data safe. It is not hard to use once you have untangled the instructions. It is installed on the PC and protects the attached drive. Once protected, a password is necessary to access the USB stick, irrespective of where it is used.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Database Encryption: Implementation of Transparent Database Encryption in MS SQL Server

Database encryption is defined as a process of converting a plain text database into a ciphertext database using encryption techniques. Its main motive is to make the data in a database unreadable to individuals with potentially malicious intentions. It also minimizes the intention of hackers to hack the database as encrypted data cannot be easily deciphered. Several techniques and methods are used by network defenders to implement encryption in the database, such as:

- **Transparent/External database encryption**: This type of database encryption methods encrypts the entire database, that is, it encrypts the "data at rest." Transparent or external database encryption uses a symmetric encryption key to encrypt the database, and all backups using a database encryption key. A risk with using this method is that the network defender can encrypt only the data that is stored in the database tables; the data that is stored in memory or cache is not encrypted. An individual with a malicious intent may access that data. Access to symmetric encryption key can lead to an access to the database content.
- **Column-level encryption**: This method is a form of partial database encryption. It encrypts the individual columns within the database tables using different encryption keys. This method is more secure, as it needs a separate decryption method for decrypting each encrypted column. However, this method minimizes the database index and search performance. Similarly, partial database encryption can be applied on individual rows, cells, and table spaces of the database table with a separate encryption key.
- **Symmetric database encryption**: This method is an enhanced transparent database encryption method where the database remains encrypted till it is not opened and

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

accessed. However, in this method, the user requires a copy of the private key to access the database content. If the network defender uses this method to encrypt the database, then there is a chance that the private key can be leaked or identified by unauthorized users.

- **Asymmetric database encryption**: This method is an improvement over symmetric database encryption, and uses only one private key to encrypt and decrypt data; however, this method uses one public key to encrypt the data and one private key per authorized user to decrypt the data. In case the public key is leaked or accessed by an unauthorized user, they would not be able to read the content of the encrypted file.

Transparent Database Encryption Architecture

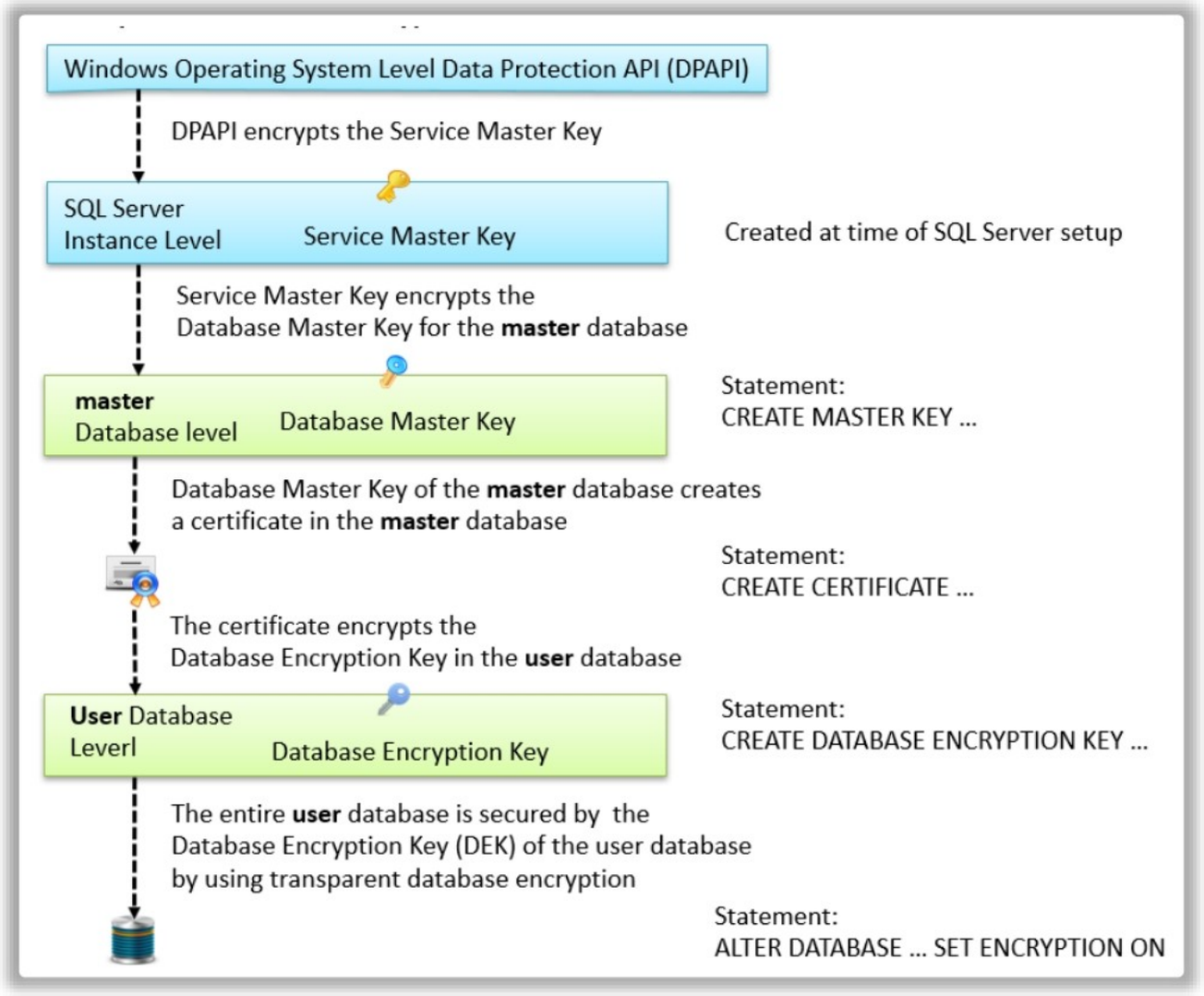


Figure 10.51: Transparent Database Encryption Architecture

Transparent Database Encryption Hierarchy

Transparent database encryption is a built-in feature to protect data at rest. Encrypting the data at rest safeguards it against cybercriminals as an attacker will not be able to decipher the encrypted data.

SQL Server Instance

- A service master key (SMK) is created while setting up an SQL server instance.

Master Database

- Data protection API (DPAPI) encrypts SMK. The DPAPI protects the SMK in the master database.
- SMK encrypts the database master key (DMK). Hence, SMK protects the DMK.

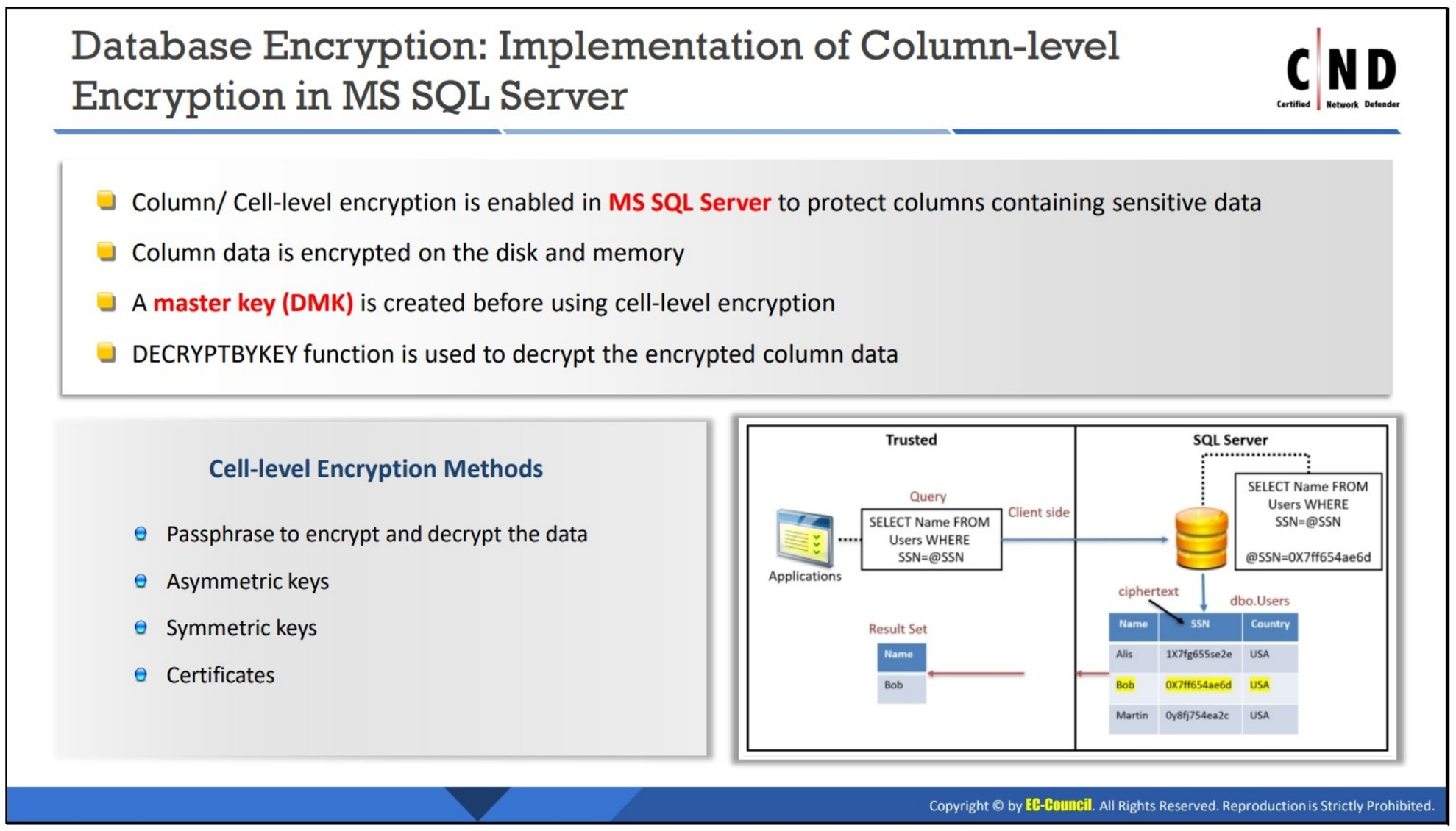
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- The DMK creates a certificate. Hence, it protects the certificate's private key.
- The certificate encrypts the database encryption key (DEK). Hence, the certificate protects the DEK in the user database.

User Database

- The entire user database is secured by the DEK using transparent database encryption (TDE). DEK protects the data in the user database.
- TDE executes a page-level encryption; the pages are encrypted before they are written to the disk, and decrypted when the user wants to read them.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



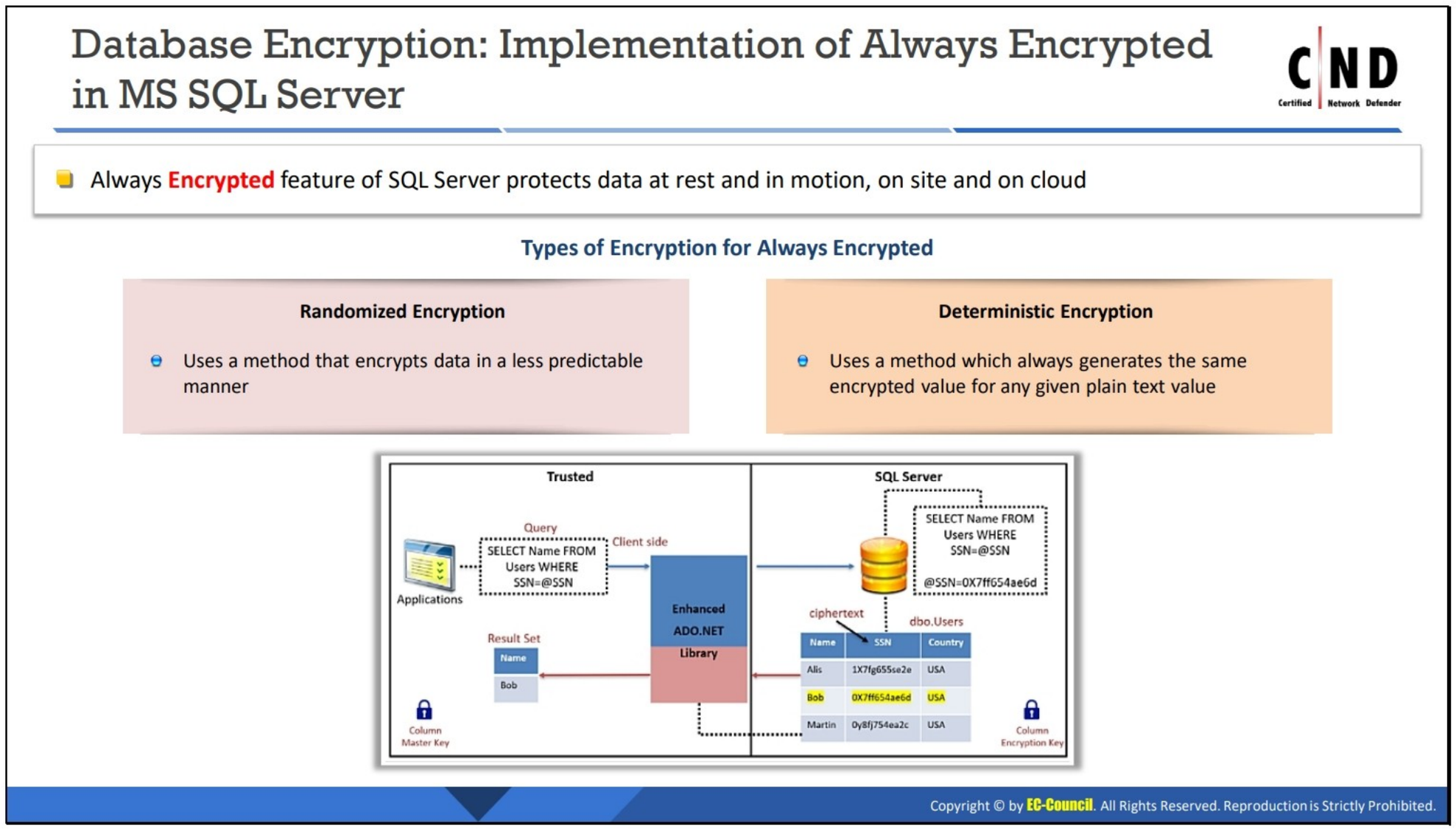
Database Encryption: Implementation of Column-level Encryption in MS SQL Server

In MS SQL server, column/cell-level encryption protects the sensitive data in a column. It encrypts the column data in a disk that will remain in an encrypted state in the memory until a user decrypts the encrypted data using the DECRYPTBYKEY function. Before using cell-level encryption, the user should create a master key (DMK).

Cell-level encryption options: The user should choose the appropriate option for encrypting data.

- **Passphrase**: The user ought to use the same passphrase when encrypting and decrypting the data; therefore, it is the least secure option.
- **Asymmetric keys**: The user should use different keys for encrypting and decrypting the data. It provides a stronger protection; however, its performance is poor, and it should not be used to encrypt large values.
- **Symmetric keys**: The user should use the same keys for encrypting and decrypting the data. It provides good protection and strong performance.
- **Certificate**: It should be signed by the DMK and could be associated with the user. It provides strong protection and good performance.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Database Encryption: Implementation of Always Encrypted in MS SQL Server

Always Encrypted feature secures sensitive data by encrypting them in client applications without revealing the encrypted keys to the data engine. Thus, it separates the client and data managers. If the Always Encrypted feature is enabled, an administrator would not be able to read the sensitive data. The always encrypted feature of SQL server protects data at rest and in motion, on site and on cloud.

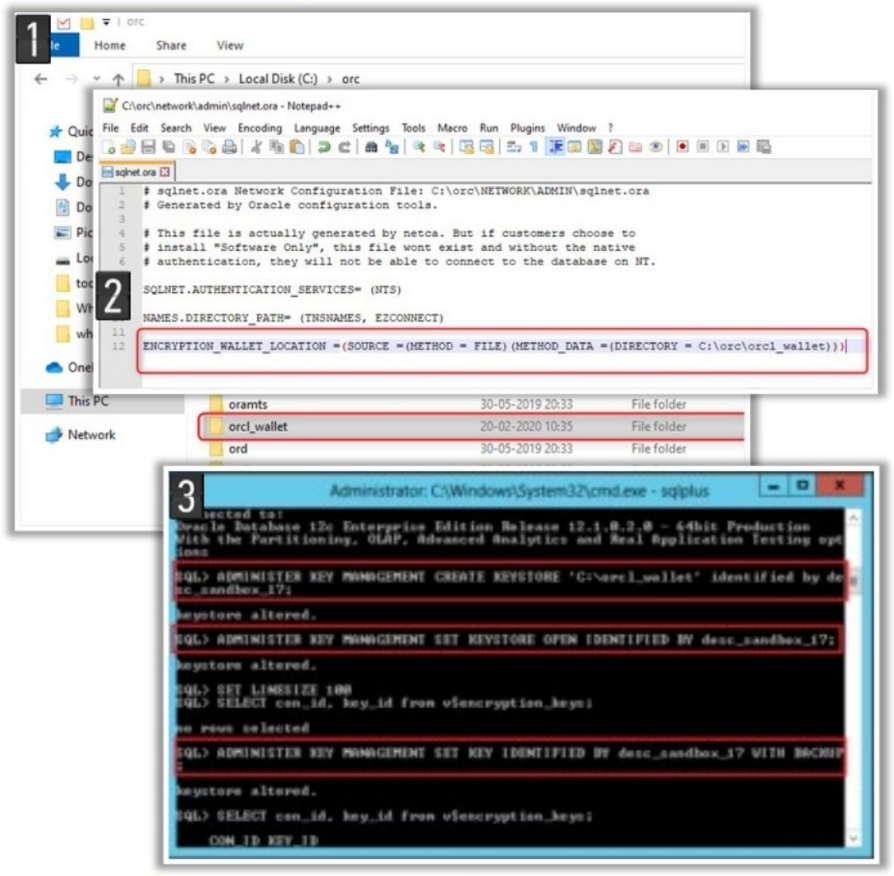
Types of Encryption for Always Encrypted

- **Randomized encryption:** Uses a method that encrypts data in a less predictable manner.
- **Deterministic encryption:** Uses a method that always generates the same encrypted value for any given plain text value.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Database Encryption: Implementation of Transparent Data Encryption in Oracle

- Transparent data encryption (TDE) enables the encryption of **one or more table columns** or a **tablespace**
- On inserting data in an encrypted column, TDE automatically encrypts the data
- On selecting the encrypted column, the data is automatically decrypted
- To implement transparent database encryption:
  - Creating a wallet file location to store all encryption key information
  - Specifying location of the wallet in the sqlnet.ora file located in the NETWORK/admin folder
  - Commands to create, open, and set the master key



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Database Encryption: Implementation of Transparent Data Encryption in Oracle (Cont'd)

Creating a New Table with an Encrypted Column Using the Default Algorithm (AES192)

```
CREATE TABLE employee ( first_name VARCHAR2(128), last_name
VARCHAR2(128), empID NUMBER, salary NUMBER(6) ENCRYPT );
```

Adding Encrypted Columns to Existing Tables

```
ALTER TABLE employee ADD (ssn VARCHAR2(11) ENCRYPT);
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

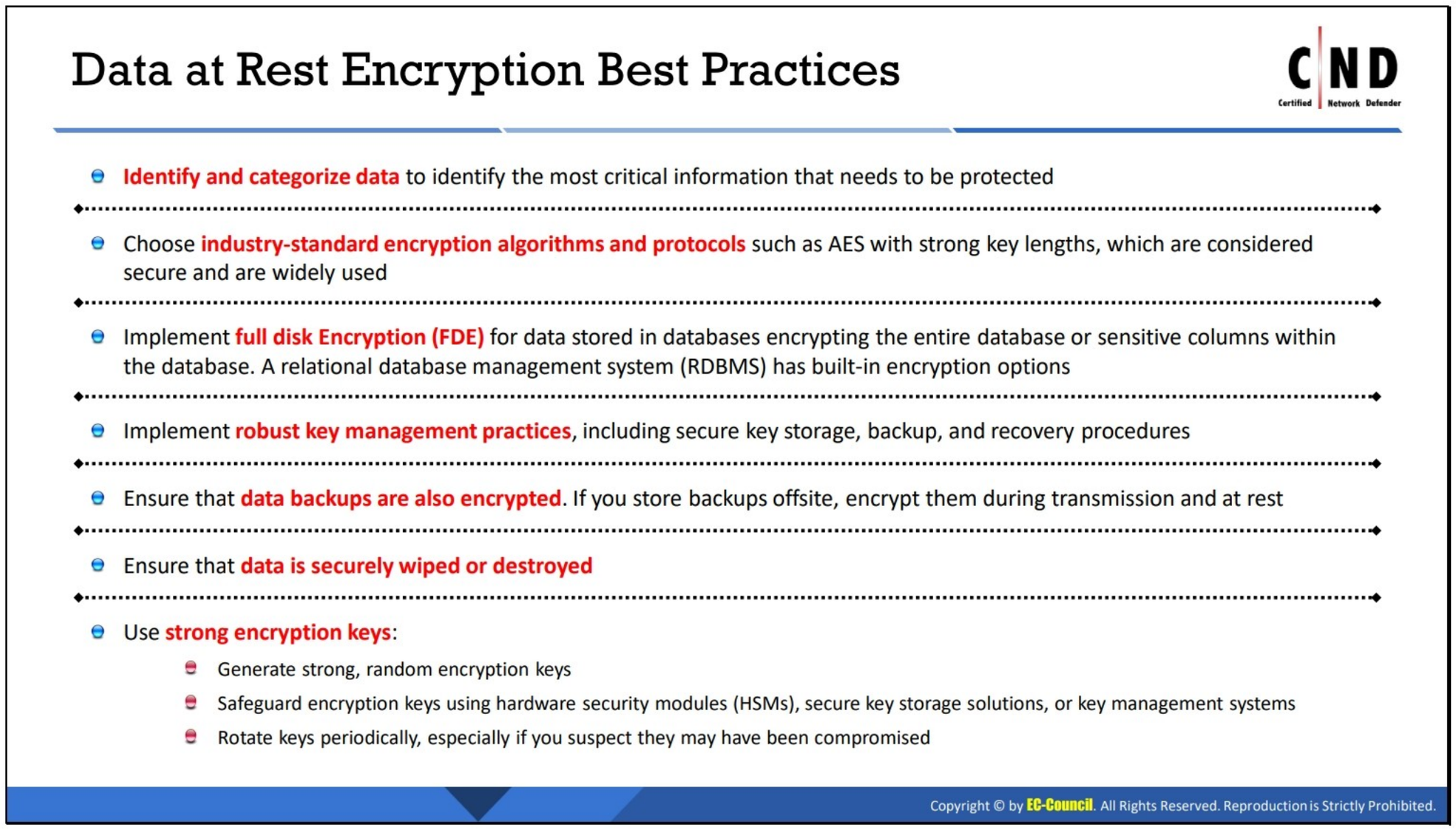
Database Encryption: Implementation of Transparent Data Encryption in Oracle

Transparent data encryption (TDE) enables the encryption of one or more table columns, or a tablespace. On inserting data in an encrypted column, TDE automatically encrypts the data. On selecting the encrypted column, the data is automatically decrypted.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

To implement TDE in Oracle, the user has to create a Keystore to store the master encryption key and set a master key. The Keystore is a type of operating system file stored outside the database. TDE uses this Keystore to encrypt data in the database.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Data at Rest Encryption Best Practices

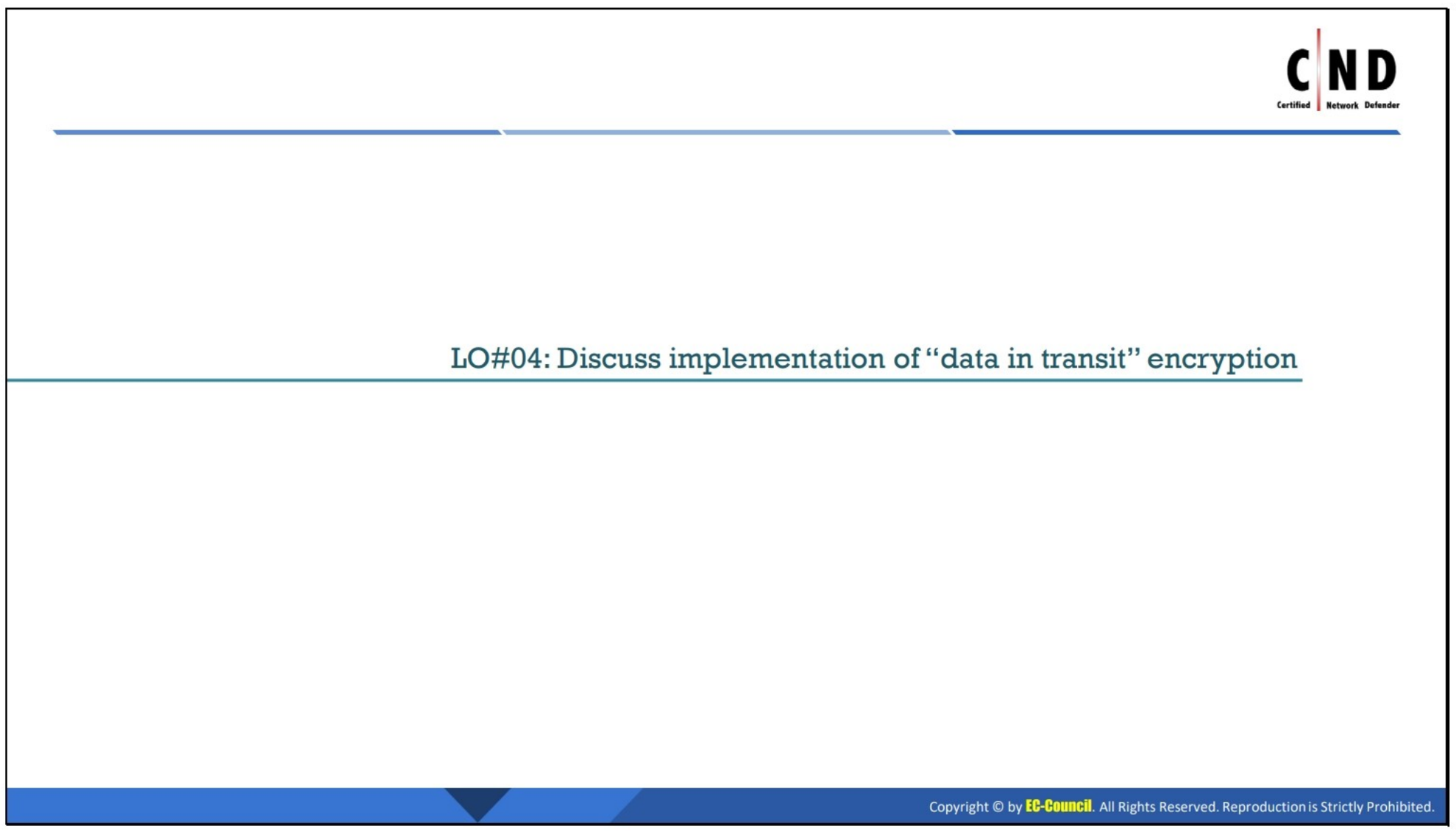
The best practices for data at rest encryption are as follows:

- **Choose strong encryption algorithms:** Using an industry standard algorithm such as advanced encryption standard (AES) to encrypt all kinds of sensitive data ensures that the data is not being accessed in an unauthorized way or by any unauthorized person. Effective data encryption algorithms help reduce the size of the data thereby reducing the usage of CPU power.
- **Implement full disk encryption (FDE):** Full disc encryption encrypts the database or selected columns within the database. The relational database management system (RDBMS) has inbuilt encryption options in it.
- **Using strong encryption keys:** Strong encryption tends to involve large numbers for the encryption key. The larger the key, the longer the time it takes to break the algorithm. A 256-bit key is considered a strong encryption key. Encryption keys can be safeguarded using hardware security modules (HSMs), secure key storage solutions, or key management systems.
- **Implement robust key management practices:** Key management system and rotation is considered a good approach to increase the confidentiality of the cryptographic keys. Separating the keys and restricting user access can significantly reduce the risk of exposing all sensitive keys.
- **Data backups and encryption:** Data backups are important as it is vital to have multiple copies of data and it needs to be encrypted. It is also vital to secure the channels from where data is retrieved as transmission of data from multiple sources can be exposed to attack surface areas. This encrypts the dataat rest and data at transmission.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Ensure that the data in the system is entirely wiped and destroyed:** Ensure that the data in the system is entirely wiped and destroyed. This prevents the unauthorized users from reading it. The authentic way to wipe the data is to physically connect any medium to a bulk wiping device.

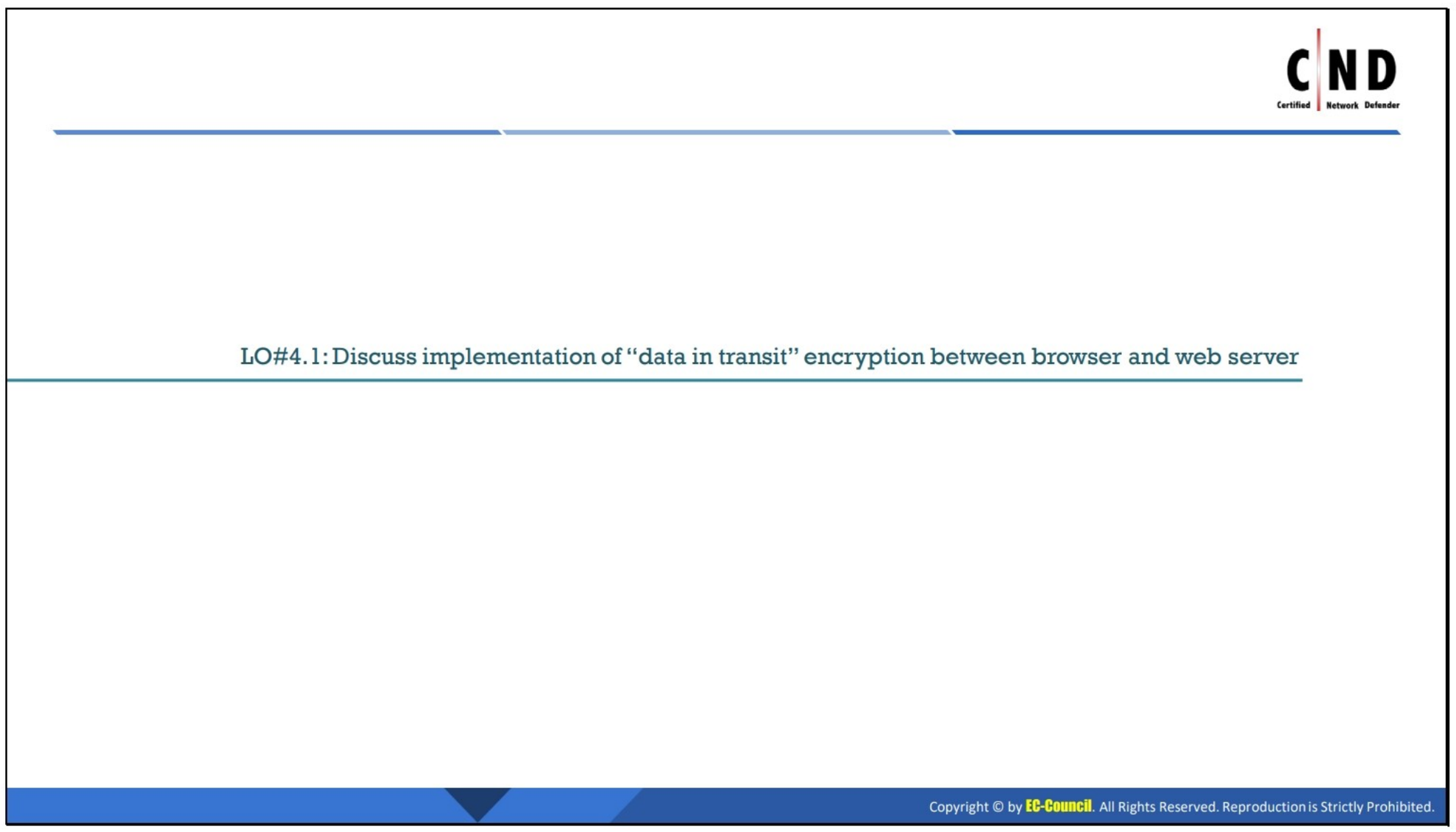
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



LO#04: Implementation of "Data in Transit" Encryption

The objective of this section is to explain the use of encryption technology to secure data in transit.

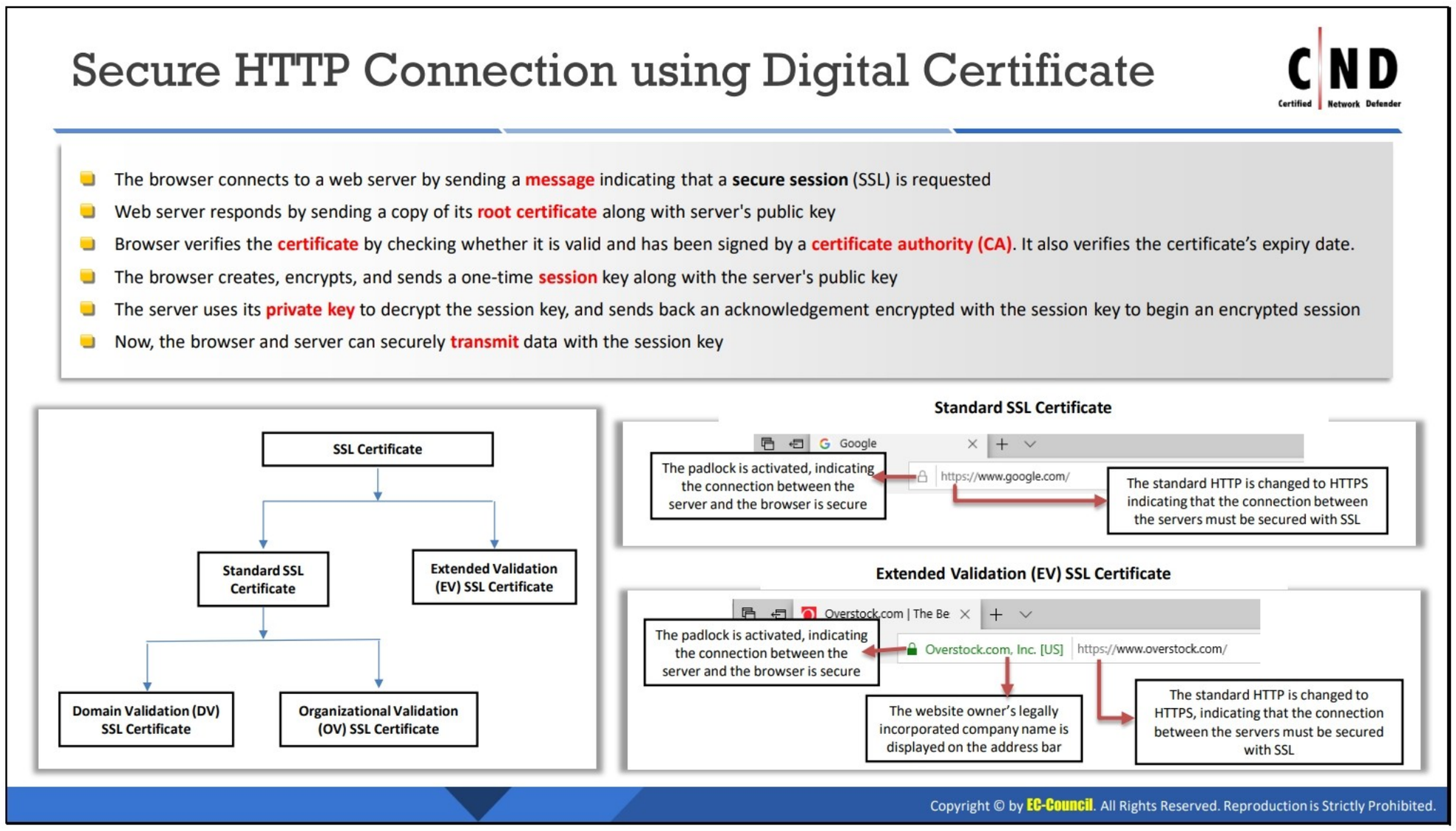
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



LO#4.1: Implementation of "Data in Transit" Encryption Between Browser and Web Server

The objective of this section is to explain the use of encryption technology to secure data in transit between client browser and web server.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Secure HTTP Connection using Digital Certificate

1. The browser makes the connection to a web server by sending it a message, indicating that a secure session (SSL) is requested.
2. The web server responds by sending a copy of its root certificate along with the server's public key.
3. The browser verifies the certificate by checking whether it is valid and has been signed by a certificate authority (CA). It also verifies the certificate's expiry date.
4. The browser creates, encrypts, and sends a one-time session key along with the server's public key.
5. The server uses its private key to decrypt the session key, and sends back an acknowledgment encrypted with the session key to begin an encrypted session.
6. Now, the browser and server can securely transmit data with the session key.

Standard SSL Certificate

This certificate is validated and issued rapidly by the CA, and is ideal for small and medium-sized businesses. A standard SSL certificate displays HTTPS instead of HTTP and a padlock. It is either domain validated or has an organizational validity.

- **Domain-validated (DV) SSL certificate**: The CA verifies only the domain ownership and gives the certificate within a few minutes. This certificate ensures that the website safeguards the user privacy.
- **Organization-validated (OV) SSL certificate**: The CA requires important business documents for validation in order to issue this certificate. This certificate is more trusted

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

than the normal DV SSL certificate. This certificate safeguards user confidentiality and increases the trust on the website.

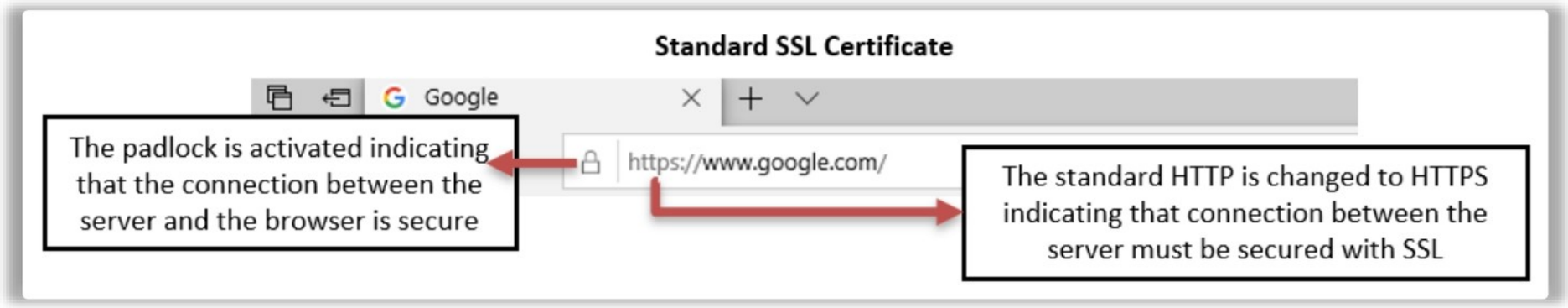


Figure 10.52: Standard SSL Certificate



Figure 10.53: Extended Validation (EV) SSL Certificate

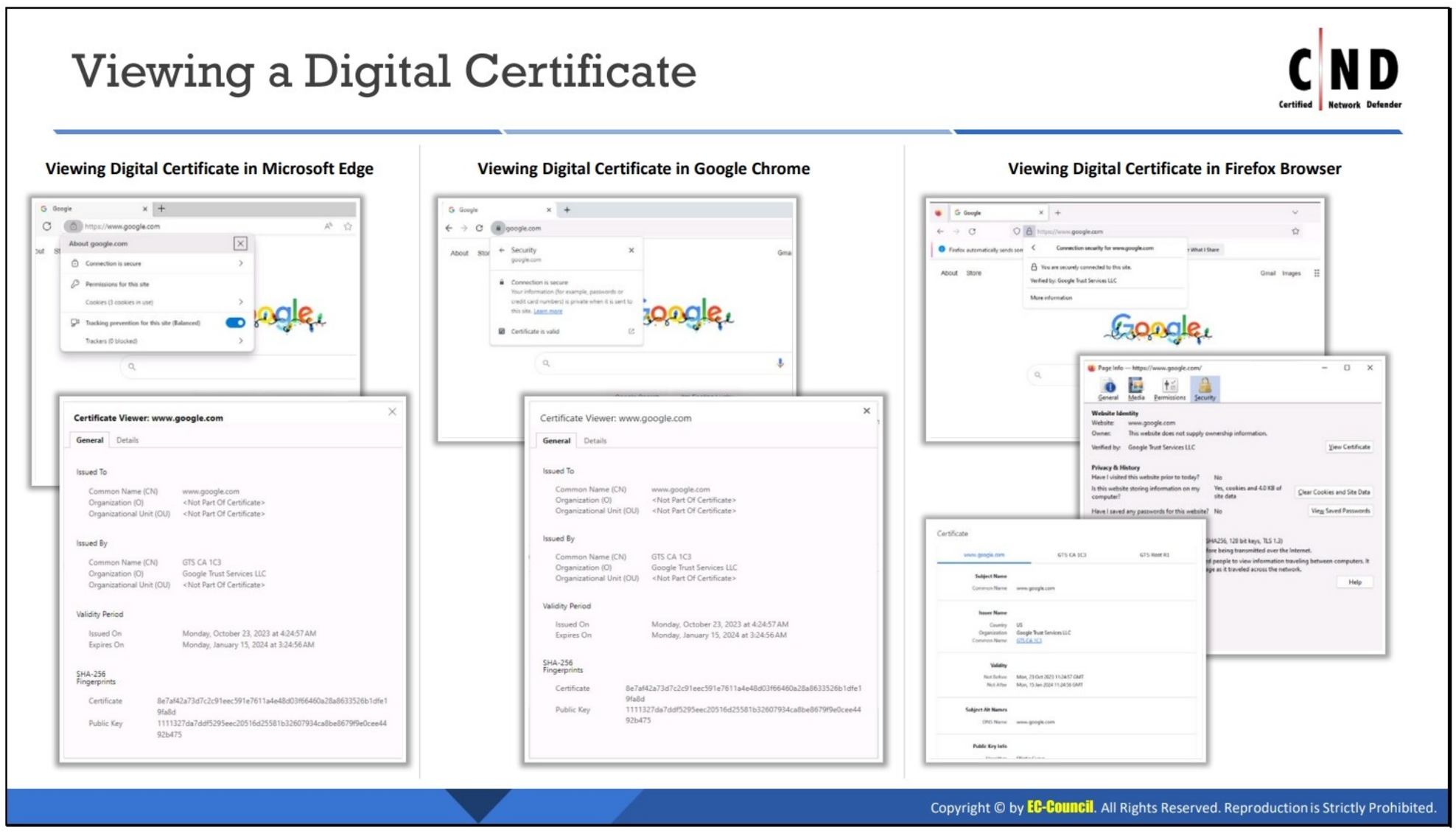
Extended Validation (EV) SSL Certificate

EV SSL is the most reliable and recommended SSL certificate. It verifies the company name in the URL and delivers a 256-bit robust encryption, which safeguards the confidentiality of the users and increases the trust and confidence in the website.

Characteristic Features of EV SSL

- The web address bar should have HTTPS
- The address bar contains the organization name
- The URL contains the company name.
- The certificate information has the CA name.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Viewing a Digital Certificate

Viewing a Digital Certificate in Google Chrome

- Type the name of the website whose certificate the user wants to view in Google Chrome browser.
- Click the lock icon in the address bar, then navigate and click on **Connection is secure/Certificate is valid**.

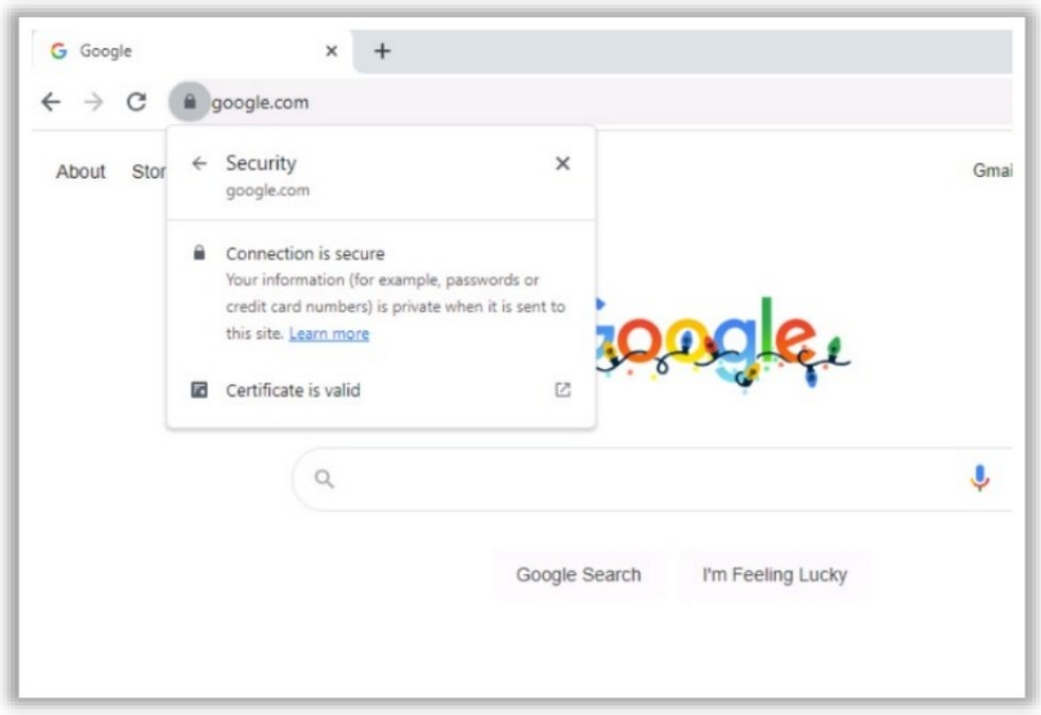


Figure 10.54: Selecting the Certificate is valid option

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- A new window will open with **General** and **Details** tabs..



Figure 10.55: Choosing General Tab

Viewing a Digital Certificate in Firefox Browser

- Enter the name of the website whose certificate the user wants to view in Firefox browser.
- Click the lock icon in the address bar.



Figure 10.56: Clicking the Lock Icon in the Address Bar

- Click **Connection secure** to see the connection details.

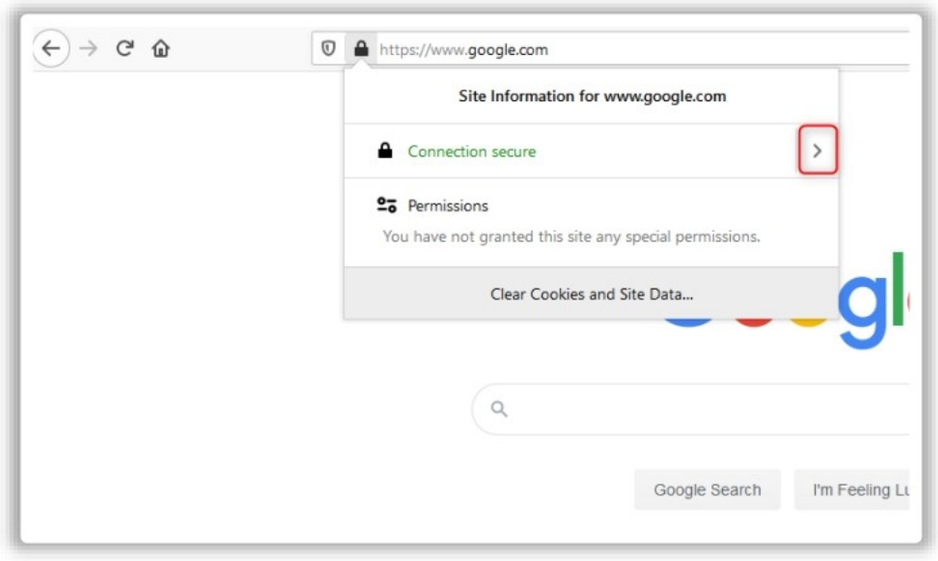


Figure 10.57: Checking the Connection Details

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Navigate to and click **More information**.



Figure 10.58: Select More Information

- A new **Page Info** window will open; click **Security** tab.
- Click **View Certificate** to view the digital certificate.

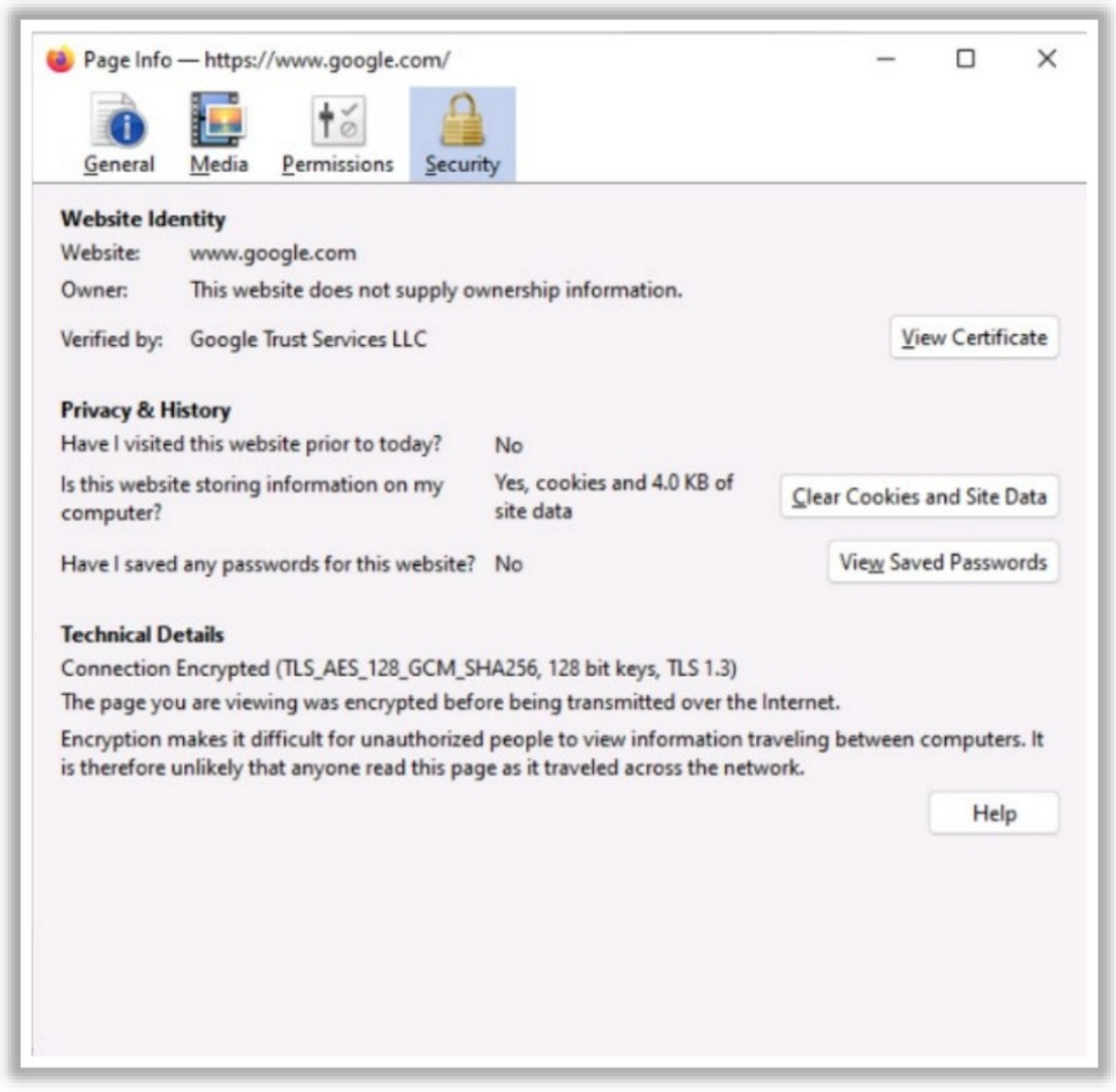


Figure 10.59: Clicking on Security Tab

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

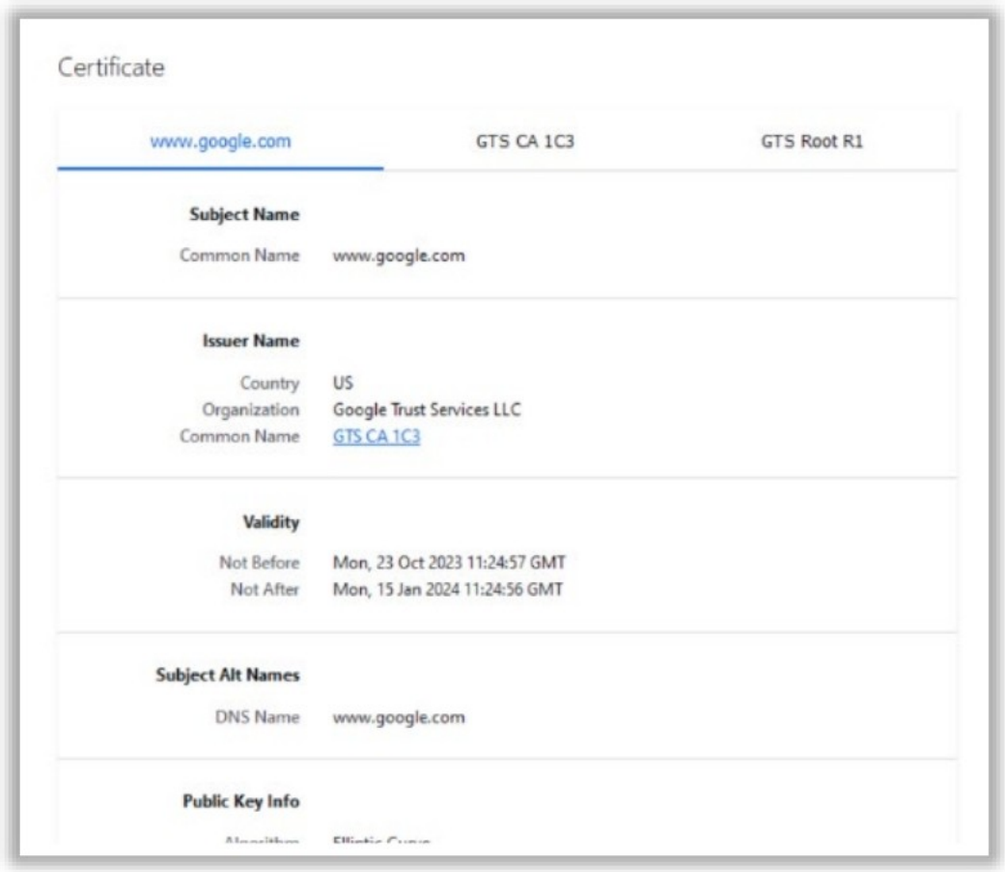


Figure 10.60: Viewing the Digital Certificate

Viewing a Digital Certificate in Microsoft Edge

- Enter the name of the website whose certificate the user wants to view in Firefox browser.
- Click the lock icon in the address bar.

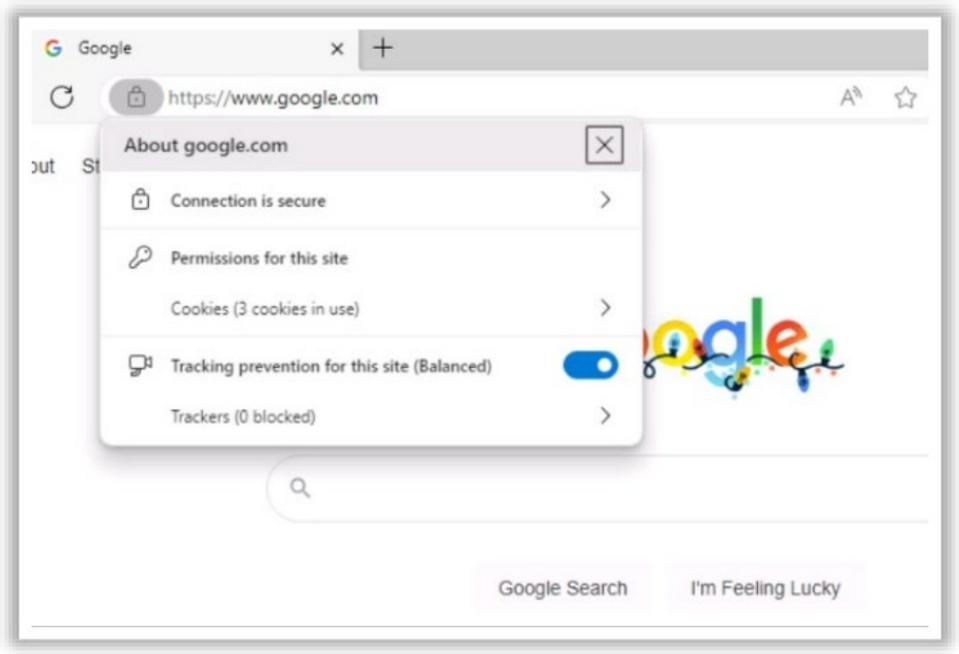


Figure 10.61: Selecting Lock Icon

- Click **Connection is secure** and then **Show certificate** icon.

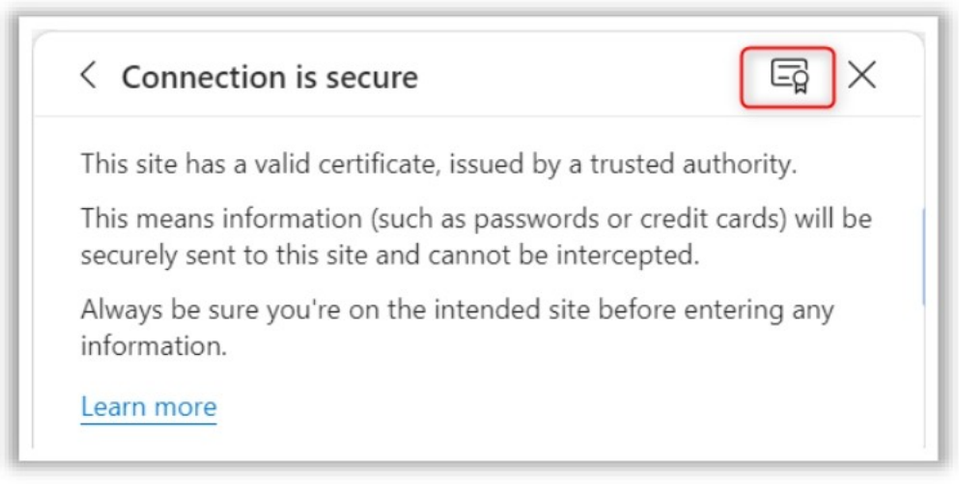


Figure 10.62: Selecting the Show certificate icon

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- A new will open with certificate details.

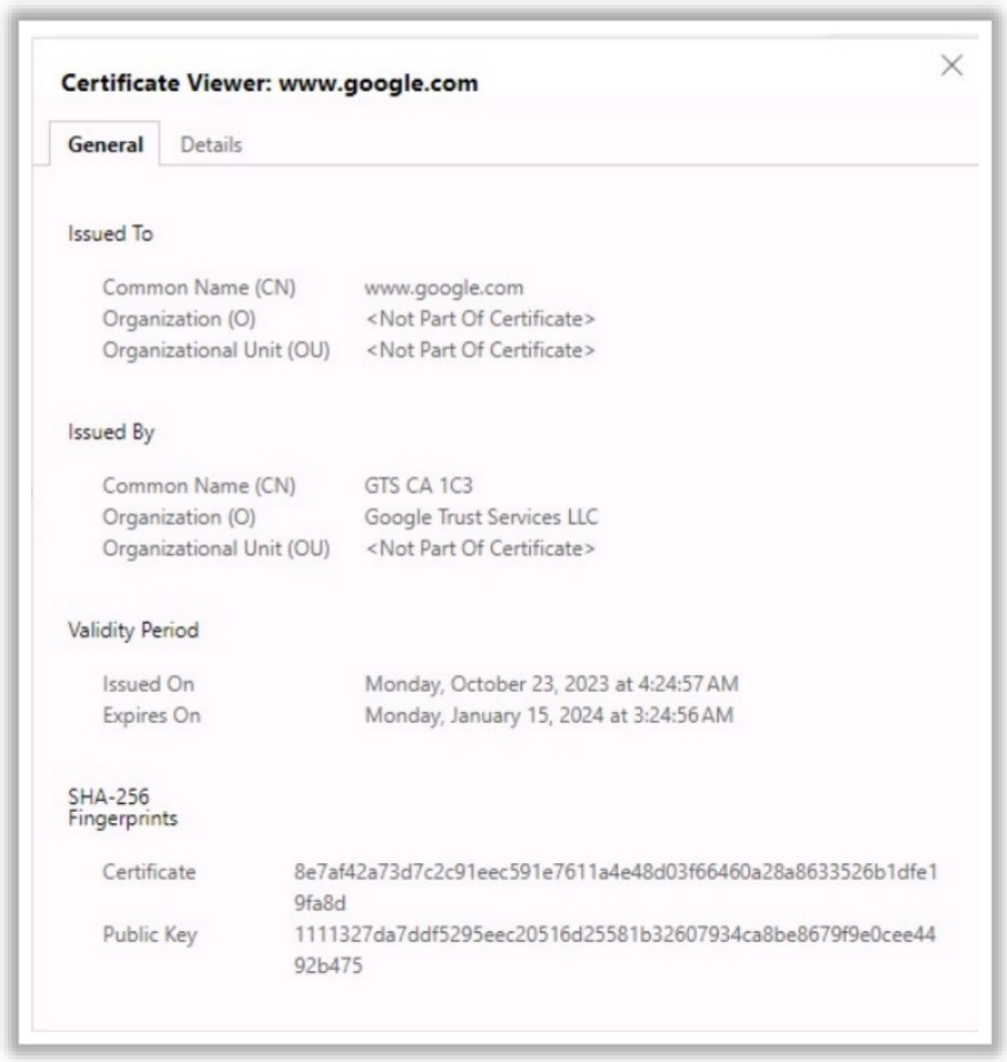
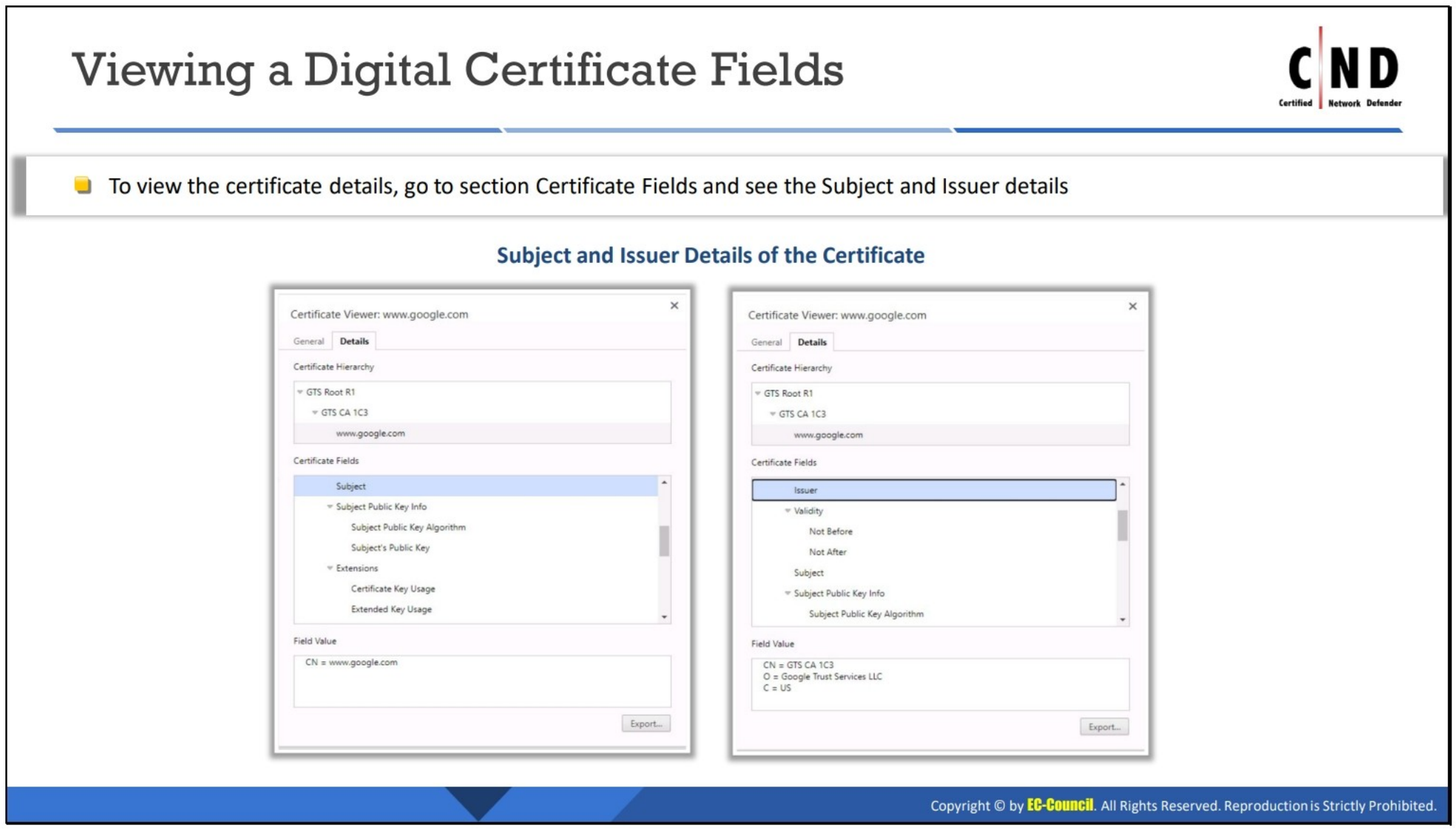


Figure 10.63: Viewing Certificate

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Viewing a Digital Certificate Fields

- Browse to the website and click on the lock icon, then navigate and click on **Connectioin is secure/Certificate is valid**.

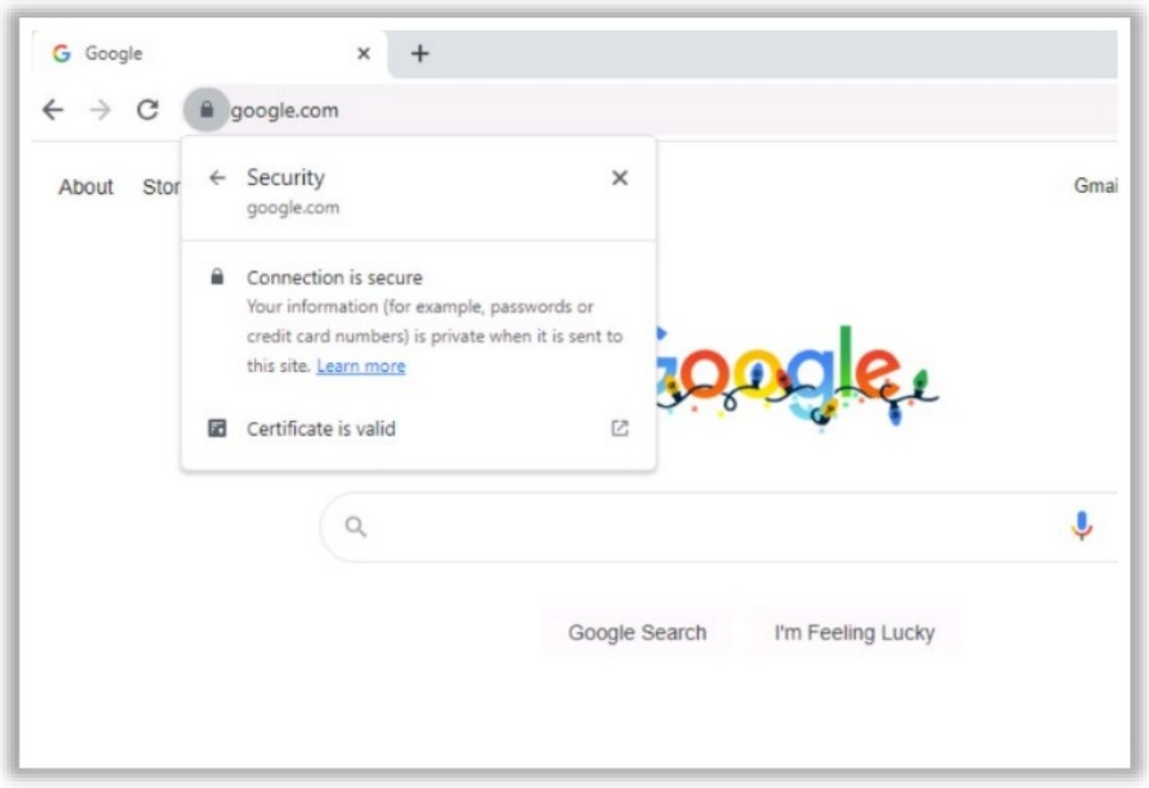


Figure 10.64: Selecting the Certificate is valid Option

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- A new window consisting of **General** and **Details** tabs will open.



Figure 10.65: Certificate Viewer Window

- Click the **Details** tab, and Under **Certificate fields** the **Subject** and **Issuer** of a digital certificate.

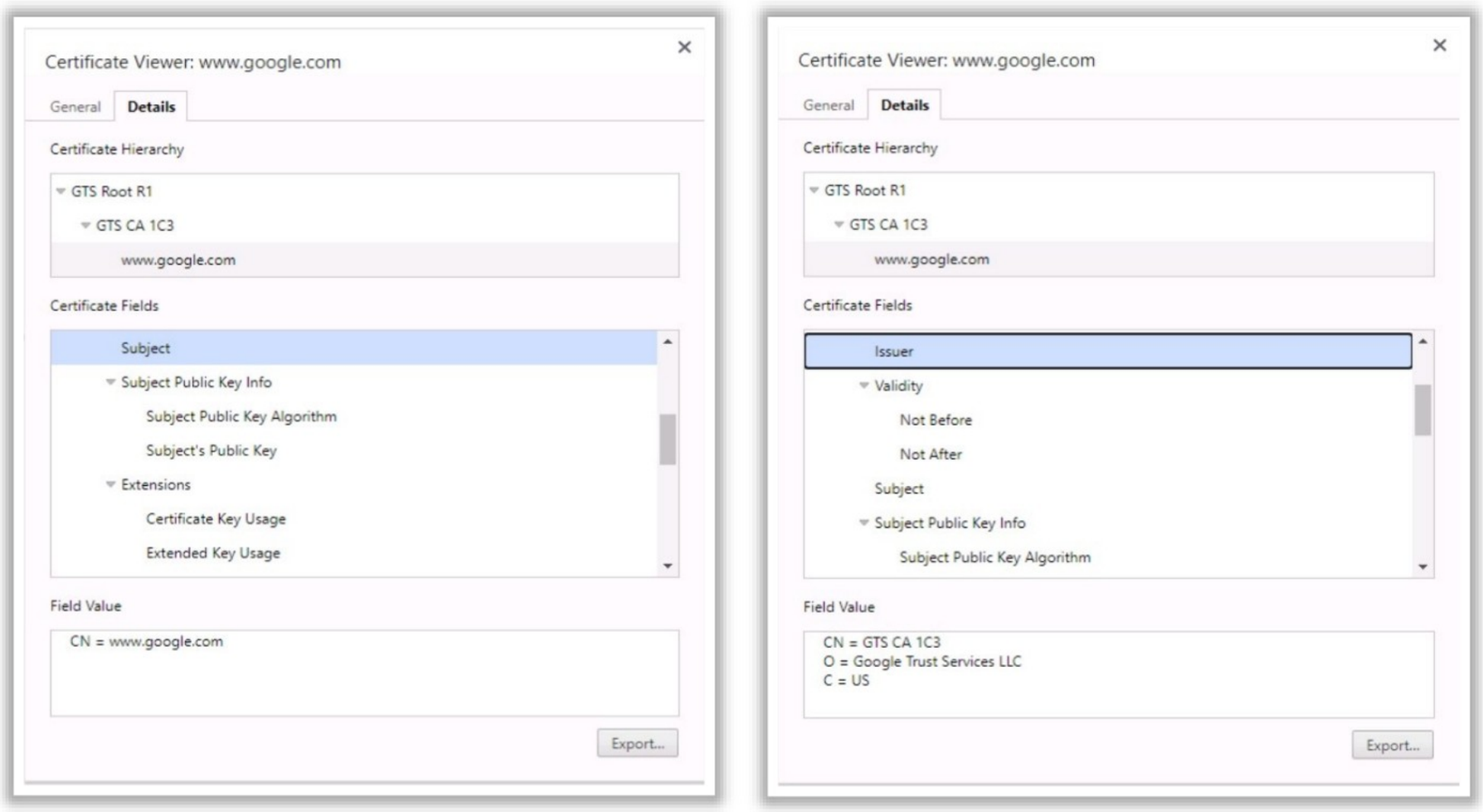
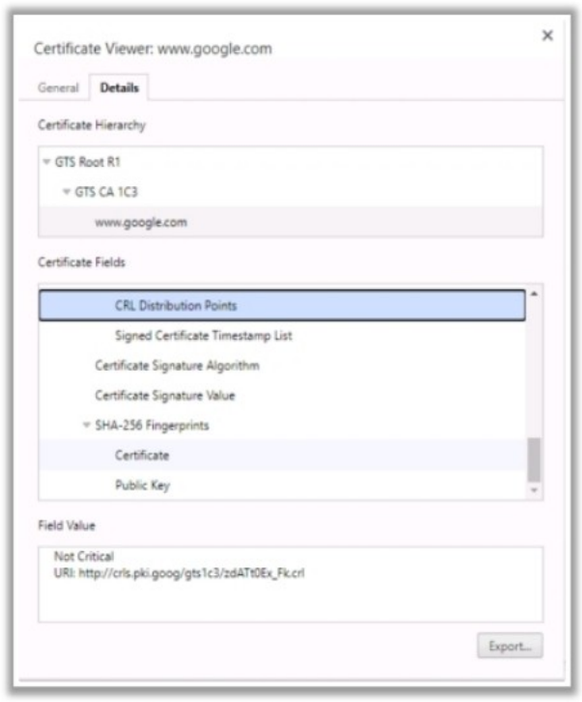


Figure 10.66: Selecting Certificate Fields

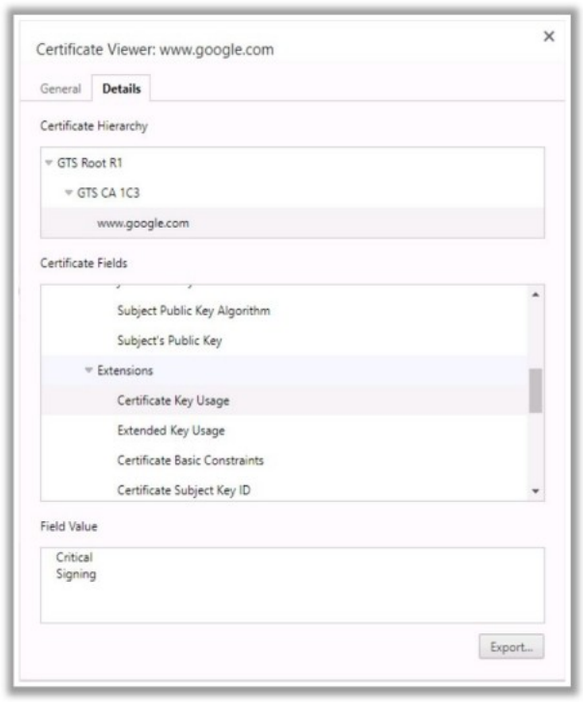
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Viewing a Digital Certificate: Extensions

- To view **Extension**, select **Extensions** in the Certificate Fields section



CRL Distribution Point and AIA Location



CRL Information

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Viewing a Digital Certificate: Extensions

- Browse to the website and click on the lock icon, then navigate and click on **Connectioin is secure/Certificate is valid**.

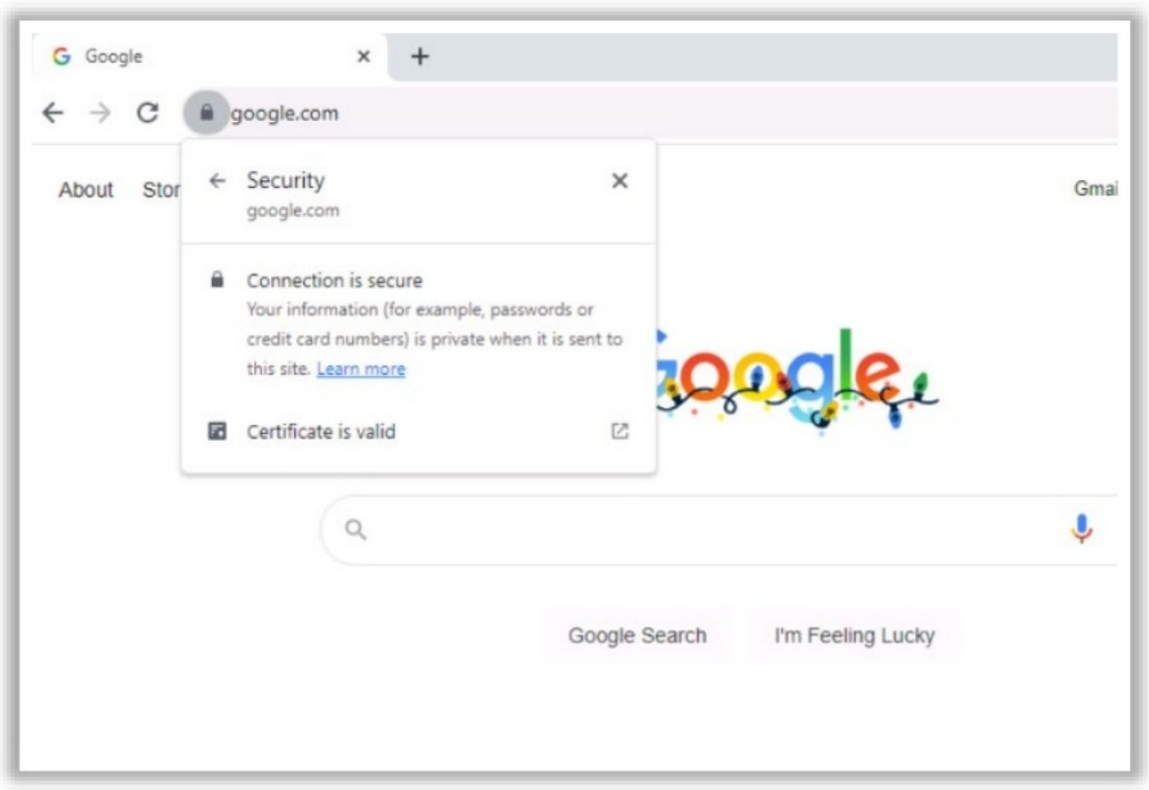


Figure 10.67: Selecting the Certificate is valid Option

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- A new window consisting of **General** and **Details** tabs will open.



Figure 10.68: Certificate Viewer Window

- Click the **Details** tab, and from the **Show** drop-down list, Select **Extensions Only**.

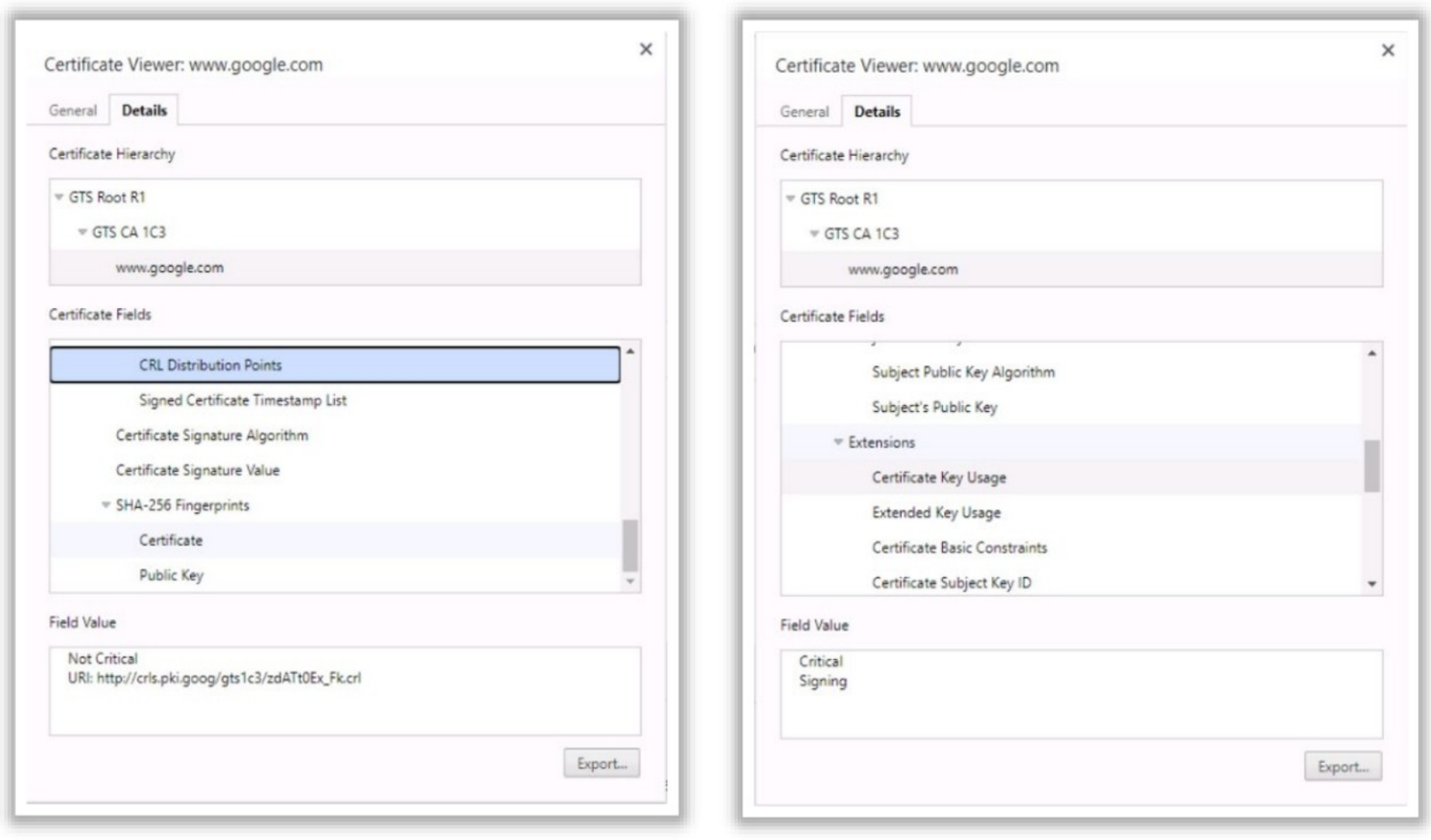
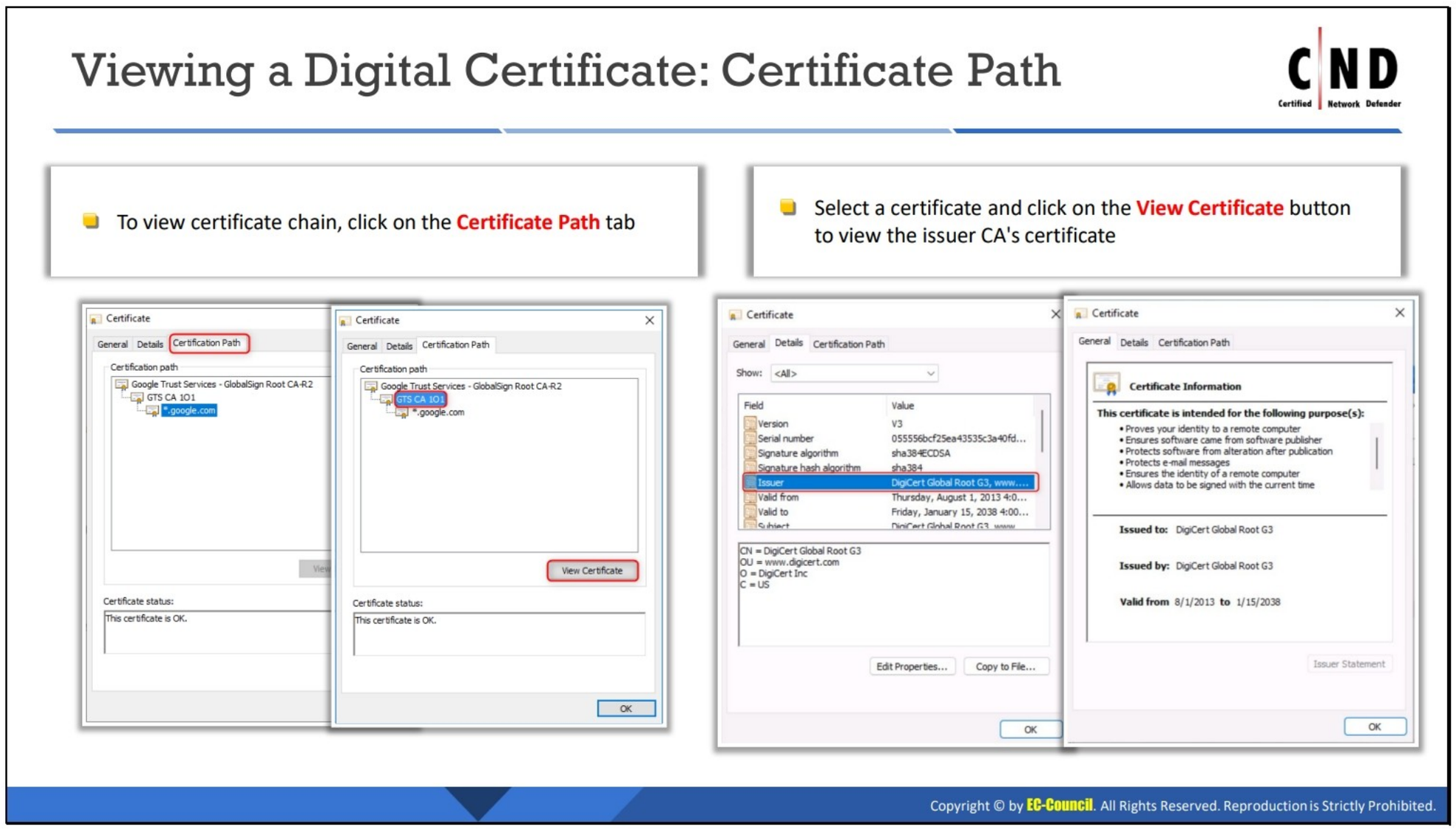


Figure 10.69: Selecting Extensions Option

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Viewing a Digital Certificate: Certificate Path

- Browse to the website and click on the lock icon, then navigate and click on **Connectioin is secure/Certificate is valid**.

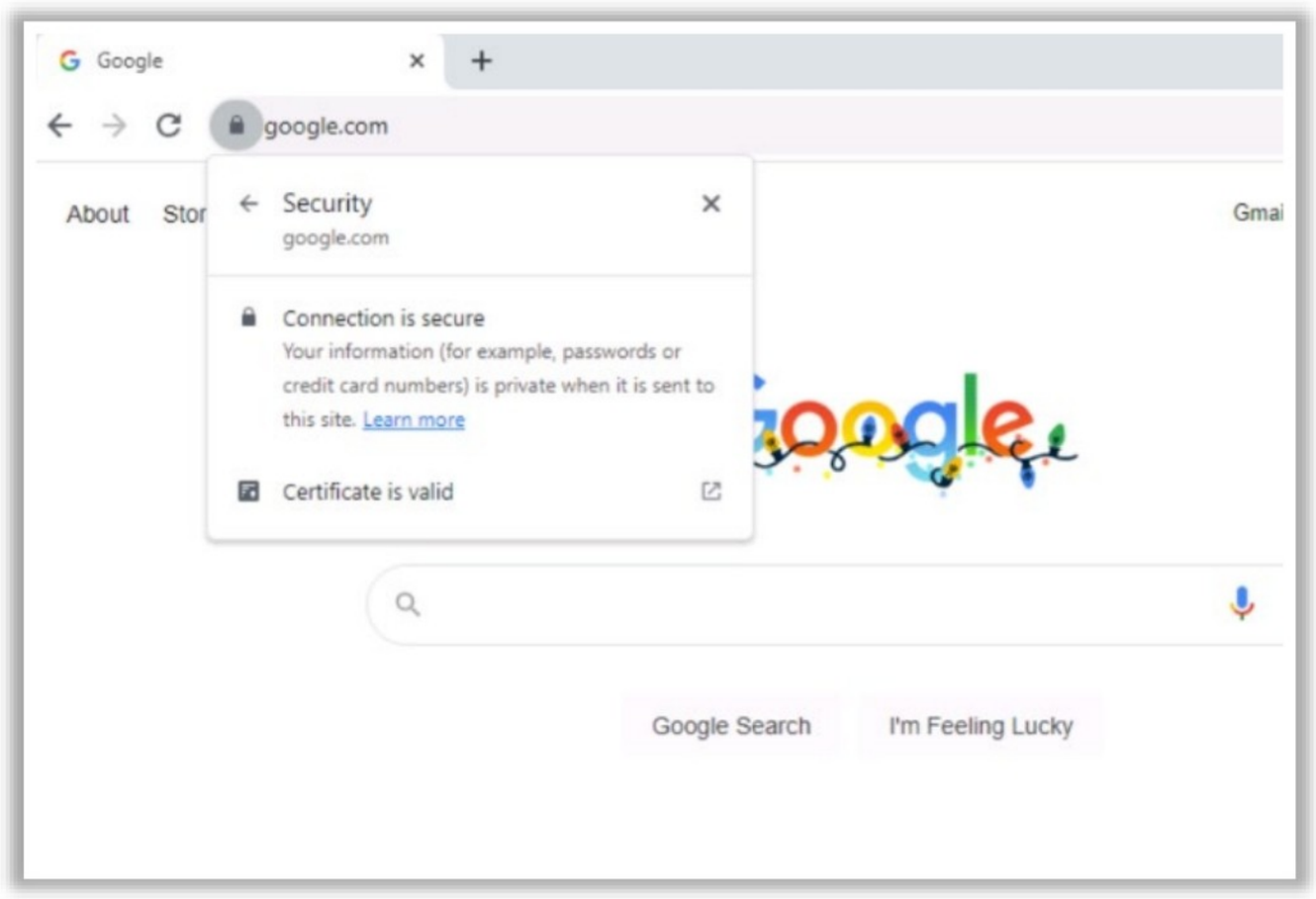


Figure 10.70: Selecting the Certificate is valid Option

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- A new window consisting of **General**, **Details**, **Certification Path** tabs will open.

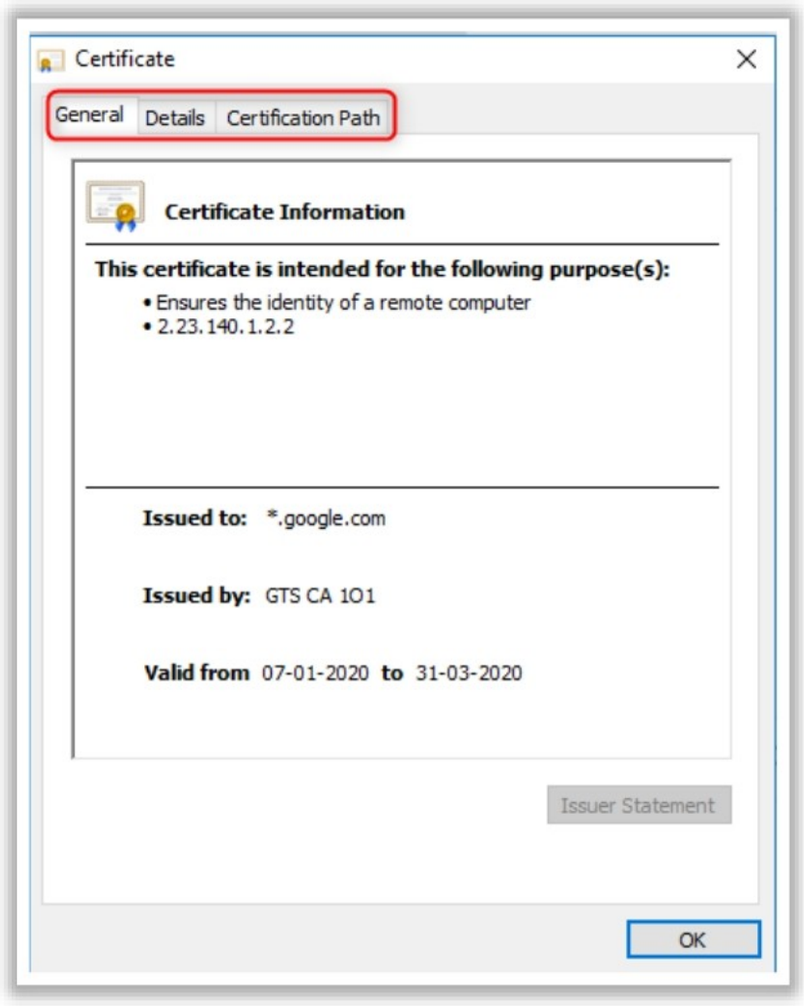


Figure 10.71: Certificate Window

- Click the **Certification Path** tab. The certificate chain is visible.

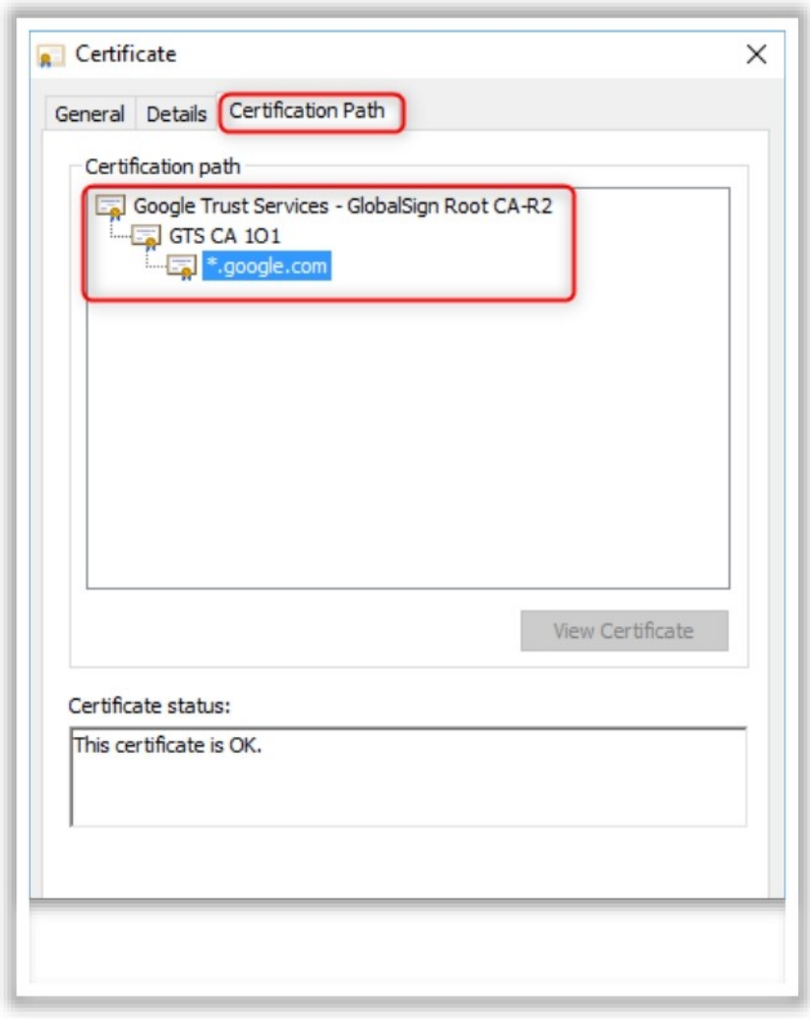


Figure 10.72: Checking Certificate Path

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Select the certificate and click on **View Certificate** to view the issuer CA's certificate**.**

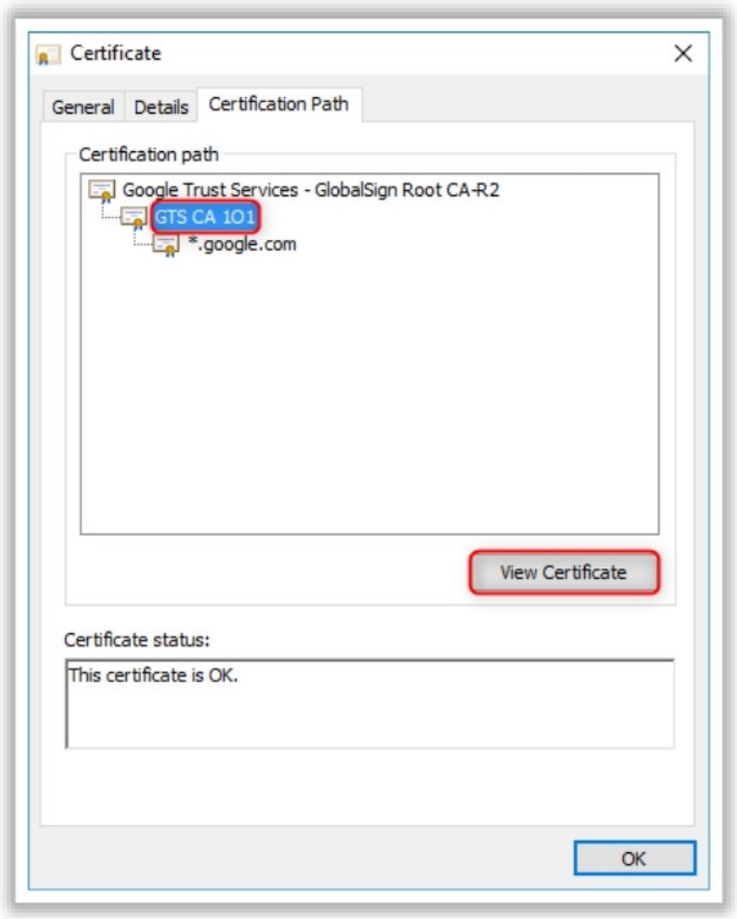


Figure 10.73: Viewing the issuer CA's certificate

- A new window consisting of **General, Details, and Certification Path** tabs will open. In the **General** tab, the certificate information will be available. In the **Details** tab, issuer information is available. In the Certification Path, the certificate chain is visible.

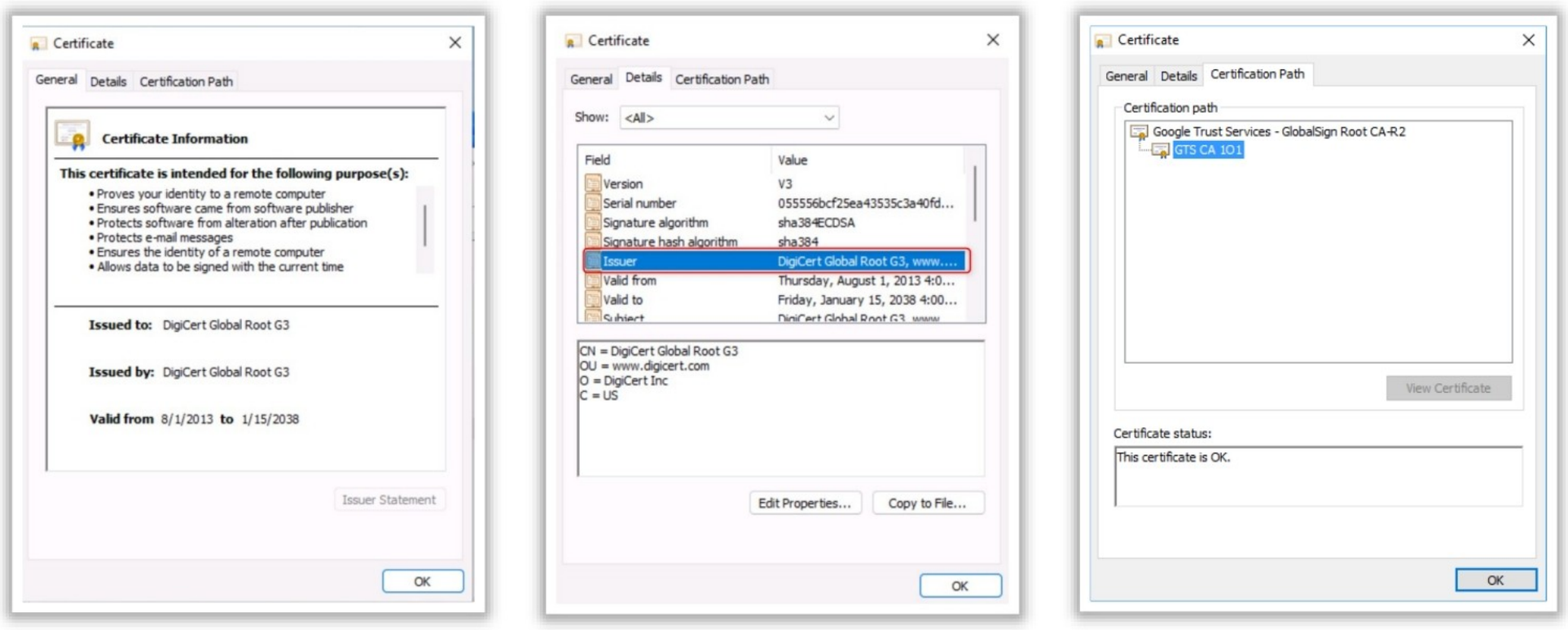
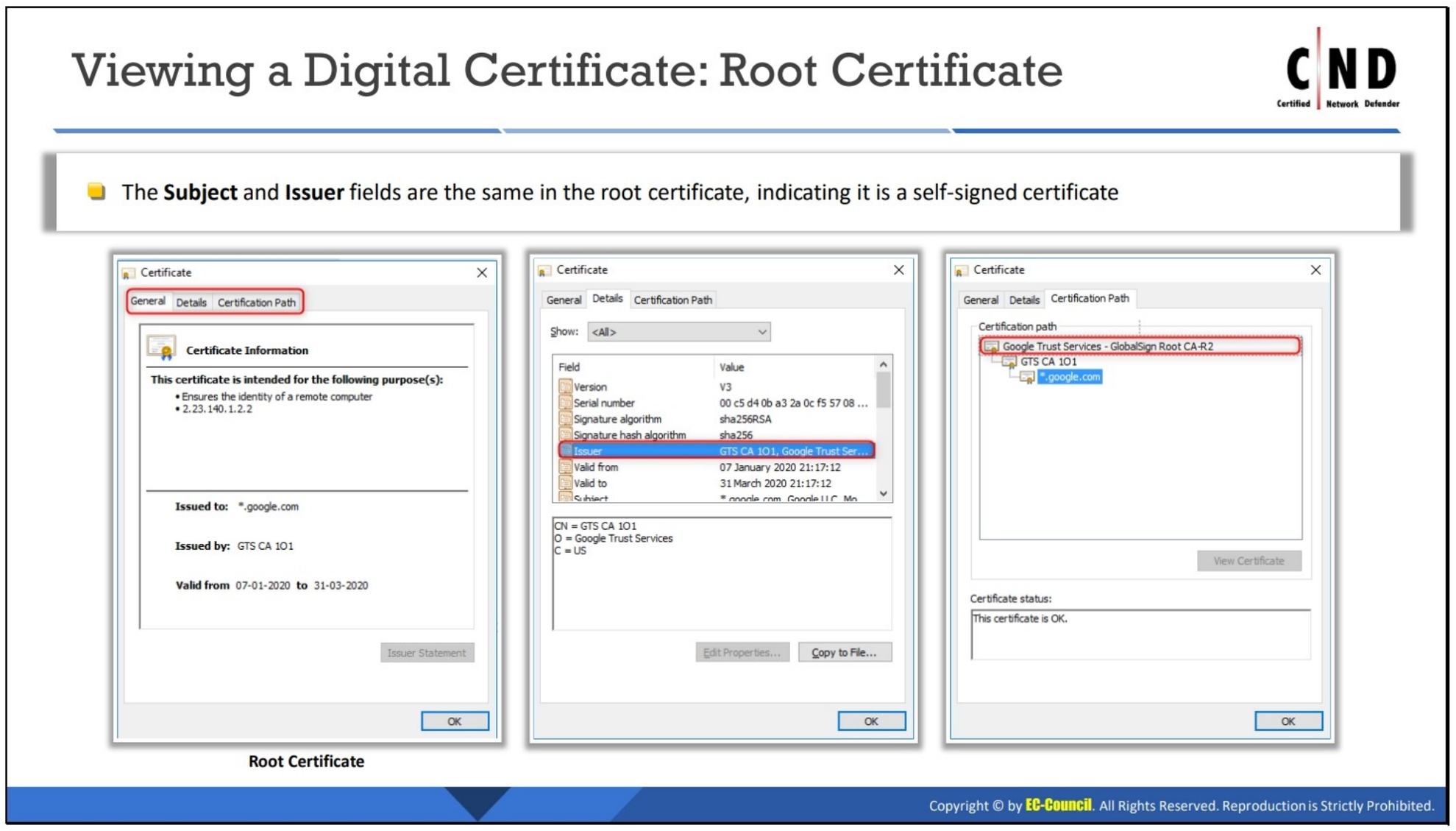


Figure 10.74: New window consisting of General, Details, and Certification Path tabs

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Viewing a Digital Certificate: Root Certificate

- Browse to the website and click on the lock icon, then navigate and click on **Connectioin is secure/Certificate is valid**.

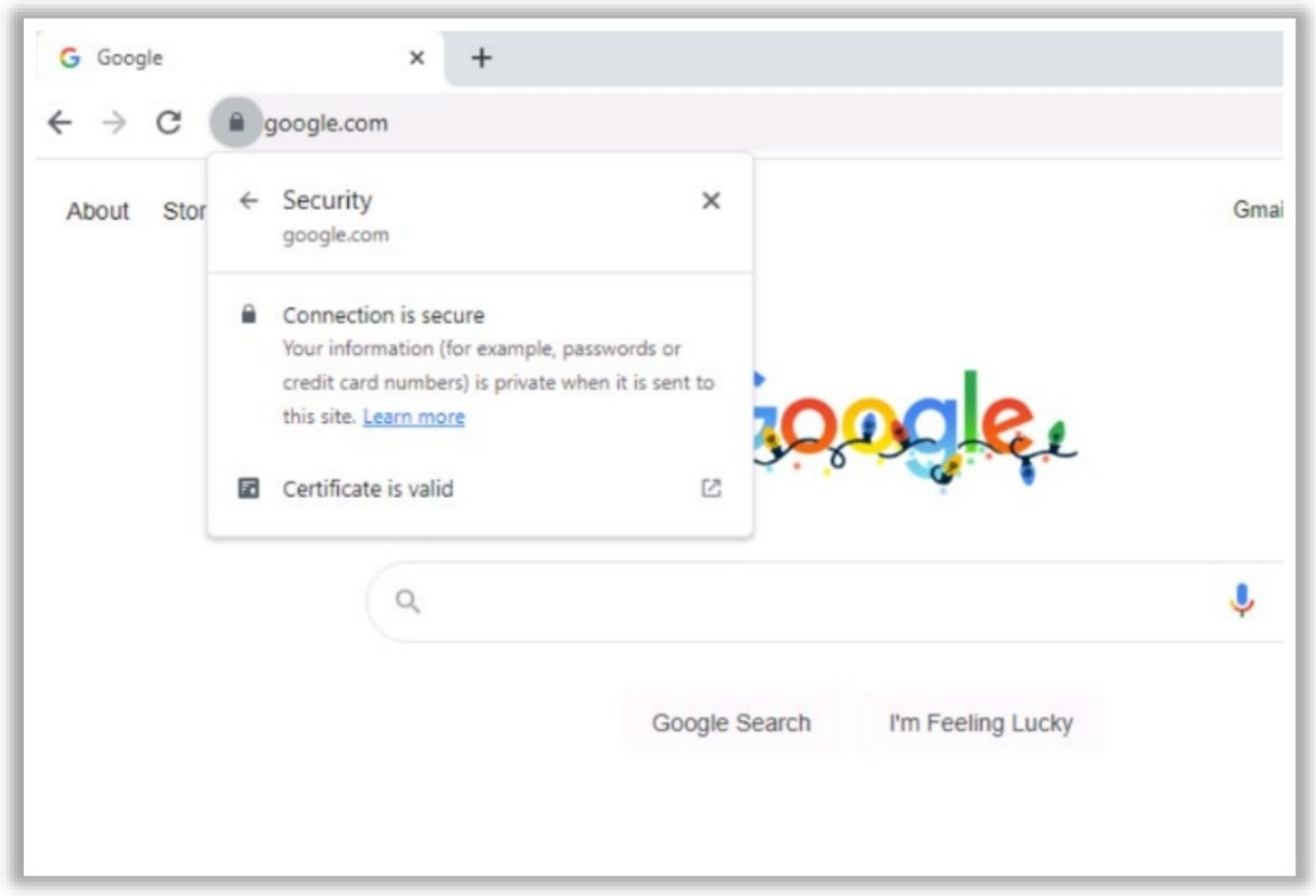


Figure 10.75: Selecting the Certificate is valid Option

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- A new window consisting of **General**, **Details**, **Certification Path** tabs will open.

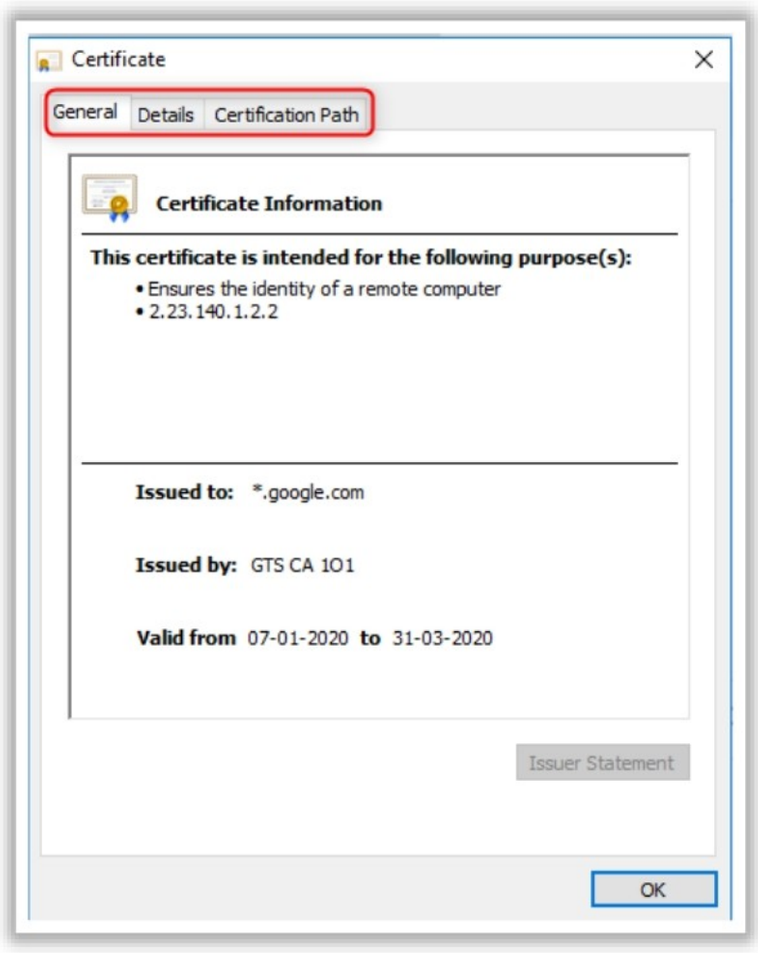


Figure 10.76: Certificate Window

- Click the **Details** tab. Fields such as **Issued to**, **Subject**, **Issuer**, or **Issued by** are the same for the root certificate, and it is certified as self-signed.

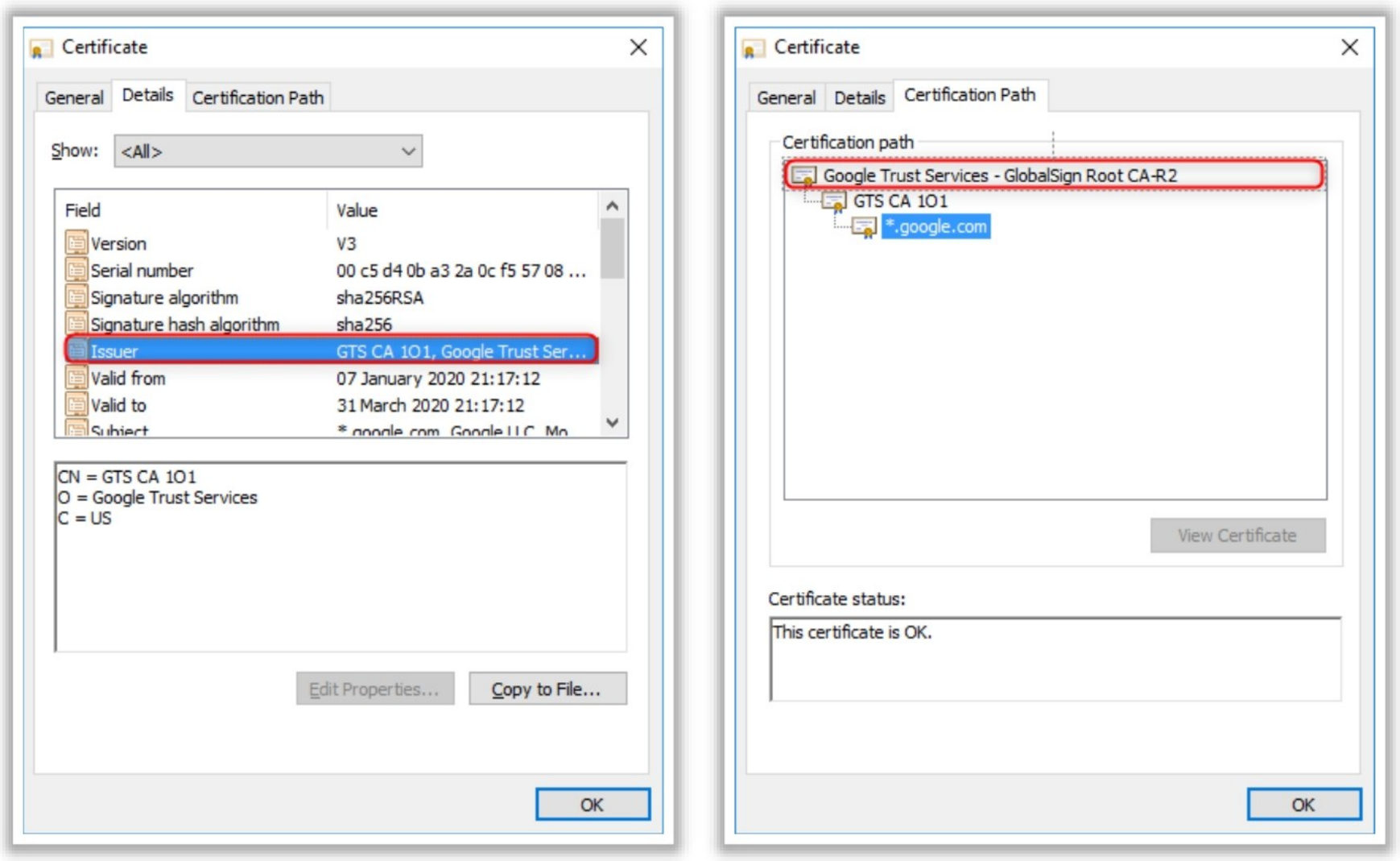
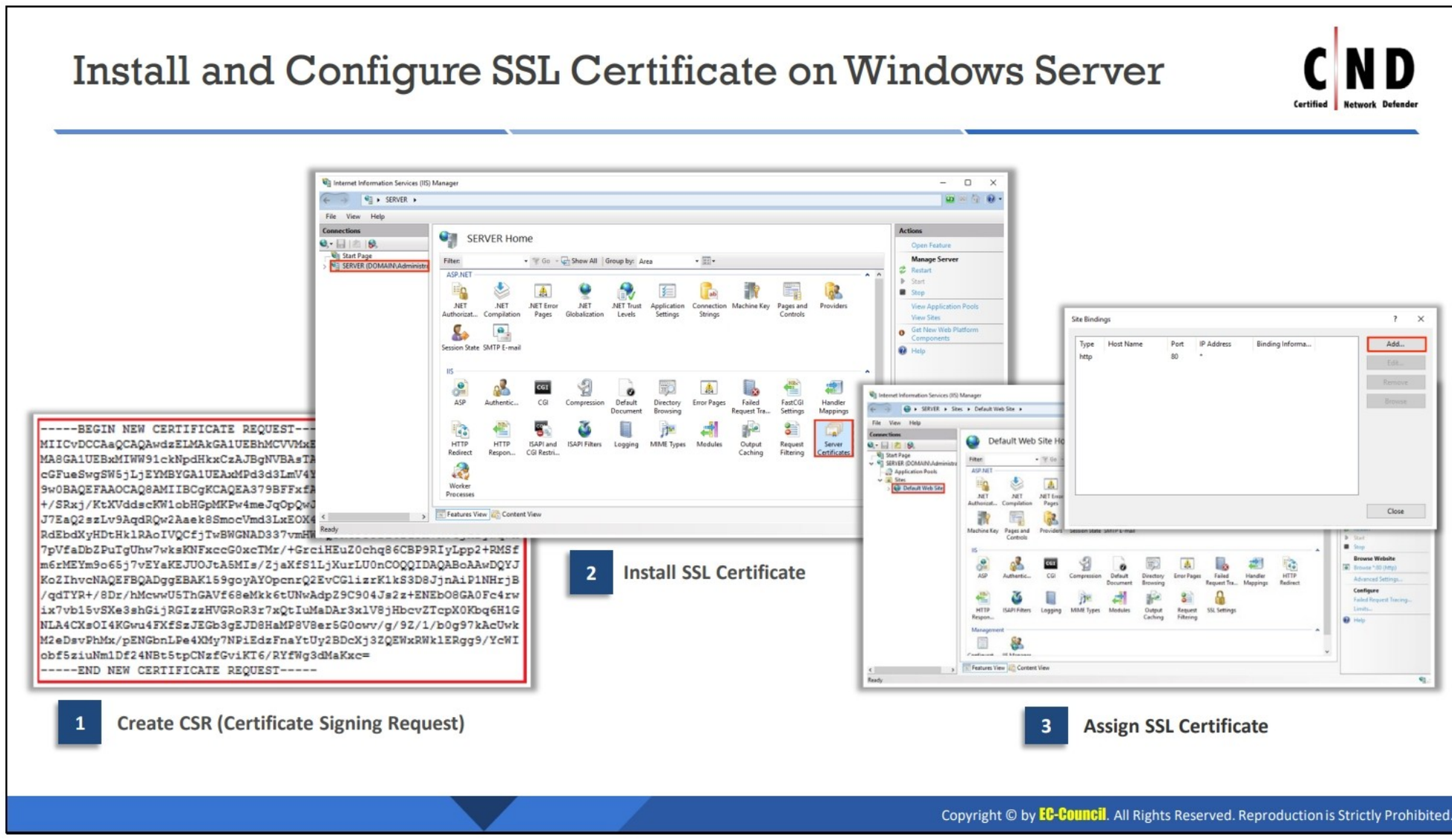


Figure 10.77: Checking the Fields of Details Tab

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Install and Configure SSL Certificate on Windows Server

Step 1: Create a Certificate Signing Request (CSR)

- From windows start menu, type **Internet Information Services (IIS) Manager** and open it.
- In the IIS Manager window's Connections menu, navigate to and select the server name.

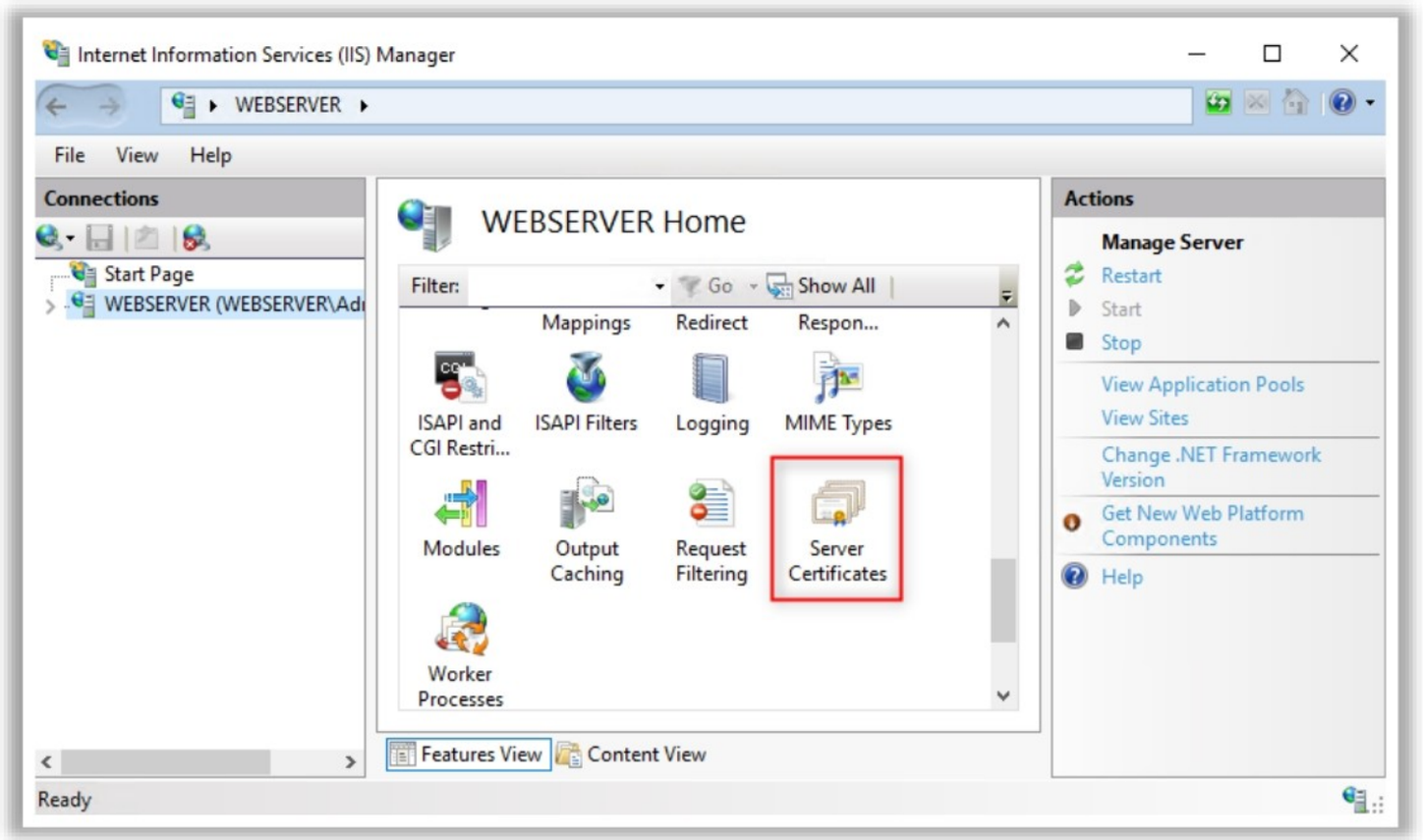


Figure 10.78: Selecting the Name of the Server

- On the server home page's IIS section, double-click on **Server Certificates**.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- On the **Server Certificates** page's **Actions** menu, **click on the Create Certificate Request** link.

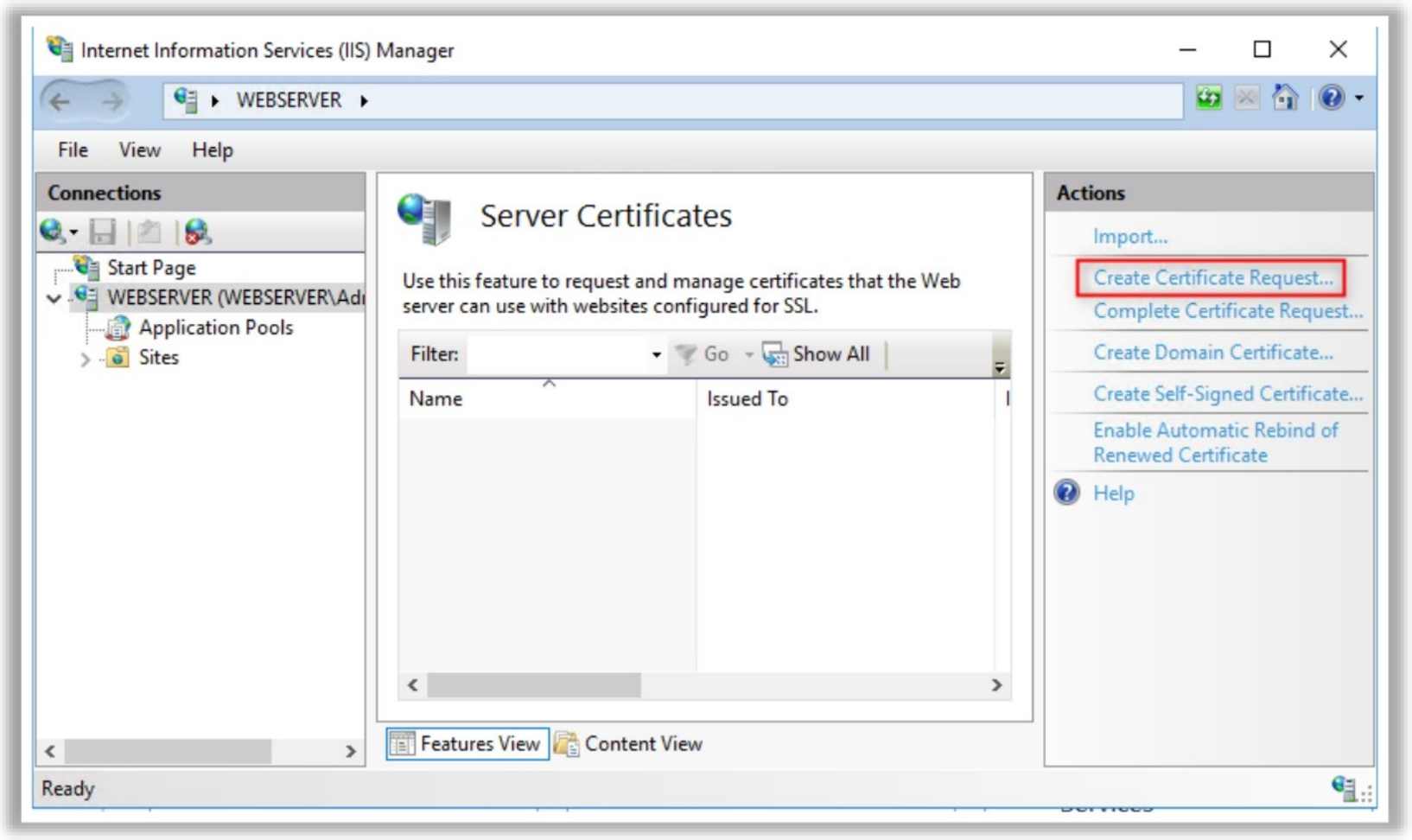


Figure 10.79: Clicking on Create Certificate Request

- In the request certificate's **Distinguished Name Properties** page, fill the following details.
  - **Common name**: Type the domain name
  - **Organization**: Enter the company's legally registered name.
  - **Organization unit**: Type the department name.
  - **City/locality**: Type the name of the city where the company is legally located.
  - **State/Province**: Type the name of the state/province where the company is legally located.
  - **Country**: Select the name of the country where the company is legally located.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Click **Next** after entering the details.

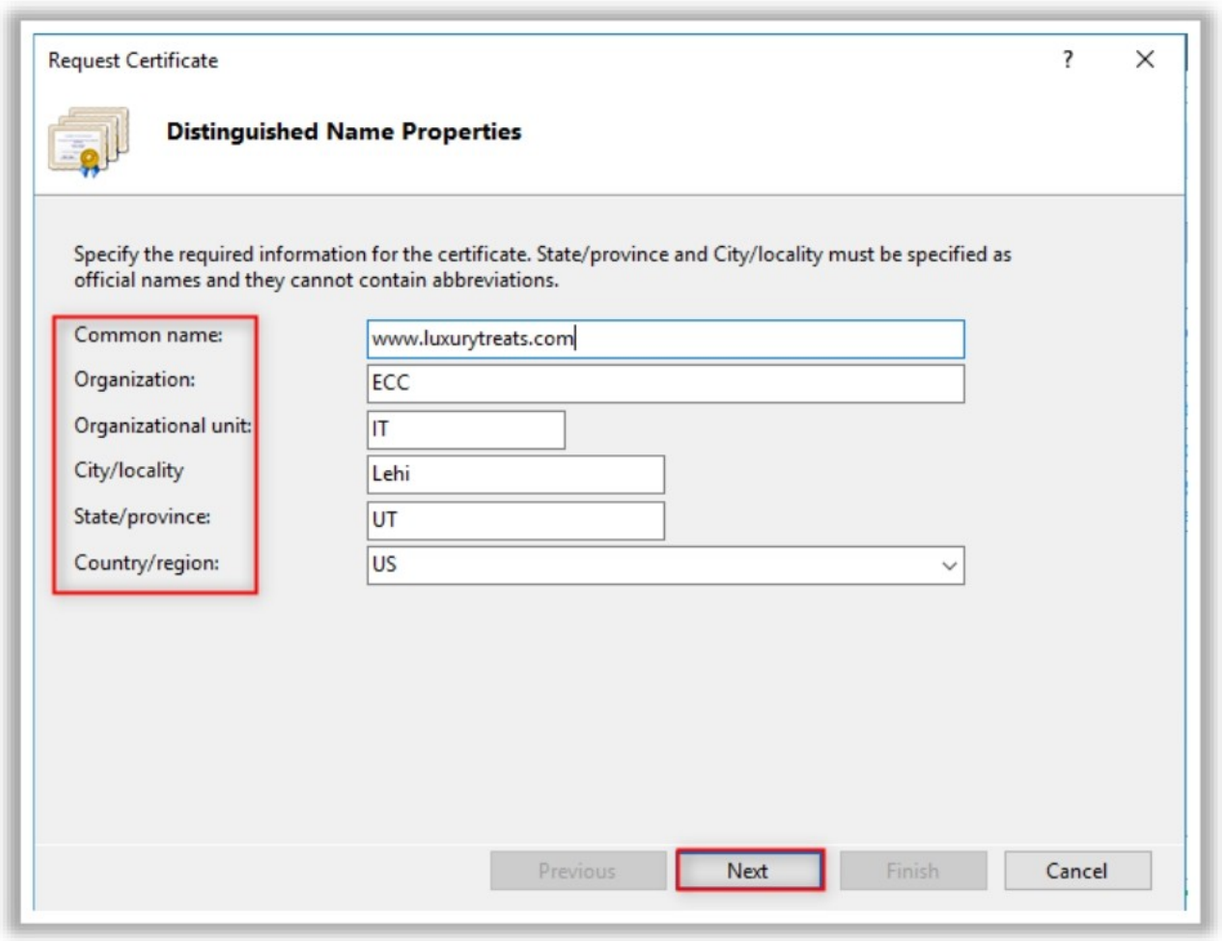


Figure 10.80: Filling Distinguished Name Properties Page

- On the **Cryptographic Service Provider Properties** page, enter the following details.
- **Cryptographic service provider**: From the drop-down menu, select **Microsoft RSA SChannel Cryptographic Provider** if the user does not have a specific cryptographic provider.
- **Bit length**: From the drop-down menu, select 2048.
- Click **Next**.

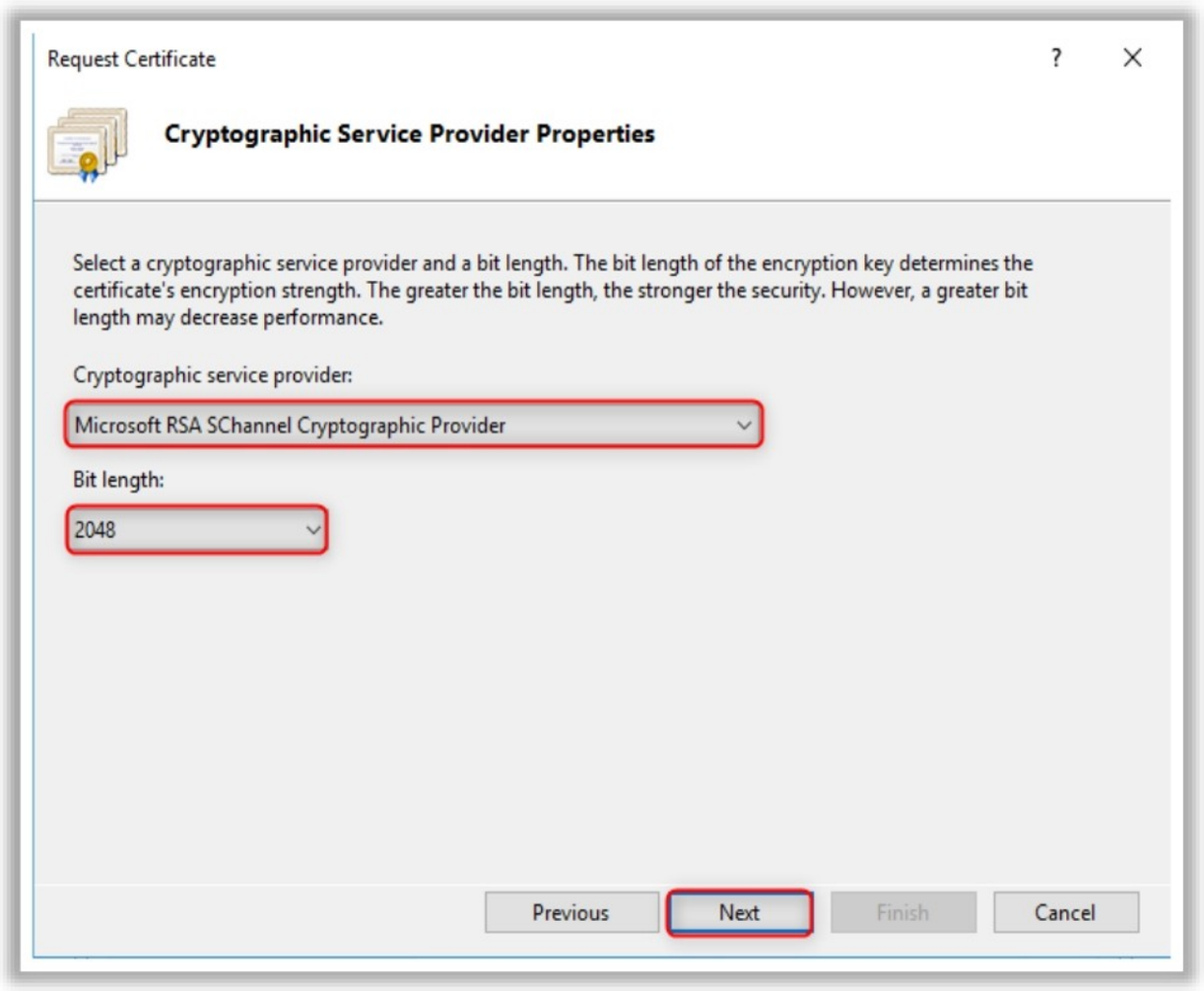


Figure 10.81: Filling Details on Cryptographic Service Provider Properties Page

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- On the **File Name** page, **Specify a file name for the certificate request**, browse to the location, and save the csr.txt file. Click **Finish**.

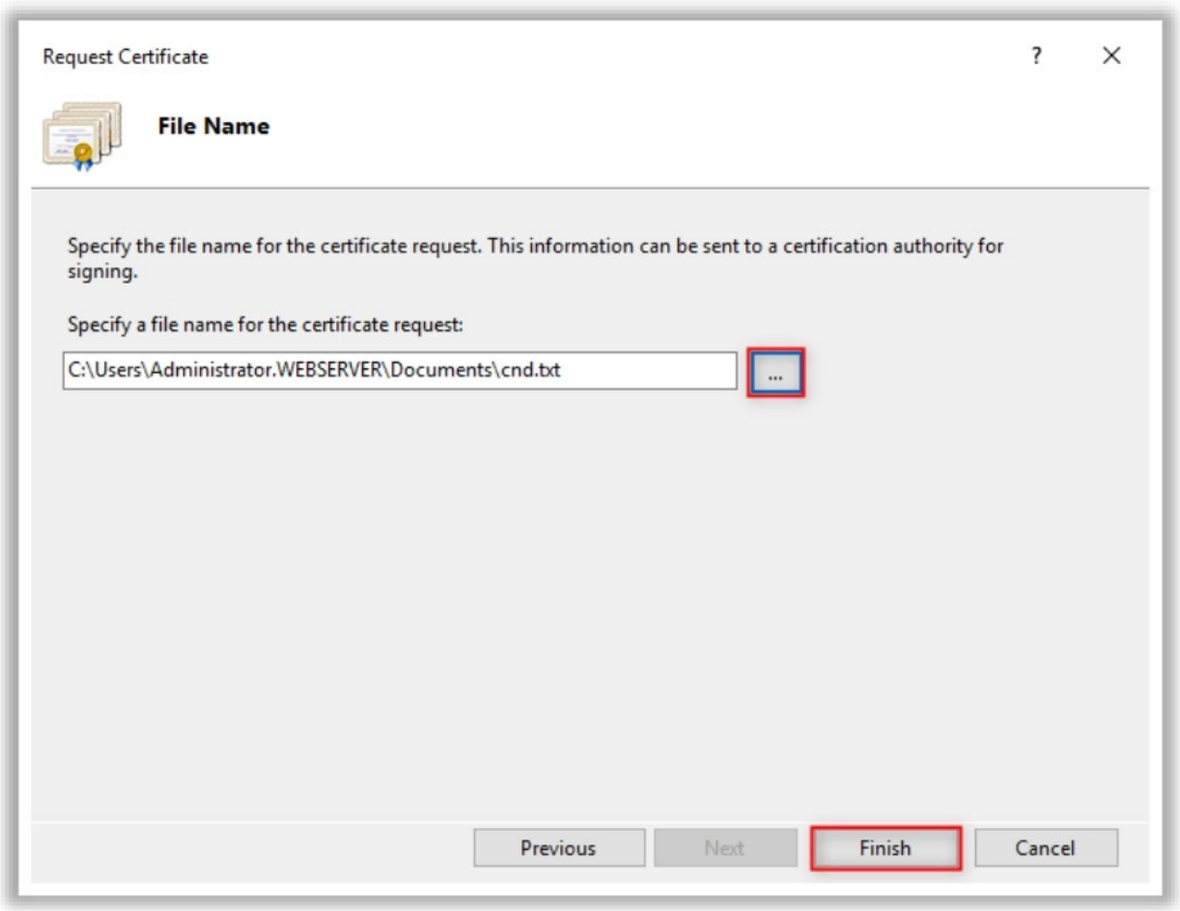


Figure 10.82: Specify a file name for the certificate request

- Open the csr.txt file in a text editor, copy the complete text including the tags, and paste it on the SSL certificate provider form.
- After receiving SSL certificate from the provider, install it.

Step 2. Install SSL Certificate

- Save the SSL certificate sent by the SSL certificate provider.
- From Windows start menu, type ***Internet Information Services (IIS) Manager*** and open it.
- In the new **IIS Manager** window's **Connections** menu, navigate to and click on the server name.

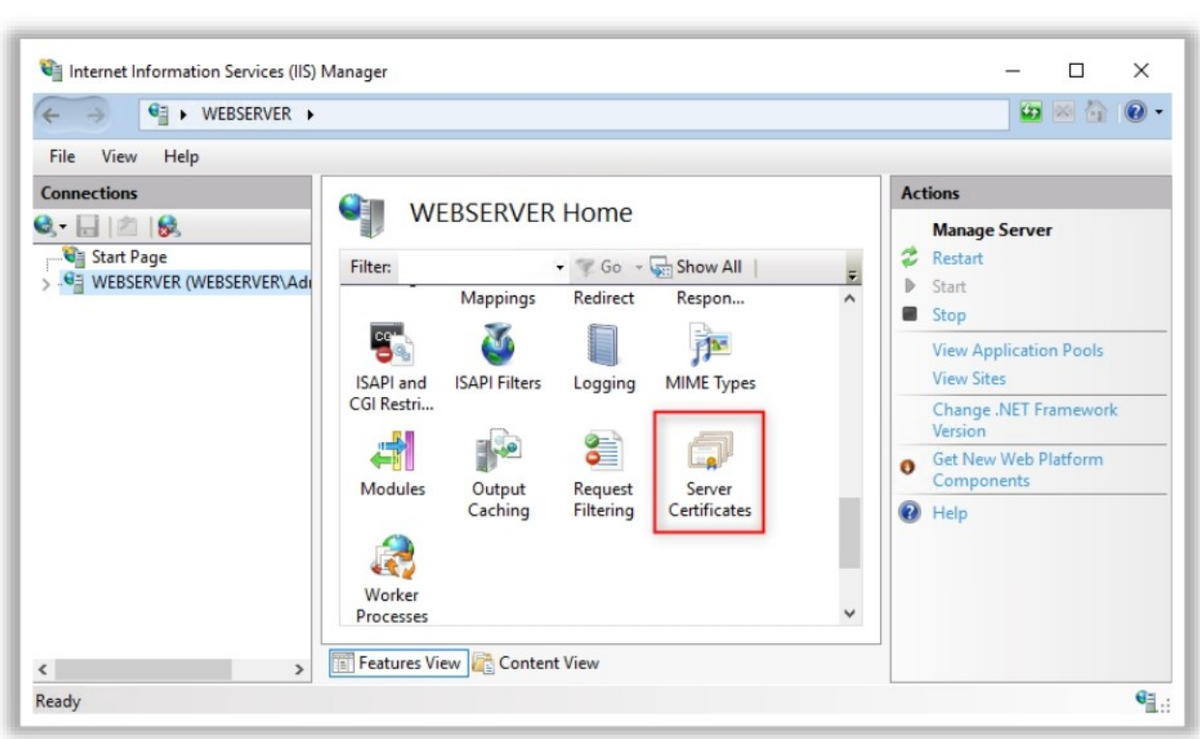


Figure 10.83: Selecting the Name of the Server

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- On the server's **Home** page (central pane) in **IIS** section, double-click **Server Certificates**.
- In the right pane's **Actions** menu, click **Complete Certificate Request** link.

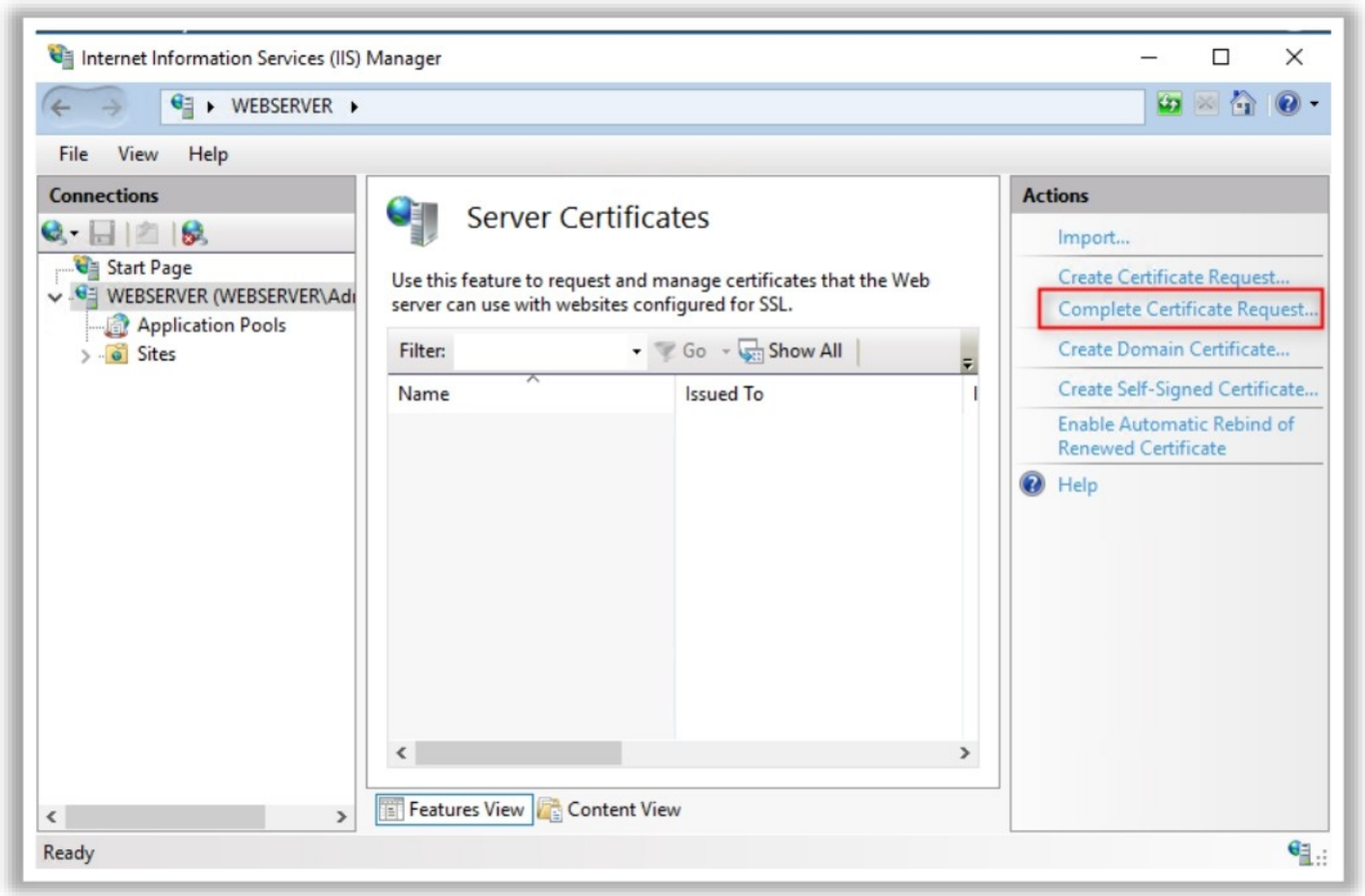


Figure 10.84: Clicking on Complete Certificate Request

- In the **Complete Certificate Request** window, fill the following details
  - **File name containing the certification authority's response**: Browse and select the saved SSL certificate sent by the SSL certificate provider.
  - **Friendly name**: Enter a friendly name for the certificate in order to identify it.
  - **Select a certificate store for the new certificate**: From the drop-down menu, Select **Web Hosting**.
- Click **OK**. Once the SSL certificate is successfully installed, assign tit to the appropriate website.

Step 3. Assign SSL Certificate

- From **IIS Manager's Connection** menu, select the name of the server on which the SSL certificate was installed, then select the site on which the user wants to use the SSL certificate.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- On the home page of the website, click the **Bindings** link under **Edit site** section of the **Actions** menu.

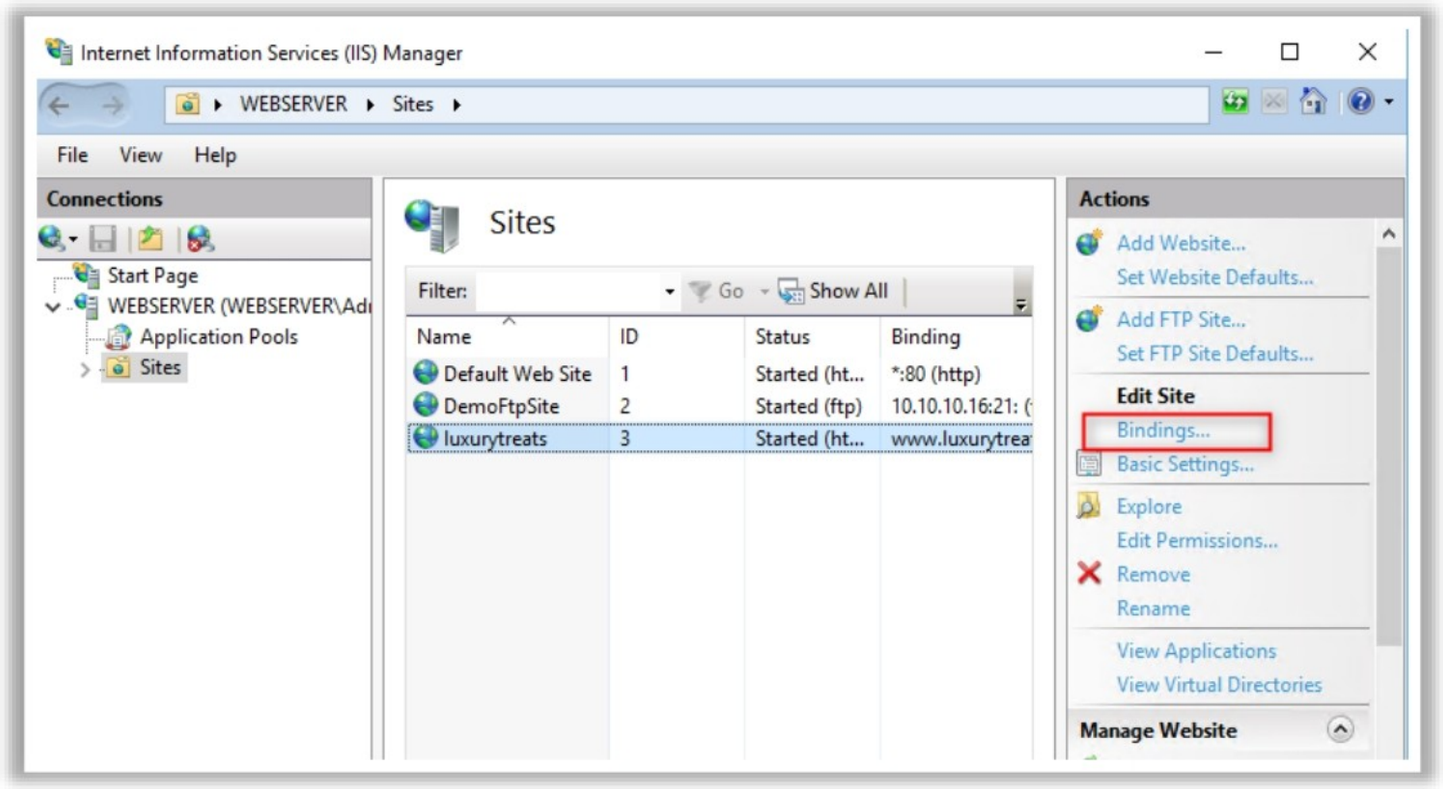


Figure 10.85: Bindings link

- In the new **Binding Site** window, click **Add.**

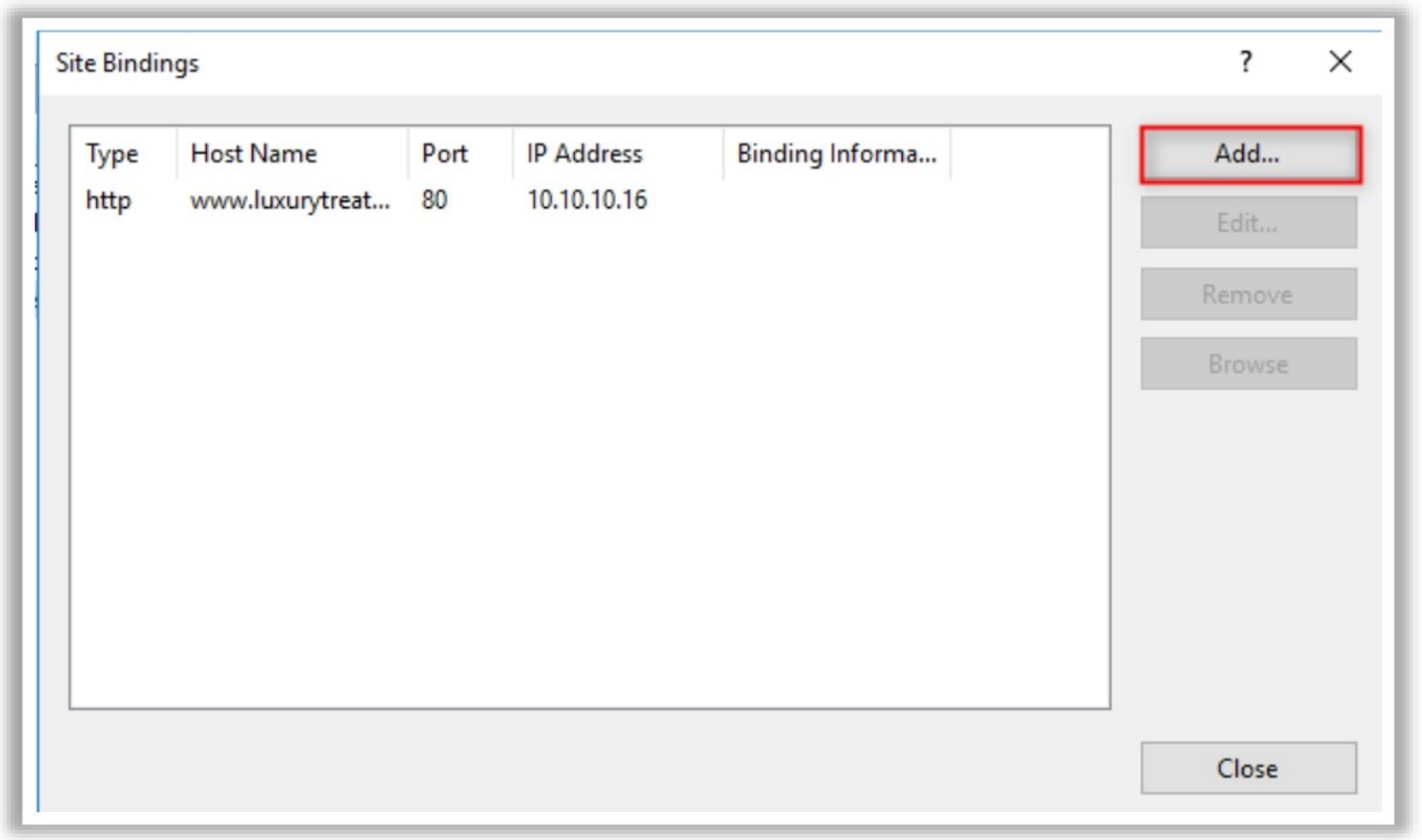


Figure 10.86: Clicking on Add Button

- Enter the following details
  - **Type**: Select **https** from the drop-down menu.
  - **IP Address**: From the drop-down menu, select IP address of the site/ All Unassigned.
  - **Port**: Type 443.
  - **SSL Certificate**: Select the new SSL certificate.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Click **OK.**

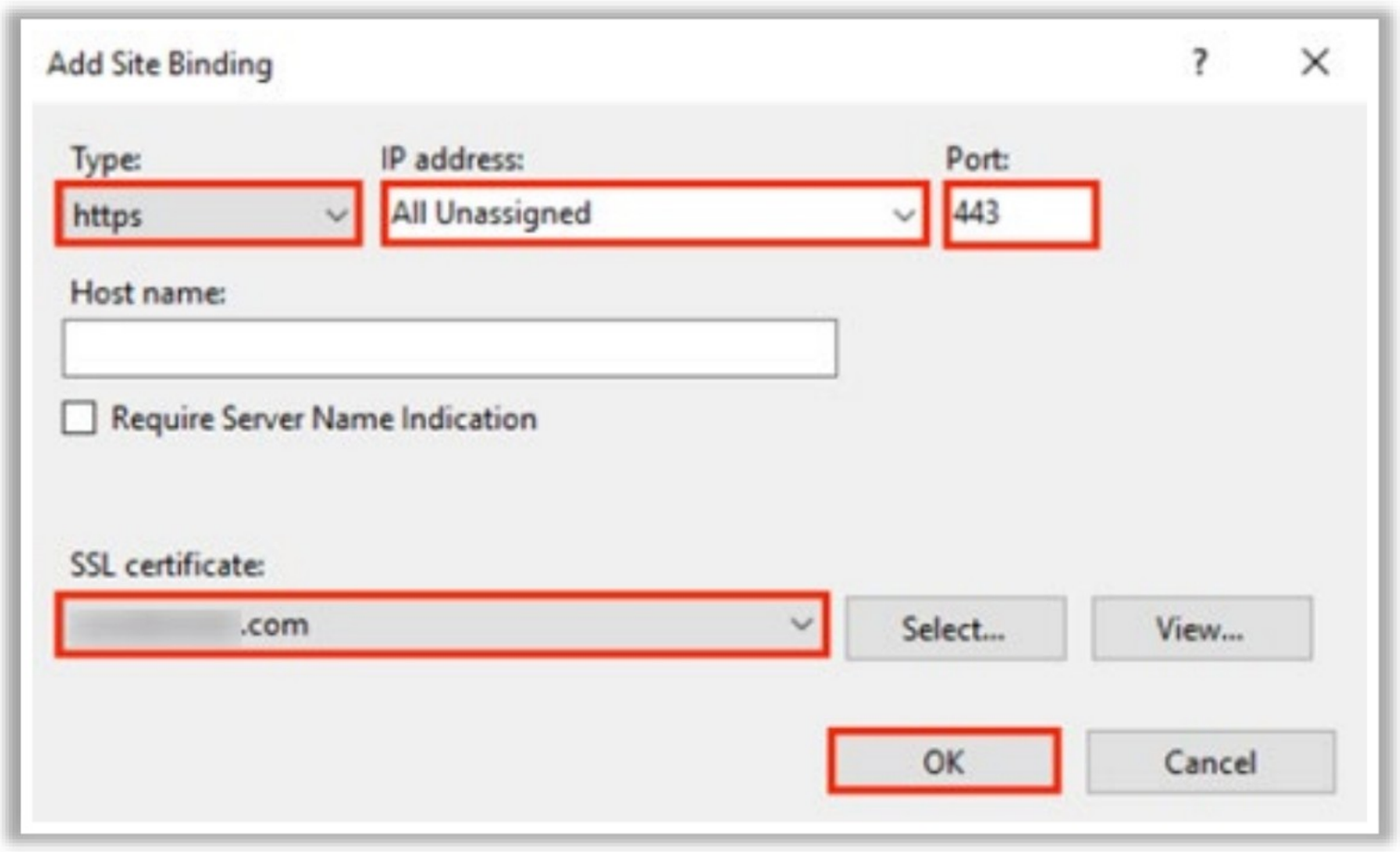


Figure 10.87: Filling Details in Add Site Binding Page

- The SSL certificate is installed, and the website is configured to accept a secure connection.

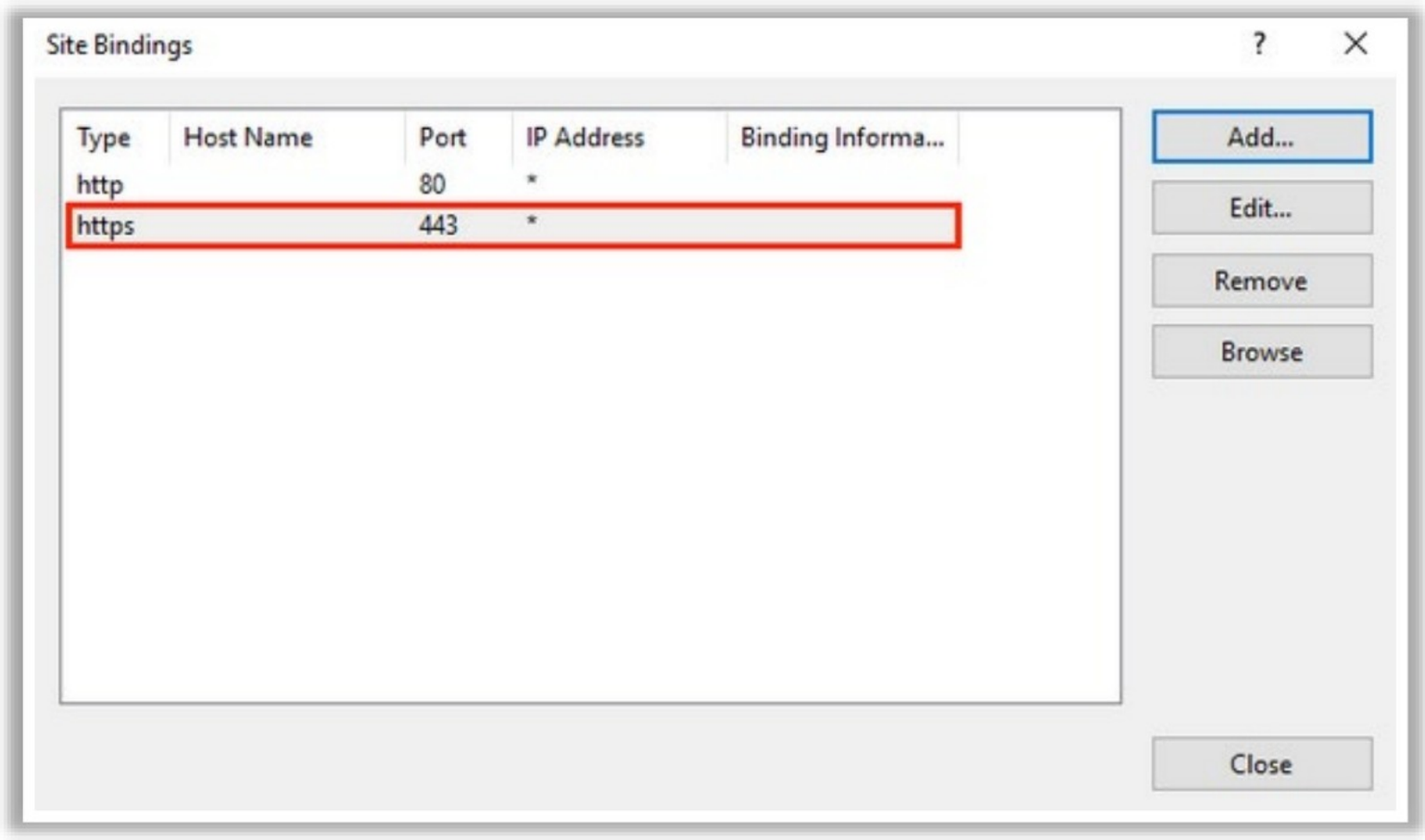
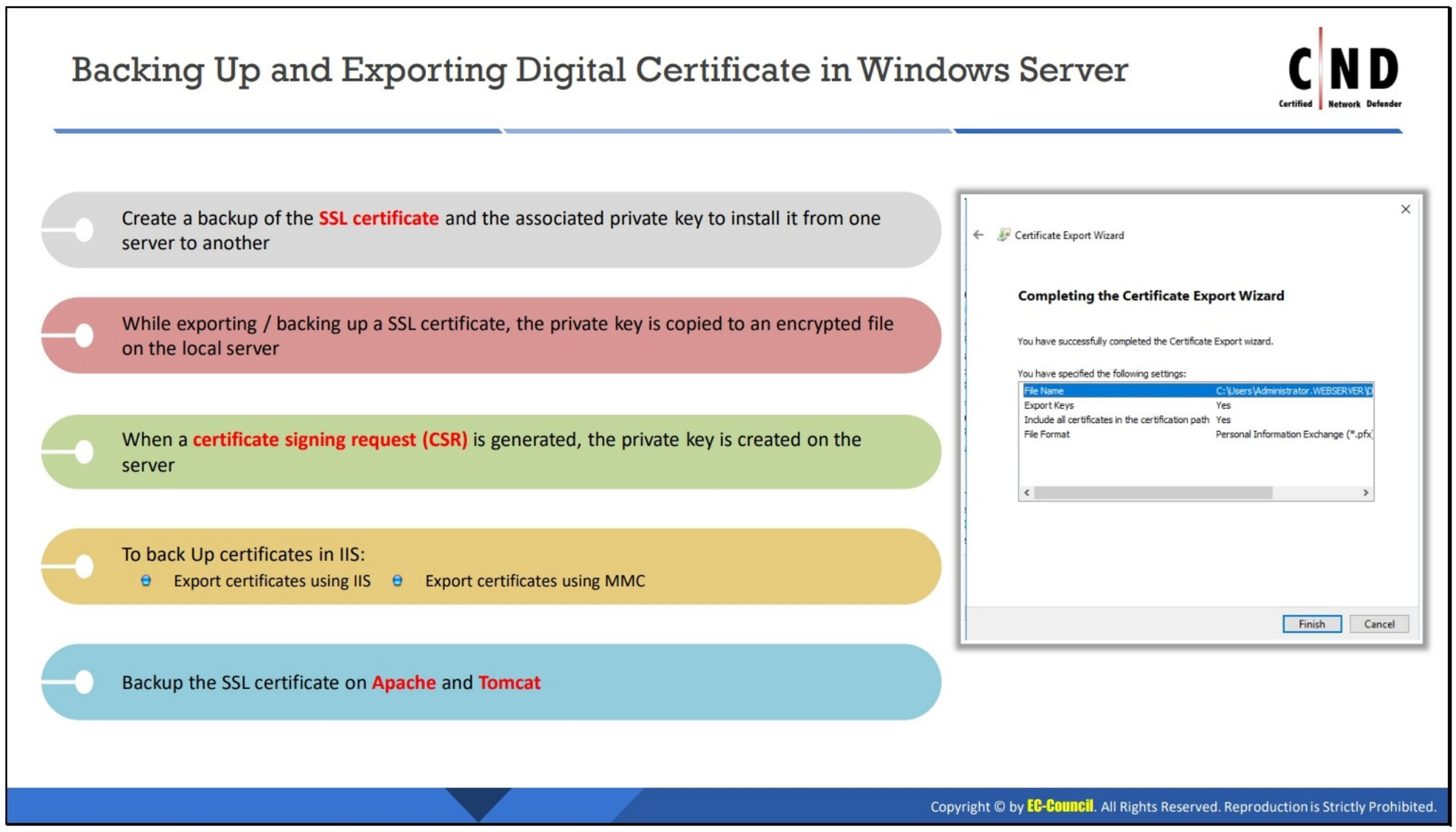


Figure 10.88: Installation of SSL Certificate and Configuration of Website to Establish Secure Connection

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Backing Up and Exporting Digital Certificate in Windows Server

Create a backup of the SSL certificate and the associated private key to install it from one server to another. While exporting/backing up an SSL certificate, the private key is copied to an encrypted file on the local server. When a CSR is generated, the private key is created on the server.

- Backup certificates in IIS.
  - Export certificates using IIS.
  - Export certificates using Microsoft Management Console (MMC).
- Backup SSL certificate on Apache.
- Backup SSL certificate on Tomcat.

Backup Certificates in IIS

The backup of SSL Certificate in ISS 7 can be done directly or using MMC.

Steps for Exporting SSL Certificates in IIS

- Open Internet Information Services Manager (IIS) 7.
- Select the **Server Name**.
- In the middle pane, click the **Server Certificates** icon.
- Select the certificate which the user wants to export.
- Provide the file name and password.
- The certificate and private key will be exported to a .pfx file.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Steps for Exporting SSL Certificate Using MMC

Step 1: Creating MMC snap-in for managing the certificates

- Press **Window+R**, and type **MMC.**

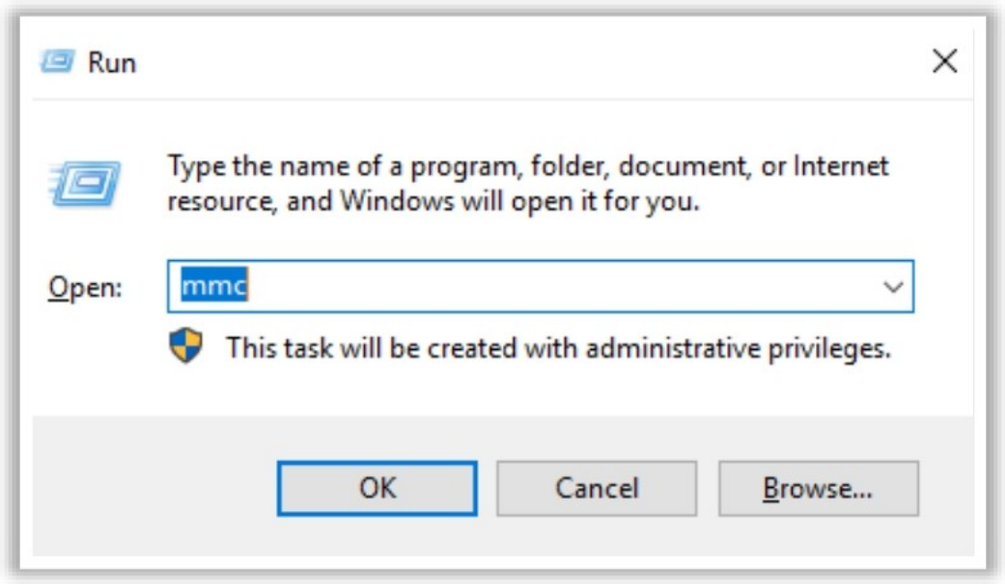


Figure 10.89: Opening MMC

- Click **File**, and navigate to **Add/Remove Snap-in.**

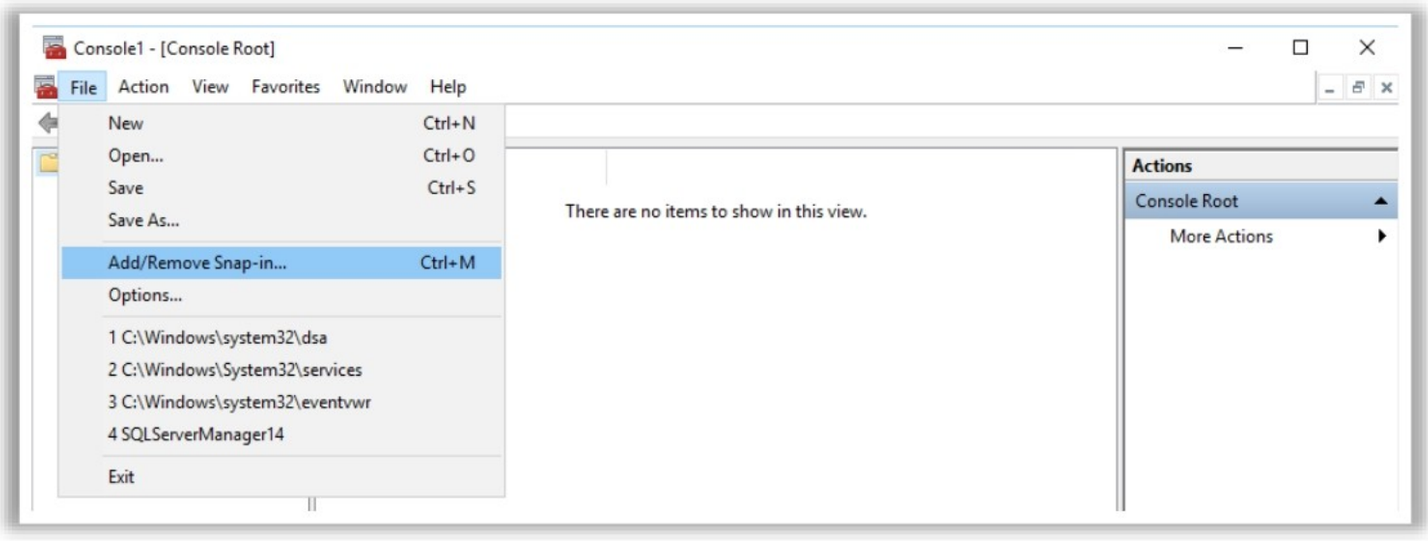


Figure 10.90: Opening Add/Remove Snap-in.

- Select **Certificate**, and click the **Add** button.

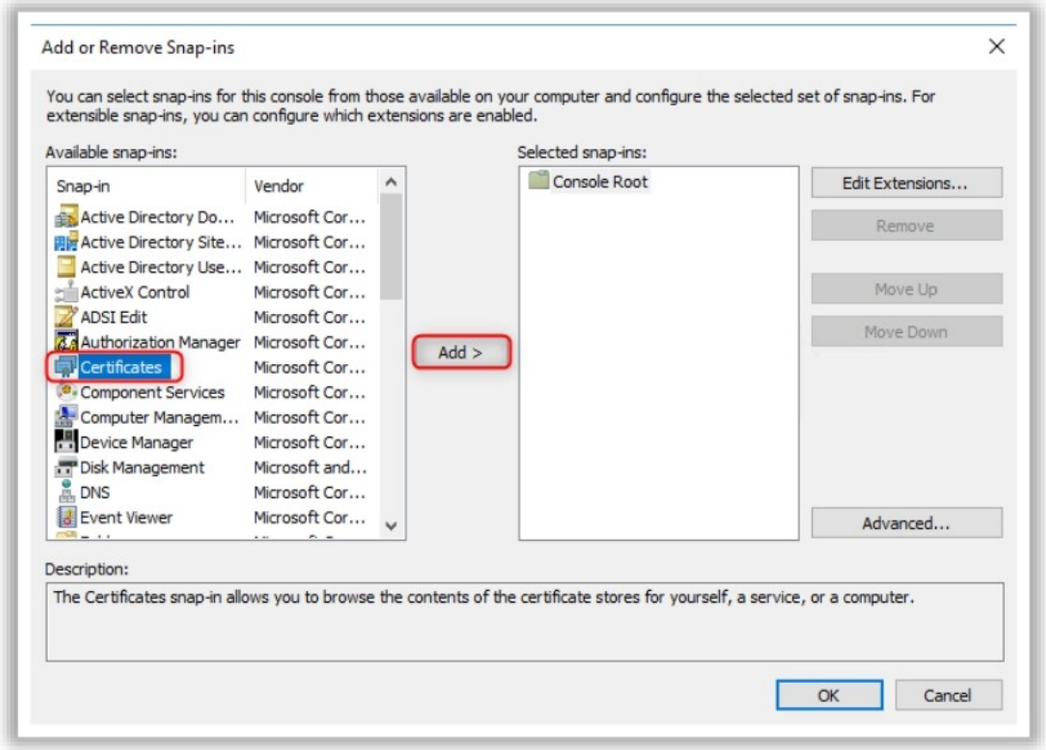


Figure 10.91: Add/Remove Snap-in Window.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Select **Computer account**.

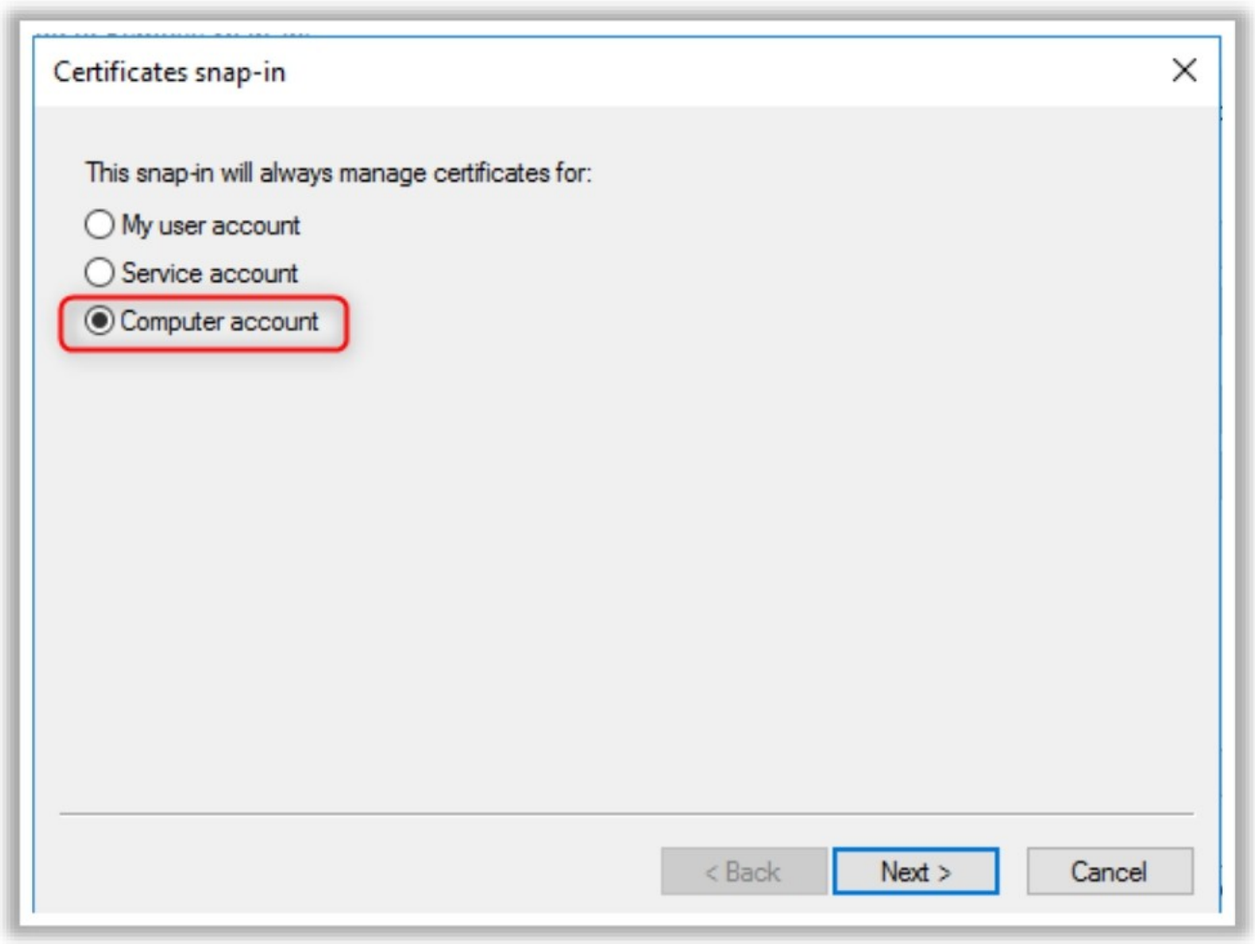


Figure 10.92: Choosing Computer Account

- Choose **Local Computer** and click **Finish**.

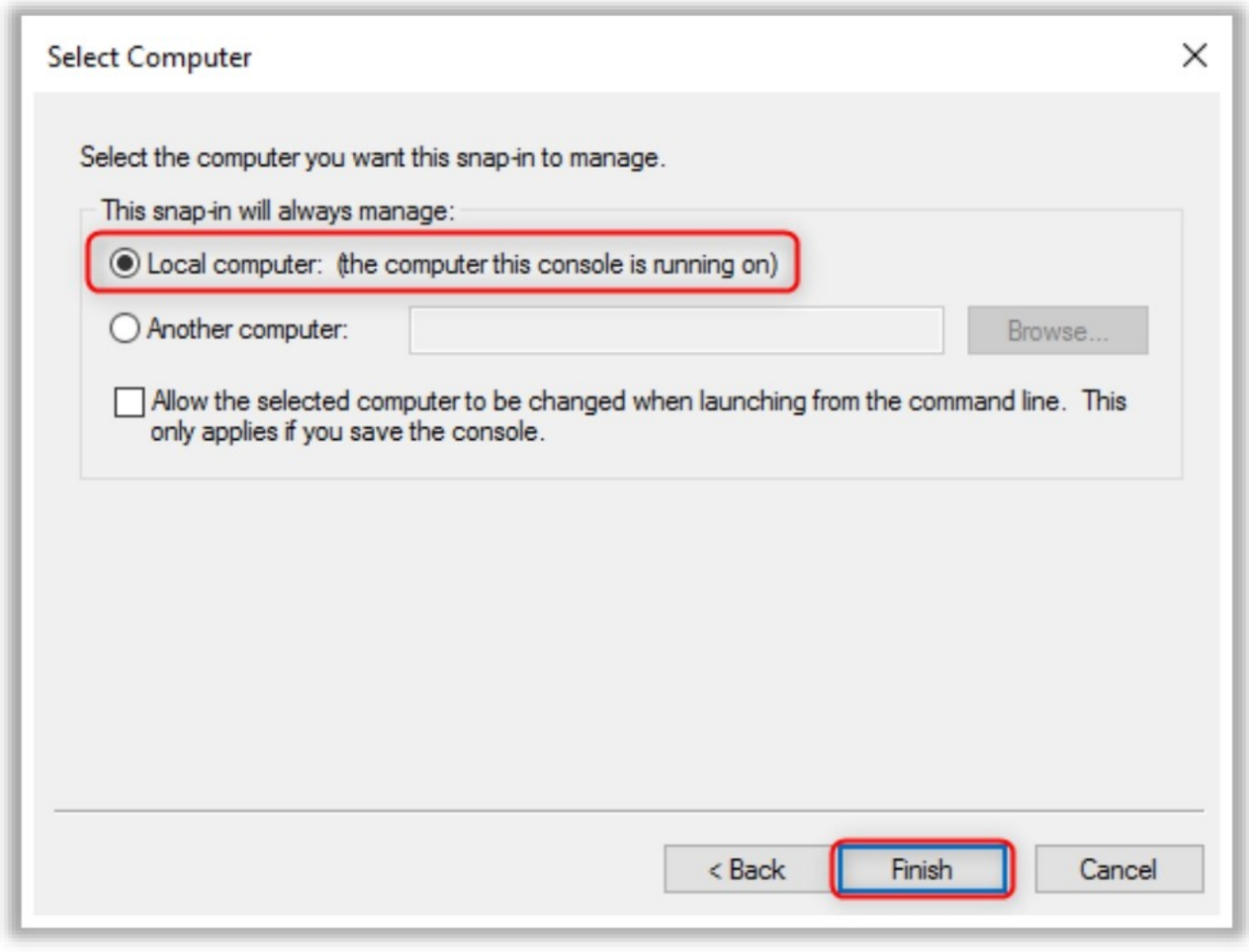


Figure 10.93: Selecting the Computer

- Close **Add Standalone Snap-in**.
- Click on **OK**.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Step 2: Export/Backup the certificate to a .pfx file

- In the center window of MMC, consecutively double-click on **Certificates (Local Computer)**, **Personal Folder**, and **Certificates**. Right-click on backup certificate and choose > **ALL TASKS** > **Export**. A **Certificate Export Wizard** will open to back up the certificate in a.pfx file.

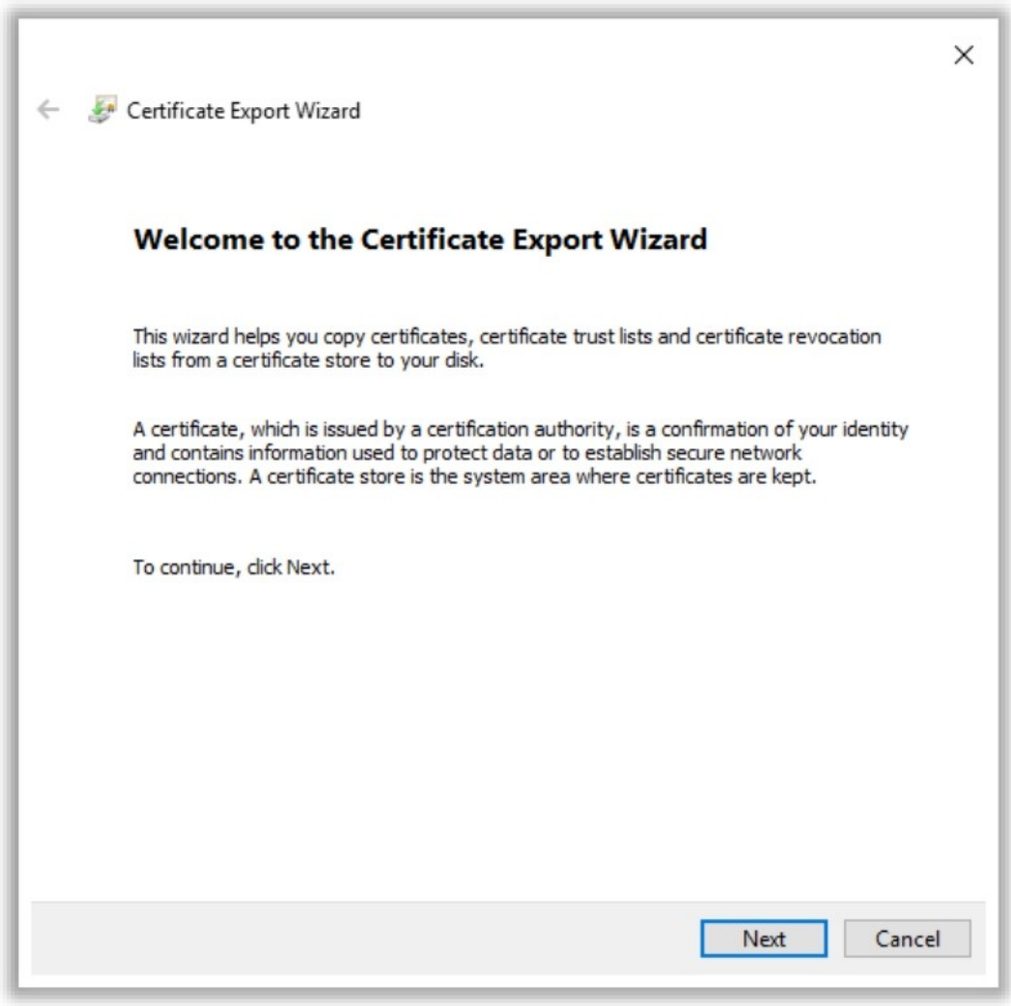


Figure 10.94: Welcome Page of Certificate Export Wizard

- Click **Next,** and choose "**Yes, export the private key**" option.

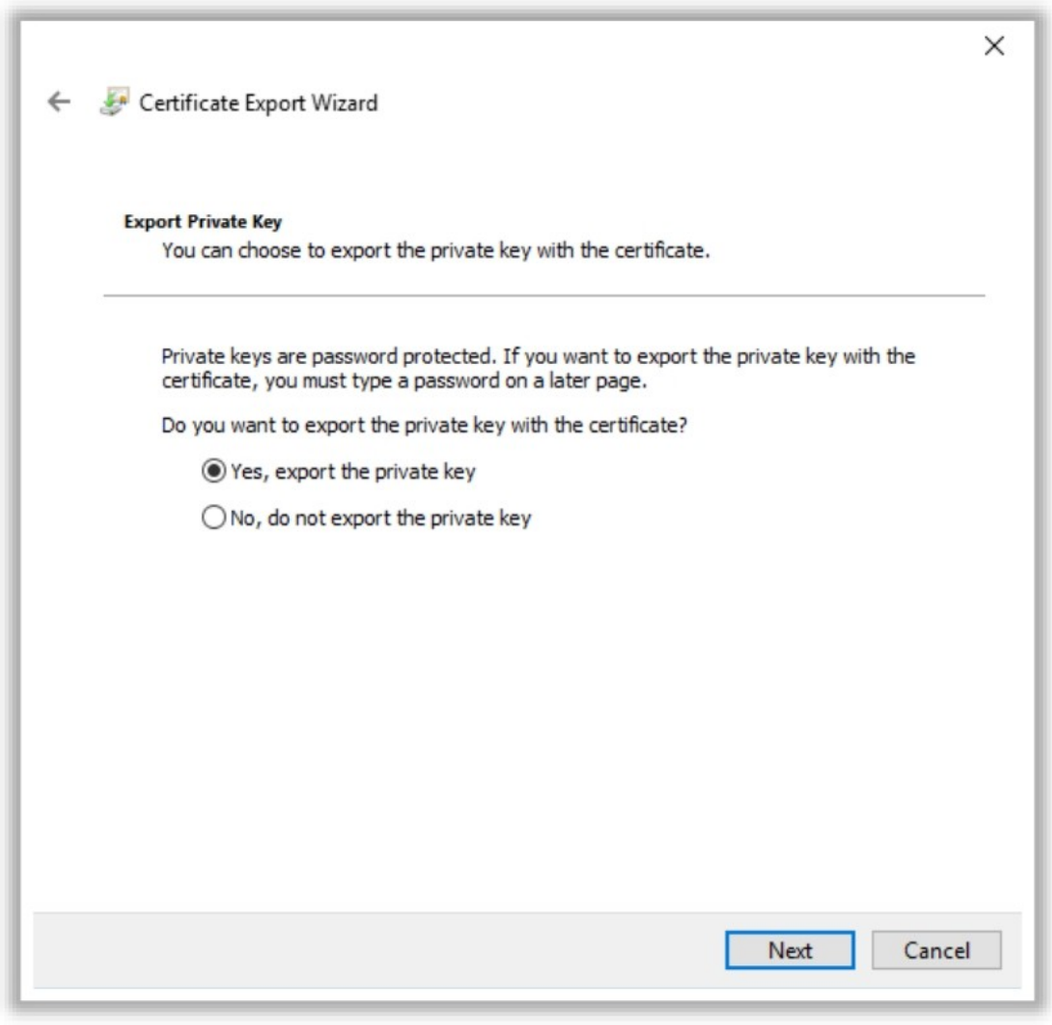


Figure 10.95: Exporting Private Key

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Click Next. In the **Personal Information Exchange** > PKCS #12 (.PFX), tick **Include all certificates in certificate path if possible**.

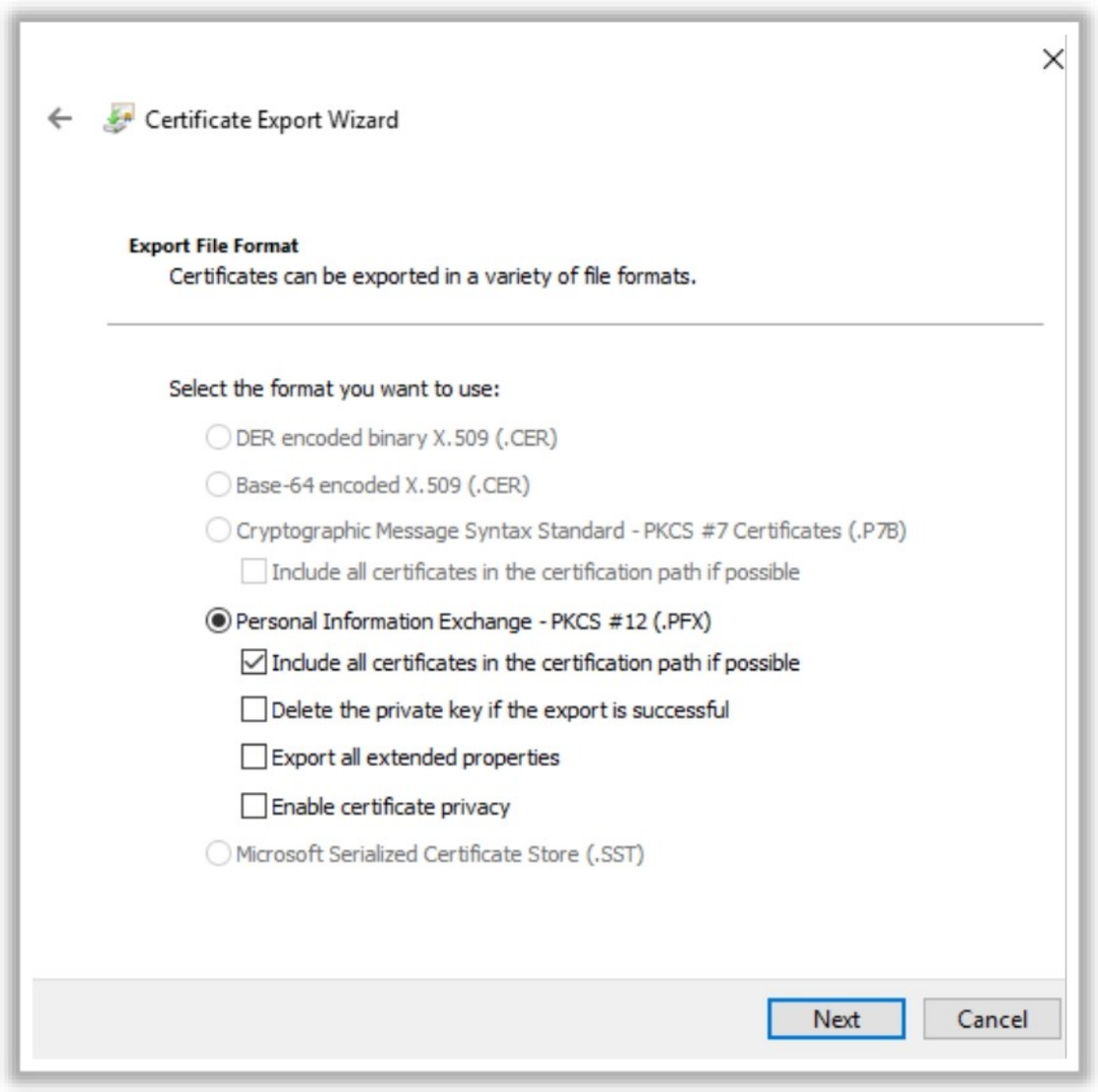


Figure 10.96: Export File Format

- Enter password and click **Next**.

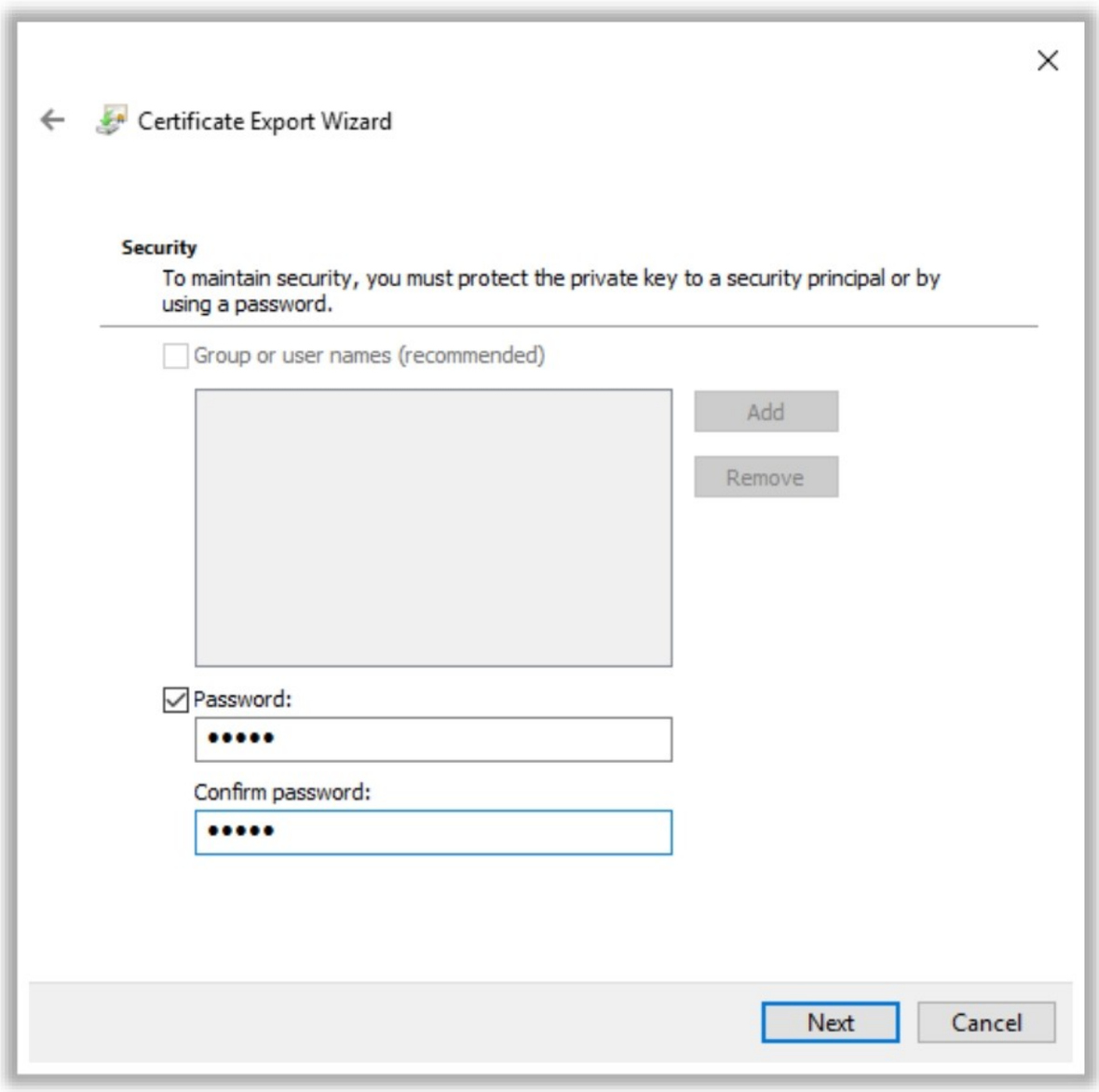


Figure 10.97: Certificate Export Security

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Specify the name of the file you want to export, and click **Next.**

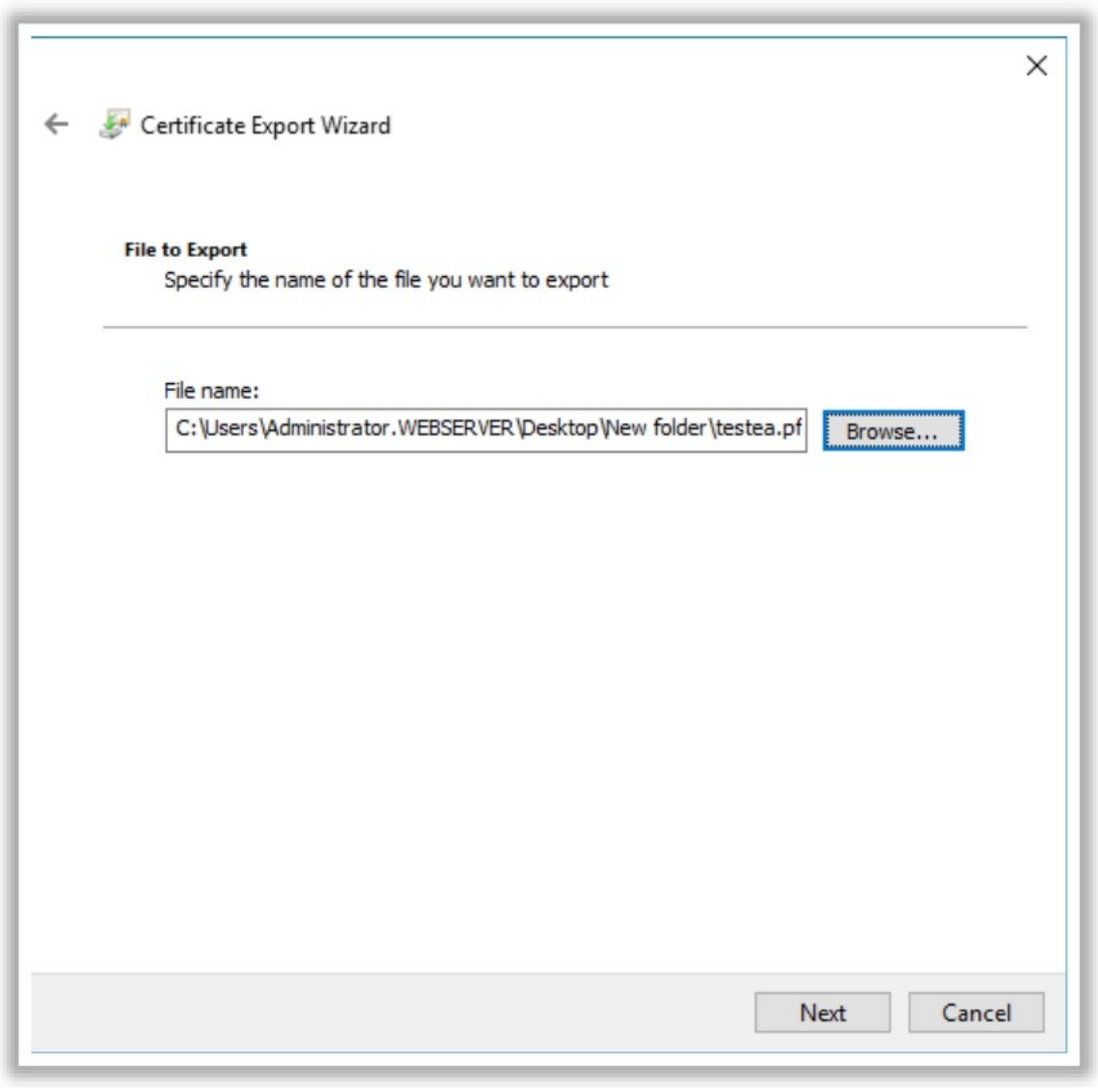


Figure 10.98: Choosing the File to Export

- In the **Completing the certificate Export Wizard** window, click **Finish.**

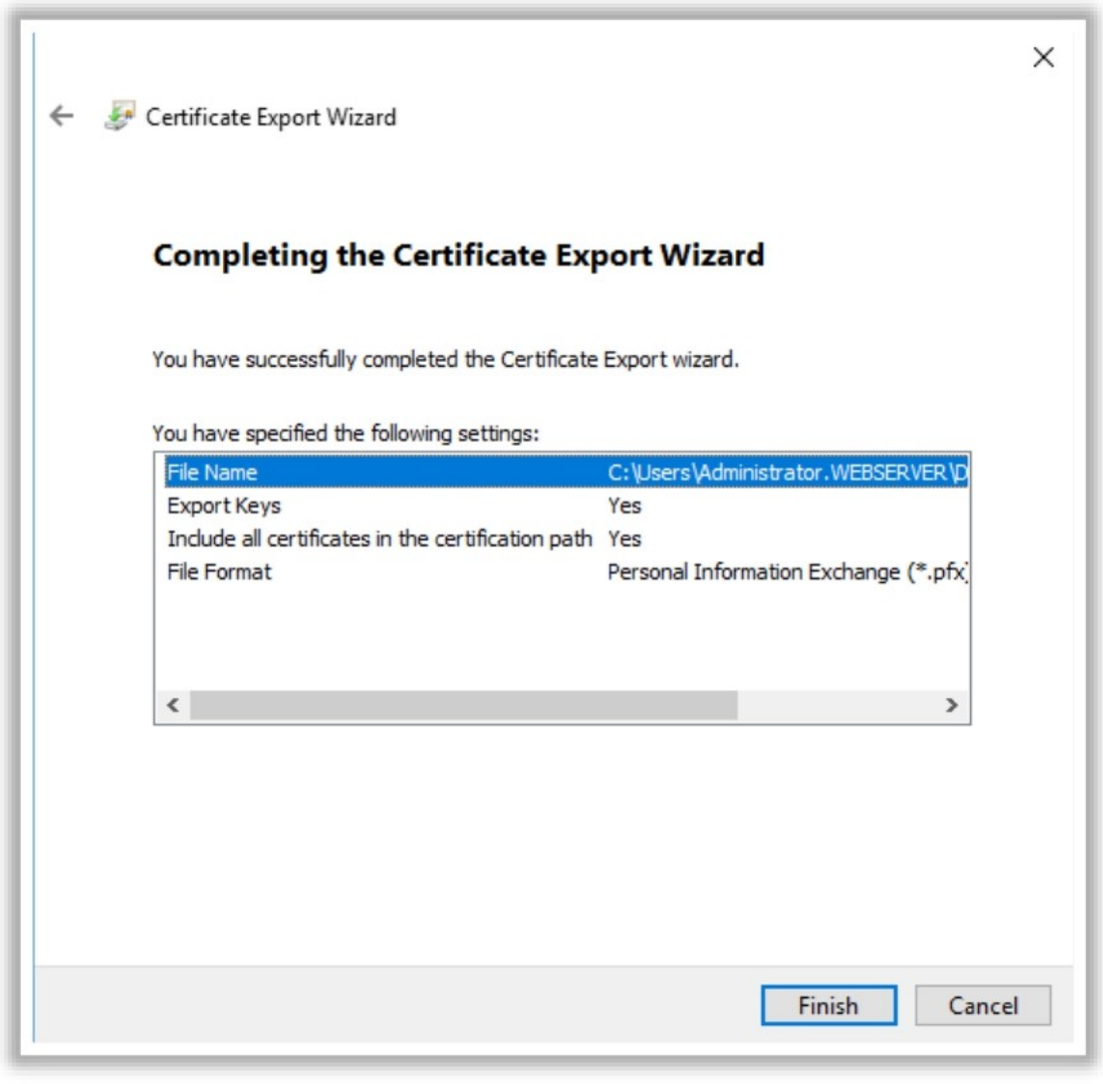


Figure 10.99: Completing the Certificate Export Wizard

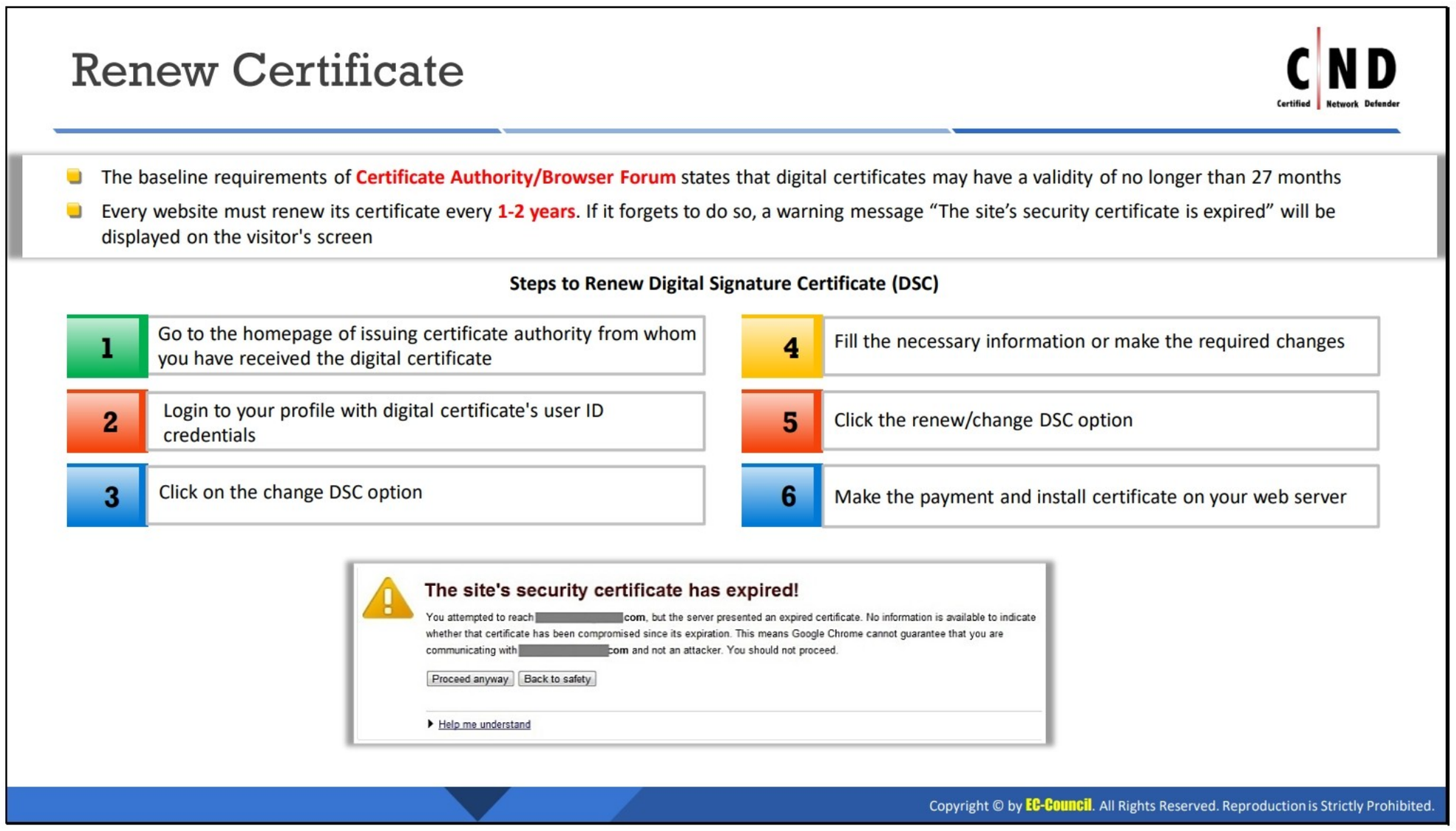
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- You will get the message "**The export was successful.**" Then, click **OK**.



Figure 10.100: Successfully Exporting the Certificate Export Wizard

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Renew Certificate

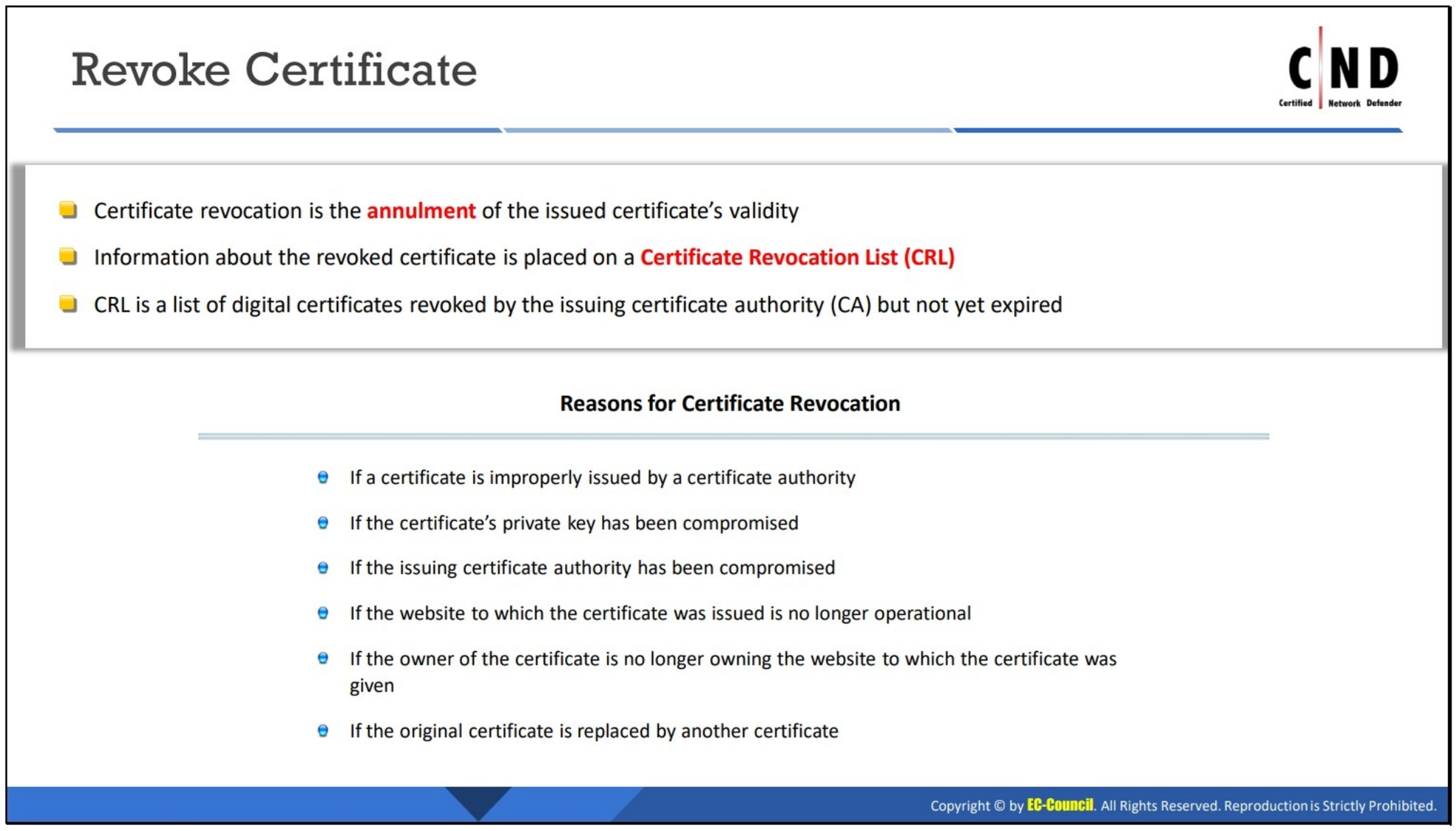
The baseline requirements of the certificate authority/browser forum states that digital certificates may have a validity of no longer than 27 months. Every website has to renew its certificate when its validity is about to expire. If it forgets to do so, a warning message "The site's security certificate is expired" will be displayed on the visitor's screen. Cybercriminals may exploit an expired SSL certificate, and steal or alter the data transferred between the server and the browser.

Steps to renew or change a digital signature certificate (DSC)

A digital signature certificate change or renewal requires a **DSC USB token,** and it is mandatory to use the **same name for renewal**. The user should follow the following steps.

- Go to the homepage of the DSC certifying authority.
- Login to the profile with the digital certificate's user ID credentials.
- Click on the change DSC option.
- Fill the necessary information or make the required changes.
- Once this is done, click the renew/change DSC option.
- Make the payment.
- Install the certificate on the web server.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Revoke Certificate

The DSC revocation cancels the issued certificate's validity. The information about the revoked certificate is placed on a certificate revocation list (CRL), which consists of digital certificates revoked by CA that did not reach their scheduled expirations and cannot be trusted. Whenever the web browser encounters a revoked certificate on any website, it will send an alert to the visitor that the particular website should not be trusted. The certificate revocation cannot be reversed, and is permanent.

CRL distribution point (CDP)

It is a shared location on the computer network for storing CRL and certificates. The client asks the CRL to determine whether the certificate that they are about to use is valid or not. Hence, the certificates are stored in a distribution point that allows the client to easily download them. CDP is a point on the shared network for downloading the certificates. If CDP is not available, the client has to install the certificate manually.

To View CDPs

- Browse to the website and click on the lock icon, then click on **View Certificate**.
- A new window consisting of **General**, **Details**, **Certification Path** tabs will open.
- Click the **Details** tab and select CDPs.

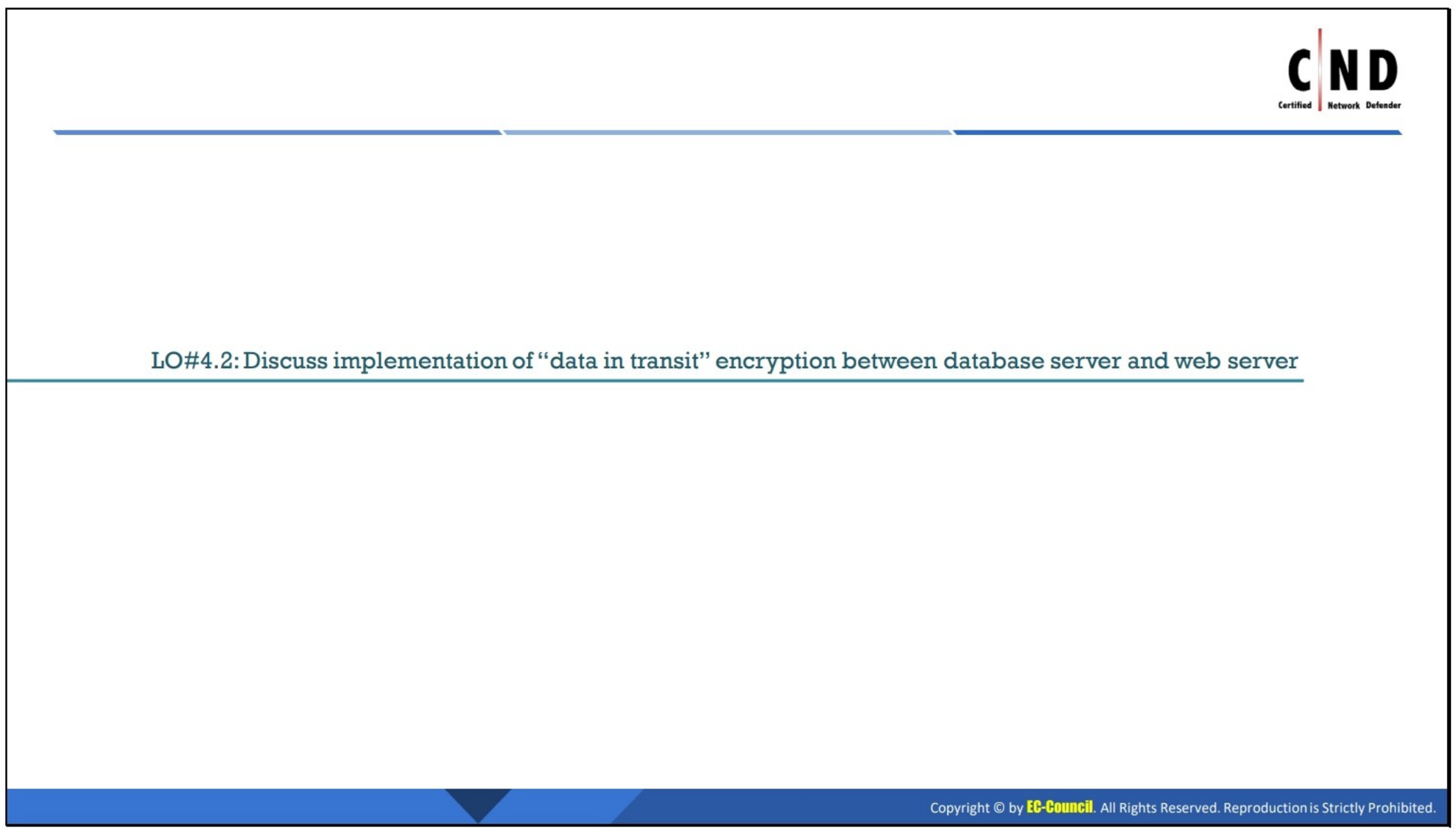
Reasons for Certificate Revocation

- If the certificate is improperly issued by a CA
- If the certificate's private key has been compromised
- If the issuing CA has been compromised

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- If the website is no longer operational
- If the owner of the certificate no longer owns the website
- If the original certificate is replaced by another certificate

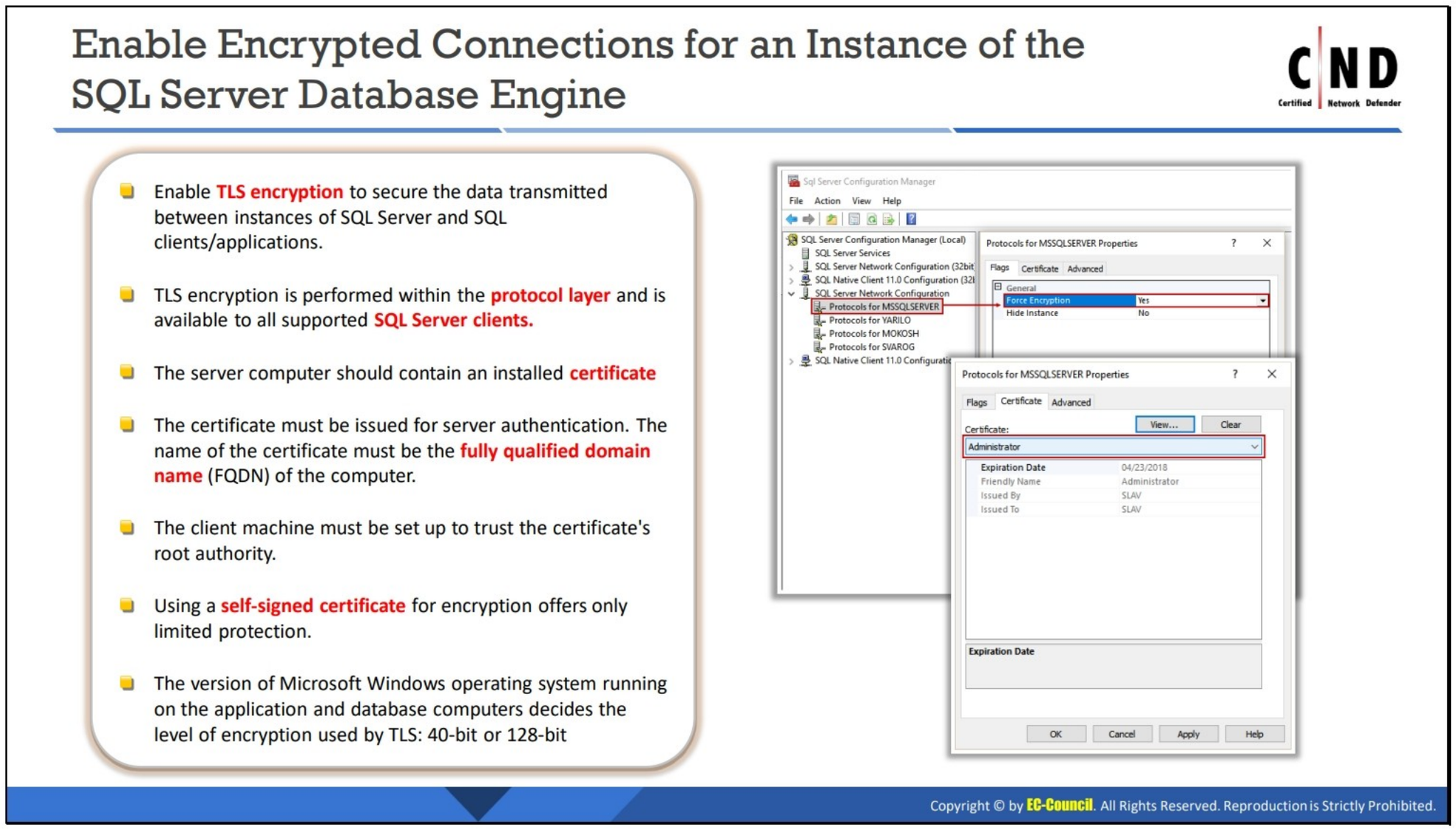
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



LO#4.2: Implementation of "Data in Transit" Encryption Between Database Server and Web Server

The objective of this section is to explain the use of encryption technology to secure the data in transit between web server and database server.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Enable Encrypted Connections for an Instance of the SQL Server Database Engine

- Enable TLS encryption to secure the data transmitted between instances of SQL server and SQL clients/applications.
- TLS encryption is performed within the protocol layer and is available to all supported SQL server clients.
- The server computer should contain an installed certificate.
- The certificate must be issued for server authentication. The name of the certificate must be the fully qualified domain name (FQDN) of the computer.
- The client machine must be set up to trust the certificate's root authority.
- Using a self-signed certificate for encryption offers only limited protection.
- The version of Microsoft Windows operating system running on the application and database computers decides the level of encryption used by TLS: 40-bit or 128-bit.

To Enable Encrypted Connections in SQL Server

- Install the certificate on the SQL server.
- Open **SQL Server Configuration Manager**.
- Navigate to **SQL Server Network Configuration** and Select the required **Protocols** for SQL server instance.
- Right-click on the Protocols and select the **Properties**.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Click on the **Certificate** tab and select the certificate from the drop-down menu.

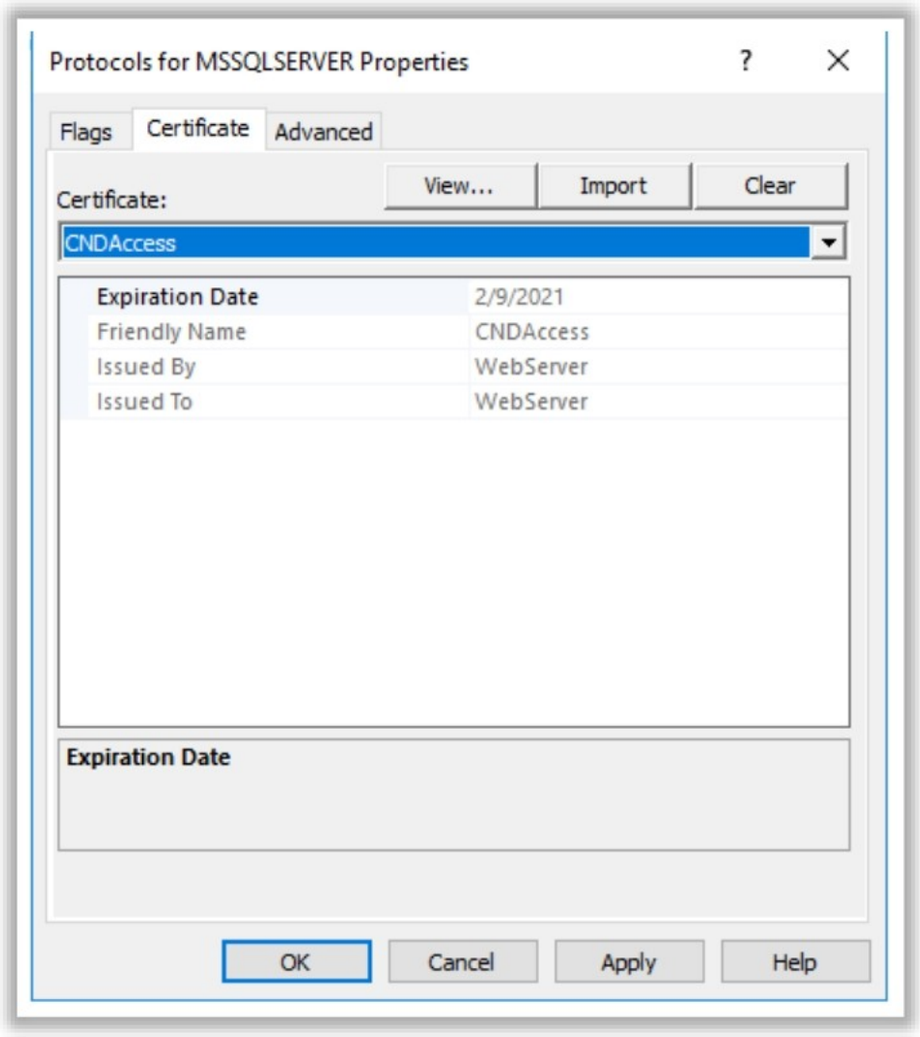


Figure 10.101: Selecting the Required Protocols for SQL server instance

- Click **Flags** tab and enable **Force Encryption**.
- Click Apply.

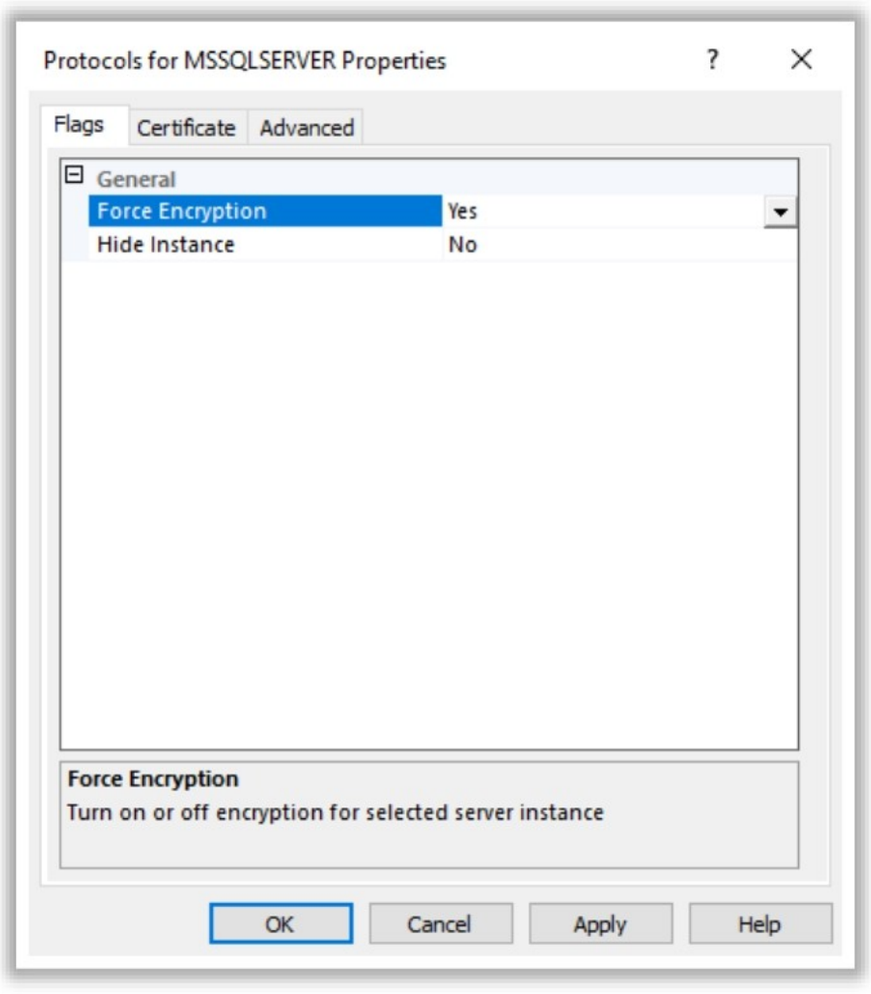
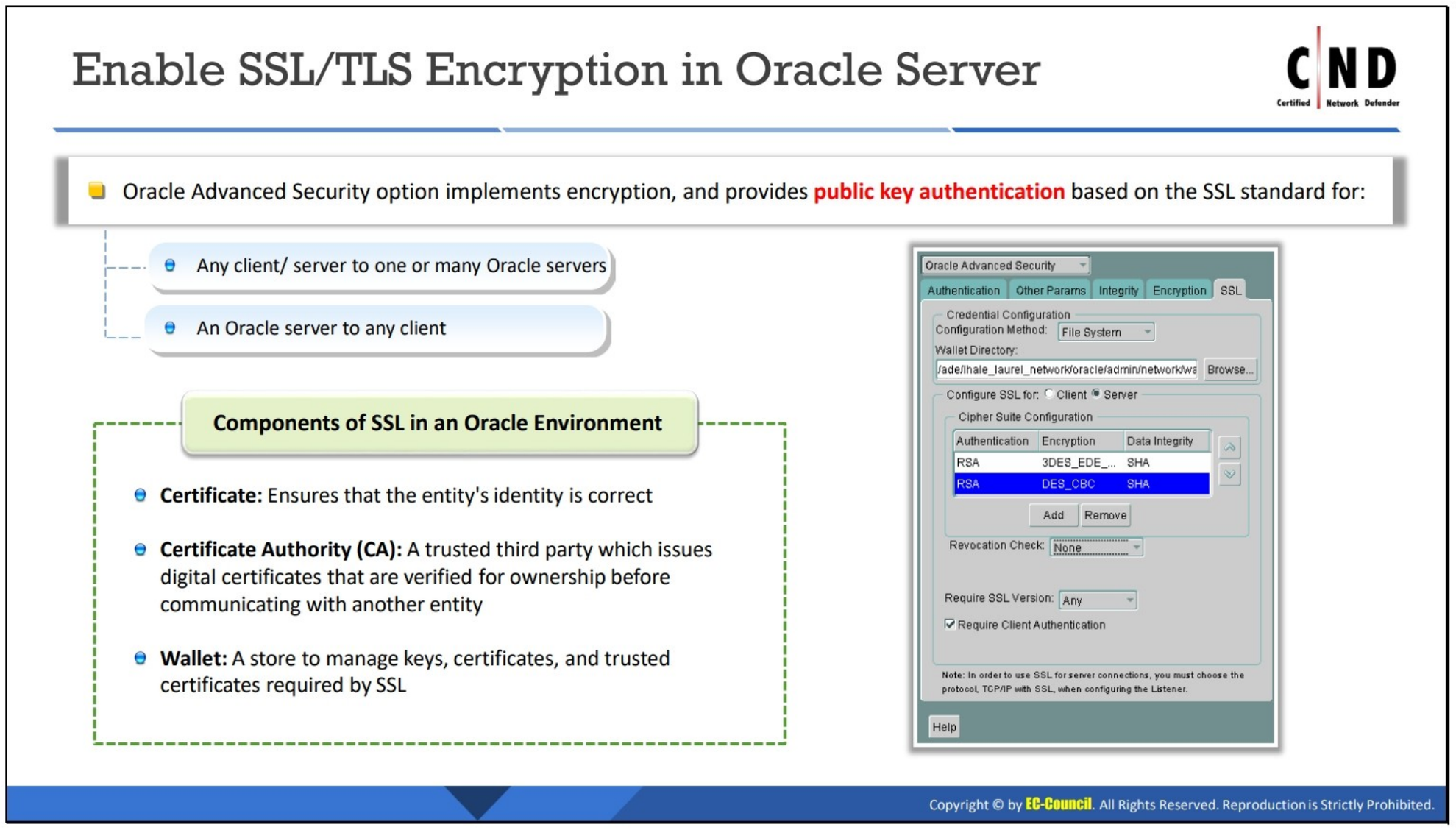


Figure 10.102: Turning on Force Encryption

- Navigate to SQL Server Services and choose the running instance which was configured. Then, right-click and select **Restart** to apply the changes.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Enable SSL/TLS Encryption in Oracle Server

Oracle Advanced Security option implements encryption, and provides public key authentication based on the SSL standard for

- Any client/ server to one or many Oracle servers.
- An Oracle server to any client.

Components of SSL in an Oracle Environment

- **Certificate**: Ensures that the entity's identity is correct, and the public key belongs to the entity.
- **CA**: A trusted third party which issues digital certificates that are verified for ownership before communicating with another entity.
- **Wallet**: A store to manage keys, certificates, and trusted certificates required by SSL.

Steps to Enable an Encrypted Connection with SQL Server

Step 1: Install Oracle Advanced Security and the Oracle Wallet Manager.

Step 2: Configure SSL on the client.

Step 3: Configure SSL on the server.

Step 4: Start the Oracle Wallet Manager.

Step 5: Create a new wallet.

Step 6: Install a certificate into the new wallet.

Step 7: Add new trusted certificates.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Step 8: Save changes to the wallet.

Step 9: For single sign-on functionality, create an auto-login wallet.

Step 10: Create a user identified globally through certificates on the Oracle server.

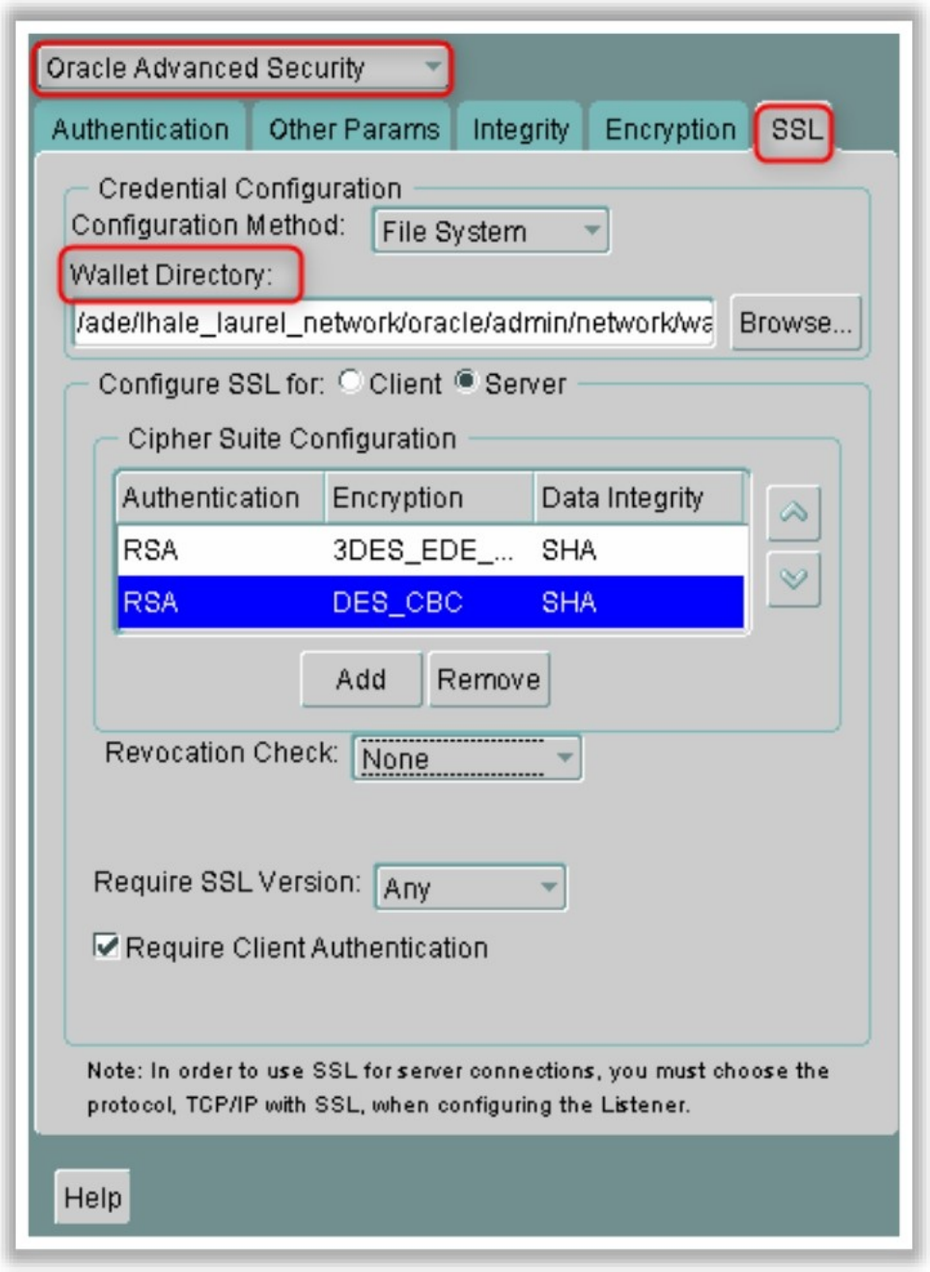
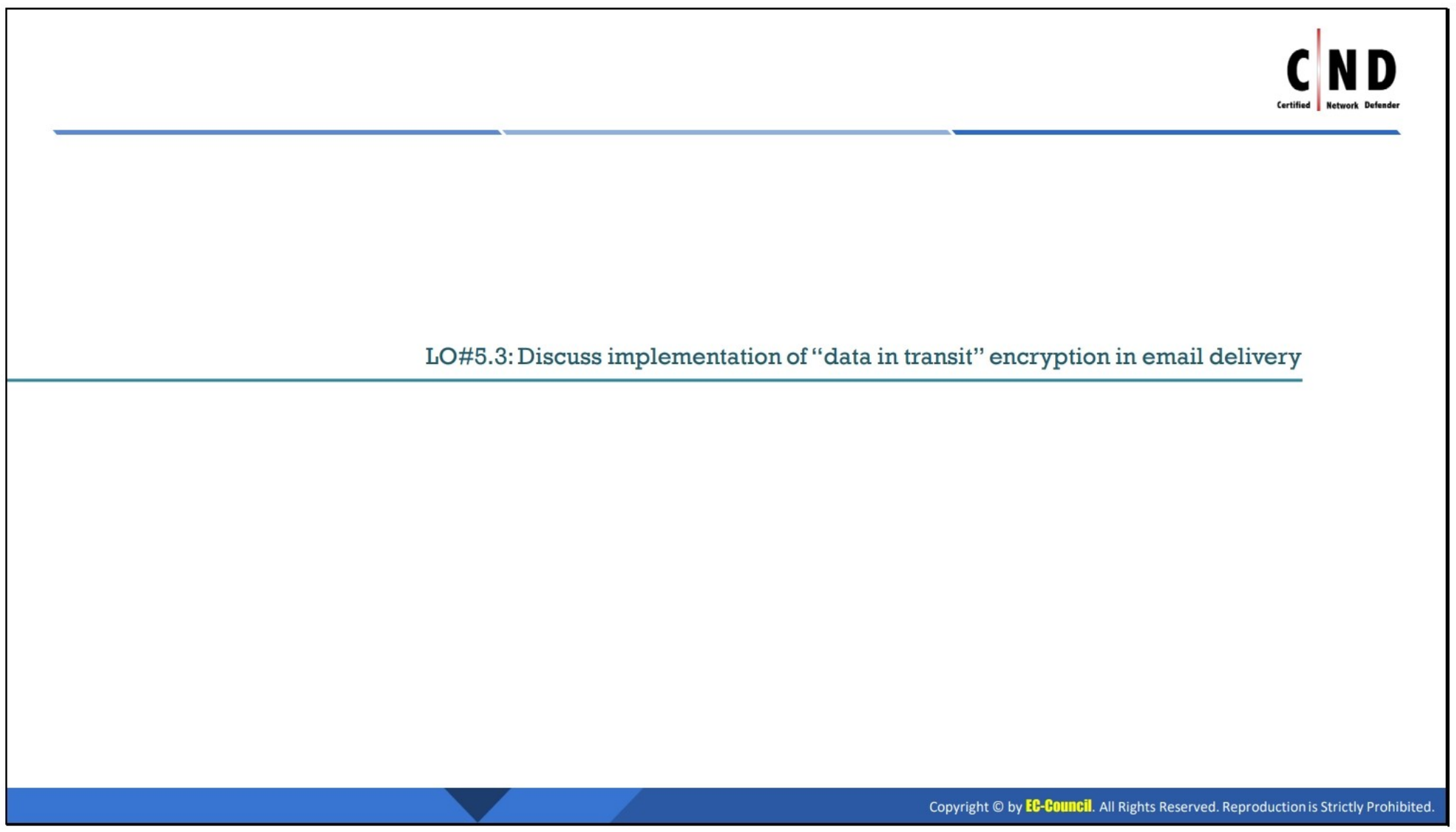


Figure 10.103: Screenshot of Enabling an Encrypted Connection with SQL Server

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



LO#4.3: Implementation of "Data in Transit" Encryption in Email Delivery

Businesses use emails as a primary source of communication as it makes it simple and easy to communicate or share information. Emails contain sensitive information about the organization such as projects, upcoming news, and financial data. If this information is accessed by a wrong person, it may result in significant losses (reputation and financial) to the organization. One can protect emails containing sensitive information by encrypting them.

The objective of this section is to explain the use of encryption technology to secure data in transit during email delivery.

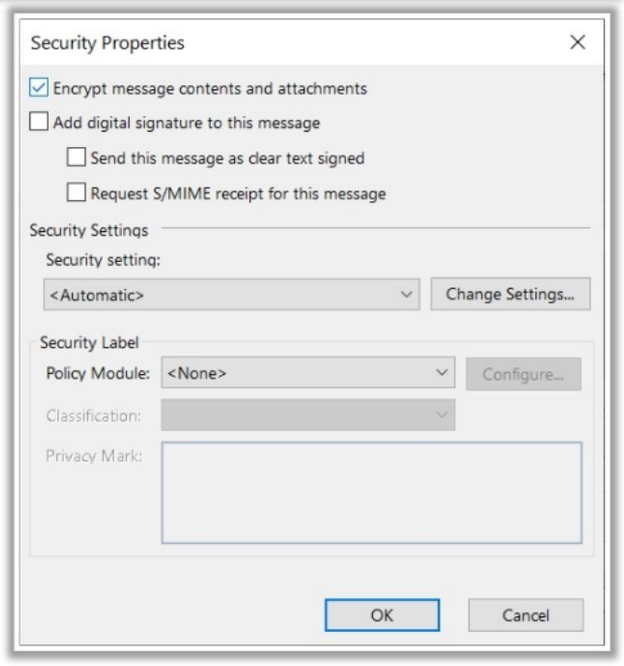
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Email Encryption: MS Outlook

- By **default**, Outlook supports the S/MIME standard
- To implement S/MIME encryption, the sender and recipient must have a mail application that supports the S/MIME standard

Steps to Encrypt a Single Message

1. In the message you are composing, click the dialog box launcher in the **More Options** group on the **Options** tab
2. Click **Security Settings**, and then select the **Encrypt message contents and attachments** check box
3. Compose your message, and then click **Send**

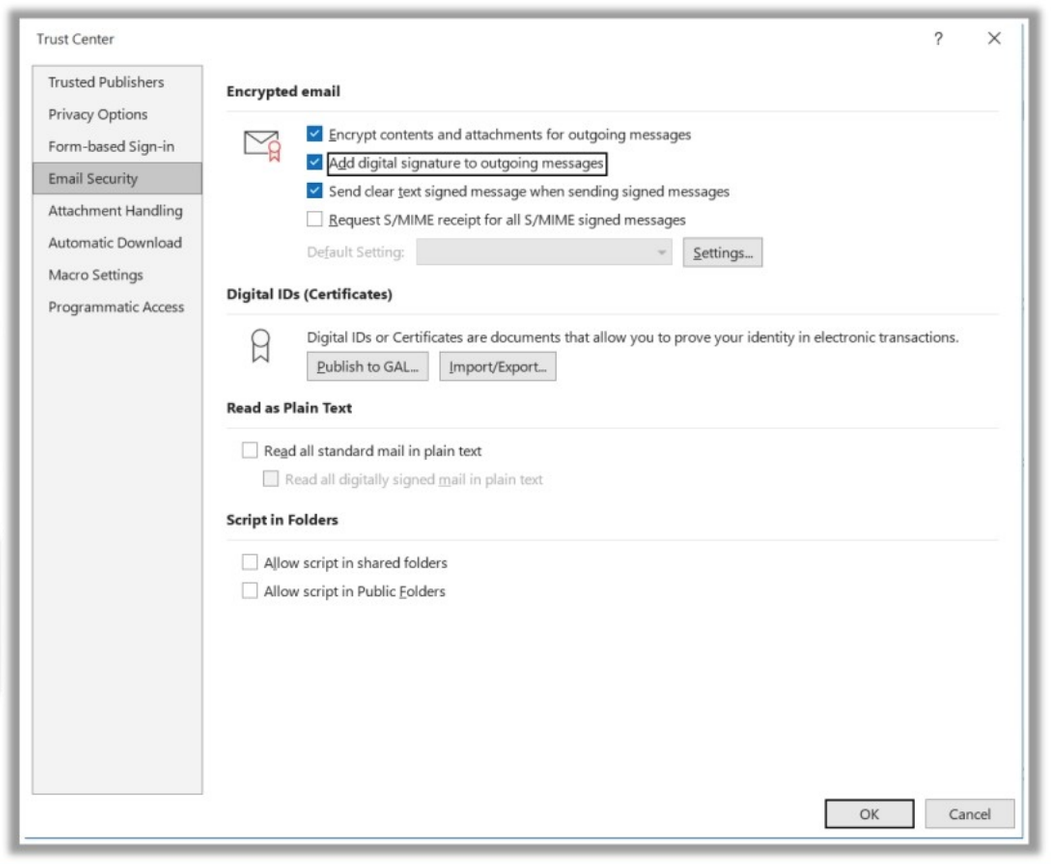


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Email Encryption: MS Outlook (Cont'd)

Steps to Encrypt all Outgoing Messages

1. Navigate to **File** tab, click **Options** → **Trust Center** → **Trust Center Settings**
2. In **E-mail Security** tab, select the **Encrypt contents and attachments for outgoing messages** check box under **Encrypted e-mail**
3. Click **Settings**, to choose a specific certificate to use for encryption



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Email Encryption: MS Outlook

MS Outlook facilitates the encryption of an email message. Only a recipient who has the secret key that matches the public key can decrypt the email message.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Outlook supports two encryption options:

- **Secure/multipurpose Internet mail extensions (S/MIME) encryption**

  The sender and recipient of the mail should have a mail application that supports the S/MIME standard to use this encryption option.

  Steps to encrypt with S/MIME:

  Adding a certificate to the keychain on your computer is necessary. After setting up the signing certificate on your computer, configure it in Outlook.

  - Under the **File** menu, Go to **Options** > **Trust Center** > **Trust Center Settings**.
  - Select **Email Security** from the left pane.
  - Select **Settings** under **Encrypted email**.

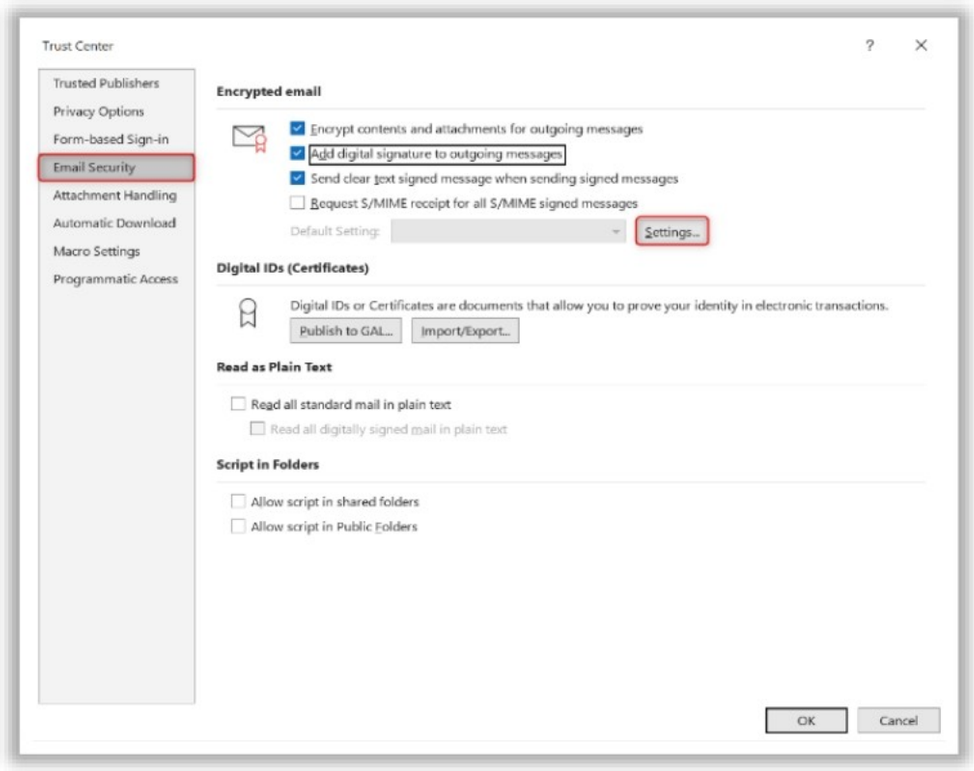


Figure 10.104: Trust Center Window

- Under **Certificates and Algorithms**, click **Choose** and select the **S/MIME certificate**.

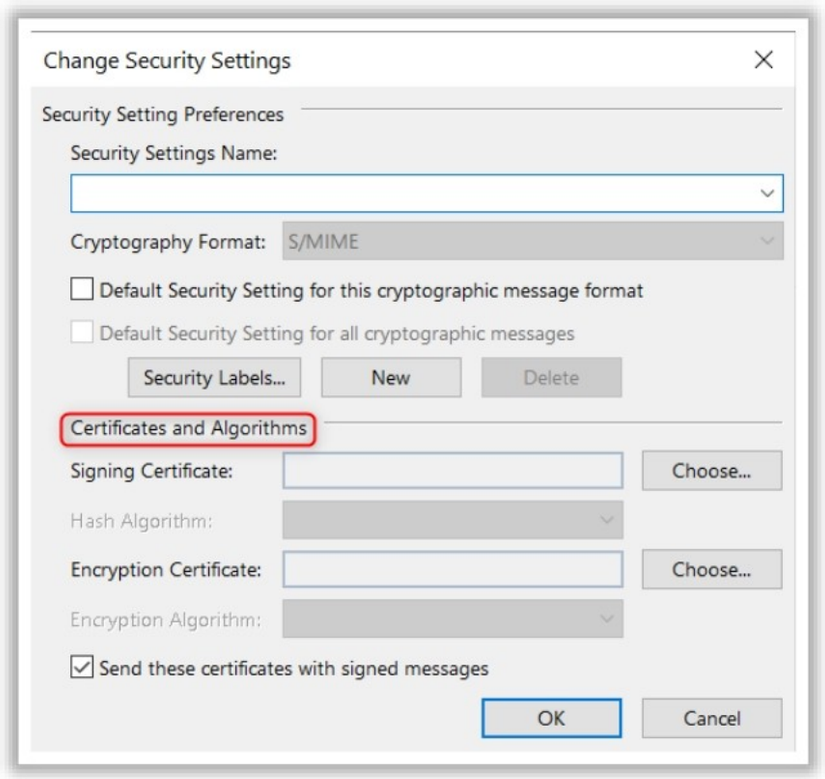


Figure 10.105: Change Security Settings Window

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Select **OK.**
- If you are an Office insider with Office 365 subscription, choose **Options**, select **Encrypt,** and pick **Encrypt with S/MIME** option from the drop-down menu in the email message.
  - See **Encrypt with S/MIME** if you have an **S/MIME** certificate installed on your system.
- For **Outlook 2019** and **Outlook 2016**, select **Options,** and then select **Permissions** in the email message.
- Finish composing the email and click **Send**.

- **Office 365 Message Encryption (Information Rights Management)**

The sender should have Office 365 Message Encryption that comes with the Office 365 Enterprise E3 license to use this encryption option.

Steps to encrypt with Office 365 Message Encryption:

- If you are an Office 365 subscriber, select **Options>Encrypt** and pick the encryption that has the restrictions you want to enforce in the email message.

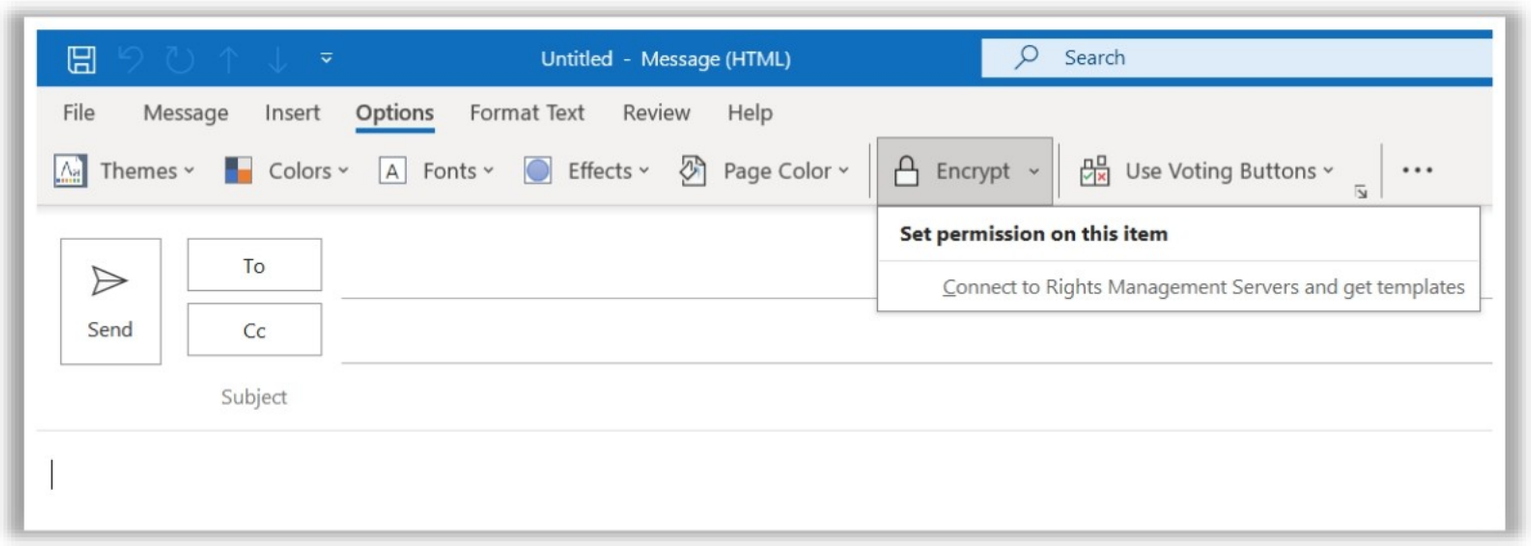
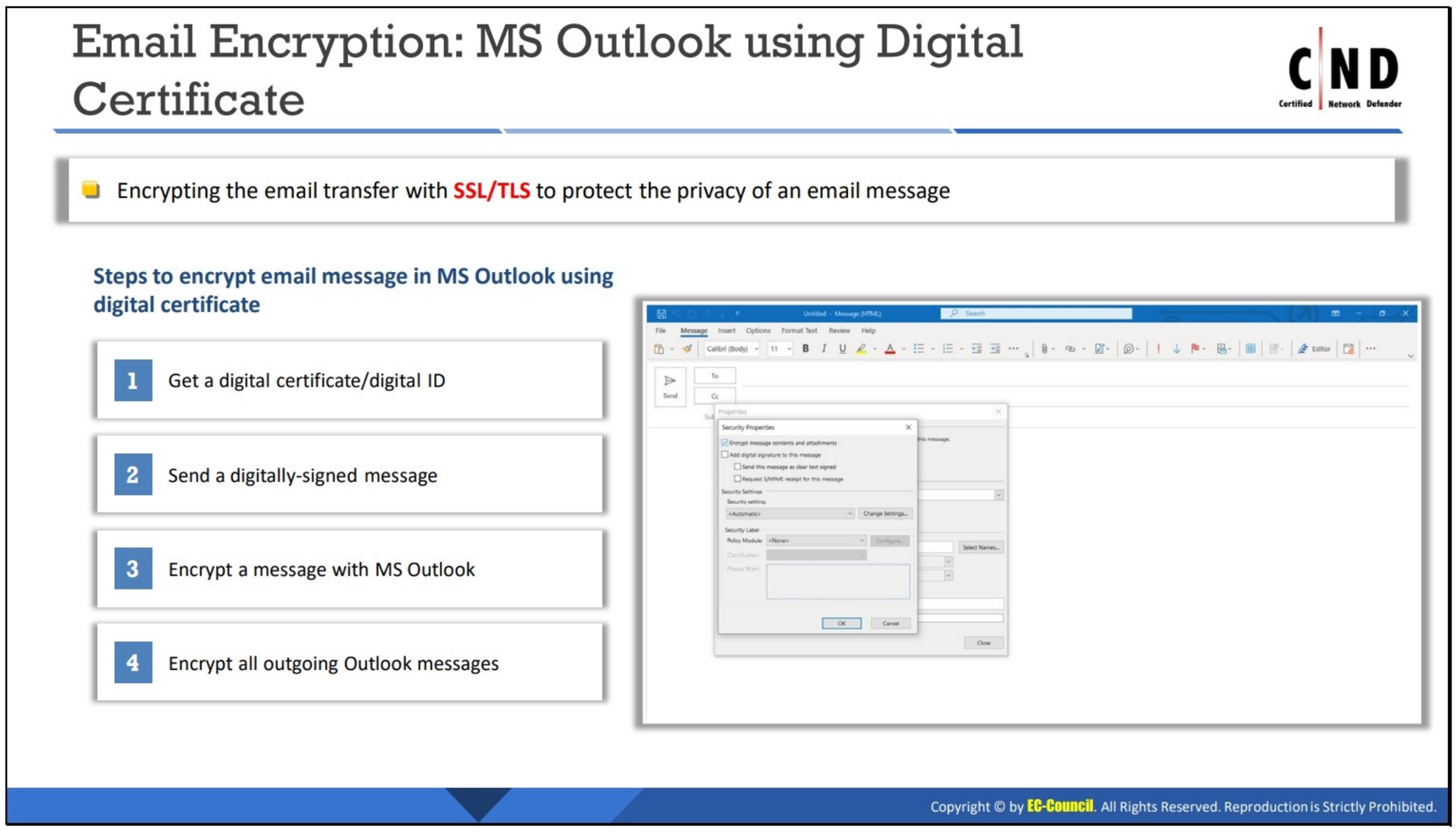


Figure 10.106: Encrypt with Office 365 Message Encryption

- For **Outlook 2019** and **2016**, select **Options > Permissions** and pick the encryption option that has the restrictions you want to enforce, such as **Do Not Forward,** in the email message.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Email Encryption: MS Outlook using Digital Certificate

To encrypt and send an email message in MS Outlook, follow the steps given below:

Step 1: Get a digital certificate/digital ID

You can get a digital certificate/Digital ID by following the steps listed below:

- Navigate to **File** Tab -> **Options** -> **Trust Center.**
- Click **Trust Center Settings**... under **Microsoft Outlook Trust Center**.

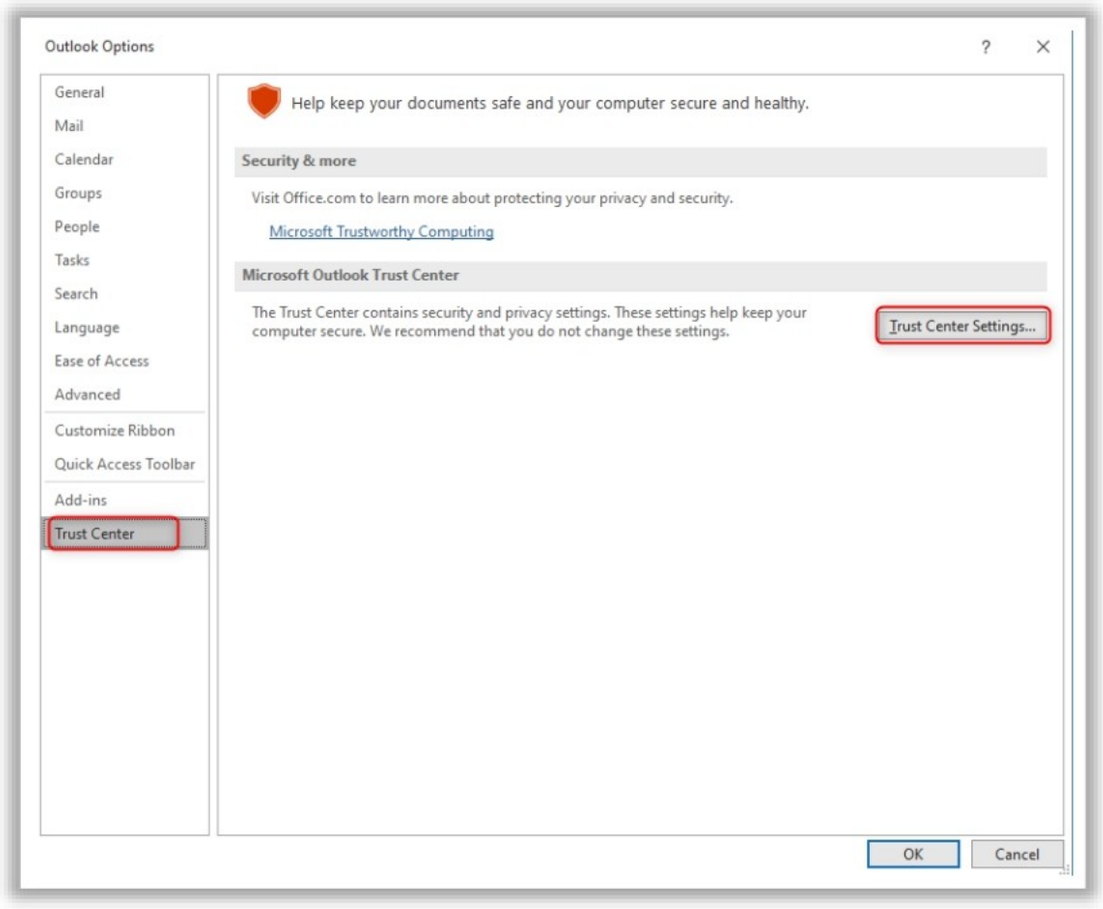


Figure 10.107: Outlook Options Window

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Select **Email Security** from the left pane, and then click **Import/Export…** under **Digital IDs (Certificates).**

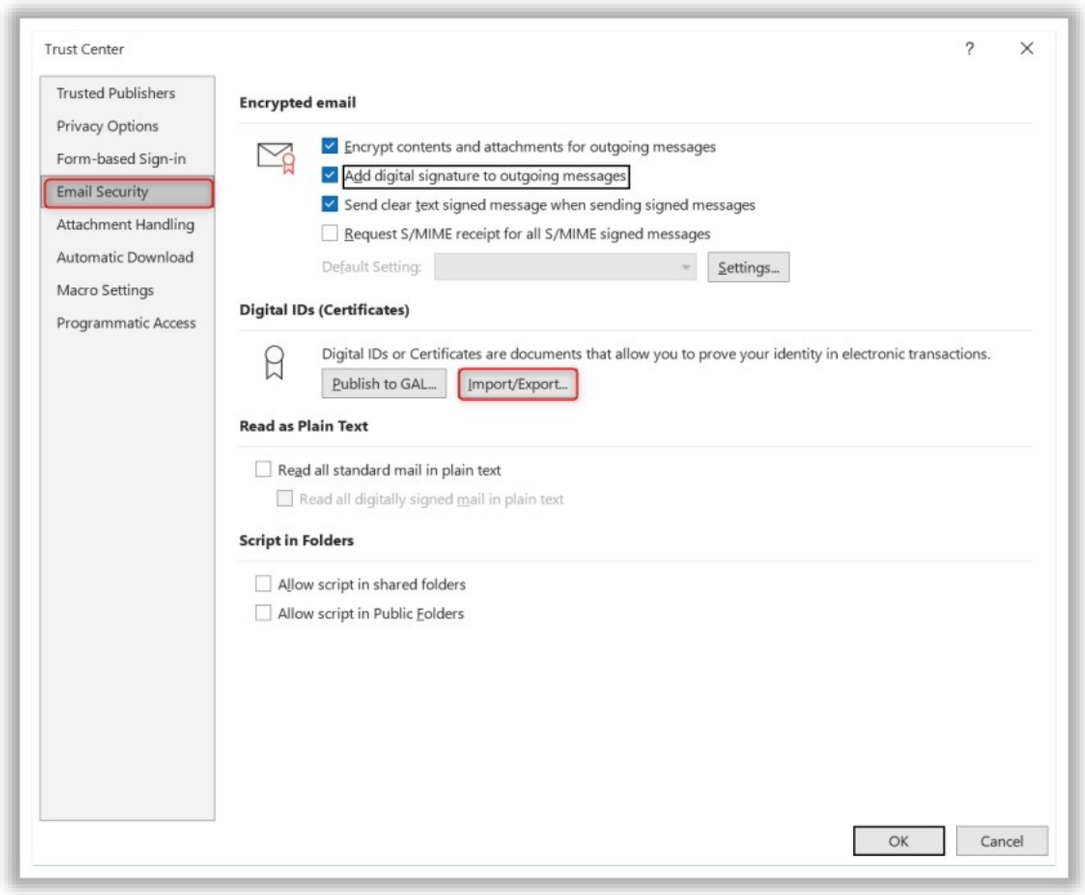


Figure 10.108: Selecting Email Security Option

- Select **Import existing Digital ID from a file** and click **Browse** to **Import File** by providing **Password.**

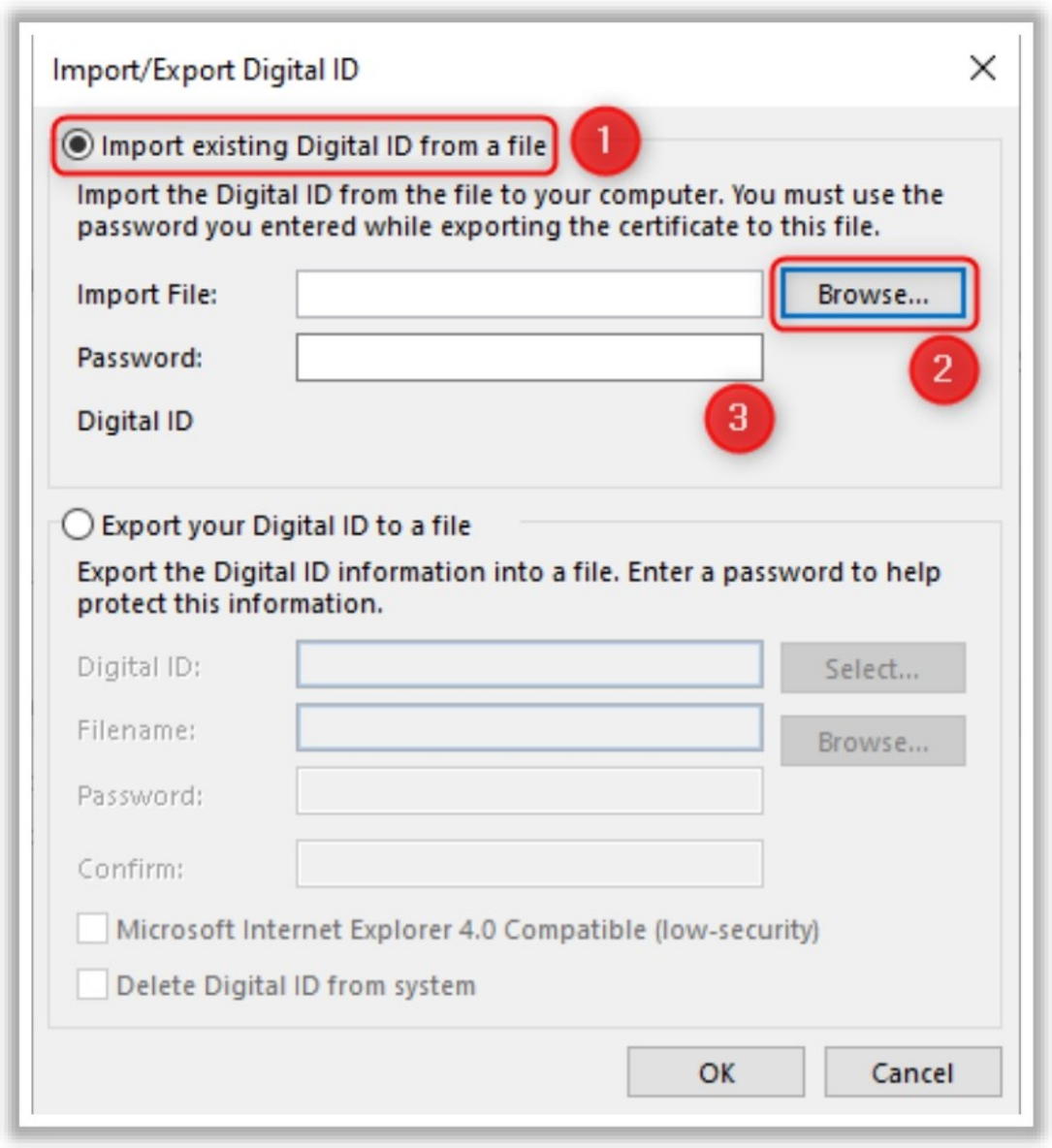


Figure 10.109: Import or Export Digital ID

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Choose an independent CA such as Comodo, DigiCert, GlobalSign, IdenTrust, etc. to get the digital certificate (digital ID), and follow the instructions.
- Once you get a digital certificate, follow the instructions to install it.

Step 2: Send a digitally-signed message

After getting the digital certificate, send the digitally-signed message to the person to whom you wish to send the encrypted message.

- Compose a new message in Outlook.
- Navigate to **Options** > **More Options** icon.

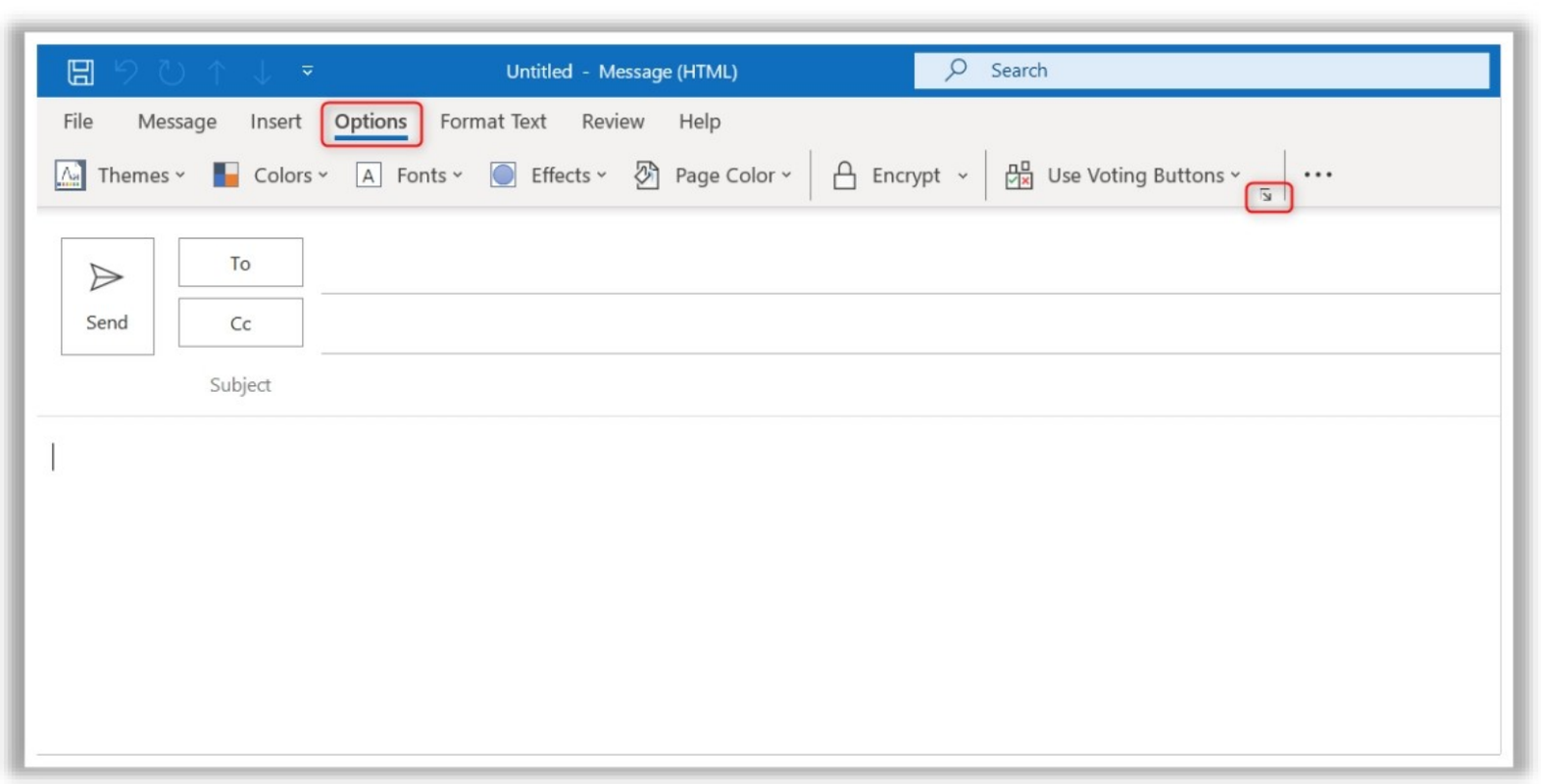


Figure 10.110: Selecting Options Tab in a New Message

- In the **Properties** window, click **Security Settings…**.

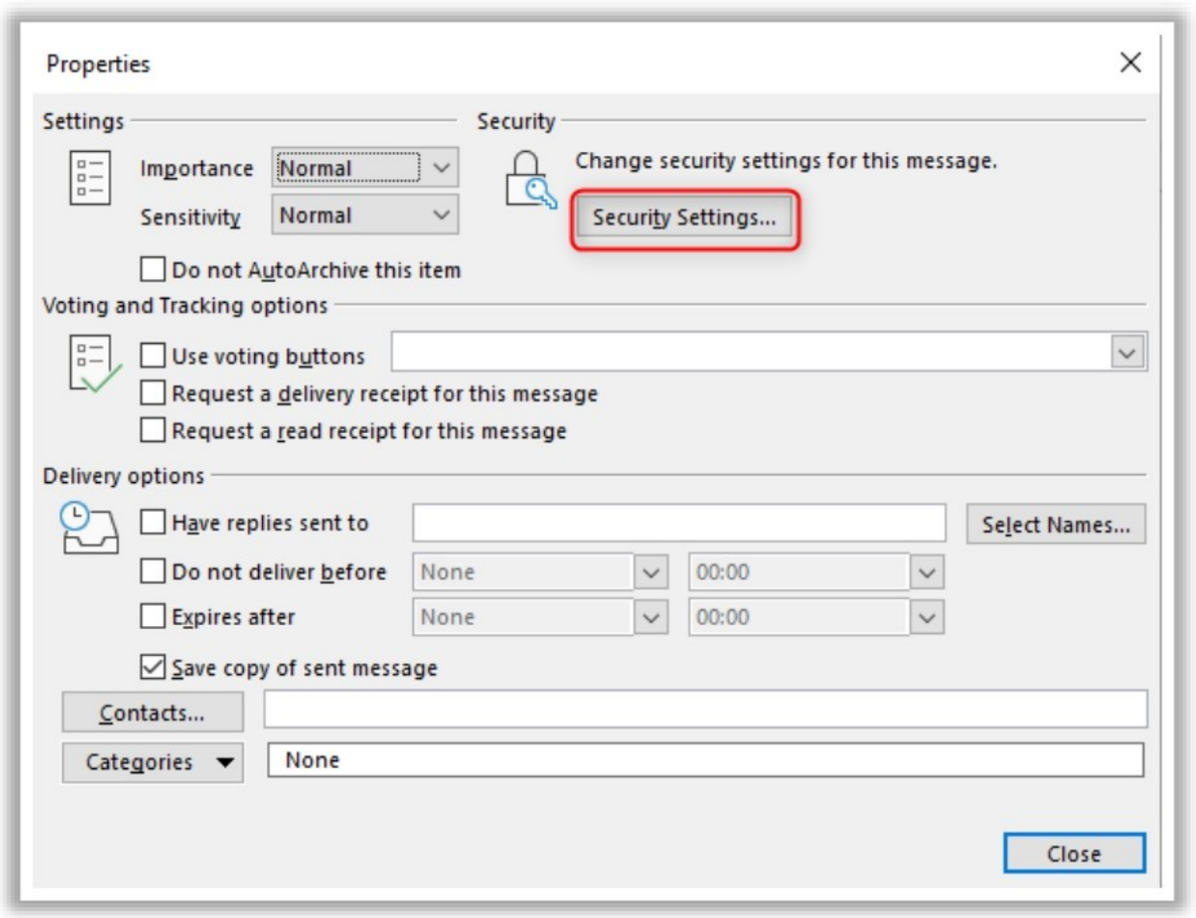


Figure 10.111: Properties Window

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- In the **Security Properties** window, check the **Add digital signature to this message** checkbox and click **OK.**

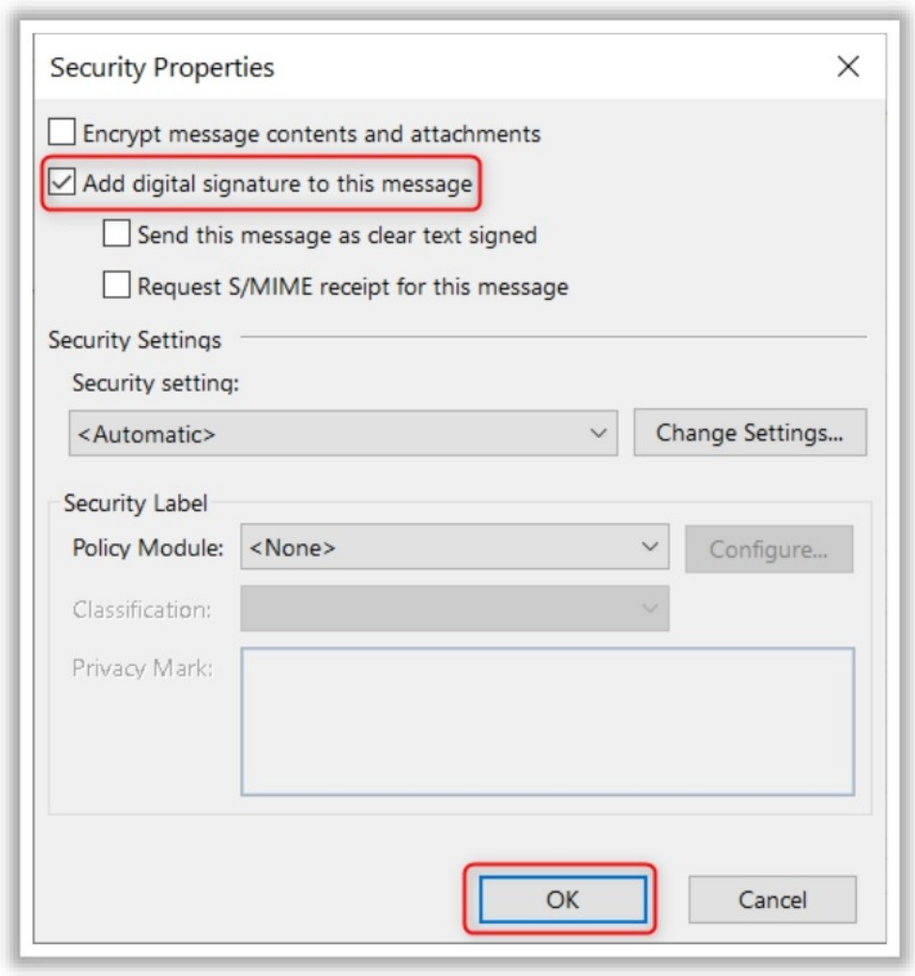


Figure 10.112: Selecting Digital Signature for the Message

- Click **Close** on the **Properties** window.
- Now, a new option will appear in the **Permission** Group: the **Sign Message** button.
- Click **Sign Message** button, and send a message to the recipient.
- Request the recipient to reply to the message with a digitally-signed message of their own.

Step 3: Encrypt a message with MS Outlook

- Compose a message you wish to encrypt in Outlook.
- Click the **File** tab, and then the **Options** tab.

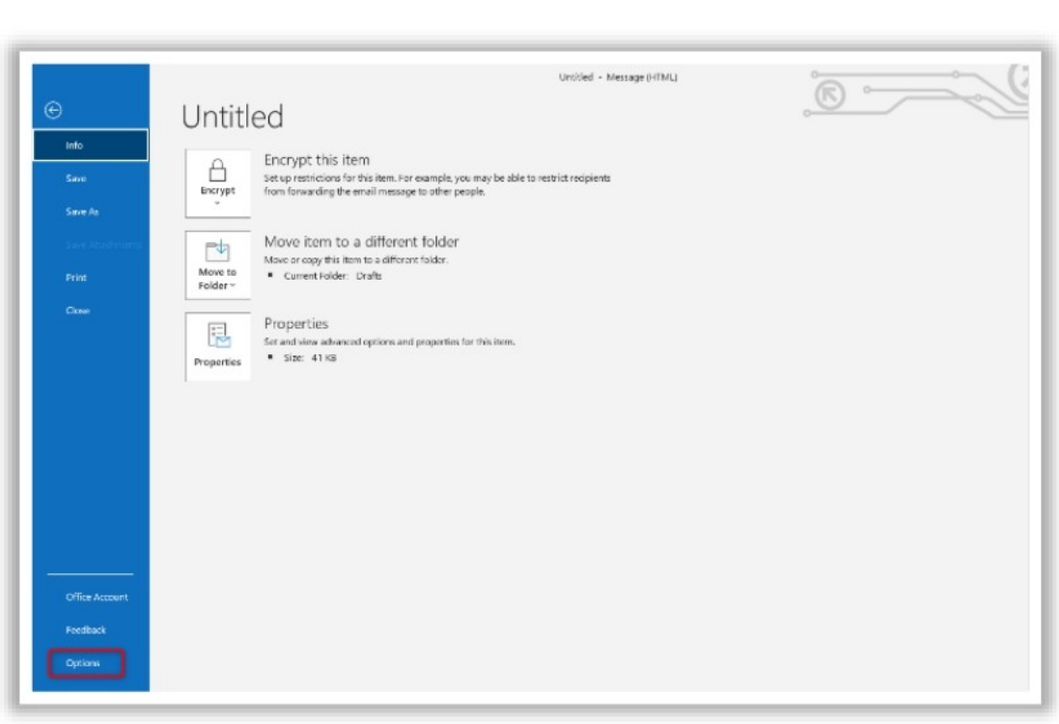


Figure 10.113: Selecting Options Tab

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- The **Properties** dialog box will appear.
- Click the **Security Settings** button.

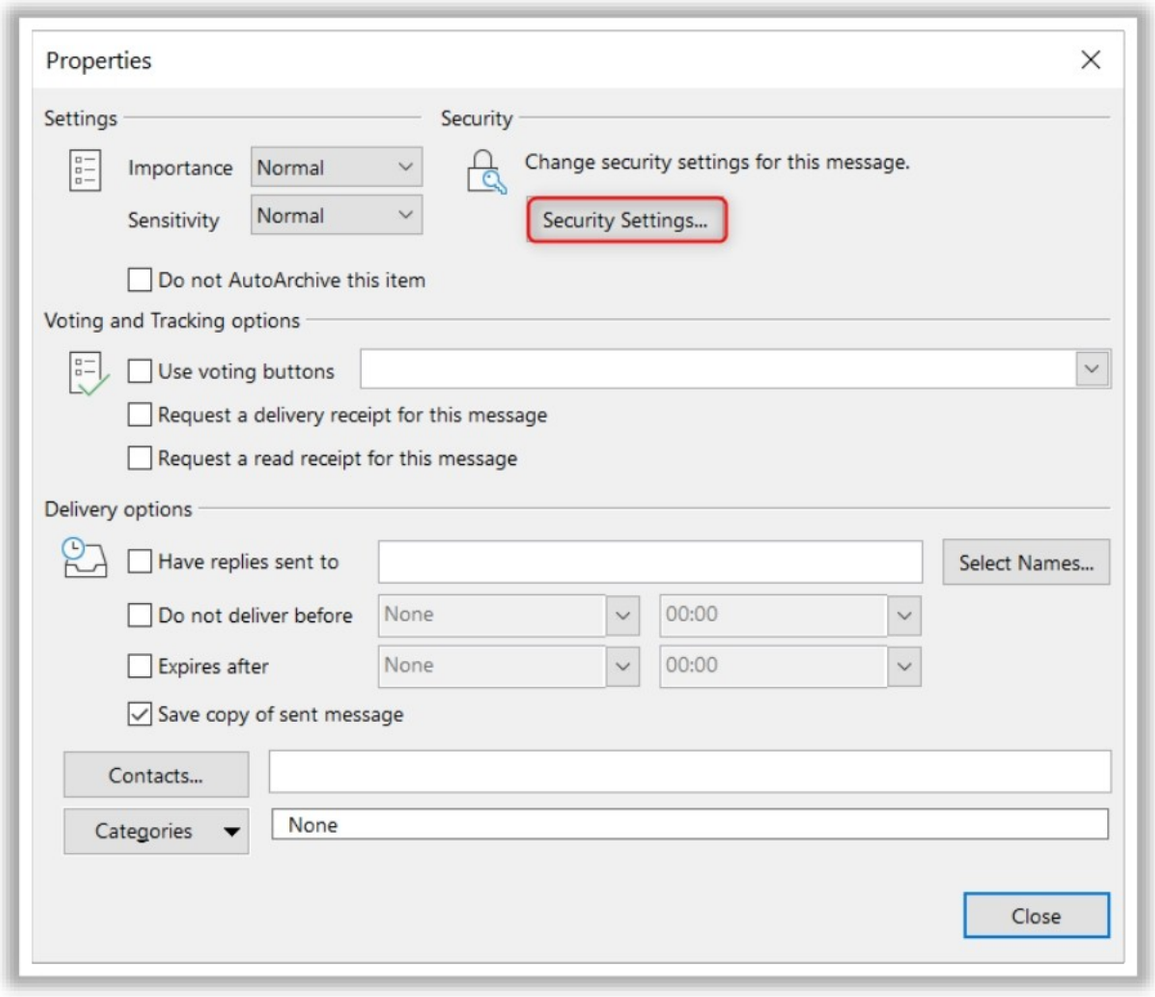


Figure 10.114: Selecting Security Settings in Properties Dialog box

- In the **Security Properties** dialog box, check the **Encrypt message contents and attachments** box and click **OK**.

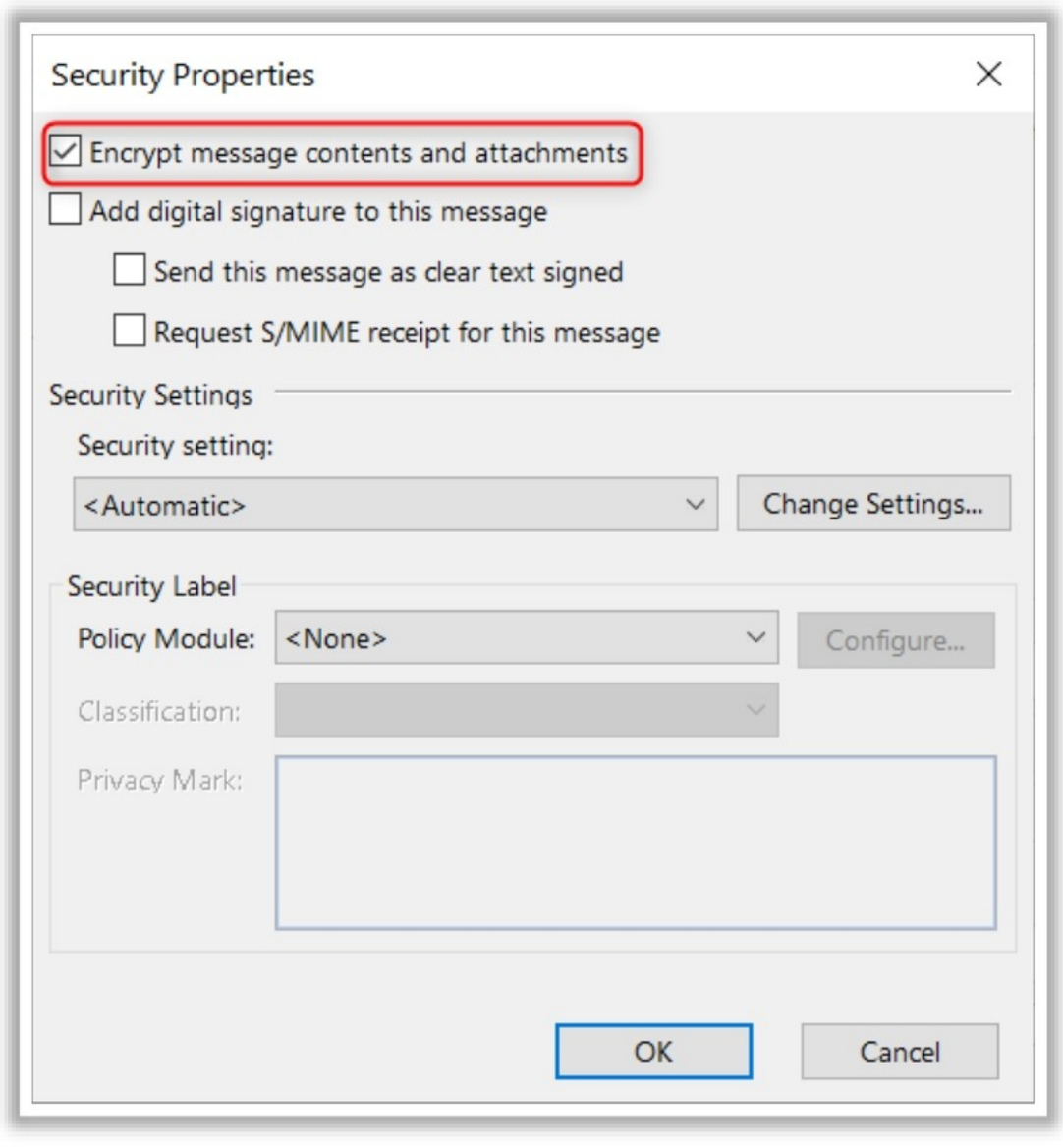


Figure 10.115: Choosing Encrypt Message Contents and Attachments in Security Properties Window

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Click **Close** on the **Properties** dialog box.
- Send the encrypted message.

Step 4: Encrypting all outgoing Outlook messages

Microsoft email account allows the encryption of all outgoing Outlook email messages. Steps to encrypt all outgoing messages are as follows:

- Navigate to **File** tab -> **Options** -> **Trust Center.**
- Click **Trust Center Settings** under **Microsoft Outlook Trust Center.**
- Select **Email Security** from the left pane, and then check the box for **Encrypt contents and attachments for outgoing messages**.

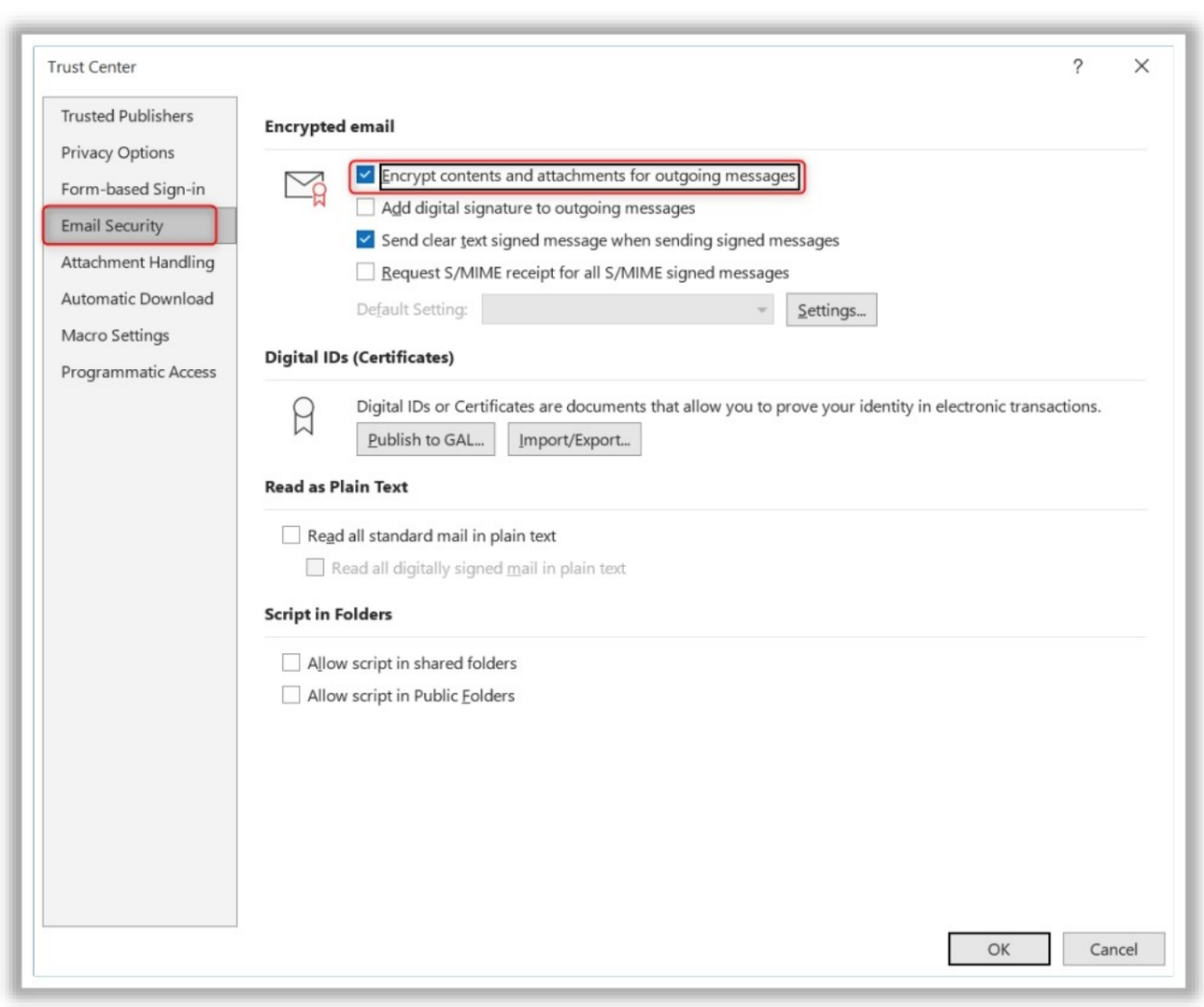


Figure 10.116: Encrypting All Outgoing Outlook messages

- Click **OK**, and then again click **OK.**

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Email Encryption: Gmail

Gmail, the email service offered by Google, is used in many organizations to send and receive emails. Google uses the standard method of Gmail TLS encryption. All messages going through Gmail be encrypted only when both sender's and receiver's email services support TLS (mostly all major mail providers support TLS). Besides offering the basic level of encryption, Gmail also supports S/MIME (secure/multipurpose Internet mail extensions) encryption. SecureGmail (Chrome extension), Firefox, etc. are some other ways of encryption in Gmail. However, these options are available only for paid G Suite Enterprise and G Suite Education accounts, and not for the free Gmail accounts.

Steps to Encrypt an Email Message Using S/MIME

S/MIME encrypts data in transit. Both the sender and receiver have to enable S/MIME for it to work. After enabling S/MIME, they share "keys" to identify each other. Now, S/MIME can be used to send encrypted email messages in the following manner:

- Compose a message.
- Add the name of the recipient to the **To** field.
- Click the **lock** icon located to the right of the recipient.
- Click on **View Details** if you want to change S/MIME settings or view the recipient's encryption level.
- Send the email message.

The S/MIME encryption level is displayed in three colors.

- **Green**: Email message is encrypted with S/MIME encryption.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Gray**: Email message is encrypted with TLS encryption.
- **Red**: No encryption. Avoid sending personal information until you have securely encrypted an email.

Steps to Encrypt Messages Using SecureGmail

SecureGmail is a Google Chrome extension by Streak. You can install it from the Chrome Web Store. Once this is done, to the Gmail page to activate it. It is activated if a **lock** is displayed next to the **Compose** button. Now, follow the steps given below to encrypt the email message.

- Click the **lock** button to compose the encrypted email.

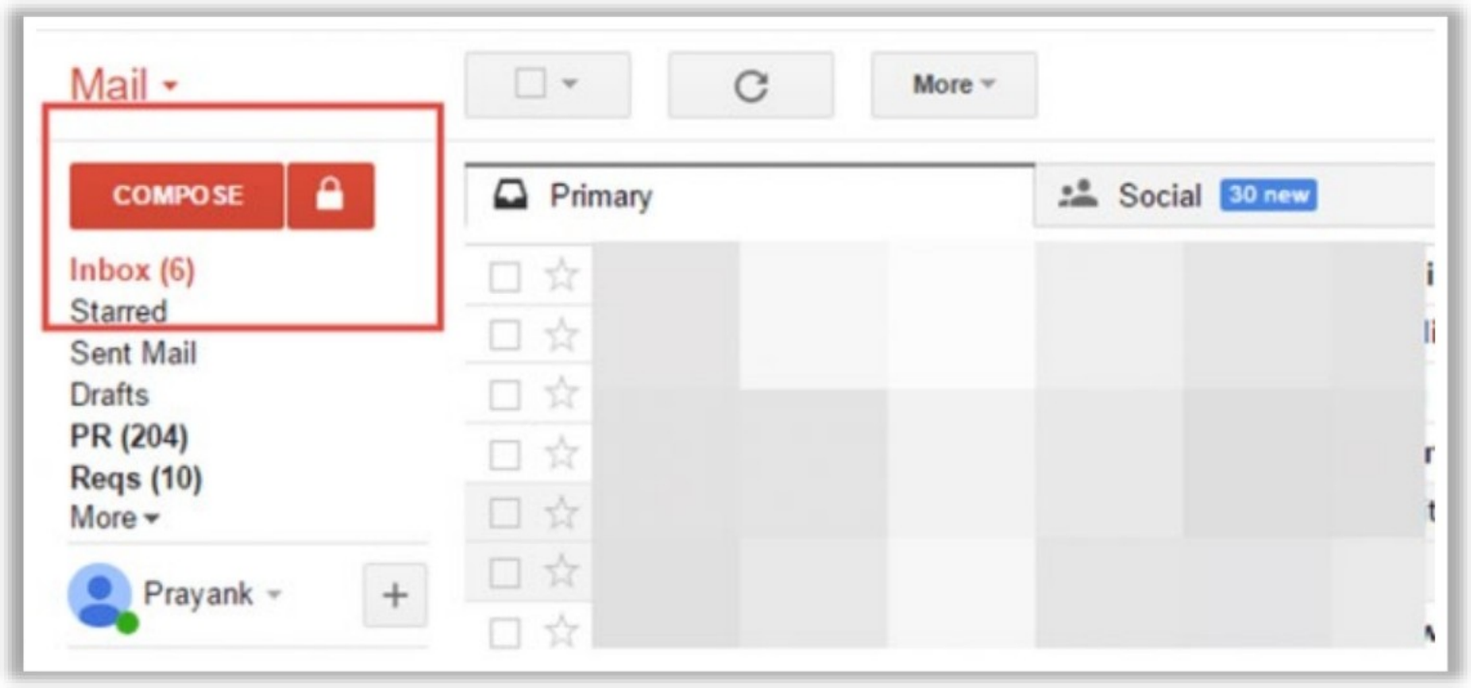


Figure 10.117: Email Composition

- Notice two changes: The header will display **Secured** with a lock symbol, and **Send** button will change to **Send Encrypted**.

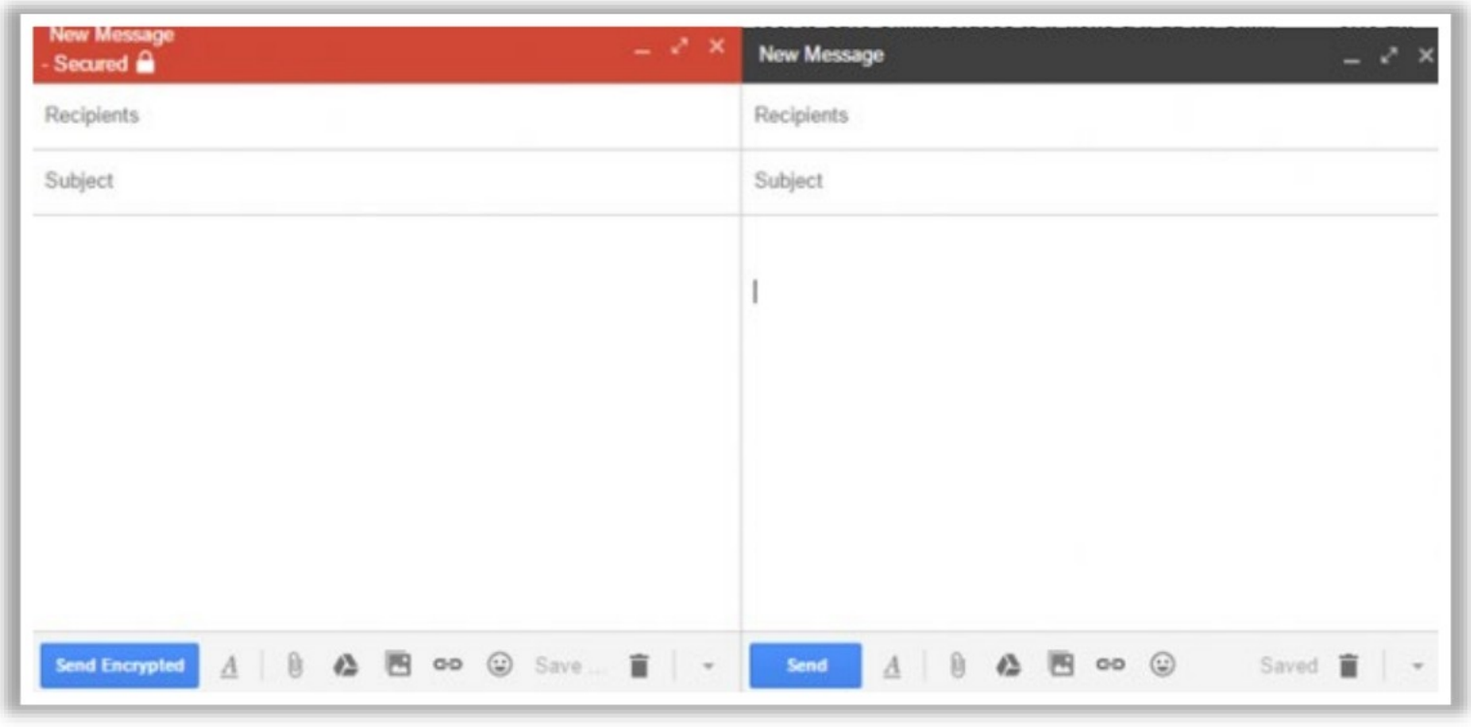


Figure 10.118: New Message - Secured

- Click the **Send Encrypted** button after composing the email.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Provide an **Encryption Password** and a **Password Hint** to decrypt the email at the recipient side.



Figure 10.119: Encrypt Message

- Click the **Encrypt & Send** button.
- Manually share the password with the recipient.

Steps to Encrypt Gmail Through Firefox

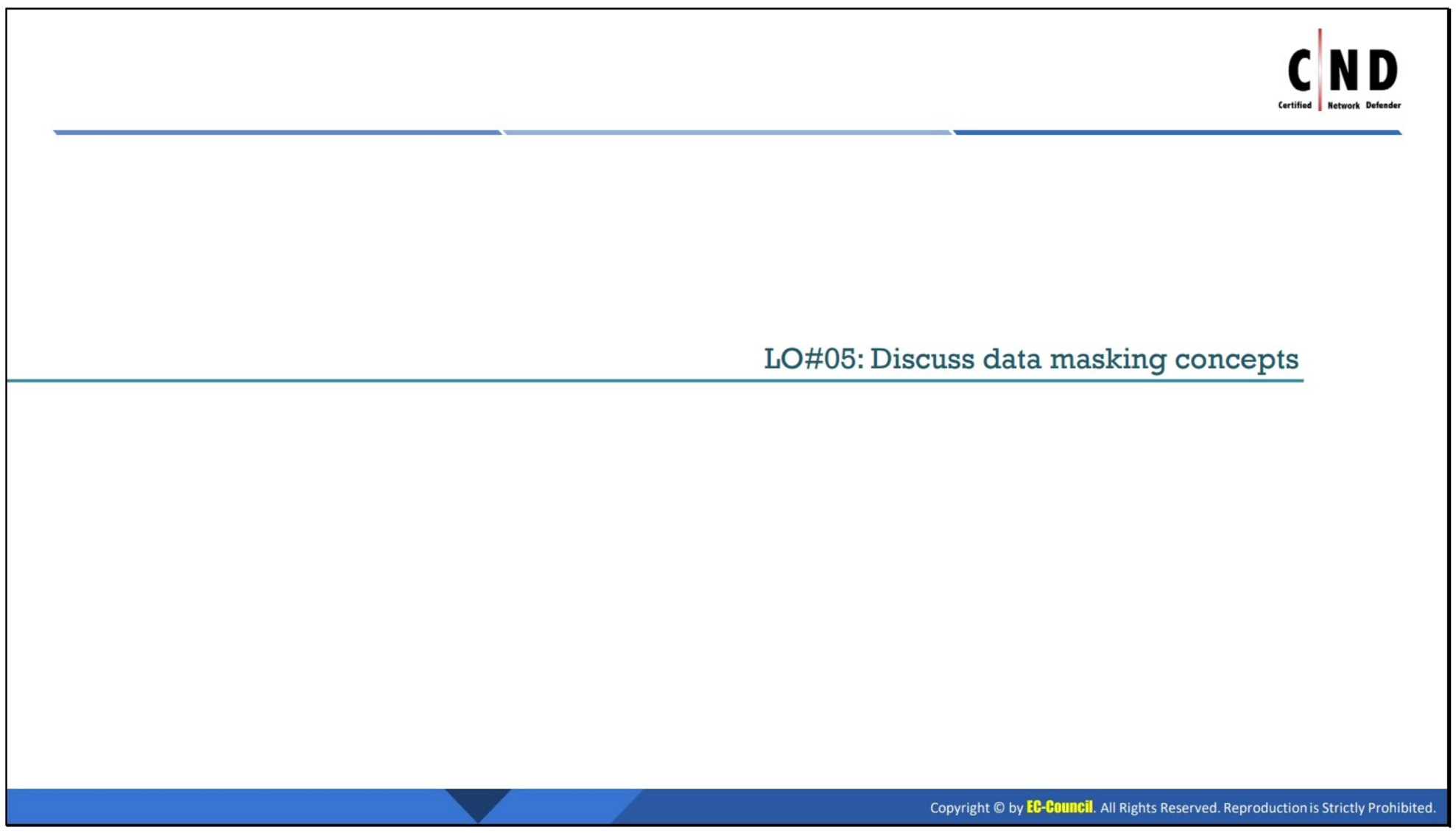
If Google Chrome is not the primary Internet browser in the system, you can still encrypt mails using Firefox. Add the **Encrypted Communications** Firefox extension and restart your browser to activate it.

- Compose an email.
- Right-click and select **Encrypt Communication**.
- Enter a password and select **OK**.

Steps to open the encrypted email by a recipient:

- You will need the **Encrypted Communications** plug-in.
- Right-click on the message and select **Decrypt Communication**.
- Enter the assigned password.

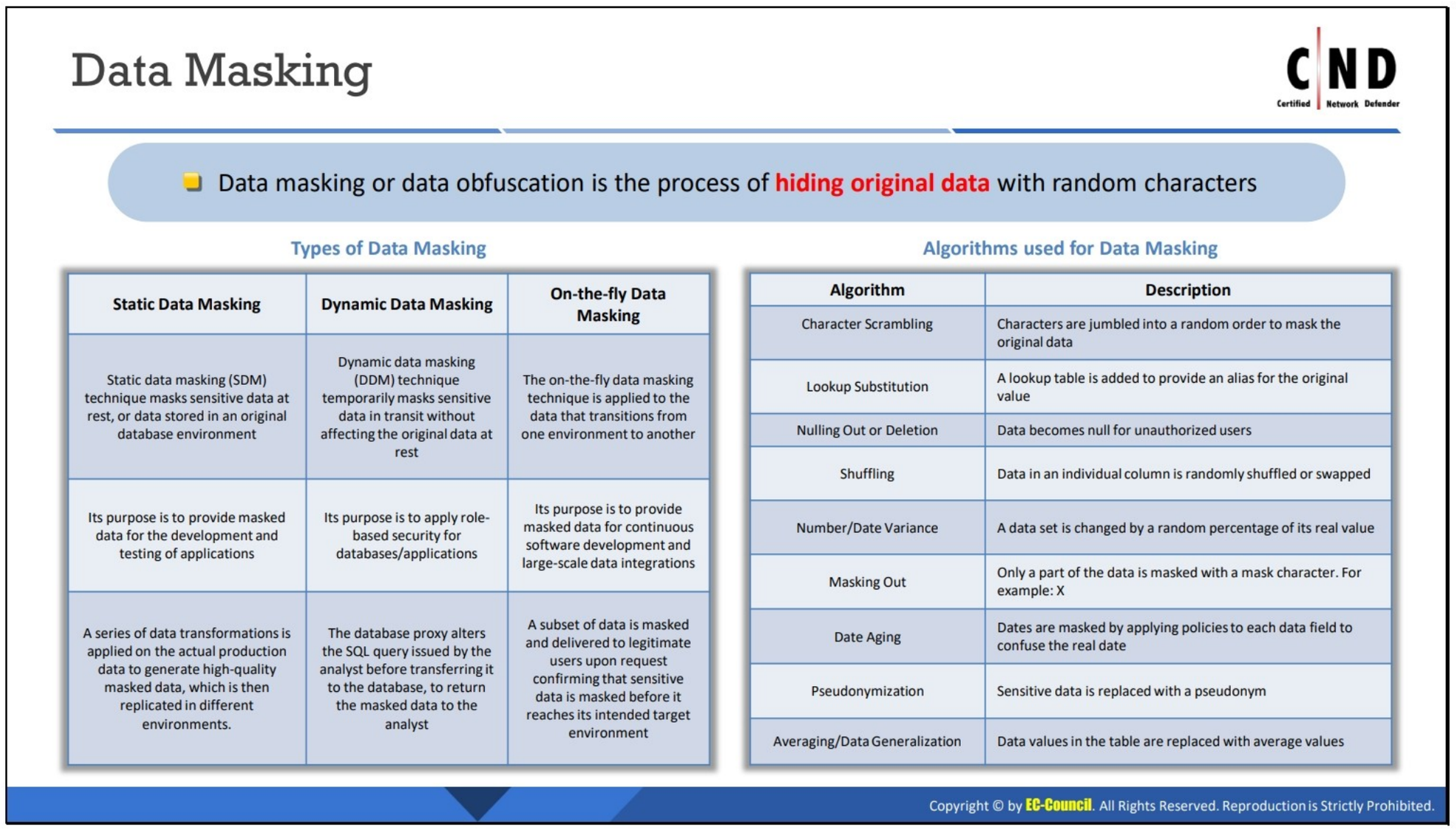
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



LO#05: Data Masking Concepts

The objective of this section is to explain various data masking techniques that can be used to secure sensitive data from prying eyes.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Data Masking

Data masking or data obfuscation is the process of hiding original data with random characters or other data. Its main purpose is to minimize unnecessary exposure of sensitive information like personally identifiable information (PII), protected health information (PHI), payment card information (PCI-DSS), and intellectual property (ITAR). It replaces vulnerable, or sensitive data with fictitious functional data that seems real, allowing it to be safely used in operations where original data is not required. In data masking, the basic format of the data remains the same, but its key values are changed. For example, a long card number is masked as follows:

2424 6789 4545 3421 will be masked as **2424 XXXX XXXX 3421**

Reasons to Include Data Masking in Data Security/Data Masking and Security

- **Protecting nonproduction data**

  In many organizations, multiple copies of production data are required for nonproduction purposes such as application development and testing, employee training, business analytics modeling, etc. Multiple copies of sensitive data increase their chances of going into malicious hands. While allowing the safe sharing of sensitive data, the data masking techniques also plays a vital role in securing these data sets and meeting compliance requirements without affecting business operations.

- **Protection against insider threats**

  Data masking allows employees to access the masked data instead of accessing the real production data to get their jobs done, which can mitigate the risk of a data breach from malicious insiders.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Protection against third parties**

  Data masking makes is safe to send personal identifiable data, payment card information, or PHI to third parties, such as market researchers.

- **Compliance with regulations**

  Data masking helps organizations comply with key regulations such as the general data protection regulation (GDPR) passed by the European Union to make personal more data secure.

Types of Data Masking

There are different types/strategies of data masking. To select a data masking type, consider the size of the organization, the location (cloud vs. on-premise), and the complexity of data you wish to secure. Data masking types include the following:

- **Static data masking (SDM)**

  SDM masks sensitive **data at rest**, or data stored in an original database environment. SDM is implemented to provide realistic data for the development and testing of applications. Realism is necessary as it helps development and testing teams to detect the defects in the early stages of a development cycle. The SDM also secures data for use in analytics and training, and facilitates compliance with standards and regulations.

  SDM applies a series of data transformations on the actual production data to generate high-quality masked data. Various approaches are used to perform SDM.

- **Statistical Data Masking**

  Certain alternatives to SDM, such as differential privacy method and DataSifter method, rely on the stochastic perturbations of data to preserve some statistical properties of the original data.

- **Dynamic data masking (DDM)**

  DDM temporarily masks sensitive **data in transit** without affecting the original **data at rest**. DDM is mainly used to provide role-based security for databases/applications, and it uses database and proxy approaches to mask a database. The database proxy alters an SQL query issued by the analyst before transferring it to the database so that the masked data is returned to the analyst.

- **On-the-fly data masking**

  Similar to DDM, on-the-fly data masking occurs on demand but for one record at a time. An extract transform load (ETL) process occurs wherever the data is masked within the memory of a given database application, which is helpful for agile companies targeting continuous delivery or continuous deployment practices.

Data masking and the cloud

There are different modes for creating test data and moving it from on-premises to the cloud, or among environments inside the cloud. If data is masked before being ingested into a cloud-native data repository, attackers would not gain anything from the stolen data following a breach. A few

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

cloud-native data services offer built-in masking tools that make the implementation of masking easier in the cloud.

Data Masking Algorithms

Some algorithms for implementing data masking to obscure confidential data are as follows:

- **Encryption**

  Different encryption algorithms are used to mask data. Users who have an authorized key can only access the data.

- **Character scrambling**

  Characters are jumbled into a random order to mask the original data. For example, an emp_id #123456 in a production data set will be masked as #425613.

- **Lookup substitution**

  A lookup table is added as an alias for the original value. It hides the authentic data to protect it from security breaches.

- **Nulling out or deletion**

  Data becomes null for unauthorized users. This technique only helps avoid the visibility of the data element.

- **Shuffling**

  Data in an individual column is randomly shuffled or swapped. The output set appears real but does not disclose any sensitive information.

- **Number and date variance**

  Number and date variance is helpful in financial and date fields. Each number/date in a data set is masked by a random percentage of its real value.

- **Masking out**

  Only a part of the data is masked with mask characters (for example, an X). This technique is mainly used to mask credit card details. For example, when an operator bills a customer's credit card for an item, they will see only the last four digits, while all other digits will be masked as XXXX XXXX XXXX 7685.

- **Date Aging**

  In this technique, dates are masked by applying policies to each data field to obfuscate the actual dates.

- **Pseudonymization**

  This approach involves substituting sensitive data with a pseudonym, effectively removing personal identifiers from data and replacing them with placeholder values.

- **Averaging/Data Generalization**

  In this technique, individual values within a table are replaced by their average values.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Data Masking Techniques

C|ND Certified Network Defender

- Data masking, also known as **data obfuscation or data anonymization**, is a technique used to protect sensitive data by replacing, hiding, or scrambling original data with fictitious or pseudonymous data while preserving the data's format and structure

Technique	Description	Example
Nulling out	Replace sensitive values with null	
Substitution	Replace sensitive values with fictional or masked data	Replacing real names with random names or replacing credit card numbers with fake numbers
Shuffling	Shuffle data within a column so that the original values are mixed up	Shuffling the order of birthdates in a dataset
Date shifting	Based on the data masking policy, it can either add or remove a date field with an acceptable range of dates	
Tokenization	Replace sensitive data with unique tokens or references that map back to the original data	Used for credit card numbers, Social Security numbers, or other identifiers
Format Preserving Encryption (FPE)	Encrypt sensitive data while preserving the original data format, such as length and character set	used for credit card numbers or other structured data
Hashing	Hash sensitive data to generate fixed-length strings	Hashing stored password

Data Masking Techniques



Data Masking Techniques

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Data Masking Techniques

Data masking, also known as data obfuscation or data anonymization, is a technique used to protect sensitive data by replacing, hiding, or scrambling original data with fictitious or pseudonymous data while preserving the data's format and structure.

- **Nulling out/nullifying:** Nullifying uses a null value to replace the actual values in the data column. The null value completely removes the data from the view. This type of deletion is easy to implement. However, the null column cannot be applied in queries or in analysis. Therefore, it can damage the data integrity and quality of the development and testing environment.
- **Substitution:** Substituting data is a method of masking data by replacing data with a different value. This method is highly effective in protecting data from data breaches, as it preserves the original look and feel of data.

  Substitution is more difficult to implement than scrambling, however, it can be used across multiple data types and offers a high level of security. For instance, credit card numbers may be replaced by numbers that meet card provider validation standards.

  While substitution is more difficult to implement than scrambling, it can be used across multiple data types and offers a high level of security. For instance, it can replace credit card numbers with numbers that meet card provider validation rules.
- **Shuffling:** It is like a substitute, but it shuffles the data in a random order using the same masking data column. For example, shuffle employee names columns across multiple employee records. The output data does not reveal any information, it ensures it is accurate. However, if one tries to know the shuffling algorithm, shuffled data is prone to reverse engineering.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

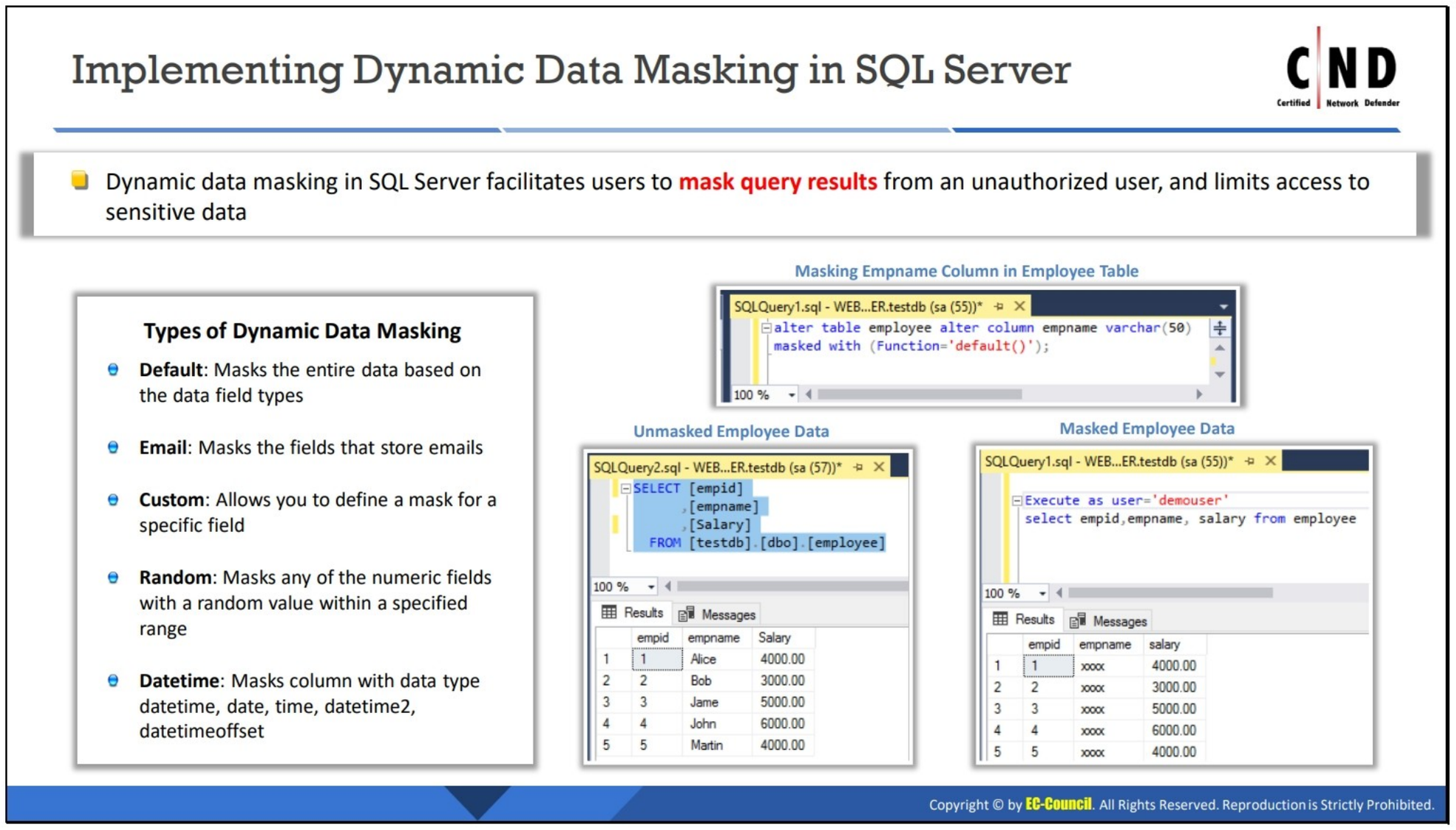
It is used to shuffle personal information such as birthdates, name, etc.

- **Data shifting:** Data shifting can add dates based on the data shifted within the policy that is implemented with an acceptable range of dates. This randomly relocates the position of each character in the cipher text based on key value.
- **Data tokenization:** Data tokenization is the process of adding unique identification symbols to the raw data. This is an exchange of sensitive data with non-sensitive data which are called tokens to avoid data breaches. This data maps back to the original data.

  This technique is mainly used in protecting unique identities and numbers such as credit cards, identity cards, and other social identity proofs.
- **Format preserving encryption (FPE):** It is an algorithm that preserves the format of the data or information such as length and character set while is being encrypted. This ensures that the existing functions of the data are not harmed or lost.

  FPE is also used to protect phone numbers, banking cards, restructuring databases, etc.
- **Hashing:** Hashing is the process of generating fixed size length output from the input variables. This is used to produce digital signatures and message authentication codes. This can be applied in protecting and storing passwords.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Implementing Dynamic Data Masking in SQL Server

Microsoft SQL Server 2019 has a built-in security feature called DDM. It hides query results from an unauthorized user and limits access to sensitive data. Only privileged users can view the unmasked data. It provides the following features:

Features

- A configurable masking policy using simple T-SQL commands.
- On-the-fly obfuscation of data in query results while the underlying data in a database remains intact.
- Database operations are not affected, and the database is not physically changed.
- Flexibility to define a set of privileged SQL users or roles for unmasked access.

Types of Masks

SQL Server 2019 provides four types of masks: default, email, custom, and random.

- **Default mask**

  This mask the entire data based on the data field types.

  - For masking string types such as char, nchar, varchar, nvarchar, text, and ntext, XXXX or a few Xs are used in case the size of the field is less than 4.
  - For masking numeric data types such as int, decimal, float, etc., “0” value is used.
  - For masking binary data types such as binary, varbinary, or image, a single byte of ASCII value 0 is used

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- For masking date and time data types such as date, datetime2, datetime, datetimeoffset, smalldatetime, and time, a 01.01.1900 00:00:00.0000000 format is used.

  Example: Phone# varchar(12) MASKED WITH (FUNCTION = 'default()') NULL

- **Email mask**

  This masks the fields that store emails. This function exposes the first letter, @, and a constant suffix ".com." For example, aXXXXXX@XXXX.com.

  Example: Email varchar(100) MASKED WITH (FUNCTION = 'email()') NULL

- **Custom mask**

  Custom Mask enables you to define a mask for a specific field. This function masks the entire data except for the first and last letters. For example, prefix, mask, and suffix.

  Example: FirstName varchar(100) MASKED WITH (FUNCTION = 'partial(prefix,[padding],suffix)') NULL

- **Random mask**

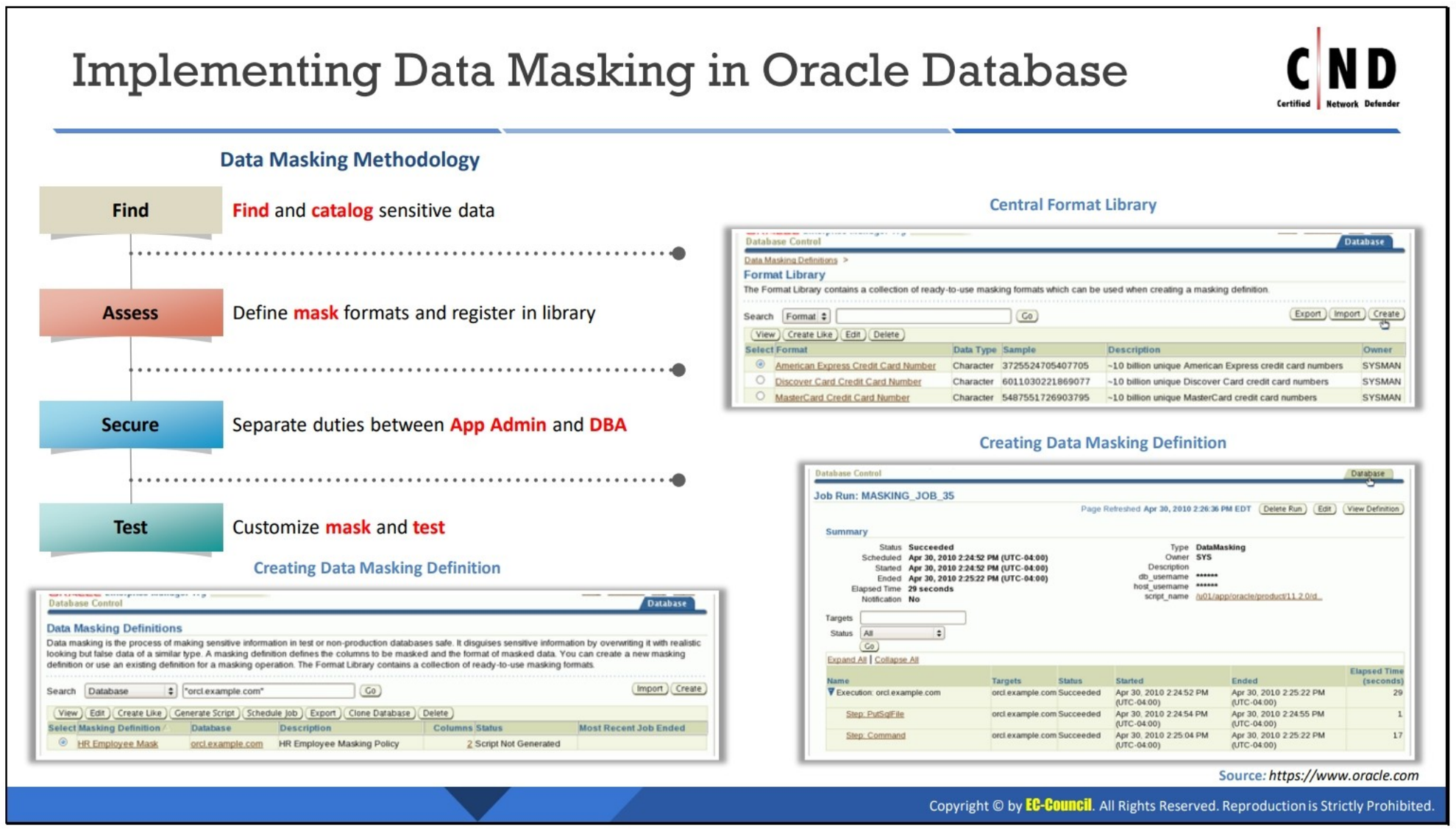
  This masks any of the numeric fields with a random value within a specified range.

  Example: Account_Number bigint MASKED WITH (FUNCTION = 'random([start range], [end range])')

- **Datetime**: Masks column with data type datetime, date, time, datetime2, datetimeoffset

  Example: ALTER COLUMN Birthday ADD MASKED WITH (FUNCTION = 'datetime("Y")')

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Implementing Data Masking in Oracle Database

Source: https://www.oracle.com

A comprehensive four-step approach is developed by Oracle to implement data masking via the Oracle data masking pack: find, access, secure, and test (FAST). These steps are:

Find

Carried out by business or security analysts, this step comprises identifying and cataloging sensitive or regulated data across the organization. Organizations, with the help of the data masking pack, and the data discovery and modeling capabilities in Oracle Enterprise Manager, can define data pattern search criteria, which will allow the network defender to find the sensitive elements.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

For example, define data patterns such as 15 or 16 digits for credit card numbers or nine-digit formatted US social security numbers.

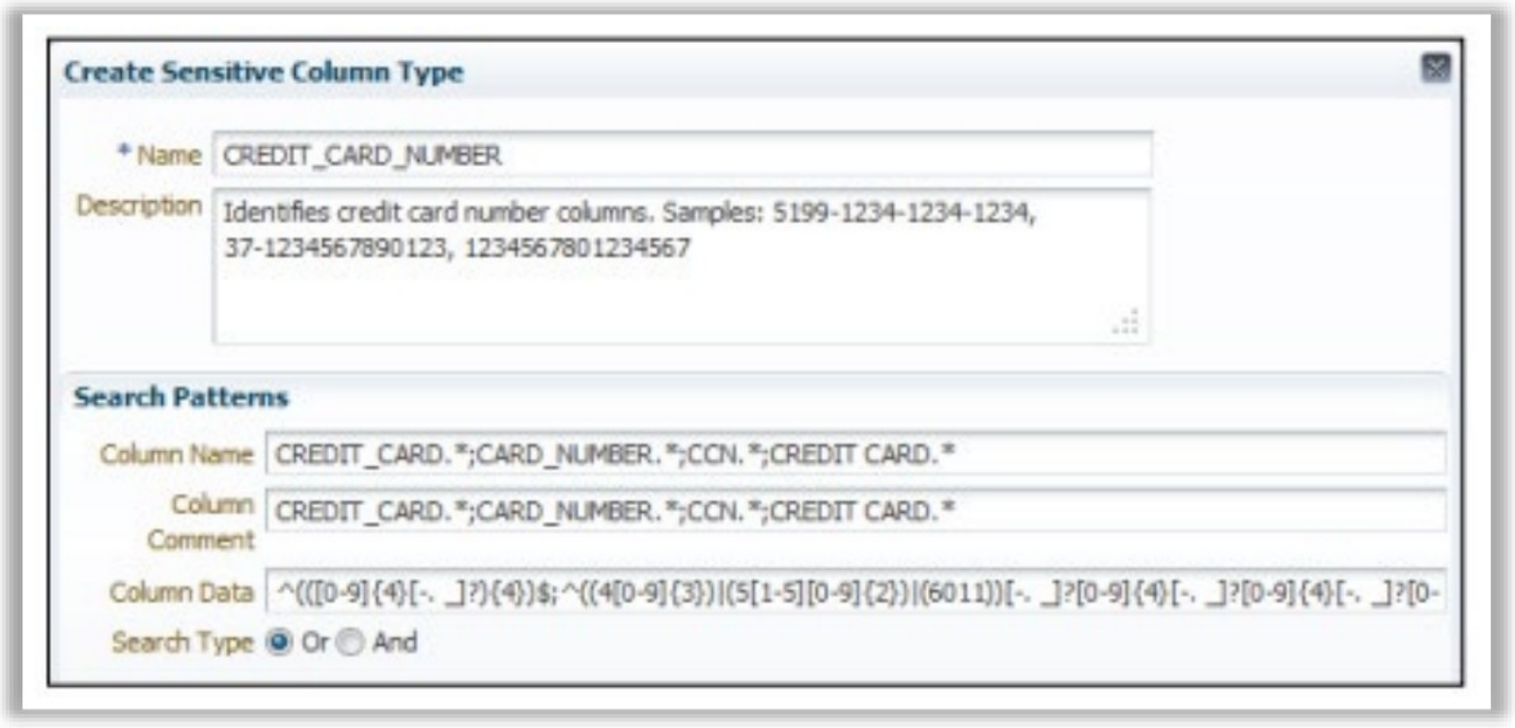


Figure 10.120: Screenshot of Create Sensitive Column Type

Sensitive Column Type definition

Once the sensitive elements are defined, the system administrator schedules a discovery job in Enterprise Manager, which will introspect the concerned database application.

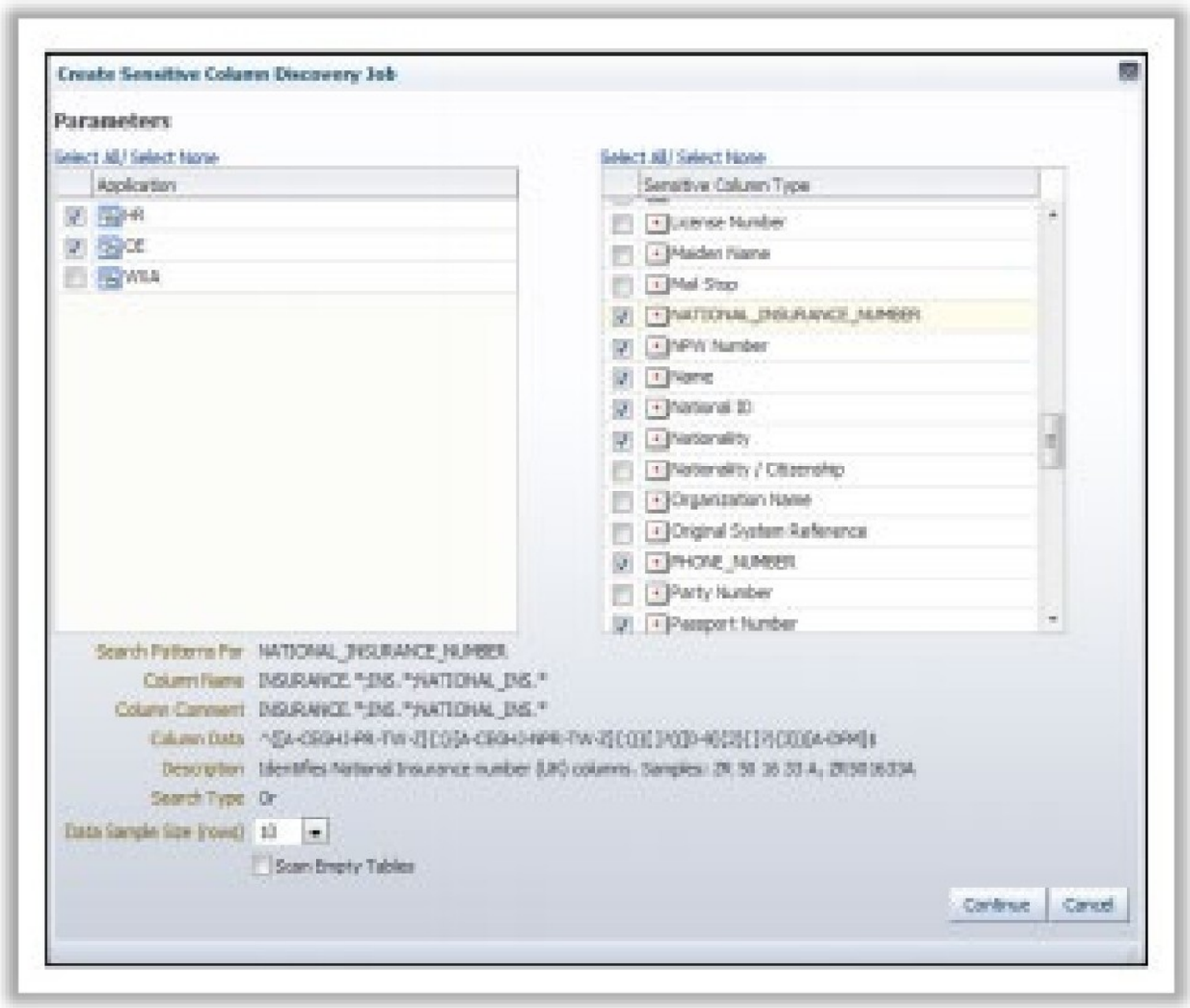


Figure 10.121: Screenshot of Create Sensitive Column Discovery Job

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Sensitive Column Discovery

The search results allow the system administrator to designate the column as sensitive for inclusion in the masking process.

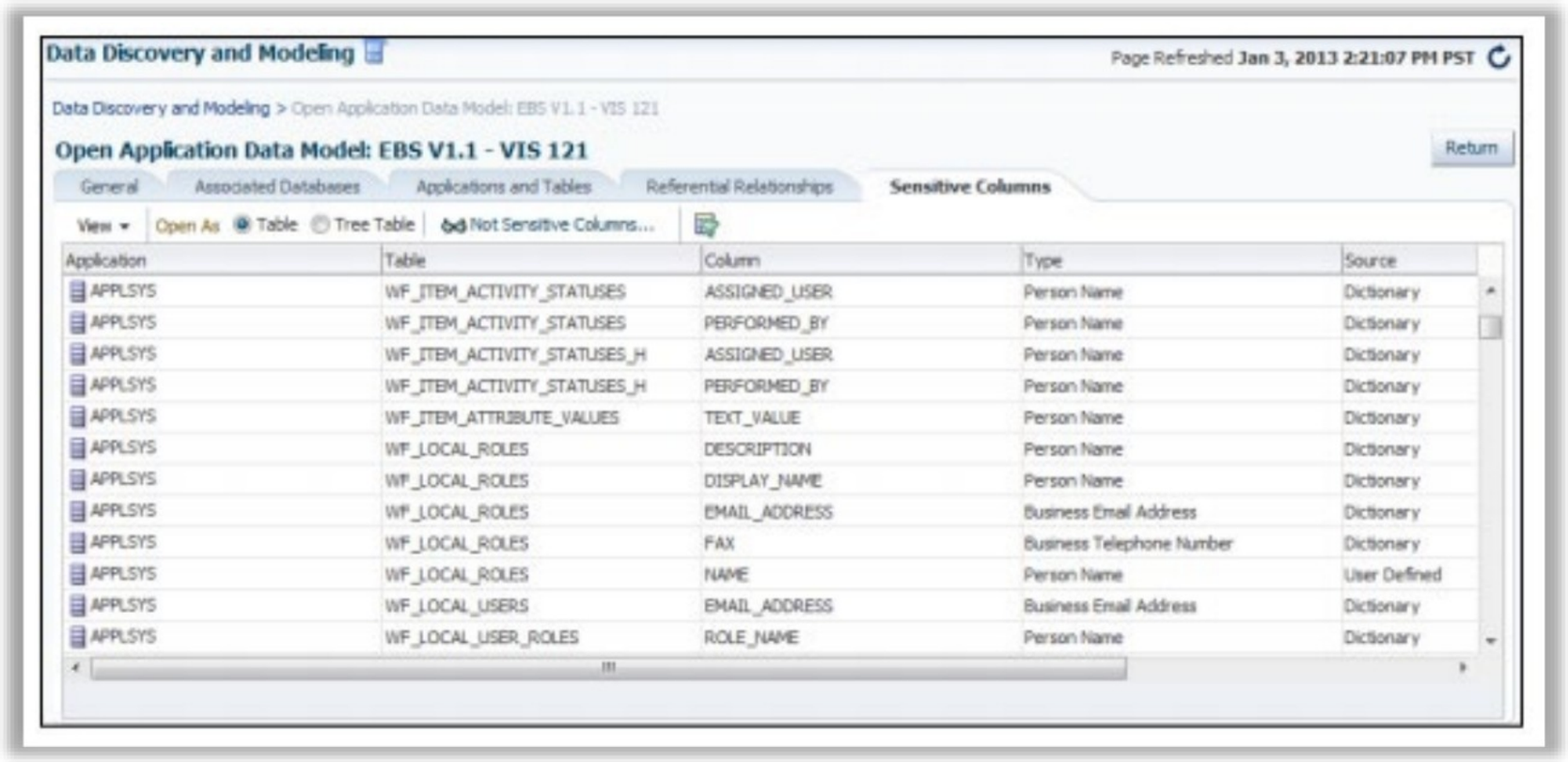


Figure 10.122: E-Business Suite Template Pre-defined Sensitive Columns

Assess

Carried out by developers or DBAs in conjunction with business or security analysts, this step identifies the masking algorithms that represent the optimal techniques to replace the original sensitive data.

Organizations, by leveraging the Format Library in Oracle Data Masking, can apply data privacy rules to sensitive data in the organization's databases, and ensure consistent compliance with regulations. If needed, organizations can create their own mask formats.



Figure 10.123: Central Format Library

Secure

Carried out by security administrators, this step executes the masking process to replace all sensitive data. Before this step, the administrators of a production environment choose whether to clone the production environment into a restricted location outside production and mask, or mask at source. Once this is finished and the masking is verified, the DBA handovers the environment to the application testers.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Test

Carried out by production users, this step executes the application processes to test whether the resulting masked data can be turned over to other nonproduction users. If further tweaking is needed for masking, the DBA restores the database to the pre-masked state, fixes the masking algorithms, and re-executes the masking routine.

The Oracle Enterprise Manager's Application Quality Management (AQM) solutions provide testing for all tiers of the application stack, which can help identify application quality and performance issues before deployment.

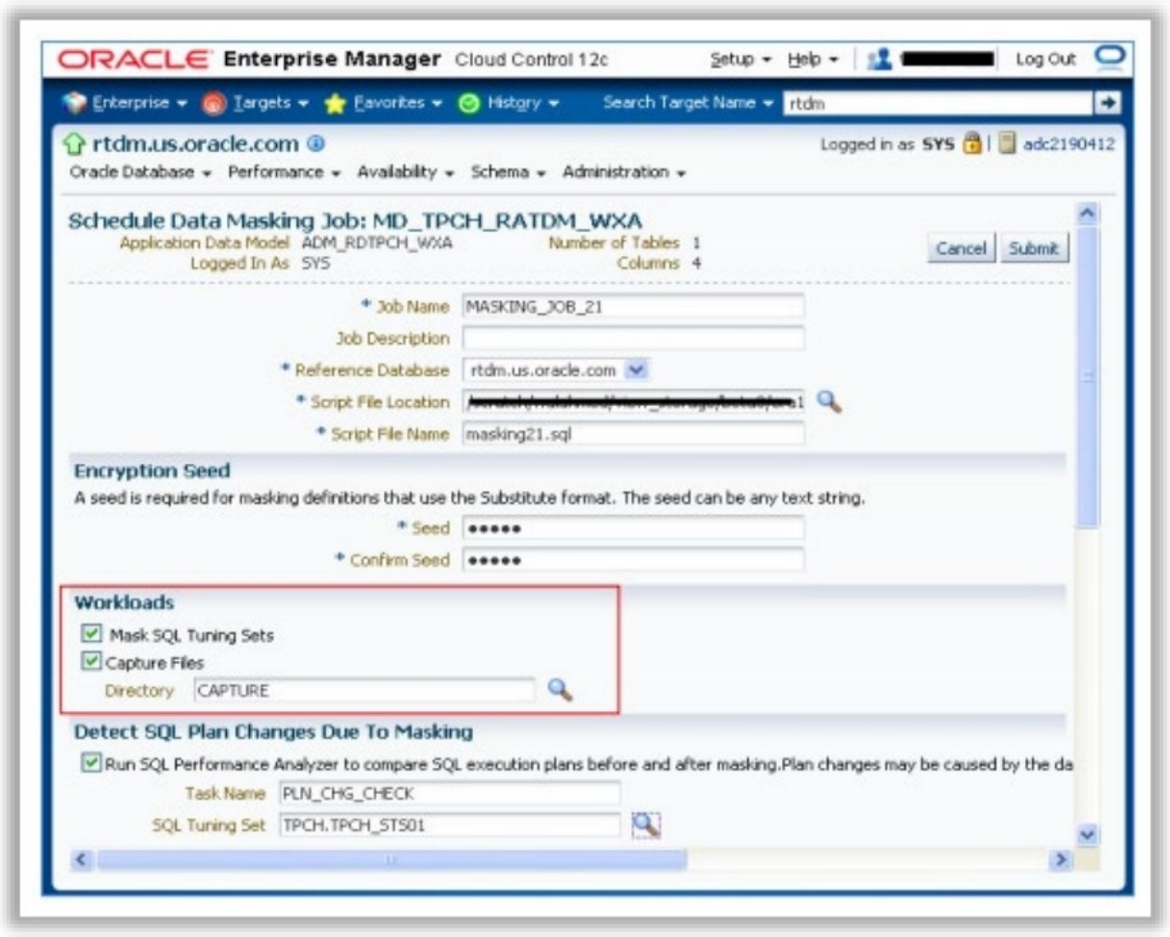
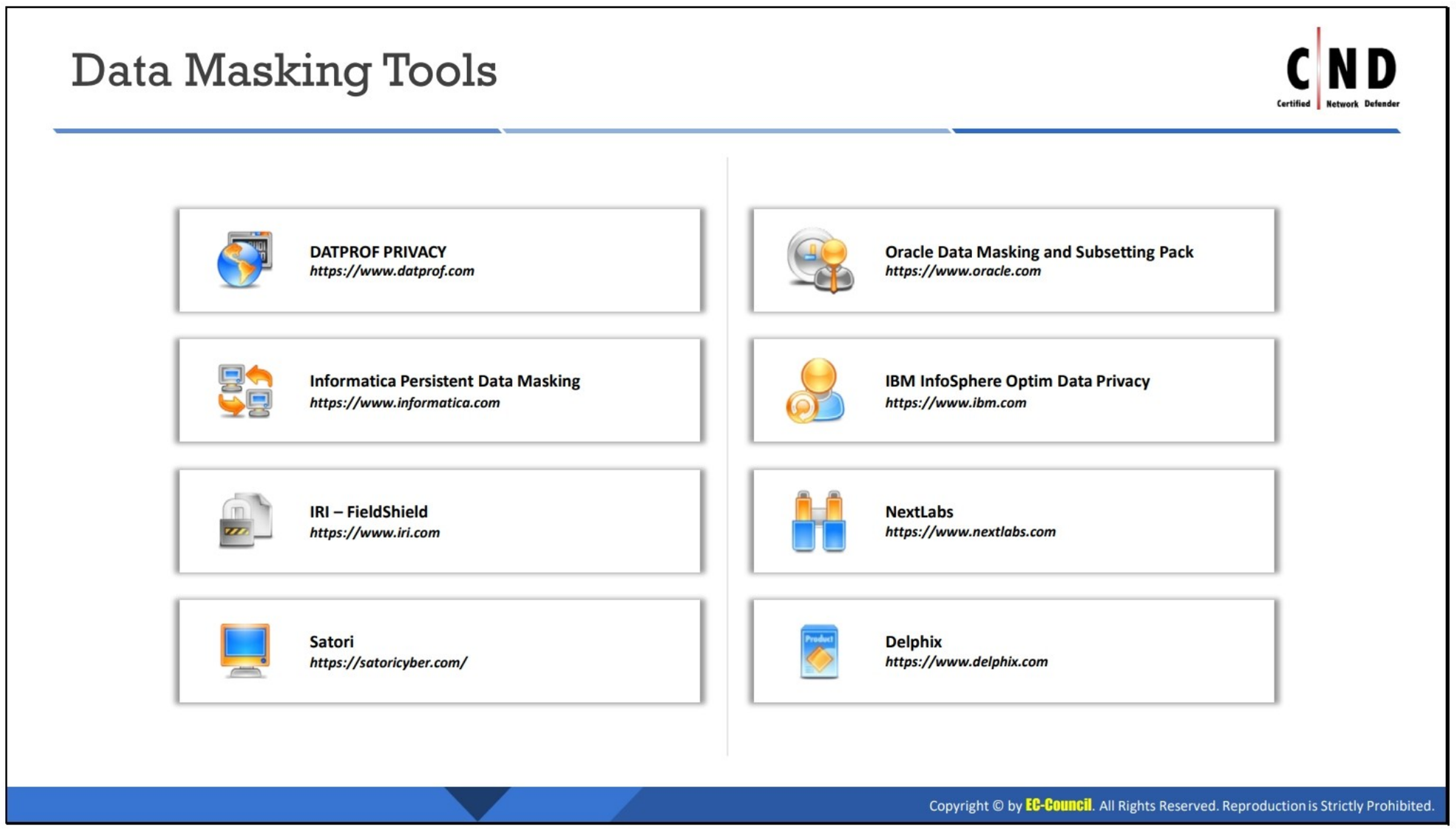


Figure 10.124: Real Application Testing Integration with Data Masking

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Data Masking Tools

Data masking tools avoid any misuse of complex information and eliminate complex data with false data. The most common tools for masking data for small-, large-, and mid-sized enterprises are as follows:

Datprof Privacy

Source: www.datprof.com

DATPROF Privacy masks production data to protect all your customer data, but software teams can still use the representative test data. It preserves the data characteristics and facilitates high performance on large data sets. It is consistent over multiple applications and databases.

Oracle Data Masking and Subsetting Pack

Source: www.oracle.com

Oracle data masking and subsetting helps database customers improve security, accelerate compliance, and reduce IT costs by sanitizing copies of production data for testing, development, and other activities, and by easily discarding unnecessary data.

Delphix

Source: www.delphix.com

Delphix provides irreversible masking, so data cannot be restored to an unsafe state. It is consistent and preserves the referential integrity of data across sources. It stays compliant with regulations and meets cloud mandates with less risk.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Informatica Persistent Data Masking

Source: www.informatica.com

Informatica Persistent Data Masking protects data by de-sensitizing and de-identifying sensitive data. It pseudonymizes data for privacy compliance and analytics.

It shields confidential data such as credit card numbers, addresses, and phone numbers from unintended exposure by creating realistic, de-identified data that can be safely shared internally or externally. It also allows you to reduce the risk of data breaches in nonproduction environments, produce higher-quality test data and streamline development projects, and ensure compliance with data privacy mandates and regulations.

IBM InfoSphere Optim Data Privacy

Source: www.ibm.com

IBM InfoSphere® Optim™ Data Privacy provides capabilities to mask sensitive data across nonproduction environments such as development, testing, QA, or training. To protect confidential data, it offers a variety of transformation techniques that substitute sensitive information with realistic, fully functional masked data. Examples of the masking techniques include substrings, arithmetic expressions, random or sequential number generation, date aging, and concatenation. The contextually accurate masking capabilities help masked data retain a format that is similar to the original information.

Satori

Source: www.satoricyber.com

Satori provides a data security solution that is implemented between users and data repositories. It enables users to automatically categorize and manage access to confidential information without altering their data or affecting their users.

IRI – FieldShield

Source: www.iri.com

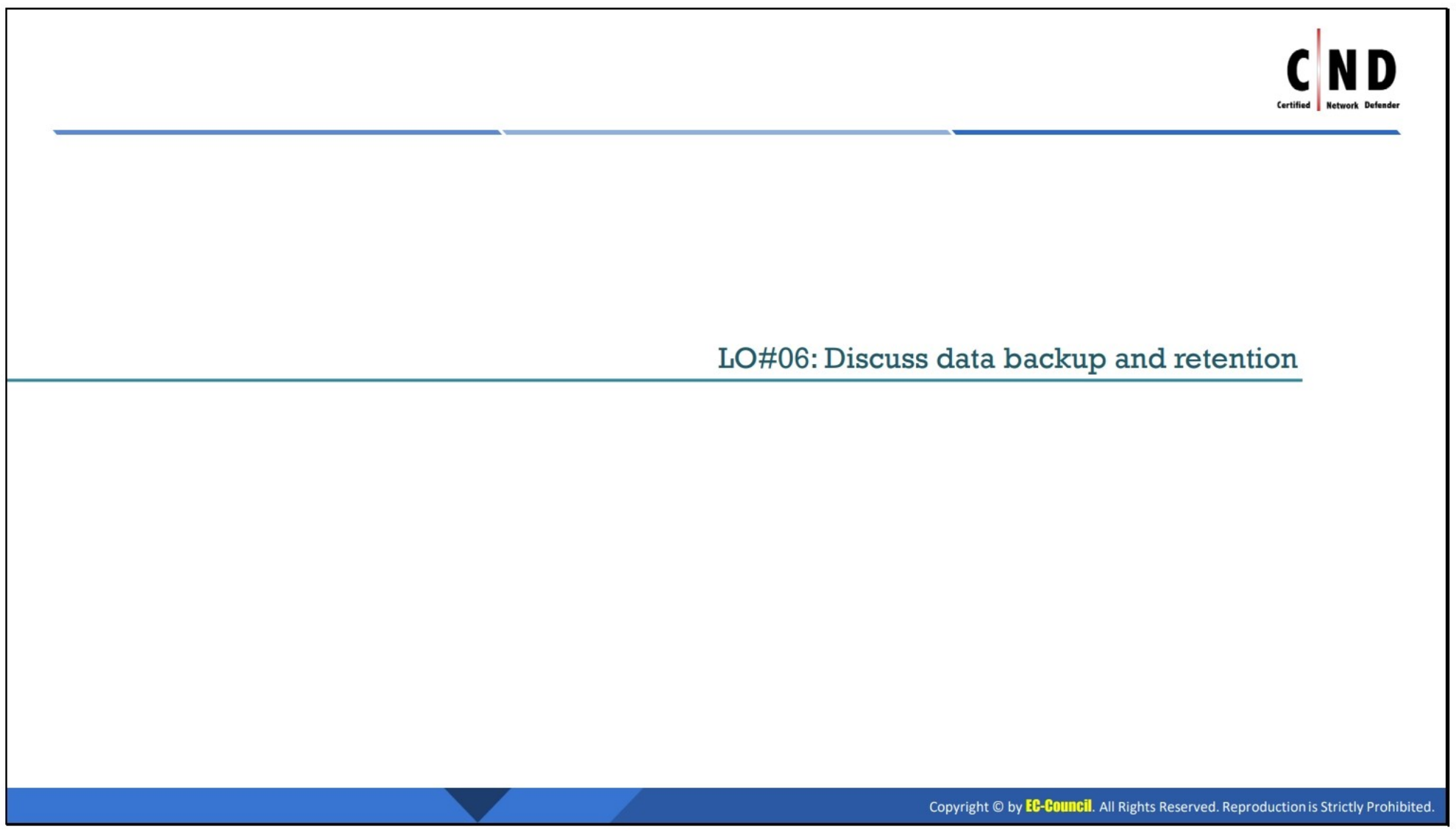
FieldShield nullifies data breaches by masking PII in DBs and files. It de-identifies data subject to CIPSEA, DPA, FERPA, GDPR, GLBA, HIPAA, PCI, POPI, etc. It also helps you verify compliance via XML audit logs and re-identification risk scores.

NextLabs

Source: www.nextlabs.com

NextLabs secures all business-critical data and applications using its dynamic authorization technology with attribute-based access control (ABAC). It identifies and classifies sensitive data, and applies digital rights to always ensure a secure collaboration.

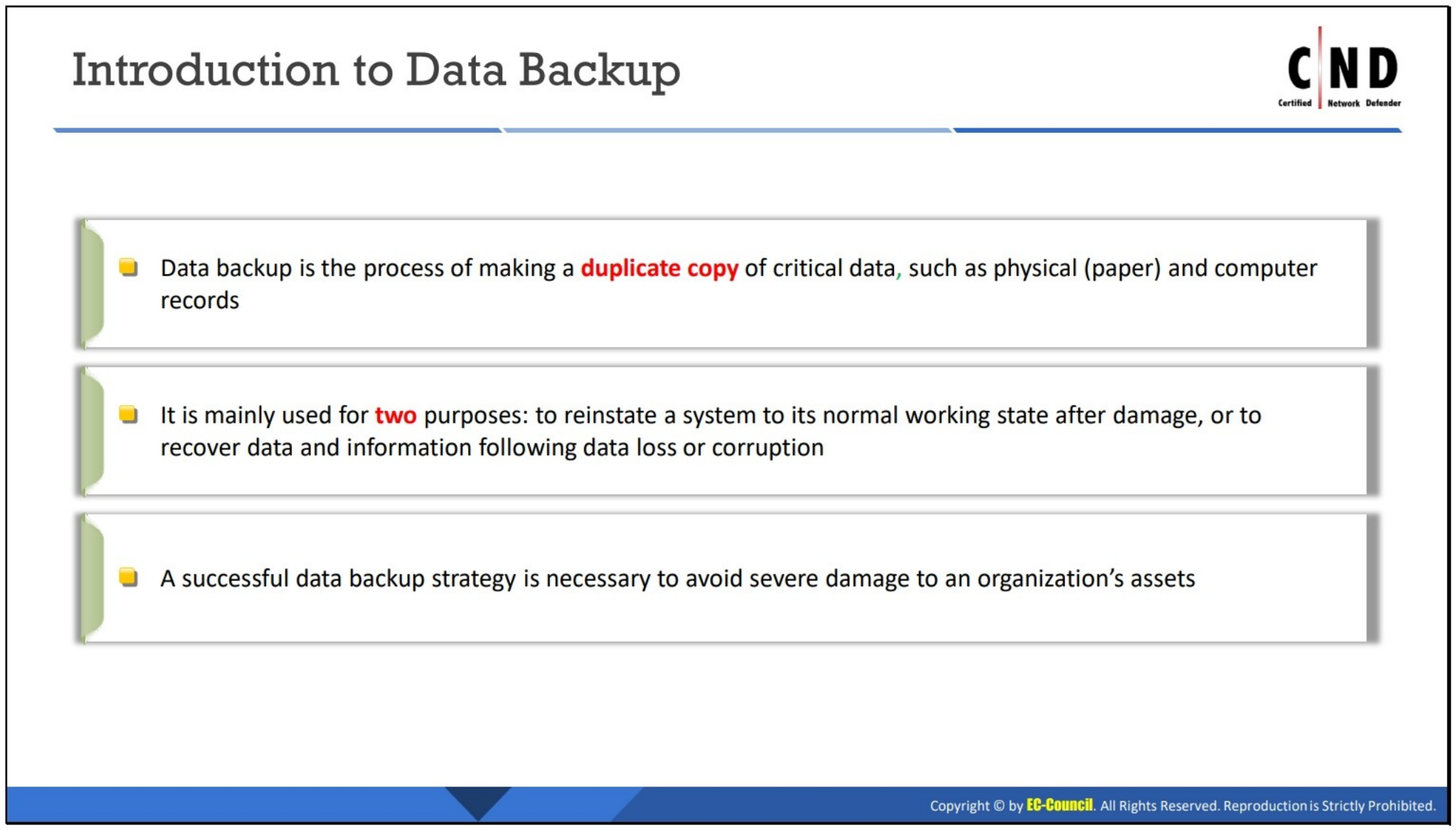
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



LO#06: Data Backup and Retention

Data loss is a major risk facing organizations today. Loss of critical data can result in a lot of damage to the organization. Any organization that encounters a critical data loss has a higher probability of facing serious issues later. Therefore, you should have a strong data backup and retention plan in place to deal with such incidents. The objective of this section is to explain the concept of data backup and retention.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Introduction to Data Backup

Data backup is the process of copying or storing important data. A backup copy will help you restore the original data when data is lost or corrupted. Backup is a mandatory process for all organizations. The process of retrieving lost files from a backup is known as restoring or recovery of files.

The main idea behind data backup is to protect data and information, and recover the same after data loss. Data backup is mainly used for two purposes: to reinstate a system to its normal working state after damage, or to recover data and information following data loss or corruption.

Data loss in an organization affects its finances, customer relationship, and company data. Data loss in personal computers may lead to the loss of personal files, images, and other important documents saved in the system.

Reasons for Data Loss

- **Human error**: Deletion of data purposefully or accidently, misplacement of data storage devices, and errors in administering databases.
- **Crimes**: Stealing or making modifications to critical data in an organization.
- **Natural causes**: Power failures, sudden software changes, or hardware damages.
- **Natural disaster**: Floods, earthquakes, fire, etc.

Benefits of Performing a Data Backup

- It offers access to critical data even in the event of a disaster, ensuring peace of mind in a workplace.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Backup of critical data prevents an organization from losing its business. It also helps them retrieve data anytime.
- Data recovery helps organizations recover lost data and ensure business continuity.

It is recommended that every organization performs a data backup on a regular schedule to run their business successfully and efficiently.

To avoid severe damage to an organization's assets, it is important to design a strategy for a successful data backup process. Going forward, this data backup strategy can act as a blue print while working on the data backup process for the entire organization. Certain companies also create a data backup policy that is required while implementing a backup strategy.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

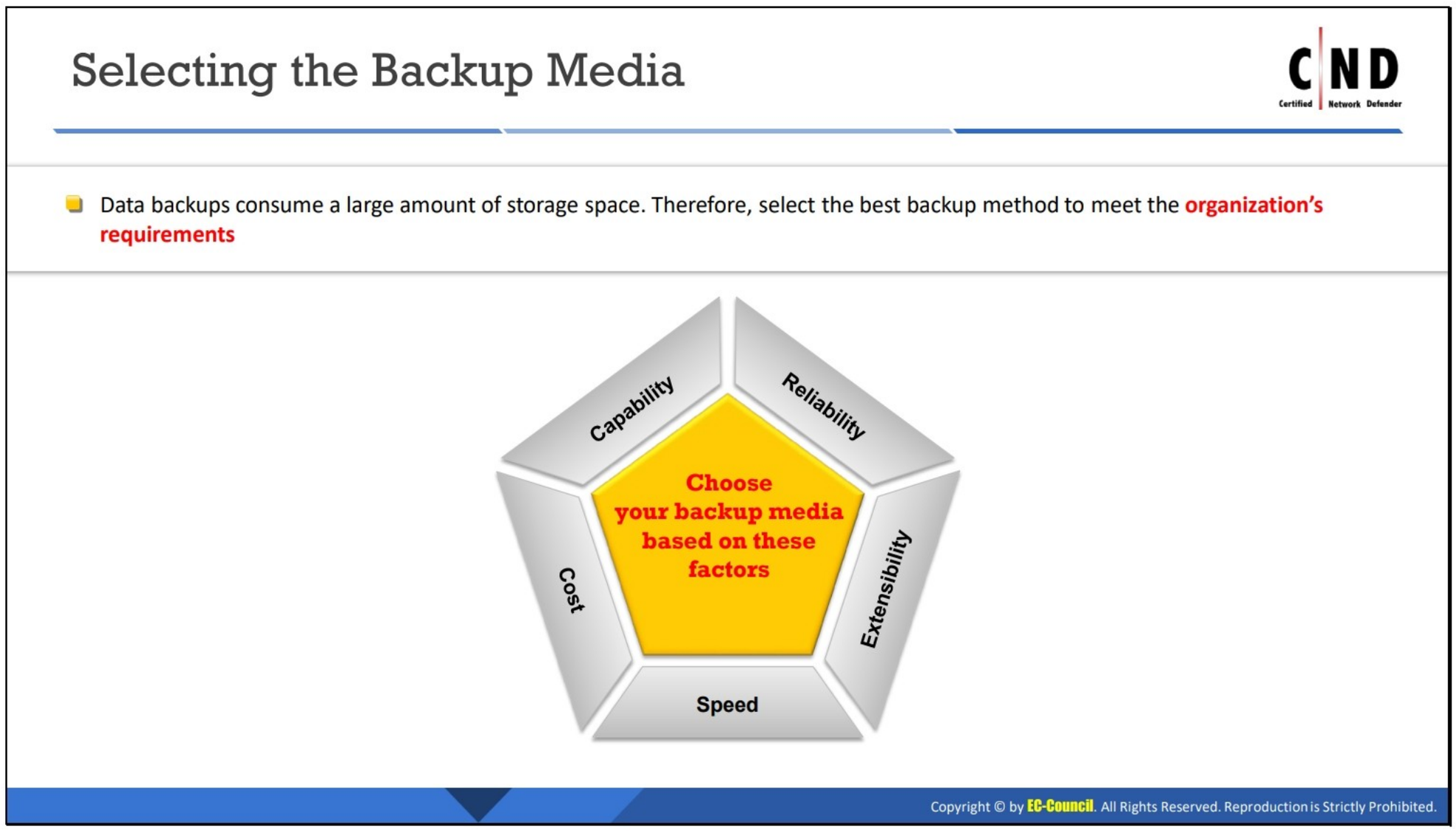


Data Backup Strategy/Plan

An ideal backup strategy includes steps ranging from selecting the right data to conducting a test data restoration drill. Although the backup strategy might differ among organizations, it is important to consider the following features before drafting a backup strategy:

- The backup strategy should have a data recovery feature from any external device. These devices may include servers, host machines, laptops, etc.
- If the data loss is because of a natural disaster, the backup strategy should not be restricted to only a certain number of incidents. The strategy should also cover the methods for recovering the data after a natural disaster.
- The strategy should include the steps to recover data at the earliest.
- The lower the cost for data recovery, the more the financial benefit to the organization.
- Auto recovery options should be included in the backup strategy as well, as they reduce the chances of human error during the recovery process.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Selecting the Backup Media

Choosing the best backup media is a common concern within most organizations. The selection of a wrong media device can lead to a segregation of data across different media devices. With a carefully considered plan, selecting an appropriate media will enable a better level of data backup.

Once the data is identified, it is important to choose an appropriate backup media to store the data. Backup media selection depends on the type and amount of data in the backup. At times, data backup consumes a large amount of space; consequently, an increased attention is necessary to select the best backup media for a situation, and to fulfill the organizational needs.

Choosing the best backup media is based on the following factors:

- **Cost**: Organization should have backup storage mediums that best fit their budget. The backup media should have more storage space than the data it will contain.
- **Reliability**: Organizations must be able to rely on the data stored on the backup media without fail. Organizations must select a media that is reliable and not susceptible to damage or loss.
- **Speed**: Organizations should select backup mediums which require reduced number of human interactions during the backup process. Speed becomes a concern if the backup process cannot be completed when a machine is idle.
- **Availability**: The unavailability of the backup medium could be an issue following data loss or data corruption. Organizations should decide on a medium that is always available.
- **Usability**: Organizations should select a media that is easy to use. An easy media type has a greater flexibility during the backup process.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Examples of Data Backup Media Devices

Media	Capacity	Advantages	Disadvantages	Illustrations
Optical disks (CD, DVD, Blu-ray)	~200 GB	• Affordable, easy to store and transport	• Several manual disk swaps may be required because of the limited data capacity • Recording and verifying a backup is slow	
Portable hard drives/USB flash drives	No limit	• Relatively higher storage capacity than optical disks • Ideal for the home or small offices • Faster recording of backups	• More expensive than DVD backups	
Tape drives	No limit	• Media for enterprise-level backups • Easy to store and transport	• Expensive	

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Examples of Data Backup Media Devices (Cont'd)

Media	Capacity	Advantages	Disadvantages	Illustrations
Network Drive	No limit	• Offers storage for multiple devices or computers • Effortlessly share and access files over the network • Home users and small businesses can use it for data storage	• Performance gets affected while transferring large files	
SD Card	~128 TB	• Small, portable, and can easily access data • Used on cameras, computers. and mobile phones to store small amount of data	• More expensive than CDs, DVDs, and backups • Gets easily damaged	

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Examples of Data Backup Media Devices

Optical Disks (DVD, Blu-ray)

DVD recordable disks can store up to 8.55 GB of data, and are readily available. DVDs store more data and are available at affordable rates, in bulk if need be. However, they are not used as much as in the past, as external hard drives are available at reasonable prices and can store more data than DVDs.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Blu-ray is compatible with both PC and consumer electronic environments. The data encoding feature in a Blu-ray allows more data storage.

- **Advantage**:
  - Less expensive and easy to store
- **Disadvantage**:
  - Slow data storage

Portable Hard Drives/USB Flash Drives

Portable hard drives are considered a better medium for data backup than a DVD or Blu-ray. They are available in high capacities, and can also be used for smaller backups. Flash drives are available in different sizes and have the ability to store large backup files.

RAID is another available hard drive option. It contains two or more hard drives. The second drive may be used to copy data stored in the first drive. This process allows important data to be preserved. Any change in the data will be automatically reflected in all other drives as well.

- **Advantages**:
  - High storage capacities
  - Extremely high speeds
- **Disadvantages**:
  - Expensive than DVD/Blu-ray
  - Less recommended for small backups

Tape Drives

A Tape drive is considered as the best media for data backup. It facilitates data backup at an enterprise level. Tape drives are used for storing programs and data.

- **Advantages**:
  - Easy to store and transport
  - Requires no user intervention
  - Tape backup is completely automatic
- **Disadvantages**:
  - Expensive for home users
  - Home computers require additional hardware and software updates

Network Drive

Network attached storage (NAS) drives are storage devices that are connected directly to a network, allowing for the storage of multiple computers or other devices. This allows for easy sharing of files and access to them from multiple devices through the network, making them a popular choice for small businesses and individuals at home.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

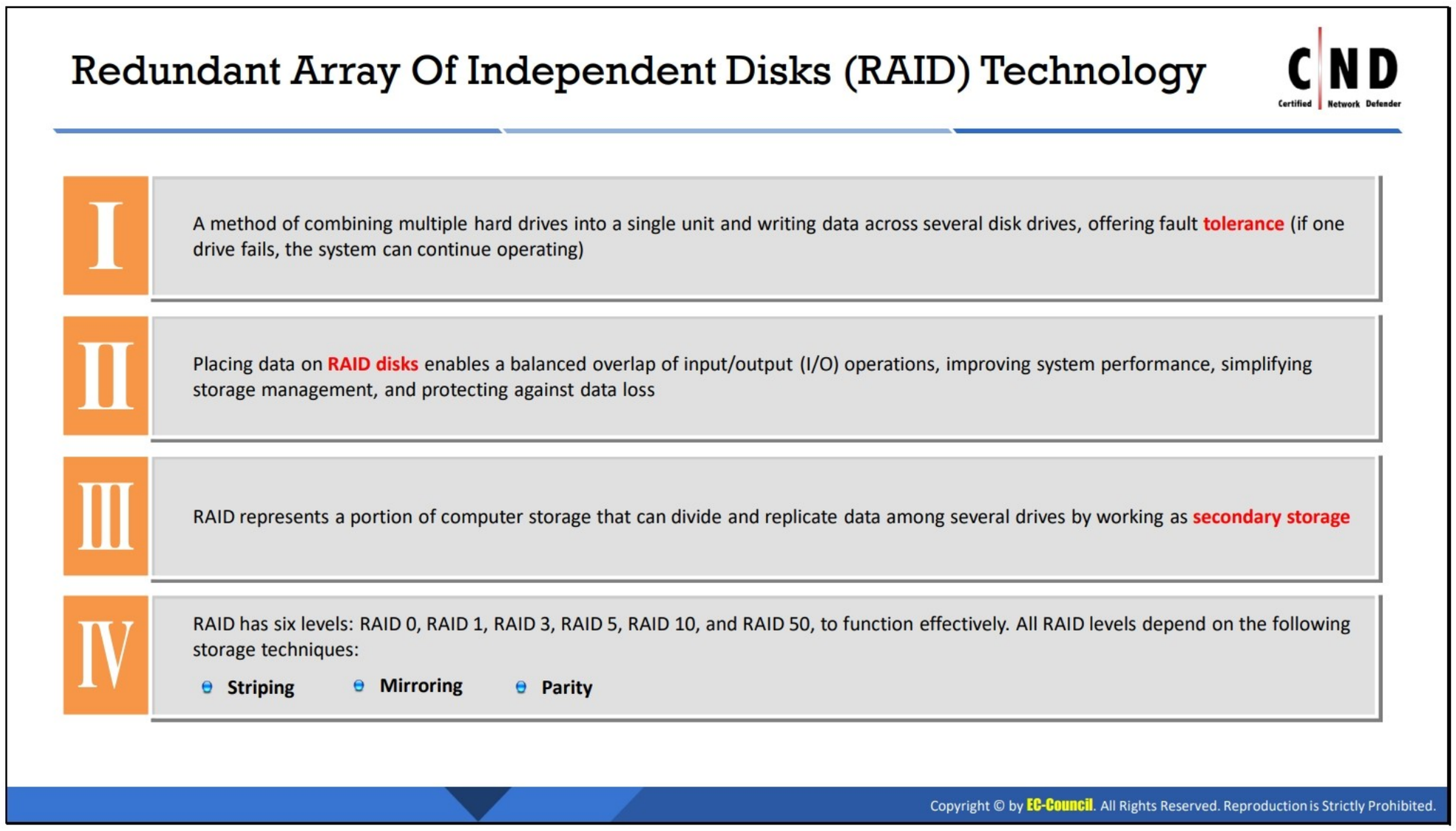
- **Advantages:**
  - NAS offers data transfer speeds comparable to those of direct-attached storage (DAS), ensuring fast access to data.
  - Provides 24/7 data availability, even for remote users.
- **Disadvantages:**
  - It increases LAN traffic.
  - It requires additional input-output processing, potentially impacting system performance.

SD Card

An SD card is a type of flash memory device that is designed to provide a secure and reliable storage solution for a variety of digital devices, such as mobile phones, tablets, digital cameras, dash cam systems, computers, and music players. It is characterized by high storage capacity, small size and weight, and is compatible with a wide range of mobile devices. It is primarily used for the storage or transfer of data and files, such as photos, music, and videos.

- **Advantages:**
  - It is removable and portable, offering flexibility in data storage and transfer.
  - Consumes minimal power and is easily accessible on PCs, making it a convenient option.
- **Disadvantages:**
  - Its limited read-write cycles restrict the device's longevity.
  - Offers slower data access speeds compared to main memory, which could impact performance.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Redundant Array of Independent Disks (RAID) Technology

Many organizations depend on RAID technology for handling their critical backup needs, especially with the increases in data flow and data volume. Organizations are expanding their networks to improve their productivity. However, this additional increase can cause network bottlenecks. The probability of losing data because of disaster, threats, mistakes, and hardware failures hamper an organization's ability to grow. RAID technology overcomes these situations providing an option for data availability, high performance, efficient and accessible recovery options without a loss of data.

Understanding RAID Technology

RAID technology is used to store data in different places on several disks. Storing the data on multiple disks improves the performance of IO operations. RAID technology functions by implementing multiple hard disks as a single logical disk. It allows a more balanced storage of the same data across an array of disks. An effective implementation of this technology helps address the complex issues in fault tolerance. The data organized in RAID levels depends on the RAID storage techniques and installation methods. Usually, the implementation of RAID is done on a server. Although personal computers do not necessarily need this technology, they can still setup and utilize it in a smaller environment than an enterprise.

RAID has six levels for functioning effectively: RAID 0, RAID 1, RAID 3, RAID 5, RAID 10, and RAID 50. Each level has the following features:

- **Fault tolerance:** Even if a disk fails to work, other disks will continue to function normally.
- **Performance:** RAID achieves high performance during read and write processes across multiple disks.

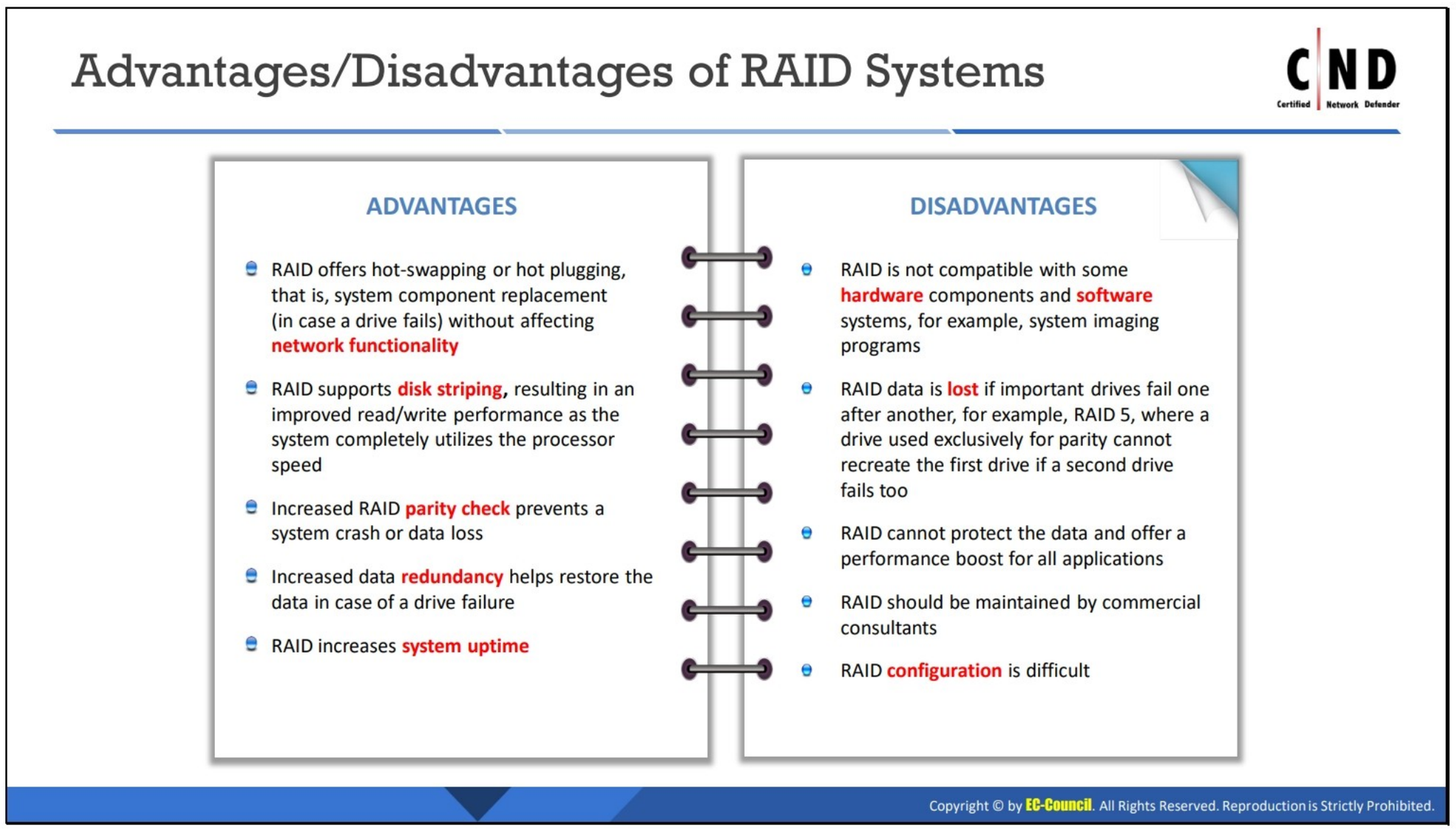
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Competence:** This is defined by the amount of data stored. The storage capacity of disks depend on the chosen RAID level. The storage capacity need not be equal the size of the individual RAID disks.

All the RAID levels depend on the storage techniques listed below:

- **Striping:** Striping divides the data into multiple blocks. These blocks are further written across the RAID system. Striping improves the data storage performance.
- **Mirroring:** Data mirroring makes image copies of the data and simultaneously stores this data across the RAID. This affects fault tolerance and data performance.
- **Parity:** Parity uses a striping method to calculate the parity function of a data block. During a drive failure, the parity recalculates the function using a checksum method.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Advantages/Disadvantages of RAID Systems

Before RAID technology was introduced, many organizations used a single drive to store data. RAID technology is now found across all storage devices in an organization. Advantages and disadvantages RAID depend on the implemented level.

Advantages of RAID Systems

1. **Performance and reliability:** RAID technology increases the read/write performance of the data on disks. The speed is much faster than when using a single drive as storage. It improves the performance by distributing the I/O. A RAID controller distributes data over several physical drives, ensuring that a single drive in the RAID system is not overburdened. RAID sustains the reliability of data even if a disk fails. Failed components can be replaced in a RAID system without shutting the system down. This feature is called hot swapping. The replacement process does not affect the network or how the other disks function.
2. **Parity check:** Parity check is a process where the RAID system compares the data stored in a crashed system with the data stored in other disks. This check process is accomplished on all drives. The parity check is performed after mirroring the data. Regular parity checks detect the probability of a system crash, thereby preventing data loss.
3. **Data redundancy:** A disk can fail anytime. Therefore, data redundancy is important for an organization. RAID provides enhanced data redundancy in case of a hardware failure.
4. **Disk striping:** Disk striping improves the read/write performance of data. The data is divided into small chunks and spread over multiple disks. Depending on the implemented RAID level, the data is divided into bytes, bits, or blocks. Data reading and writing can be done simultaneously on a RAID system.

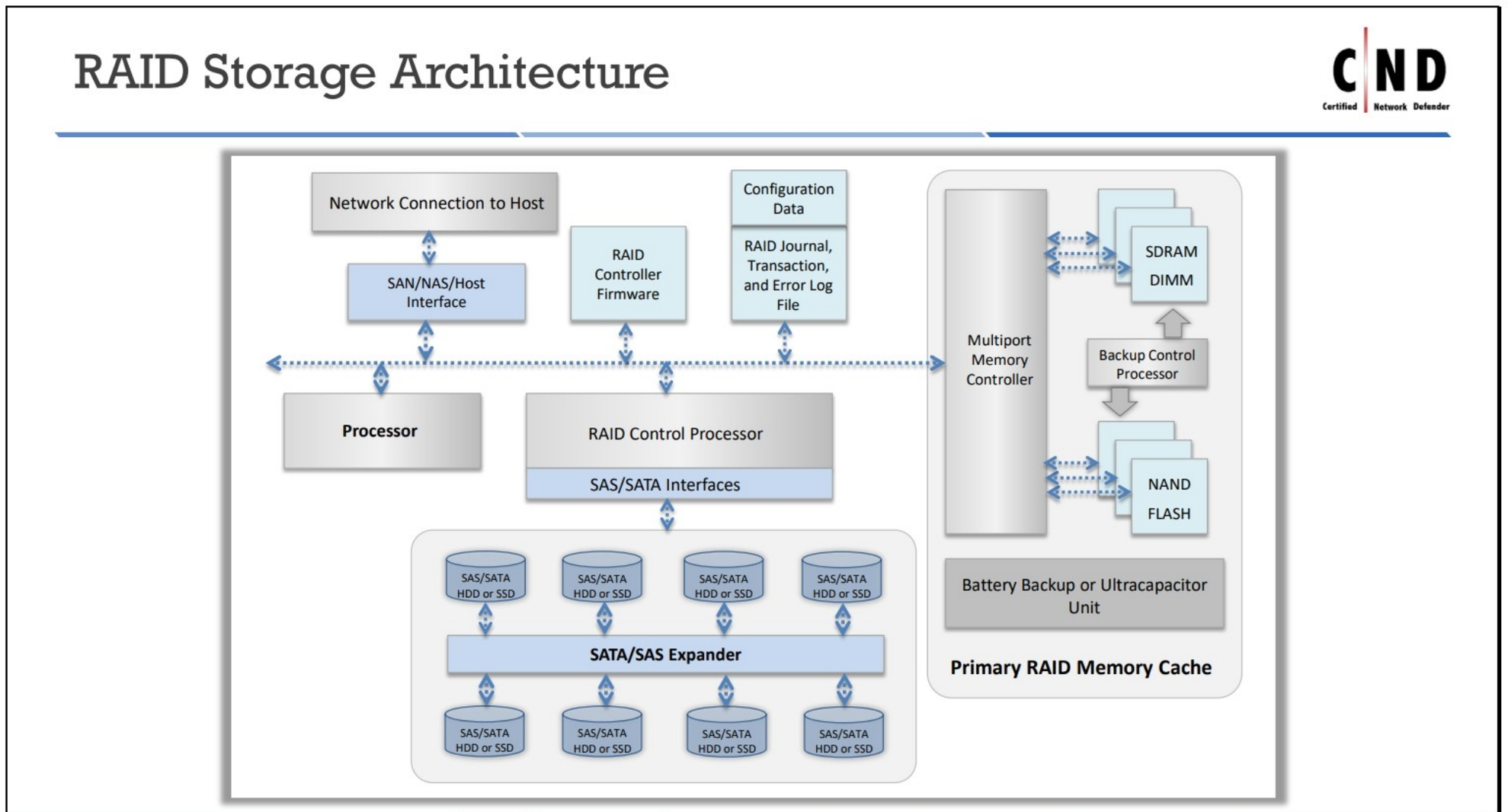
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

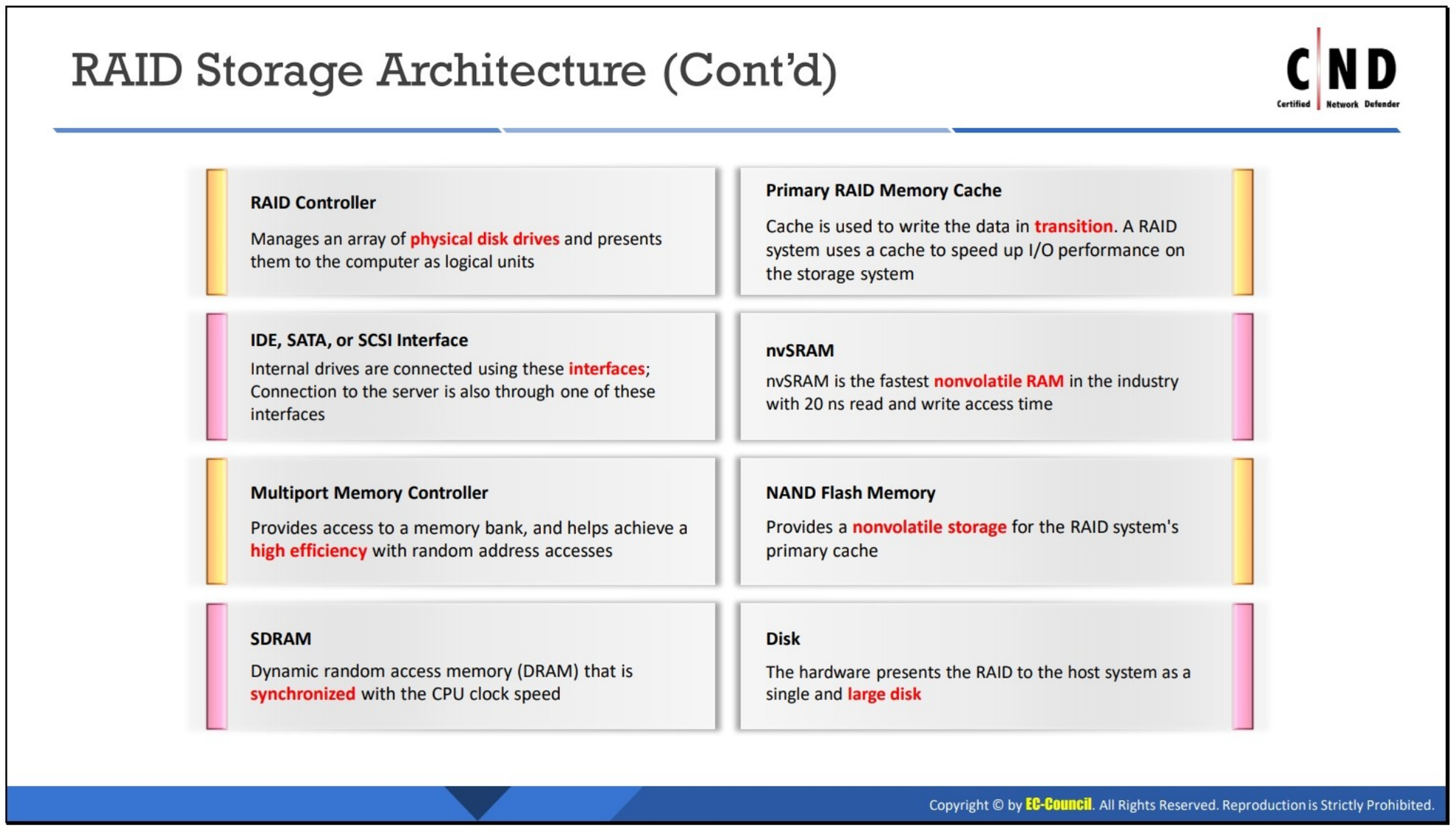
5. **System uptime:** This metric detects the reliability and stability of a computer. System uptime defines the time till which a system can be left unattended without any assistance. Configuring RAID on a system helps enhance system uptime. A high system uptime in an organization signifies a high productivity.

Disadvantages of RAID Systems

1. **Writing network drivers:** RAID technology is designed to be widely used on servers. A major disadvantage of RAID technology is the writing of all network drivers. RAID technology is complex, and this process can be time consuming.
2. **Noncompatibility:** Different systems support different types of RAID drives. Certain hardware or software components may not be compatible with the RAID drive configured on a server. This noncompatibility may lead to the RAID not functioning properly. The compatibility between RAID drives, hardware, and software must be checked prior to configuring a system. RAID can protect data for all applications available on the network.
3. **Loss of data:** All RAID drives function in the same environment. They can become nonfunctional because of mechanical issues. Thus, the potential data loss increases if the disks fail one after another. When two drives fail at the same time, recovering the data from the disk becomes difficult.
4. **Time consumed in rebuilding:** The increase in drive capacity has been much more than the increase in transfer speed. Recovering data from drives with a large storage capacity can be time consuming. In such scenarios, rebuilding a failed disk can also be time consuming. Increasing the number of drives does not help increase the data transfer speed.
5. **Cost:** Implementation of RAID technology can be costly. Organizations need to hire consultants to sustain its performance. It also requires external RAID controllers and hard drives to function correctly, and this adds to the overall cost.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





RAID Storage Architecture

The RAID architecture depends on two principles: redundancy and parallelism, providing a wide range of storage options with better performance and freedom from disk failures. The Internet's increasing footprint has led to an increase in the use of RAID systems because of their high data storage capabilities and management systems. Many available RAID implementations depend on the following factors: parallelism, duplication, and redundancy.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

In a RAID architecture, a switch receives the data from servers connected to the network. The switch then sends the data to the processor at a later stage. The processor transfers the received data to a RAID controller. The RAID controller may be implemented either as a hardware using a RAID-on-Chip (ROC) or in a software. The ROC can contain the I/O interfaces, a processor, a host interface, and a memory controller. The ROC is installed directly in a motherboard using an expansion card, or in an external drive enclosure.

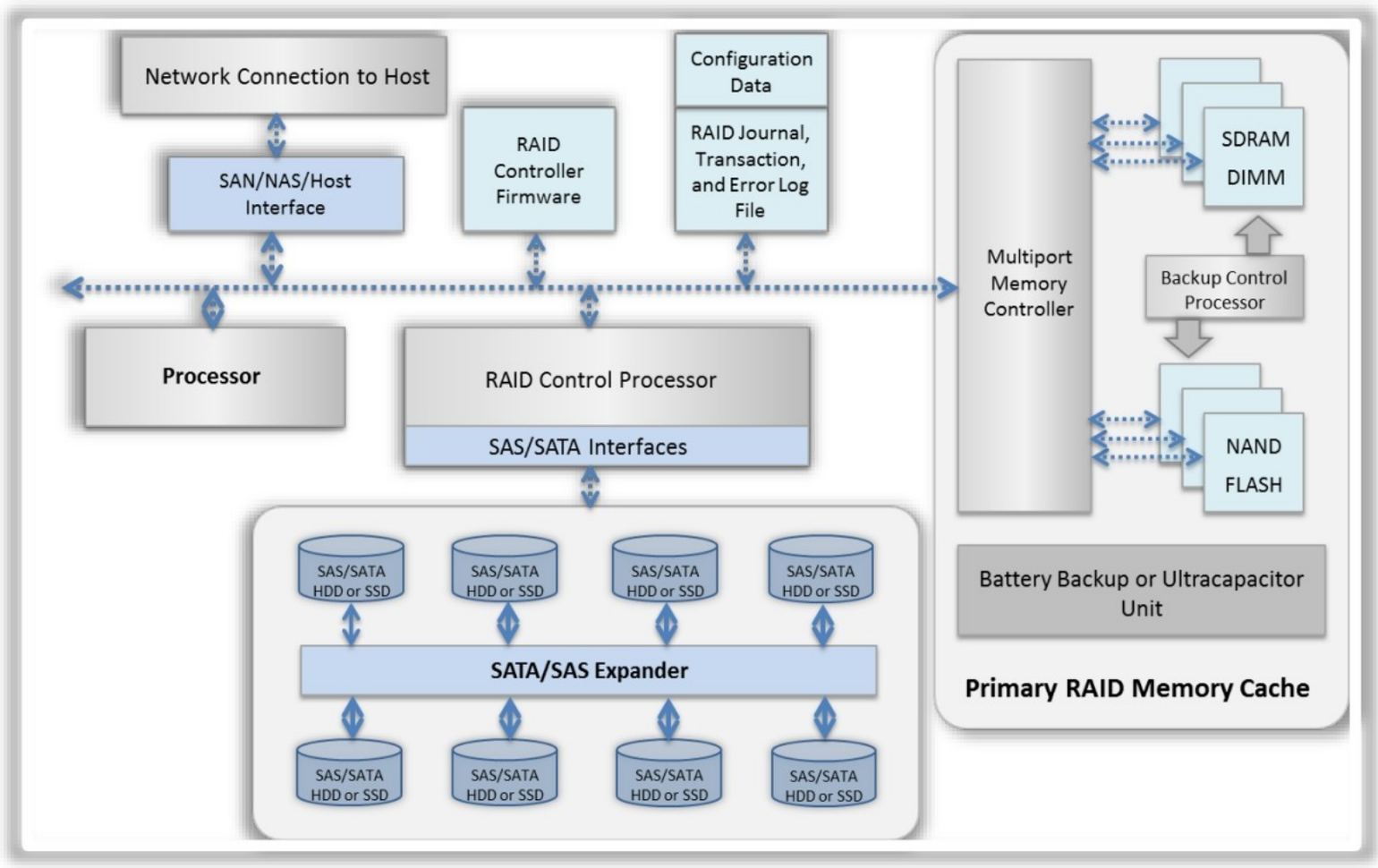


Figure 10.125: RAID storage architecture

The RAID storage architecture outlines how the RAID server functions. The processor controls the entire functioning of the drive arrays and interfaces. It provides flexible and high-performance functions. The architecture in the figure above shows a RAID system can depend on hard disk drives (HDDs) as well as SSDs. The processor requires DRAM and NAND flash memory. The NAND flash memory provides a nonvolatile storage to the primary RAID memory cache.

A battery backup or an ultra-capacitor unit in the primary RAID memory cache is helpful when the RAID control processor suffers from a power failure. In this scenario, the battery backup independently copies the DRAM contents to the NAND flash memory. A battery backup is an inexpensive alternative during a power loss. The architecture shows the requirement of a nonvolatile memory in the RAID controller firmware, RAID journal, and transaction and error log files.

Major Components of a RAID Architecture

- **RAID controller**: This is either hardware- or software-based, and contains the HDDs or solid state drives as a single logical unit. A RAID controller has the permission to access multiple copies of files present on multiple disks, thereby preventing damage and increasing the system performance. In a hardware RAID, a physical controller manages the RAID array with a controller in the form of a PCI card that supports SATA or SCSI. A software RAID works similarly to a hardware RAID, except that their performance is lower than the former.
- **Primary RAID memory cache**: The RAID controller has a direct access to the cache memory, enabling faster read and write access to the storage system. The cache is used to store the

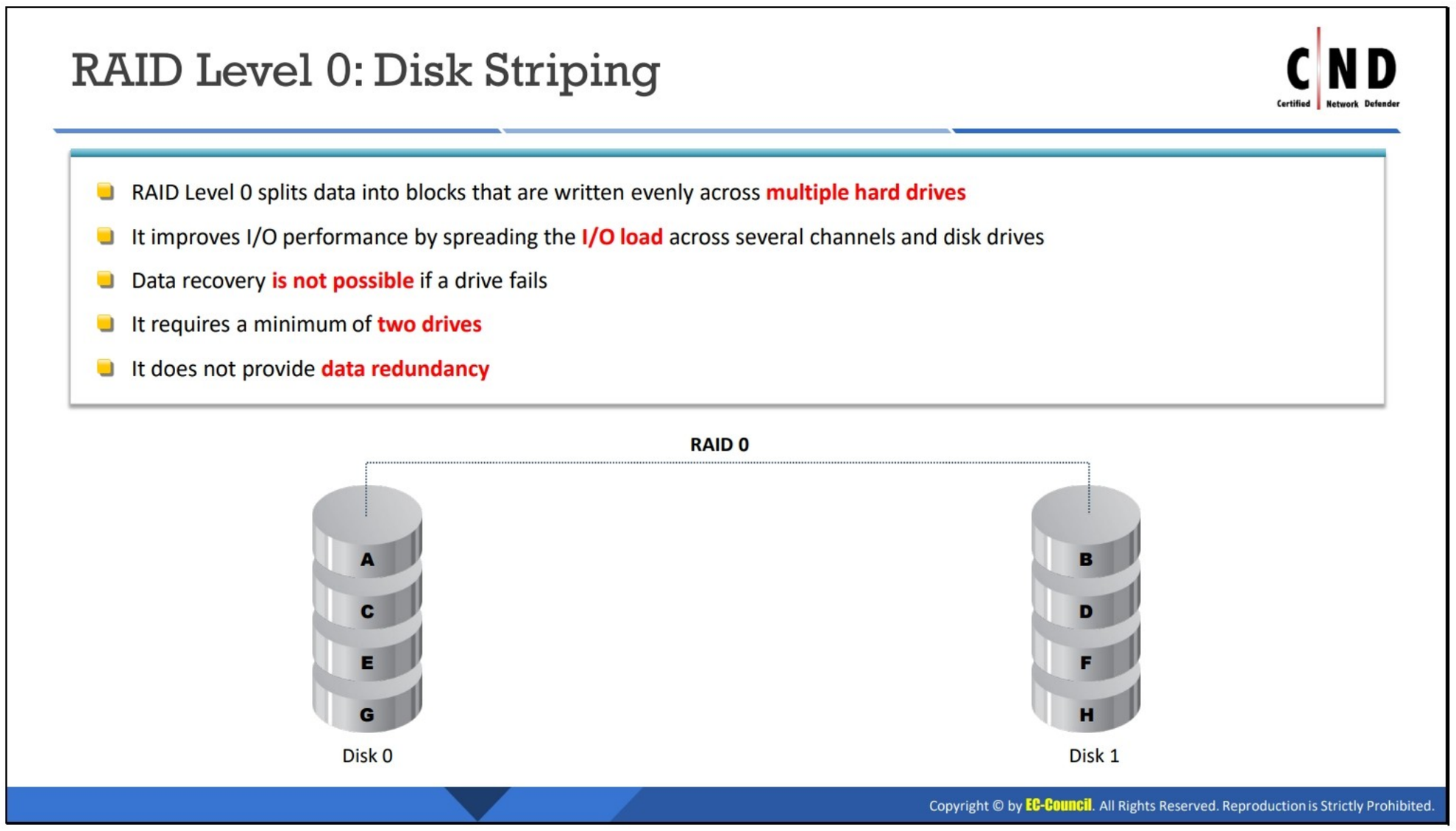
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

changing data. The cache memory is bigger in size and uses high-speed SDRAMs. A normal cache memory has a write cache and a separate read cache. The read cache decreases the latency of the read process. There are two types of write cache memories:

- **Write-through mode**: This bypasses the cache memory and writes the data directly to the disk after the host sends it. The host sends the next data item after receiving a confirmation that the writing process has been completed.
- **Write-back mode**: Data sent from the host is written to the cache memory. The host may perform other actions while the RAID controller transfers data from the cache to the disk drive. The RAID controller acknowledges the write process to the host soon after writing the data to the cache. Issues may arise if a RAID controller sends an acknowledgment before the data has been completely written on the disk.

- **IDE, SATA, or SCSI interfaces**: IDE, SATA, or SCSI are device cables that transmit read/write signals to and from the drive. These are mostly used for internally connecting the drives. Moreover, servers are connected using these interfaces.
  - **IDE**: Integrated drive electronics (IDE) allows the connection of two devices per channel. It is normally used for internal devices as the cables are large and flat.
  - **SATA**: Serial ATA deals with hot plugging and serial connectivity. The hot plugging technique may be used to replace computer components without shutting down the system. SATA enables only one connection per connector, and is not flexible for industrial purposes.
  - **SCSI**: Small computer system interface (SCSI) allows multiple devices to be connected to a single port at the same time. SCSI uses a parallel cable for attaching internal and external devices.
- **nvSRAM**: Nonvolatile SRAM, or nvSRAM, has a faster read and write process because of the presence of a standard asynchronous SRAM interface. nvSRAM ensures adequate data storage capabilities without the need for a battery during a shut down. nvSRAM is best used in applications that require high speed and nonvolatile storage at a low cost, such as in the medical industry. nvSRAM backups the data even in the event of a power failure.
- **Multiport memory controller**: An MPMC provides access to memory for up to eight ports. A memory controller can be present as a separate chip or as an integrated memory.
- **NAND flash memory:** Flash memory is a storage medium designed from electrically erasable programmable read-only memory (EEPROM). NAND and NOR are two types of flash memories. Its primary aim is to reduce cost and increase capacity. It does not require power to retain the data. It can improve its read-write cycles with reduced voltage demands.
- **SDRAM:** Synchronous dynamic random access memory or synchronous DRAM (sDRAM) is a memory that is synchronized with the processor's clock speed. This increases the number of instructions the processor can process. SDRAM speed is measured in Mega Hertz (MHz). It is divided into several sections called banks that allow the device to operate on several memory access commands simultaneously.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



RAID Level 0: Disk Striping

Depending on the requirement of your organization, you can choose any RAID level. RAID levels are based on performance, fault tolerance, or both.

RAID 0 deals with data performance. In this level, data is broken into sections and written across multiple drives. The storage capacity of RAID 0 is equal to the sum of the disks' capacities in the set. RAID 0 does not provide fault tolerance. A failure of one disk can lead to the failure of all disks in a level 0 volume. The probability of recovering data from a RAID level 0 is minimal.

The data distribution in a RAID level 0 is equal among all the disk sets, resulting in high performance. With concurrent high performance, the throughput of the read and write operations on multiple disks is equal to the throughput of the array of disks. Increased throughput is an advantage of RAID 0, considering that data recovery is not available. Software and hardware RAID controllers support RAID 0, helping boost server performance.

Example: Assume that the IT infrastructure has a hard disk with high performance. The data in the hard disk is transferred at a remarkably high speed. All the large and critical files are stored in this disk. However, if this disk fails, the entire contents of the files will be affected, leading to the unavailability of the data. It is advisable not to store any critical data in a RAID level 0.

Advantages of RAID Level 0

- **Read and write performance:** RAID level 0 has a good read and write performance. The performance is even better when the controller supports independent reads and writes to different disks in the array.
- **Cost:** RAID level 0 is more cost effective than the other RAID levels.

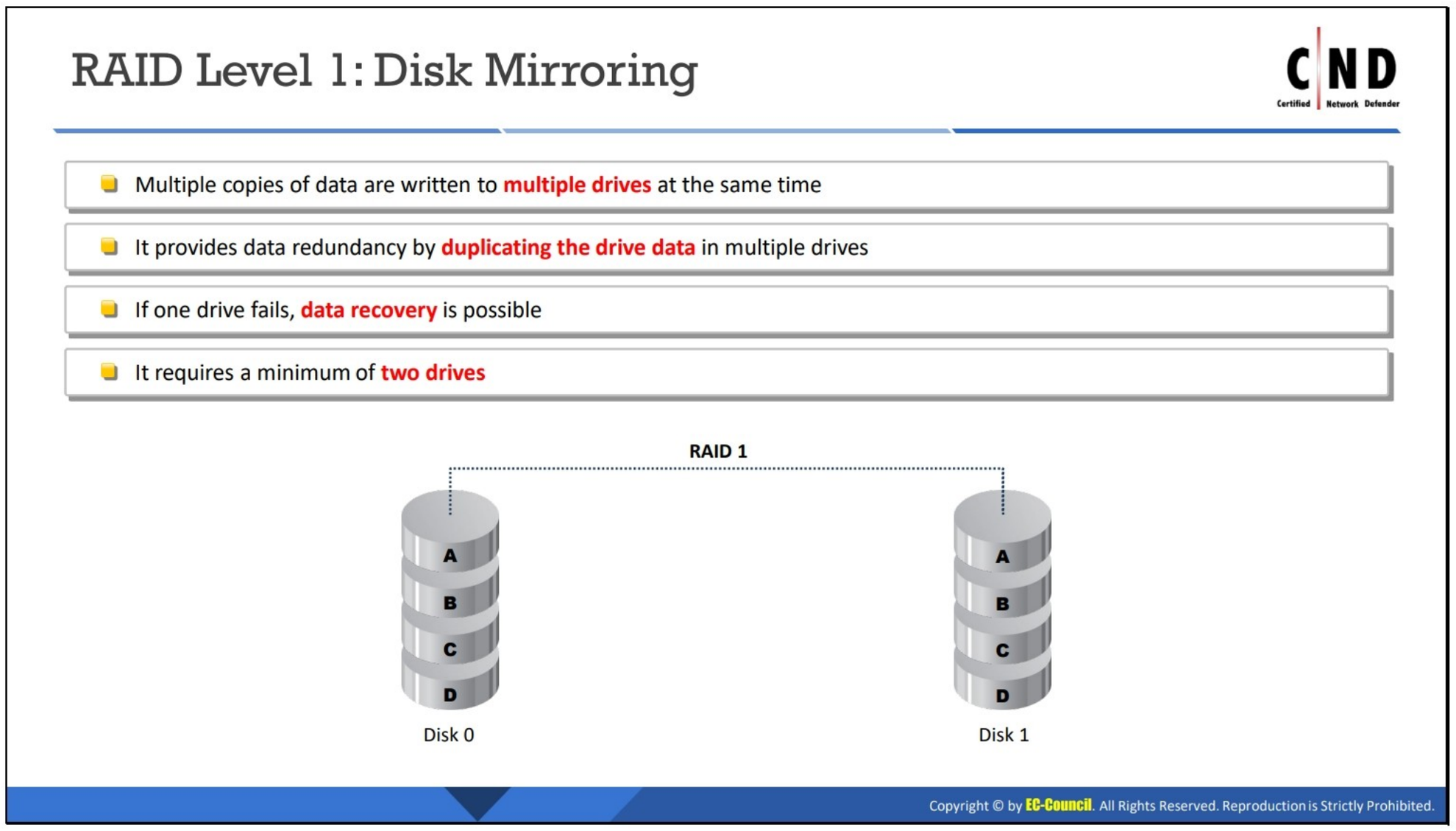
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Implementation:** Is easy to implement as the data is divided in a sequential set of blocks. There is no storage loss as the maximum capacity is utilized.

Disadvantages of RAID Level 0

- **No redundancy:** With no data redundancy, data loss is greater.
- **Noncritical data:** Data that is not critical to the organization can be stored on RAID level 0. This level does not use mirroring. Recovery is not possible if critical data is lost on RAID level 0.
- **Unreliable:** If one disk fails, the entire network will be affected.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



RAID Level 1: Disk Mirroring

A typical RAID 1 contains an exact copy of the data on two or more disks. RAID 1 writes data on multiple drives and multiple mirror drives at the same time. The failure of one drive does not affect the data on other drives. This allows data retrieval from the mirror drive. Similar to RAID 0, RAID 1 provides no parity, stripping, or spanning of disk space across multiple disks. RAID 1 can be used in accounting, payroll, and other financial applications.

RAID 1 is suitable in environments where read performance matters more than write performance. RAID 1 has improved read performance because the data in a disk can be read at the same time simultaneously.

RAID level 1 provides data reliability in case of a disk failure as it can still provide access to the same data mirrored on other disks. In a RAID 1 hardware implementation, a minimum of two disks are required. In a software RAID 1, data can be copied to a disk volume. RAID 1 reduces the total disk capacity by half.

Example: If a RAID 1 server is configured with two 4TB drives, the storage capacity will be 4 TB and not 8 TB.

The drive that accesses the data first will service the request. The write throughput in RAID 1 is always slower because every drive needs to be updated. Thus, its performance is limited by the slowest drive. It is only as fast as its slowest drive. RAID 1 will continue to function as long as there is at least one working drive.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

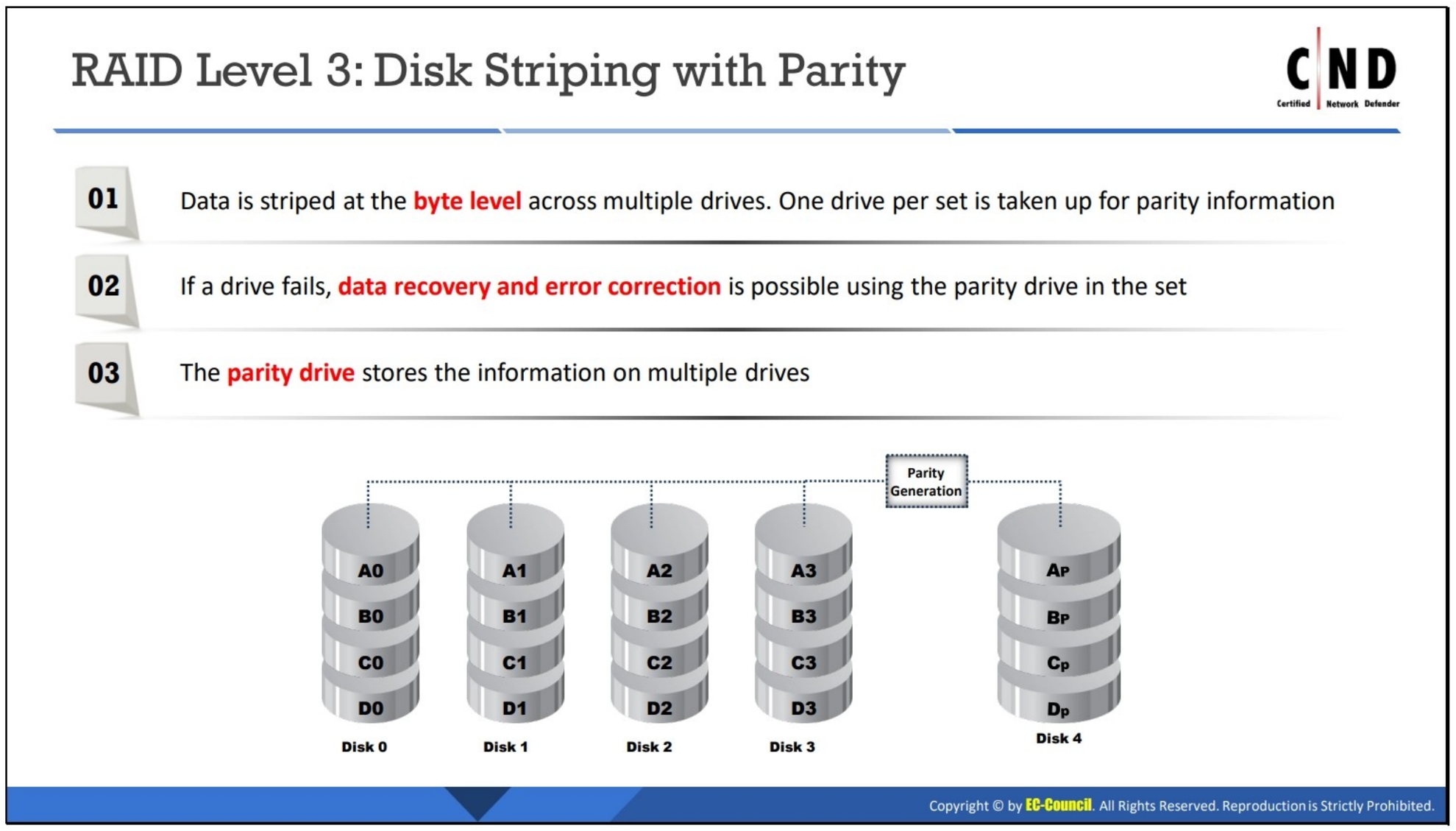
Advantages of RAID Level 1

- **High read performance:** Because there are two disks, the read performance is higher in a RAID level 1 system. Data can be read simultaneously while being written on the other disk. Thus, the redundancy is excellent.
- **Compatibility:** RAID 1 is compatible with hardware and software RAID systems, including controllers.
- **Reliability:** The mirroring feature in a RAID 1 ensures the data will be available, making it more reliable than a RAID level 0.

Disadvantages of RAID Level 1

- **Capacity:** RAID level 1 undergoes duplexing, which needs twice the amount of disk space for storage.
- **Hot swapping unavailable:** If a disk fails to run, it cannot be replaced while the server is still in operation. This is called hot swapping. RAID level 1 does not support hot swapping.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



RAID Level 3: Disk Striping with Parity

RAID level 3 is disk striping with parity. It uses striping and parity as its main features to store data. To implement a RAID level 3 system, a minimum of three disks are required. The data is stored on multiple drives at the byte level. This RAID level dedicates one drive to store the parity information. The byte level division allows the drives to work simultaneously. At any point in time, either a read operation or a write operation can take place. RAID 3 is a good choice for specialized databases or single-user systems.

The RAID level 3 has a high transfer data rate along with data security. It can perform data recovery and error correction by calculating an exclusive OR (XOR) of the information recorded on the parity drive.

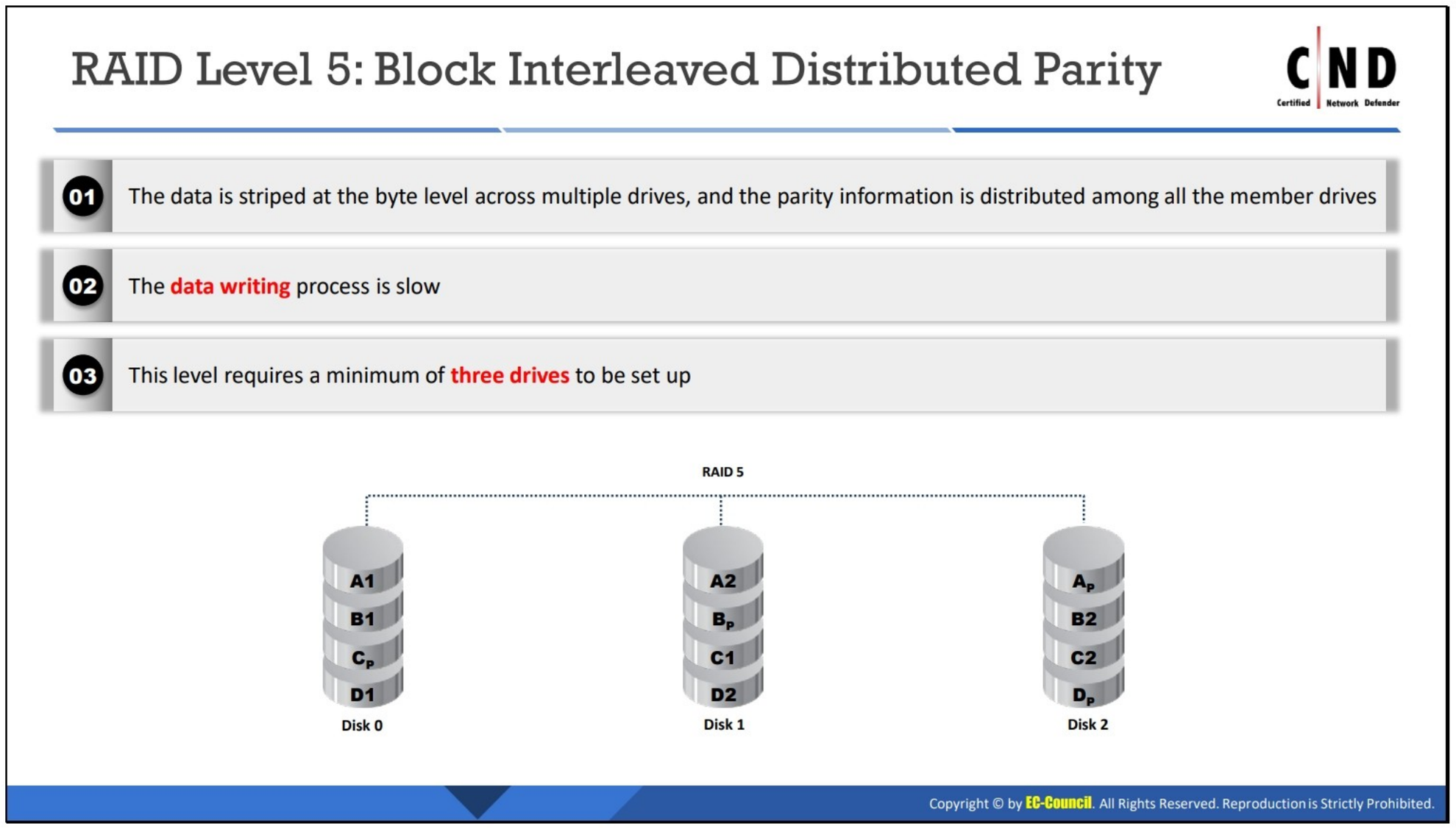
Advantages of RAID Level 3

- **High throughput:** RAID level 3 provides a high throughput for read and write operations for large data transfers.
- **Resistant:** This RAID level is resistant to disk failures and breakdowns.

Disadvantages of RAID Level 3

- **Complexity:** Installation and configuration of a RAID level 3 system is complex. Its implementation necessitates a larger amount of resources.
- **Slow performance:** Random operations affect its performance, thereby reducing its speed.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



RAID Level 5: Block Interleaved Distributed Parity

RAID level 5 involves a block-interleaved distributed parity; it includes a block-level striping with a distributed parity. The parity information is distributed among all drives except one. The data chunks in a RAID level 5 system are larger than the regular I/O size, but they can be resized. To prevent data loss following a drive failure, data can be calculated from the distributed parity.

The RAID 5 needs at least three disks; however, more than three disks can be used for a better performance. RAID 5 is not a good choice for write operations on the system. Rebuilding the RAID 5 array following a disk failure takes a long time. The performance can be degraded when the array is being rebuilt, making it vulnerable to additional disk failures. This level offers significantly better read performance as the disks independently process the data requests.

RAID 5 is most often found in file and application servers, database servers, along with web, email, and news servers.

Advantages of RAID Level 5

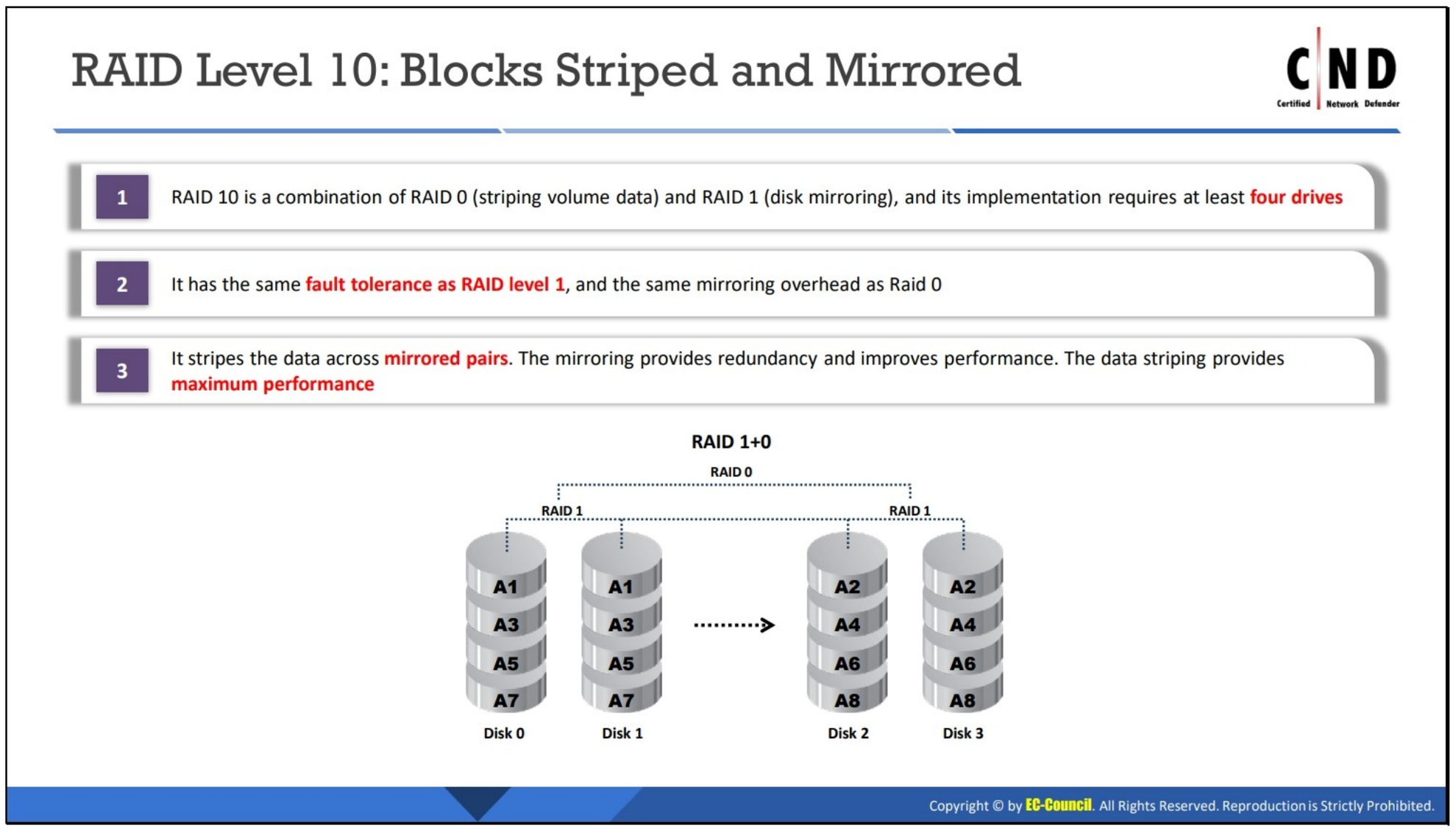
- **Read data:** Among all RAID levels, level 5 has the highest read data transaction rates.
- **Withstand failure:** RAID 5 can withstand the failure of a single drive, and is not affected by the loss of data.
- **Hot swapping:** In case of a disk failure, the failed disk can be replaced with a new one, without a server shutdown.

Disadvantages of RAID Level 5

- **Slow write operation:** Servers built using RAID 5 suffer from performance issues with write operations, and these can eventually result in reduced speeds.

Example: Employees accessing a database on a RAID 5 server will reduce the server's production time.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



RAID Level 10: Blocks Striped and Mirrored

RAID level 10 includes disk striping and mirroring in a nested hybrid RAID level. It is a combination of RAID level 1 and RAID level 0. It is also called as a "stripe of mirrors." This level can symbolically be represented as RAID 1+0 or RAID 10. RAID 10 includes the mirroring of RAID 1 without parity and the striping of RAID 0. The performance of RAID 10 is higher than a RAID 1. RAID level 10 has the same fault tolerance as RAID level 1. It requires a minimum of four drives for its operation. RAID 10 is a great choice for database servers, web servers, email servers, etc., and can be implemented on hardware or software.

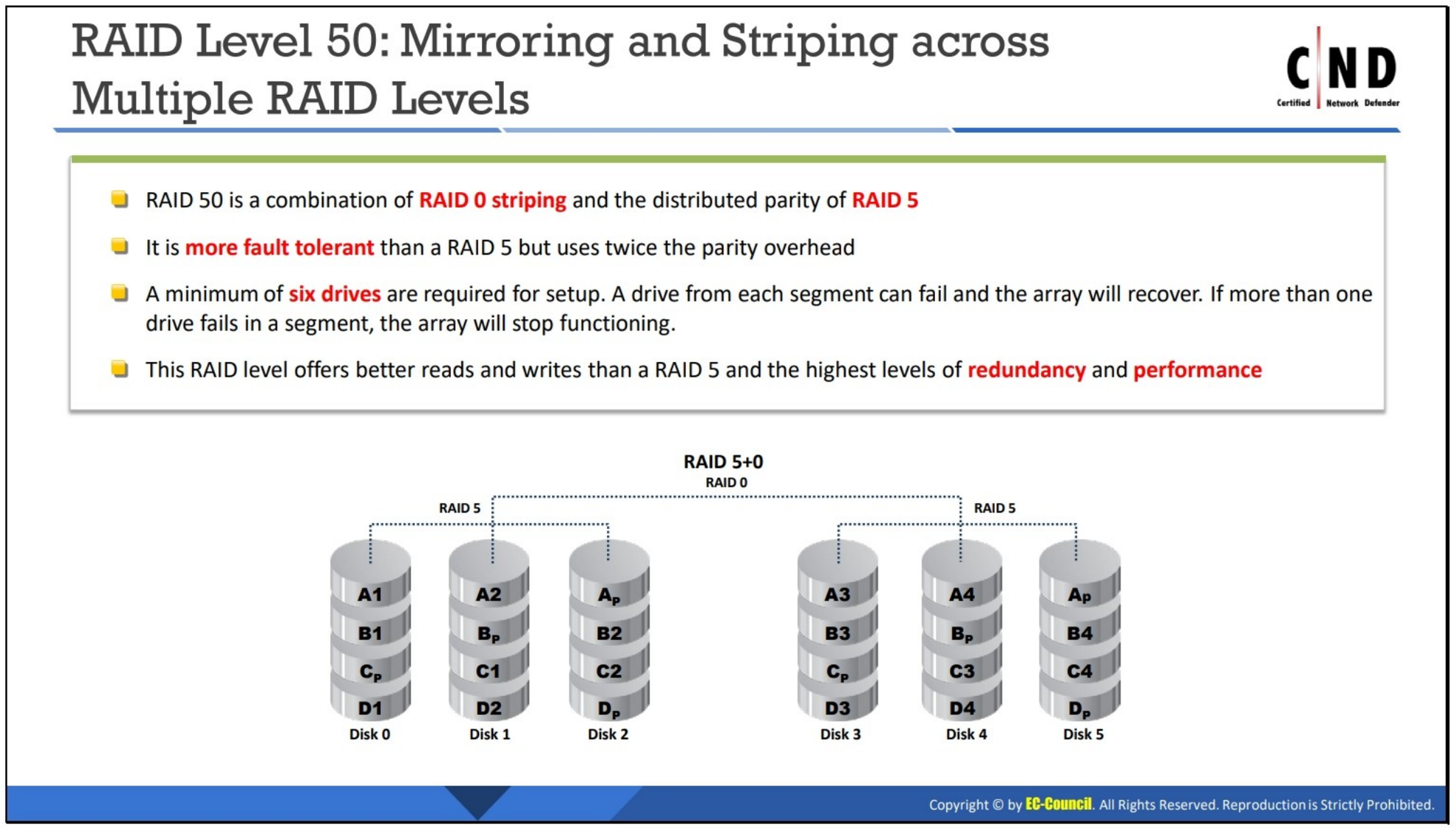
Advantages of RAID Level 10

- **Improved I/O operations:** With a combination of RAID levels 1 and 0, it provides improved I/O operations.
- **Better throughput:** Compared with other RAID levels, RAID 10 provides better throughput and higher latency.
- **Efficient write operations:** The write operations are efficient in this level. Therefore, RAID 10 is often implemented on database servers and other servers that perform write operations.

Disadvantages of RAID Level 10

- **Expensive:** RAID 10 is expensive than other RAID levels as it requires twice as many disks.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



RAID Level 50: Mirroring and Striping across Multiple RAID Levels

RAID level 50 includes mirroring and striping across multiple RAID levels. This level is a combination of a level 0 block-level striping and a level 5 distributed parity. The configuration of RAID level 50 requires a minimum of six drives. This level undergoes a hot swapping process when a disk fails.

RAID 50 is an improvement over RAID 5, specifically for its write operation and fault tolerance. RAID level 50 can be implemented on servers that run applications requiring higher fault tolerance, capacity, and random access performance. This level offers data protection and faster rebuilds than a RAID 5 system. A failed disk in a segment only affects that segment and not the entire array. Only that segment is then rebuilt. The rest of the array functions normally.

Advantages

- **Security:** The data stored in a RAID 50 is more secured than in a RAID 5. With a larger storage capacity, this level offers better security than RAID 5.
- **Nondegradable:** With the use of a minimum of six drives in the configuration, failure of one disk does not impact the server function on this level.
- **Read and write performance:** The read and write performance of RAID level 50 is far better than RAID level 5.

Disadvantages

- **Controller:** Only a sophisticated controller can handle RAID level 50.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Selecting Appropriate RAID Levels

RAID	Disk Utilization	Fault Tolerance	Large Data Transfers	I/O Rate	Data Availability	Key Problems
Single Disk	Fixed 100%	No	Good	Good	Single drive MTBF	Data lost when disk fails
RAID 0	Excellent 100%	No	Very Good	Very Good	Poor MTBF of drive	Data lost when any disk fails
RAID 1	Moderate 50%	Yes	Good	Good	Good	Use double the disk space
RAID 3	Good – Very Good	Yes	Very Good	Good	Good	Data lost when any disk fails
RAID 5	Good – Very Good	Yes	Good – Very Good	Good	Good	Lower throughput with disk failure
RAID 0+1	Moderate 50%	Yes	Good	Very Good	Good	Use double the disk space
RAID 1+0	Moderate 50%	Yes	Very Good	Very Good	Very Good	Very expensive, not scalable
RAID 30	Good – Very Good	Yes	Very Good	Excellent	Excellent	Very expensive
RAID 50	Good – Very Good	Yes	Good – Very Good	Excellent	Excellent	Very expensive

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Selecting Appropriate RAID Levels

Selection of any RAID level should be based on the needs of the organization and the features offered by each level.

Points to Consider While Selecting RAID Levels

- **Application performance needs**: Not all RAID levels are useful for all applications and data needs. Choose an appropriate RAID level according to other factors such I/O needs, storage capacity, fault tolerance, etc.
- **Capacity:** Each RAID level offers different amounts of storage capacity. The choice of a RAID level depends on the capacity required. For example, if 30 drives are needed, RAID 50 or 60 is a better choice, with three segments of ten drives each. You could do a RAID 5 but the rebuild process would be tedious, along with other associated problems. One drive is lost to parity for each segment. Thus, only 27 drives will be available toward the capacity requirements. Thus, a loss of capacity can lead to performance gains.
- **Cost:** Both performance and capacity cost money. Therefore, it is necessary to weigh in the trade-off between performance and capacity. Capacity can be lost, and performance gained. Losing a small capacity may be worth the performance gains. All this depends on where the RAID system will be utilized. One has to strike a balance between both capacity and performance, and what works best for the organization.
- **Availability:** Choose a RAID level that matches the availability requirements of the organization.

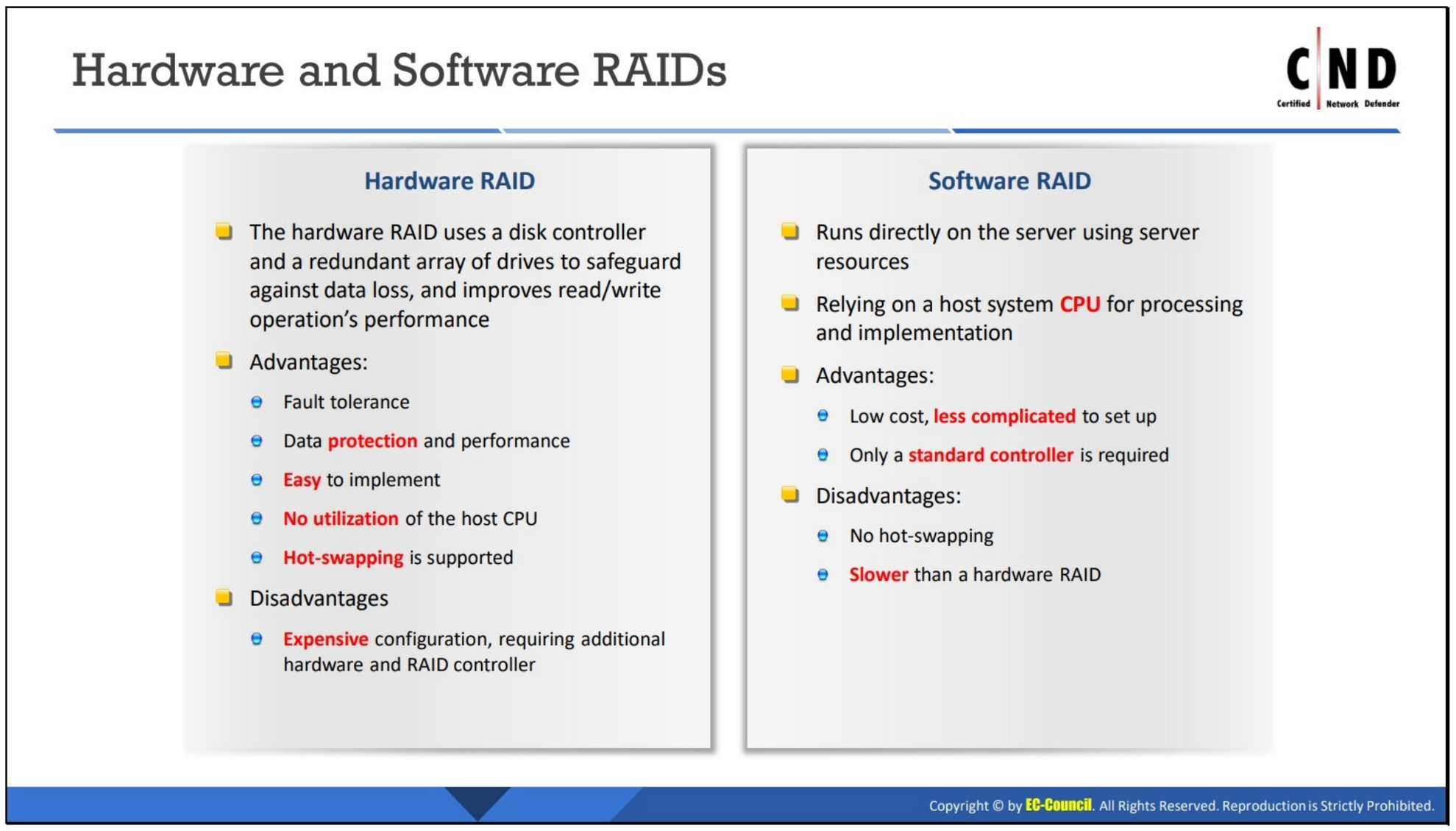
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

The following table will help you in selecting an appropriate RAID for your organization.

RAID	Disk Utilization	Fault Tolerance	Large Data Transfers	I/O Rate	Data Availability	Key Problems
Single Disk	Fixed 100%	No	Good	Good	Single drive MTBF	Data lost when disk fails
RAID 0	Excellent 100%	No	Very Good	Very Good	Poor MTBF of drive	Data lost when any disk fails
RAID 1	Moderate 50%	Yes	Good	Good	Good	Use double the disk space
RAID 3	Good – Very Good	Yes	Very Good	Good	Good	Data lost when any disk fails
RAID 5	Good – Very Good	Yes	Good – Very Good	Good	Good	Lower throughput with disk failure
RAID 0+1	Moderate 50%	Yes	Good	Very Good	Good	Use double the disk space
RAID 1+0	Moderate 50%	Yes	Very Good	Very Good	Very Good	Very expensive, not scalable
RAID 30	Good – Very Good	Yes	Very Good	Excellent	Excellent	Very expensive
RAID 50	Good – Very Good	Yes	Good – Very Good	Excellent	Excellent	Very expensive

Table 10.2: Selecting Appropriate RAID Levels

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Hardware and Software RAIDs

Choosing between a hardware and software RAID depends on the requirements of the organization as well as the IT infrastructure needs. The organization should consider their budget before selecting a specific RAID type, as hardware costs more than a software-based RAID system.

Hardware RAID

This is where the processing is done, such as on a motherboard or a RAID expansion card. In a hardware-based RAID, logical disks are configured and mirrored on the hardware. A physical controller is located on the PCI bus and manages the application data and operating system(s). The controller prevents the drives from data loss and enhances the read-write operations.

RAID levels 0, 1, 3, and 5 are compatible with a hardware RAID. A hardware RAID provides an efficient and nonstop recovery from media failure. Performance based advantages are much higher with a hardware RAID. For example, the implementation of RAID level 5 will better enhance data throughput than a software-based RAID. Multiple controllers can be added to improve read-write performance and total storage capacity.

A hardware RAID can be implemented with a complex and critical setup, or with large databases.

- **Advantages:**

  1. **Write-back mode:** A typical hardware controller has a battery backup unit (BBU). The hardware RAID can work in a write-back mode because of the BBU feature. If there is a power failure while writing data to a drive, the data will not be lost or deleted.

     The BBU plays an important role in the write-back mode.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

2. **Hot swapping:** Many controllers in a hardware RAID support hot swapping. A disk can be replaced while the server is still running, while not affecting the organization's productivity.
3. **Higher throughput:** With the availability of a BBU, a hardware RAID offers a higher read and write throughput, thereby increasing the RAID level's overall performance.
4. **Rebuild:** Rebuilding disk sets can be easier with the availability of a BBU. A BBU speeds up the rebuild process by decreasing the total amount of time it takes to rebuild.
5. **Overhead:** A hardware RAID requires external hardware to function. It does not affect the CPU or RAM overheads on the host machines.
6. **Boot loader:** A hardware RAID can recover from a boot loader failure.

- **Disadvantages:**

1. **Expensive:** A hardware RAID implementation requires an external RAID card or external hardware. This adds to the overall implementation cost, making it more expensive.

Software RAID

A software RAID uses software instead of hardware for its implementation. Unlike a hardware RAID that uses a controller, a software RAID uses system processors and other applications to work. A software RAID is implemented in the operating system or at the kernel level. The performance of a software RAID depends on the CPU performance. A software RAID relies on a standard host adapter, and executes all I/O commands using mathematical calculations. RAID levels 0, 1, and 5 are compatible with a software RAID.

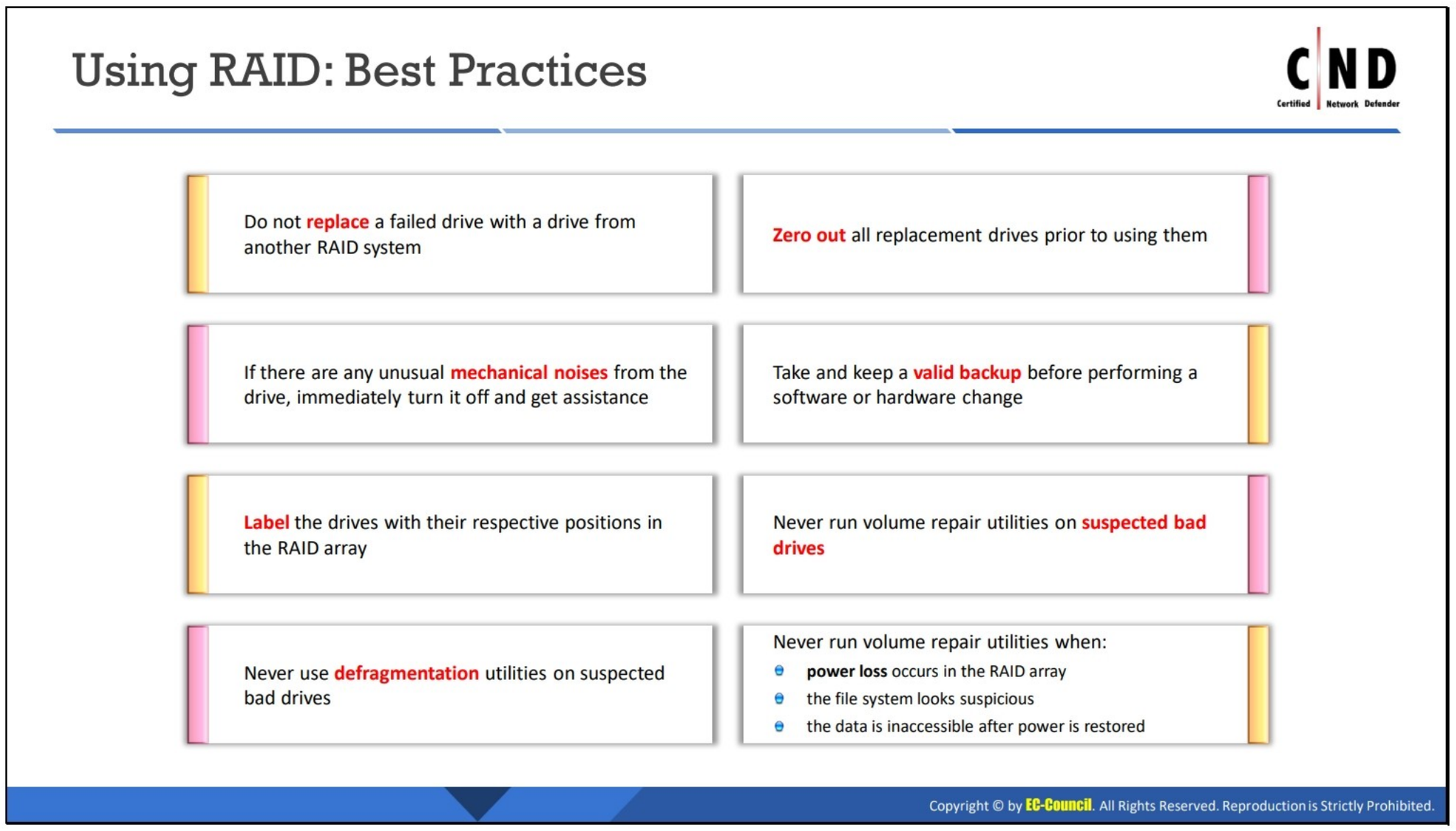
- **Advantages:**

1. **Cost effective:** A software RAID is part of the operating system. Thus, no additional items are needed, which keeps the cost for its implementation under control. It is more cost effective than a hardware RAID implementation.
2. **Simplicity:** A software RAID does not need a hardware controller. Thus, there are no complexities in its implementation.
3. **Duplexing:** Duplexing in a software RAID requires only a standard controller.

- **Disadvantages:**

1. **Performance:** The performance of a software RAID depends on the CPU usage, as it uses the CPU cycle of the host machine. Thus, a software RAID's performance is lower than that of a hardware RAID.
2. **Boot loader failure:** A software RAID requires an operating system to function. Thus, a boot loader failure will lower disk performance.
3. **Compatibility:** Certain software and operating systems may not be compatible with the RAID levels. This can lead to a conflict with the disk array.
4. **Advanced features unavailable:** Software RAID does not offer hot swapping or drive swapping features.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

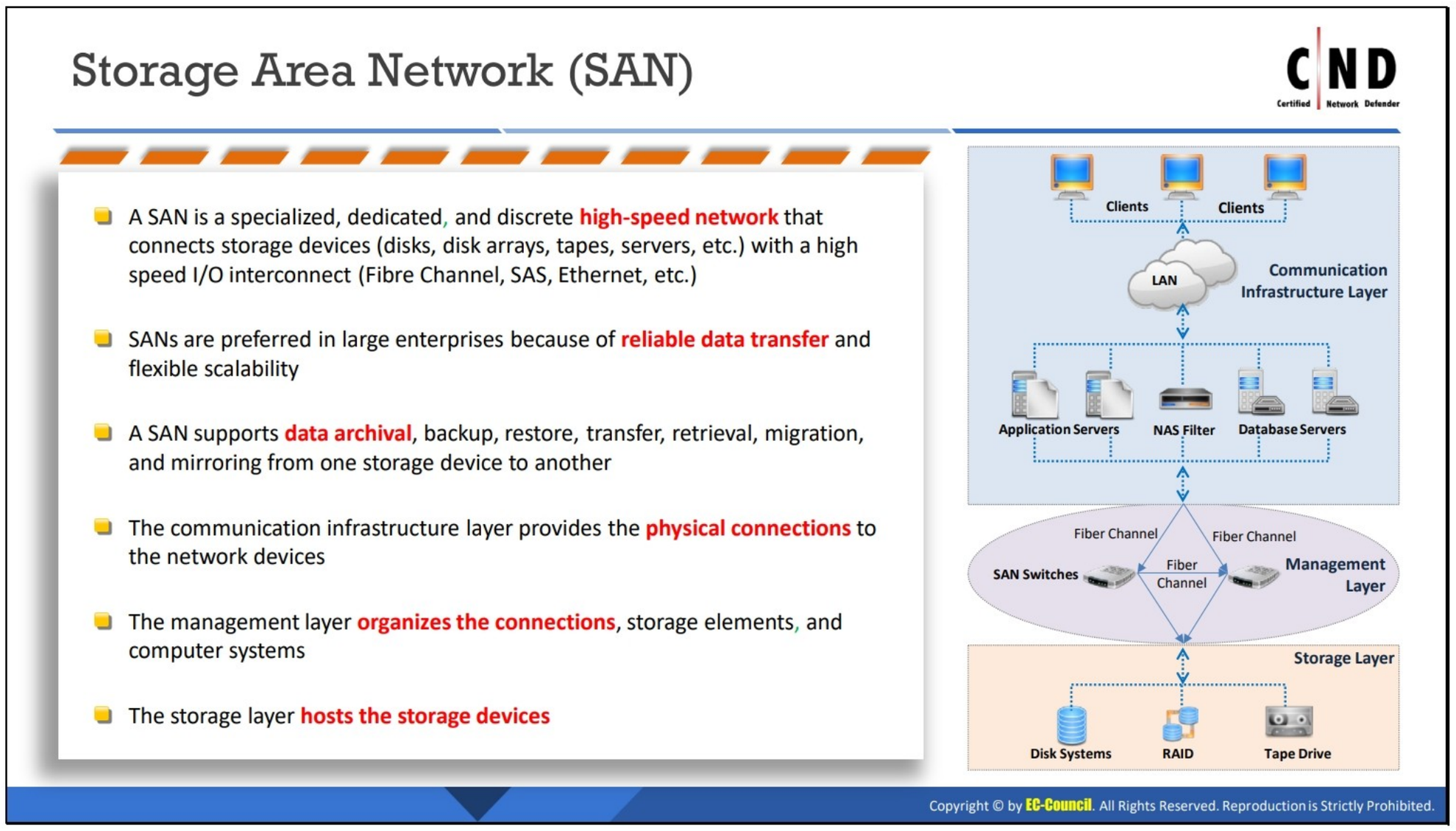


Using RAID: Best Practices

The following are some additional best practices for selecting and using RAID:

- Always select a RAID level that can handle the workload.
- Always be cautious about the storage capacity while selecting a RAID level.
- Do not lose the balance between cost and performance.
- Always ensure the chosen RAID level is according to the needs of the organization.
- Avoid replacing a failed drive that was a part of another RAID system.
- Always seek assistance if there are any unusual noises from the system.
- Label hard drives with their respective RAID array positions.
- Always select a RAID group according to the logical unit numbers accommodated by the server.
- Avoid making any changes to the data in a RAID.
- Always use hard drives of equal sizes in RAID groups.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Storage Area Network (SAN)

A storage area network (SAN) is a high performance network that interconnects storage devices with multiple servers. The role of a SAN is to transfer stored resources available on the common network and reorganize them on an independent and high-performance network. This helps the servers to share their storage across the network. Primarily, a SAN enhances storage devices such as tape drives, disk drives, file servers, RAID, etc. A SAN implementation makes disk maintenance controllable and easier. The implementation needs a cable, a switch, and host bus adapters. Each storage system on the SAN must be interconnected, and in case of a physical interconnection, the bandwidth should support extreme data activities.

We know that systems in a network connect to storage devices. However, a SAN implementation is necessary to ensure that all systems in a network are connected to each available storage device on the network. SAN allows these systems to take the ownership of storage devices; systems can exchange the ownership of storage devices among themselves.

Understanding Storage Sharing

The working of a SAN depends on client-server communication. Every organization has multiple servers that are connected to the systems.

Example: If computer A needs some data from computer B, it will need a copy of the data from the server to which computer B is connected. This can be done through file transfer, inter-process communication, and backup. Although the data is transferred from computer B to computer A, it is possible that computer A may encounter untimely data errors, an expensive transfer between the two servers, or other operational processes. SAN architecture is the perfect solution for this issue. In SAN architecture, all servers are connected to storage devices such as tape drives, RAIDs, disk systems, etc. through a fiber channel. Thus, instead of communicating with

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

computer B for the data, computer A can directly get a copy of the data from the storage devices connected to the servers. For this process to be successful, data storage devices act as a common access point for all the servers.

SAN storage sharing eliminates the scheduling of data transfers among servers. It reduces the cost of data transfer among servers. Storage devices help in timely transfer of data. SAN storage offers only block-level operations that do not provide file abstraction.

However, if the file systems are structured on top of SAN, file access is provided which is known as a SAN file system.

Now-a-days, in large organizations, SAN is a storage pool for servers that are connected via a network. The fiber channel is now replaced by iSCSI, which has become the choice of many mainstream organizations. Whatever be the size of the organization, SAN has become a consolidation of workloads in the network.

Types of SAN

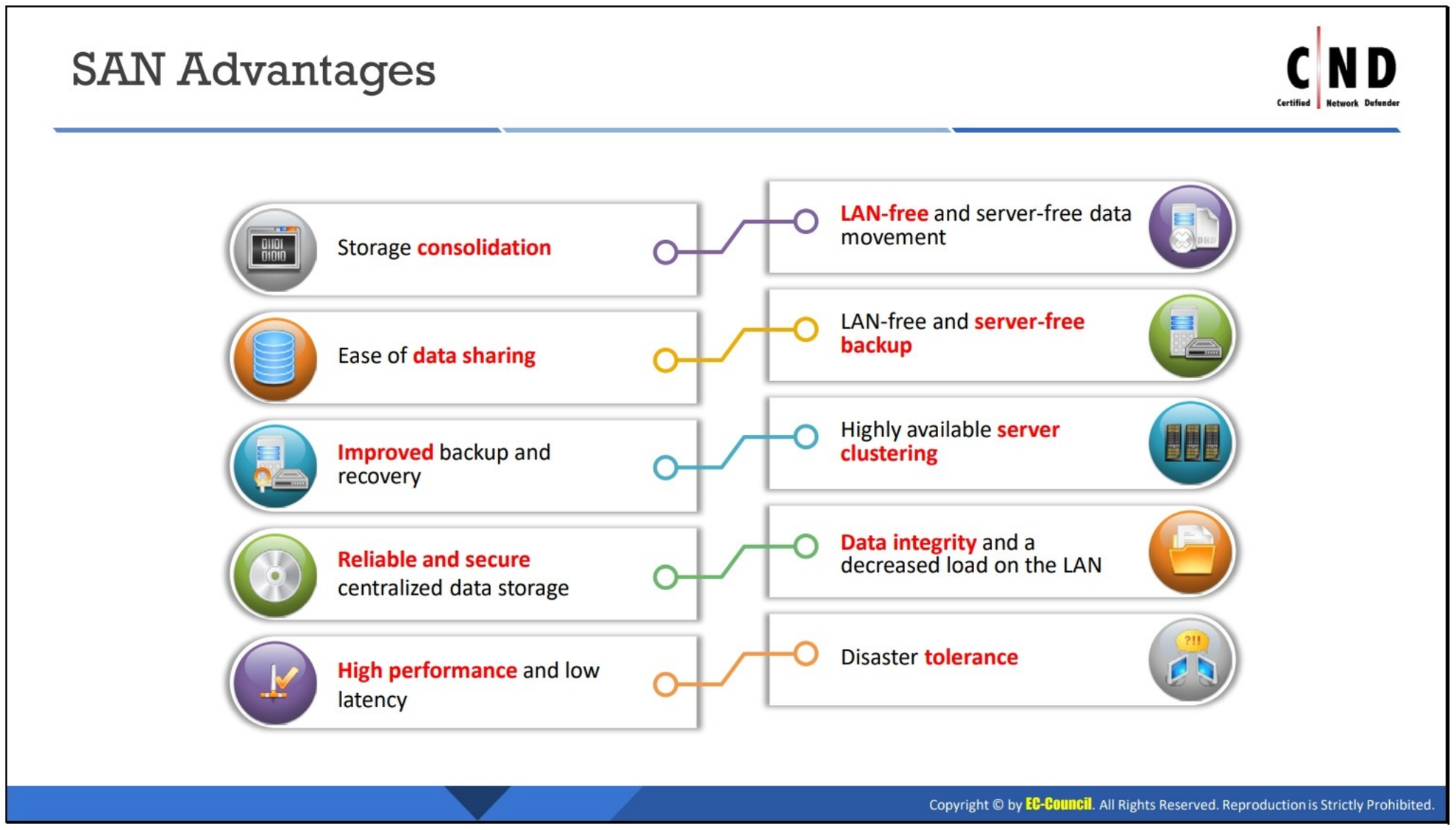
1. **Virtual SAN (VSAN):** VSAN by Cisco is a logical partitioning within the physical SAN. VSAN allows the allocation of some or entire network storage resources to logical SANs. VSAN is mainly used in cloud computing and virtualization environments. It can be used to build a virtual storage.

   The working of VSAN is similar to a traditional SAN; since it has a virtualized environment, the addition or relocation of end users is possible. This will not affect or change the physical layout of the network. Implementation of VSAN enhances the entire network's security.

2. **Unified SAN:** Unified SAN is also known as network unified storage or multiprotocol storage. It allows the applications and files to perform actions through a single device. It handles data storage and block-based input/output operations. It merges files and block-based access in a single storage network. Unified SAN is cost effective as it saves the hardware expenses. By storing the combined modes in a single device, a unified SAN is easily manageable, although it is advisable to deploy critical applications on block-based storage systems.

3. **Converged SAN:** A converged SAN uses a common network arrangement for network and SAN traffic. This reduces the SAN's cost and complexity. Converged SANs depend on 10 Giga-bit Ethernet and network ports.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



SAN Advantages

With rapidly developing technologies and increasing data volumes, organizations need a storage device that can fulfill and handle their needs. The below-mentioned advantages of SAN help in its deployment in an IT infrastructure.

Advantages

1. **Capacity:** SAN performance is directly proportional to the network type. A SAN allows unlimited sharing of data, regardless of the storage capacity. Its capacity can be extended limitlessly to thousands of terabytes.
2. **Easy sharing:** SAN data is easily shared between systems as it maintains an isolated traffic. The traffic does not interfere with the normal user traffic, thereby increasing data transfer performance.
3. **Security:** If a SAN is configured correctly, the data is secured. Chances of device intrusion is minimal.
4. **Productive:** A SAN is scalable; adding a new disk to the network does not stop the SAN's productivity. When adding a new hard disk, a reboot or shut down is not required.
5. **Availability of applications:** The algorithms in a SAN storage array offer data protection. This results in the availability of applications at all times.
6. **Fast backup:** A data mirror copy can be created instantly. These mirror images can be used as a backup whenever required.
7. **Bootable:** A SAN can run a server without a physical disk, and it can be booted by the SAN. This feature permits access to all page files and applications.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

8. **Distance connectivity:** For better security, storage devices can be kept at an isolated location. One of the features of a SAN is that it can connect with devices up to a distance of ten kilometers.
9. **Recovery:** A SAN is the most reliable data recovery option. Even when the servers are offline a SAN remains available.
10. **Effective utilization:** A SAN is an appropriate option for storage space than local disks. If a system requires more storage, a SAN dynamically allocates the required space. This process is similar to virtual machines.

The implementation of a SAN is beneficial to an organization, especially when considering budget constraints, availability, and employee expertise.

Disadvantage

1. **Very costly:** The implementation cost of a SAN can significantly exceed the available budget. A SAN is an investment, and should only be implemented if it meets the goals of the organization.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

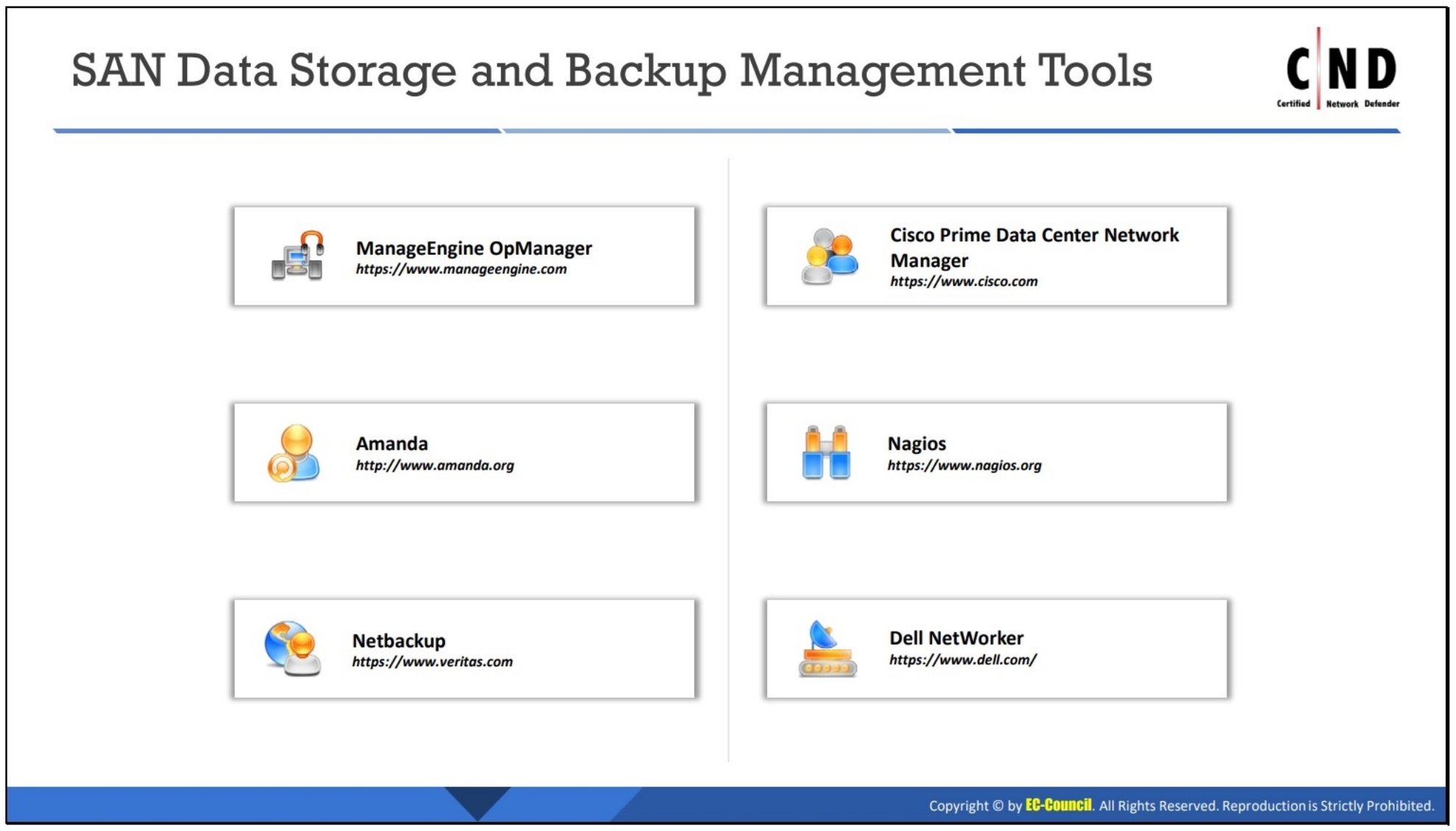


SAN Backup Best Practices

Additional best practices for an effective design, implementation, and performance of a SAN:

- The implementation of SAN technology should incorporate future enhancements in the storage plan of the organization.
- Additional attention is required during the design phase.
- Select topologies that could enhance the performance.
- Always implement smaller SANs for better management.
- Always label the fiber switches as this makes it easier to locate and differentiate between switch types.
- Always prepare a cable connection documentation for the SAN network.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



SAN Data Storage and Backup Management Tools

ManageEngine OpManager

Source: http://www.manageengine.com

OpStor helps reduce the clutter of point products in storage by providing a deep insight into backup and maintenance schedules. It also provides a detailed server, client, node, disk, and plug-in report for single and multiple-node configurations of an EMC Avamar backup server.

Amanda

Source: http://www.amanda.org

The advanced Maryland automatic network disk archiver (AMANDA) is a backup system that allows the administrator of a LAN to set up a single master backup server to back up multiple hosts to a single large-capacity tape or disk drive. Amanda uses native tools (such as GNUtar, dump) for backup, and can back up a large number of workstations running multiple versions of Unix/Mac OS X/Linux/Windows.

Symantec Storage Foundation Basic

Source: http://www.symantec.com

The Symantec Storage Foundation (SF) Basic provides a complete solution for heterogeneous online storage management. It is designed for the heterogeneous online storage management of edge-tier workloads with up to four file systems, four volumes, and two processor sockets per system.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

NetBackup

Source: www.veritas.com

NetBackup reduces complexity and makes data protection as manageable as possible for limited staff. NetBackup provides a single solution for the entire enterprise, available on a converged platform, and built to require minimal administration in even the largest, most dynamic environments.

Cisco Prime Data Center Network Manager

Source: http://www.cisco.com

The Cisco Prime Data Center Network Manager (DCNM) is designed to efficiently implement, visualize, and manage the Cisco Unified Fabric. It includes a comprehensive feature set, along with a customizable dashboard that provides enhanced visibility and automated fabric provisioning for dynamic data centers.

Nagios

Source: https://www.nagios.org

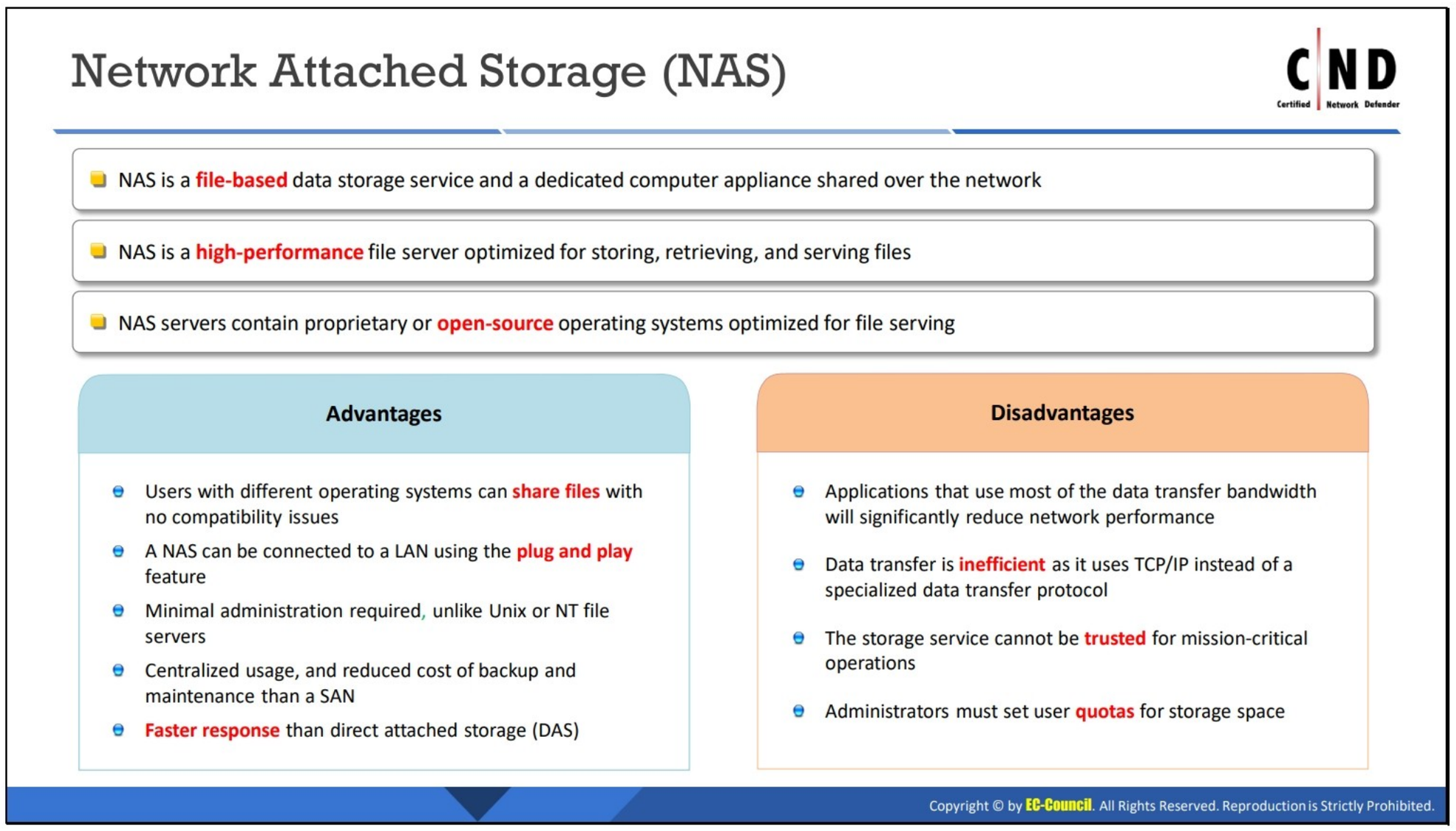
Nagios provides complete monitoring of SAN solutions, including disk usage, directories, file count, file presence, file size, RAID array status, and more.

Dell NetWorker

Source: https://www.dell.com

NetWorker is available as part of Dell Data Protection Suite, which offers comprehensive data protection software applications and tools. NetWorker is delivered as software and as a virtual edition.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Network Attached Storage (NAS)

NAS is a storage device connected to a network. It stores and retrieves data from a centralized location. NAS provides a dedicated shared storage space for a local area network. Implementing a NAS eradicates the server file sharing process on the network. The NAS contains one or more logically arranged storage devices. NAS offers file storage through a standard Ethernet connection.

NAS devices do not use an external device management, and they are operated through a web-based utility. Since it resides on every node on the LAN, it has its own IP address. NAS is similar to a file server. NAS devices are scalable, vertically as well as horizontally. A NAS implementation is accomplished using large and clustered disks.

NAS has evolved from supporting virtualization to data replication and multiprotocol access. A clustered NAS is one such example of the NAS evolution. In a clustered NAS infrastructure, access is provided to all files, irrespective of their physical location. It does not require a closed-source operating system such as Windows. Certain devices run on a stripped down OS such as FreeNAS, or any other open-source solutions.

NAS devices are in high demand in small enterprises because of their effectiveness, low cost, and scalable storage capacity. They are classified into three types based on the number of drives, drive capacity, and scalability.

High-end or Enterprise NAS

This type of NAS is used mainly in business environments where scalability is a concern. Enterprise NAS provides the ability to increase the amount of storage space and redundant power supply.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Small – business Level NAS or mid-market NAS**: Mainly used in business environments requiring one hundred terabytes (100 TB) of data.
- **Low-end or desktop NAS**: Usually used by small business users or home users who require only local storage space.

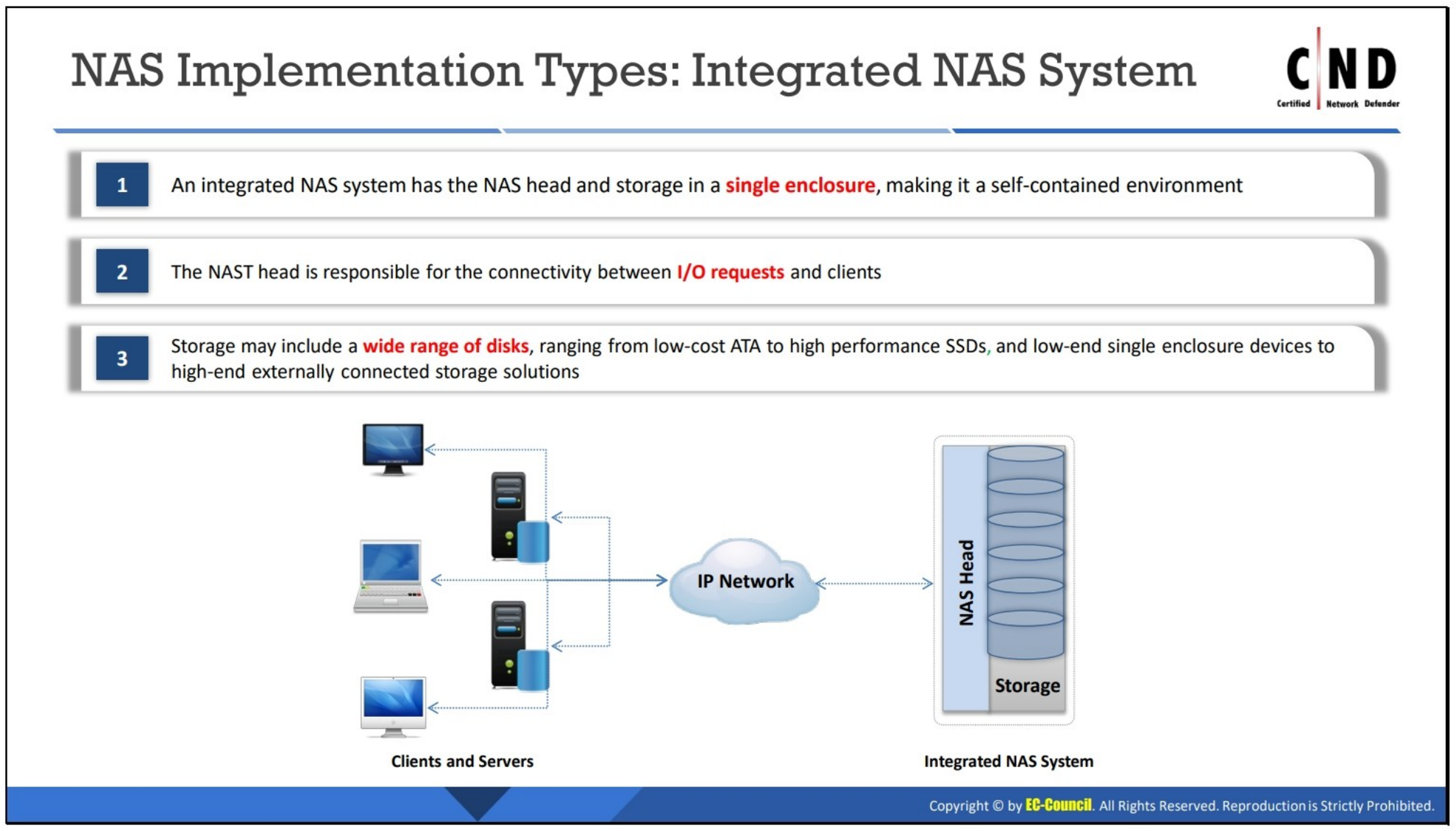
Advantages

1. **Accessibility:** A NAS system stores data as files, and is compatible with CIFS and NFS protocols. Multiple users can access the files simultaneously using an Ethernet network. Computers in a shared network can access the data either through a wireless or a wired connection.
2. **Storage:** NAS deployment in a network increases the amount of storage available to the other systems. A NAS system can store up to 8 TB data. A NAS is most appropriate for storing large applications or video files.
3. **Efficient and Reliable:** NAS assures an efficient transfer of data and reliable network access. If a system in a network fails, the functioning of other systems is not affected. A NAS server can also be created to give users the ability to access large files or applications.
4. **Automatic backup:** Certain NAS devices are configured with an automatic backup feature. The data is available on the user system as well as on the server hard drive. Changes made on the user system are reflected on the server hard drive as well. Automatic backup is not time consuming and assures the security of data.

Disadvantages

1. **Consumption:** NAS shares the network with other host machines, and this tends to consume a larger amount of network bandwidth. For remote NAS systems, the data transfer performance will depend on the available bandwidth. It is advisable to avoid storing databases on a NAS, as the server response time fluctuates depending on the bandwidth.
2. **Network congestion:** A large backup process can affect the function of an IP network and may lead to network congestion.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



NAS Implementation Types: Integrated NAS System

An integrated NAS system includes all the NAS components in a single frame. To provide connectivity to all clients, the NAS head connects to the IP network. An integrated NAS frame may vary from a low-end device to high-end solutions with external storage arrays.

Low-end devices focus more on data storage than disaster recovery or performance. These are primarily used in small organizations where the amount of available storage space a may increase. Increasing the amount of storage space also increases the management overhead because of an increased number of devices in use.

High-end devices provide additional amounts of storage space and higher scalability.

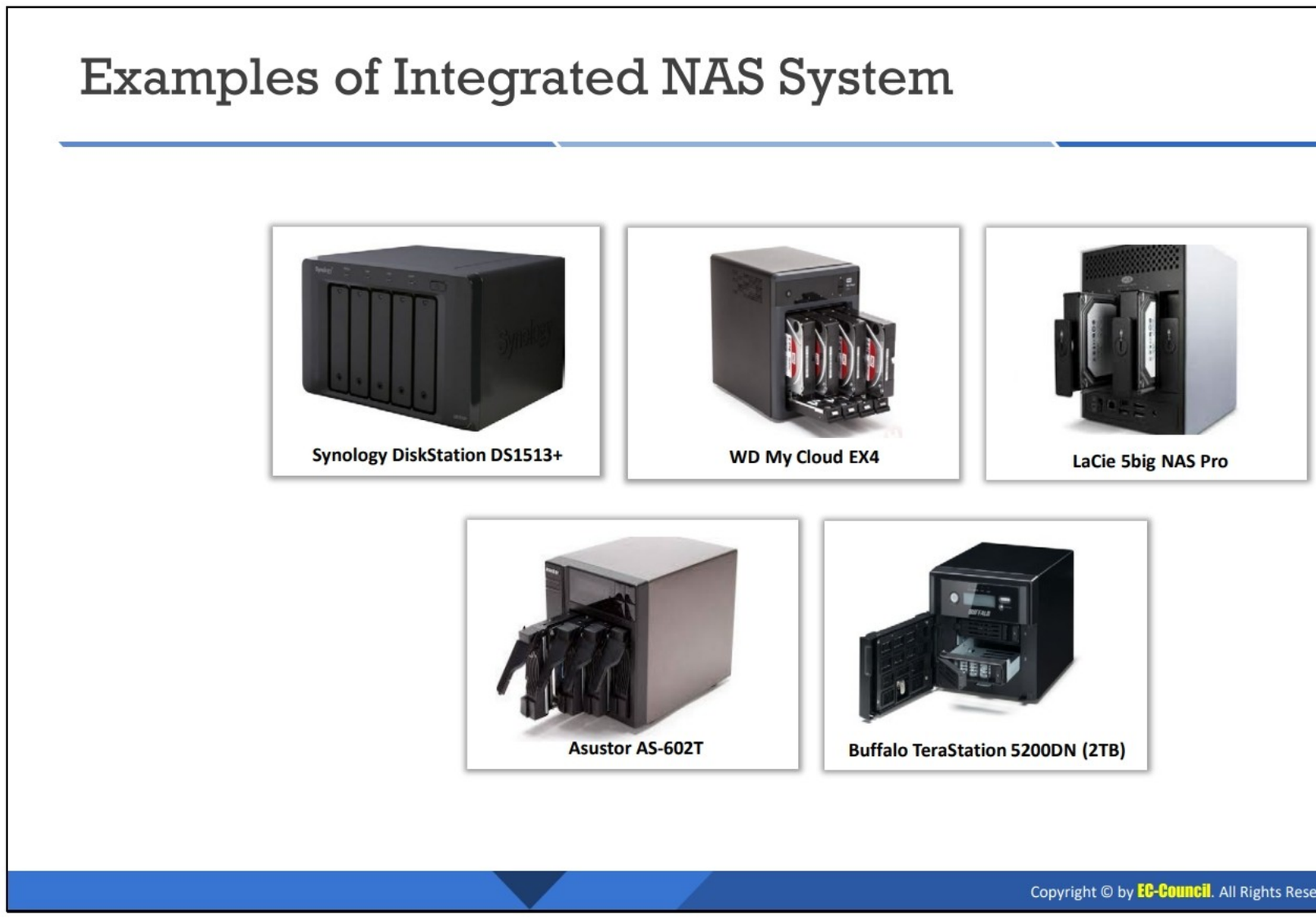
Advantages

- Easy to implement
- Uses simple tools

Disadvantages

- Limited capacity and performance
- No performance upgrade

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Examples of Integrated NAS System

Synology DiskStation DS1513+

Source: https://www.synology.com

The Synology DiskStation DS1513+ offers massive dynamically scalable storage space, stellar performance, and a robust web interface, along with supporting a large number of useful features for home, small, and medium business applications.

WD My Cloud EX4

Source: www.wdc.com

WD My Cloud EX4 offers data redundancy, Windows server integration, and an excellent set of personal cloud features. It is affordable and extremely easy to use. It is not the fastest NAS, nor does it include many advanced features, but still combines great ease of use into an affordable personal cloud system that is excellent for a connected home.

LaCie 5big NAS Pro

Source: www.lacie.com

The LaCie 5big NAS Pro offers super-fast performance and has an excellent drive bay design. The NAS server is also easy to use and can dynamically scale up its storage space.

Asustor AS-602T

Source: https://www.asustor.com

ASUSTOR NAS devices provide optimal data protection through RAID technology. They support a diverse array of automatic backup solutions, guaranteeing the security of data. Seamless cross-

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

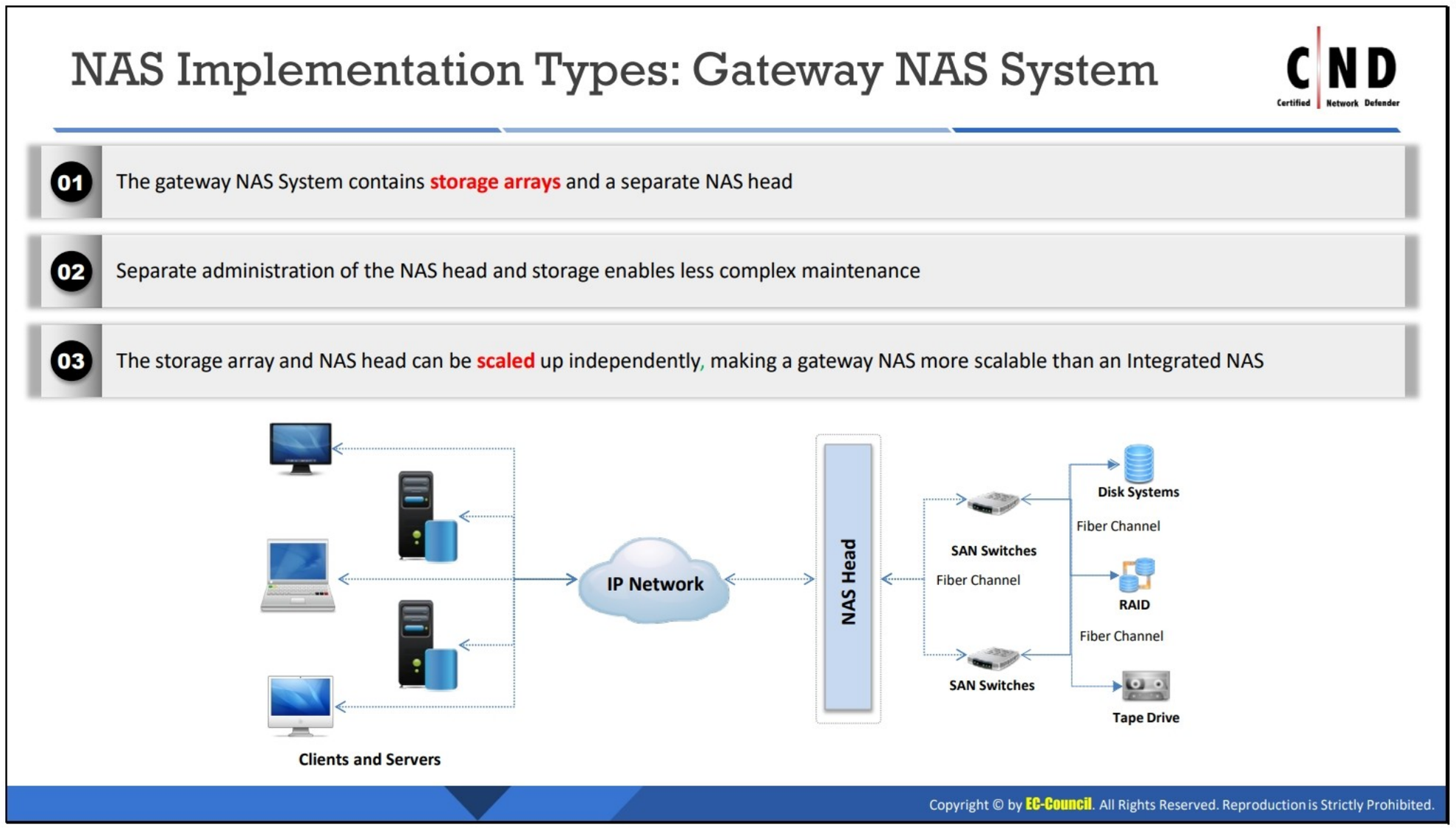
platform file sharing allows an easy connection to the NAS device no matter what OS is used, such as Windows, Mac OS, or Unix-based.

Buffalo TeraStation 5200DN (2TB)

Source: www.buffalotech.com

TeraStation 5200 is a high performance 2-drive network storage solution ideal for businesses and demanding users requiring a reliable RAID based NAS and iSCSI storage solution for larger networks and business-critical applications.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



NAS Implementation Types: Gateway NAS System

A NAS gateway is considered as an appliance attached to an already existing SAN. In this NAS implementation, a SAN deals with the storage and a NAS gateway deals with a section of the block storage capacity. File-based storage is used in a gateway implementation.

The drawbacks of a gateway NAS implementation are:

- The NAS hardware is comparatively costlier than other file servers.
- Difficult for users to manage the block-level storage of SAN, which is attached to the NAS head.
- The NAS GUI is entirely different from that of a SAN, making its management difficult for users.

A NAS gateway system includes an independent NAS head and multiple storage arrays. A NAS gateway requires additional management functions than an integrated NAS. It provides high scalability as the NAS head and storage arrays scale up according to the requirements of the organization. A NAS gateway, when combined with a SAN, provides a large storage capacity.

Increased scalability by adding more NAS heads can make it difficult to determine the network requirements for a gateway environment. A fiber channel SAN may be used for the connection between a gateway NAS and a storage system.

Advantages

- Ability to use available SAN storage.
- Upgrades front-end and back-end separately.

Disadvantages

- Capacity depends on the available storage space on the NAS system.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



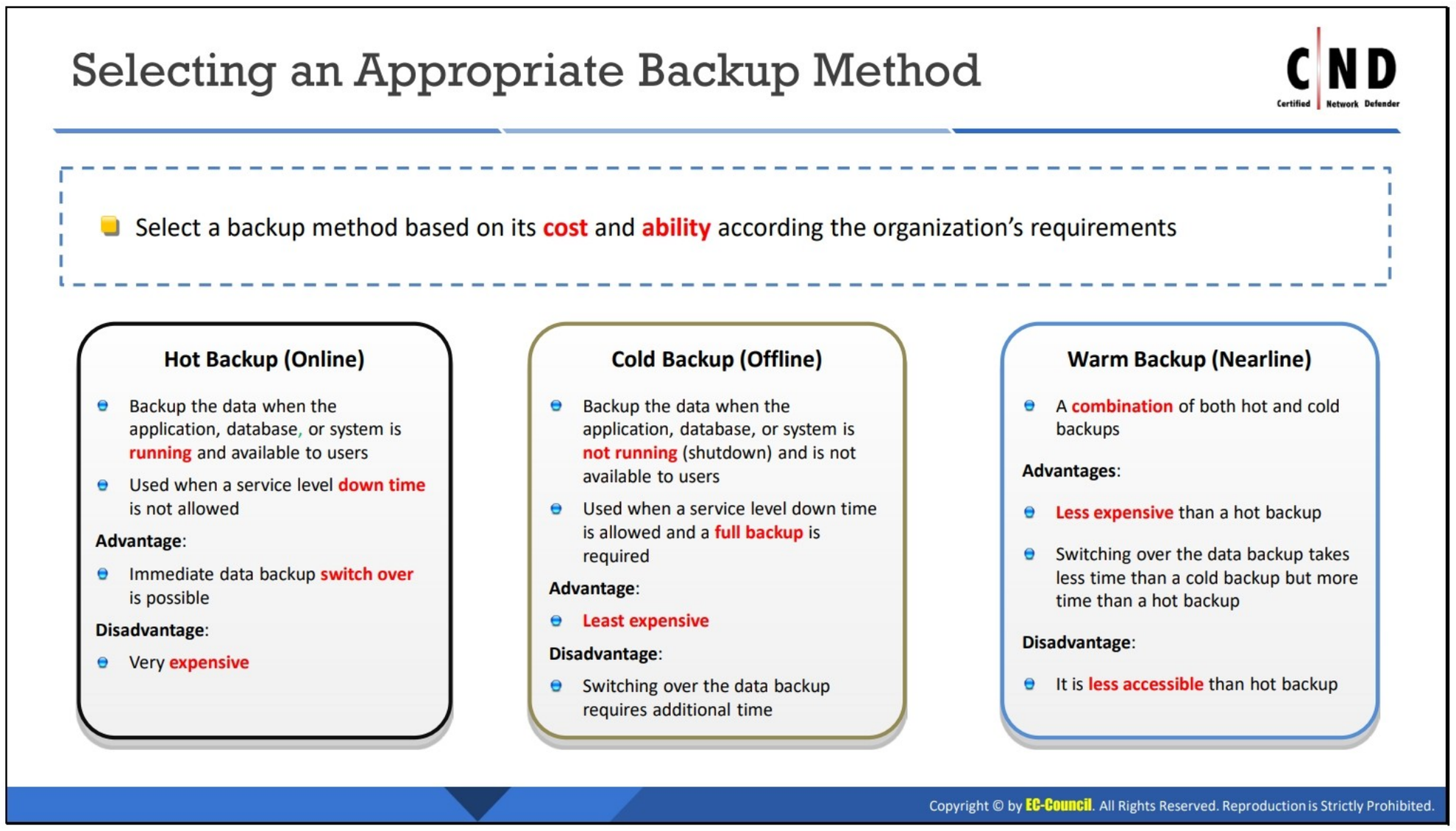
Gateway NAS System: FreeNAS

Source: http://www.freenas.org

FreeNAS is an operating system that can be installed virtually on any hardware platform to share data over a network. It is the simplest way to create a centralized and easily accessible location for data. FreeNAS with ZFS protects, stores, and backups all data. FreeNAS is used everywhere, from homes to small businesses and large enterprises. Some FreeNAS features are as follows:

- **Web interface**: Simplifies administrative tasks. Every aspect of the FreeNAS system can be managed from a web interface.
- **File Sharing**: SMB/CIFS (Windows file sharing), NFS (Unix file sharing), AFP (Apple file sharing), FTP, and iSCSI (block sharing).
- **Snapshots**: Snapshots of the entire file system can be created and saved at any time. Files can be then accessed as they were when the snapshot was created.
- **Replication**: The replication feature is used to send snapshots over the network to another system for a true offsite disaster recovery.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Selecting an Appropriate Backup Method

Organizations can choose any backup method depending on their budget and IT infrastructure. The different types of data backup methods are:

Hot Backup

A hot backup is a popular backup method. It is also called as dynamic backup or active backup. In a hot backup, the system continues to perform the backup even when the user is accessing the system. Implementation of a hot backup in an organization avoids downtime. However, changes made to the data during the backup process is not reflected in the final backup file. In addition, while the backup is in process, the users may find the system to be slow. A hot backup is an expensive process.

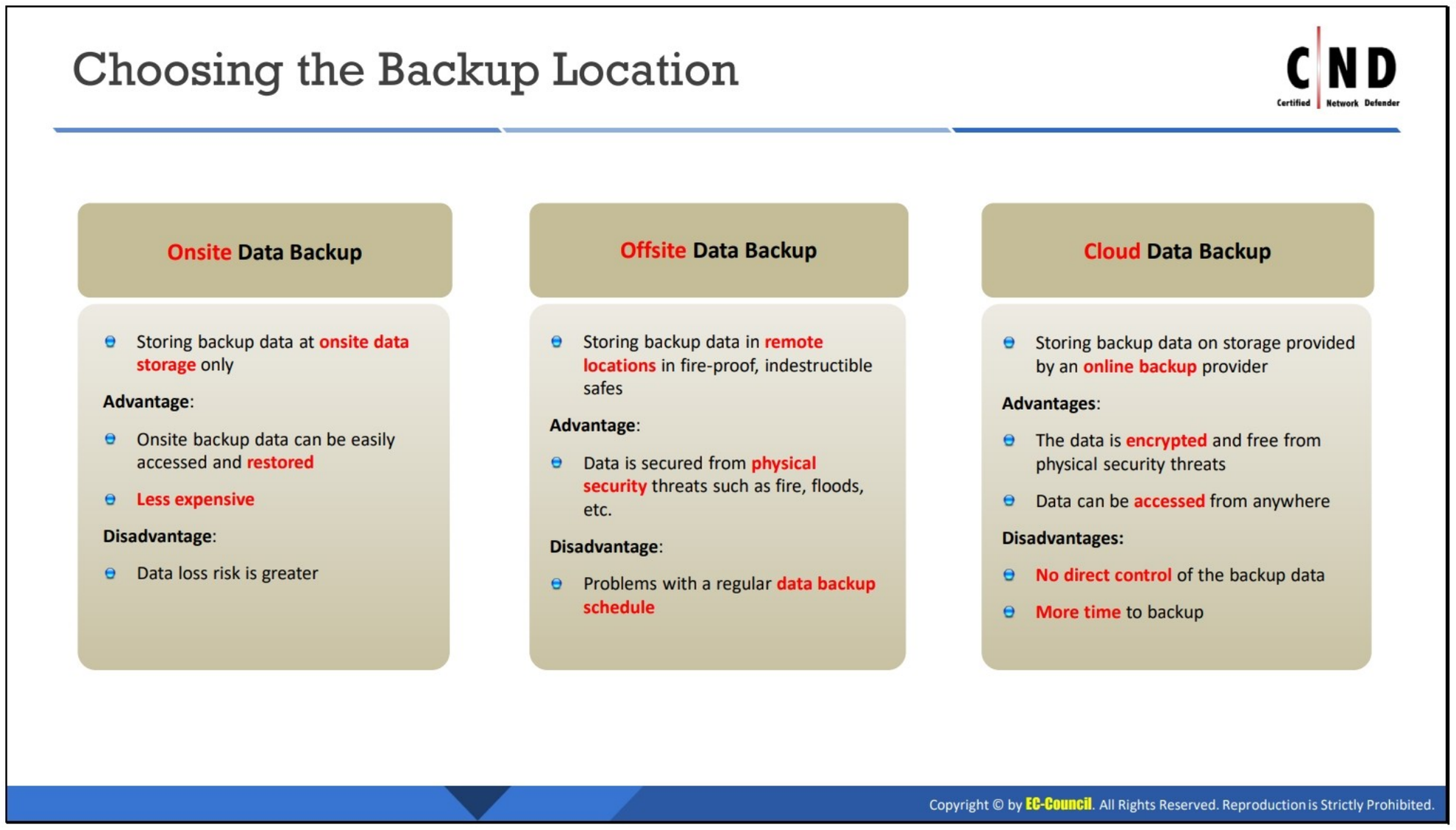
Cold Backup

A cold backup is also called an offline backup. A cold backup can take place when the system is not working or is not accessible by users. A cold backup is the safest backup method as it avoids the risk of copying the data. A cold backup involves downtime as the users cannot use the machine until the process is back online. A cold backup is not as expensive as a hot backup.

Warm Backup

A warm backup is also called a nearline backup. It will have a connectivity to the network. In a warm backup, the system updates are turned on to receive periodic updates. It is beneficial when mirroring or duplicating the data. The warm backup process can take a long time, and can be conducted in intervals that can last from days to weeks.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Choosing the Backup Location

Onsite Data Backup

This type of backup is performed within an organization. Onsite backup uses external devices such as a tape drive, DVD, hard disk, etc. The choice of external storage will depend on the amount of data to be backed up.

- **Advantages:**
  - Provides immediate access to data.
  - Less expensive.
  - Media used for onsite backup is readily available and costs less.
  - Faster recovery.
  - Enhanced scalability.
  - Internet access is not required.
- **Disadvantages:**
  - Requires direct human interaction to perform the backup.
  - Susceptible to theft or natural disasters.

Offsite Data Backup

In an offsite backup, the backup is done at a remote location. It either stores the data on physical drives, online, or a third-party backup service. Storing the data online helps in having an updated data backup available.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

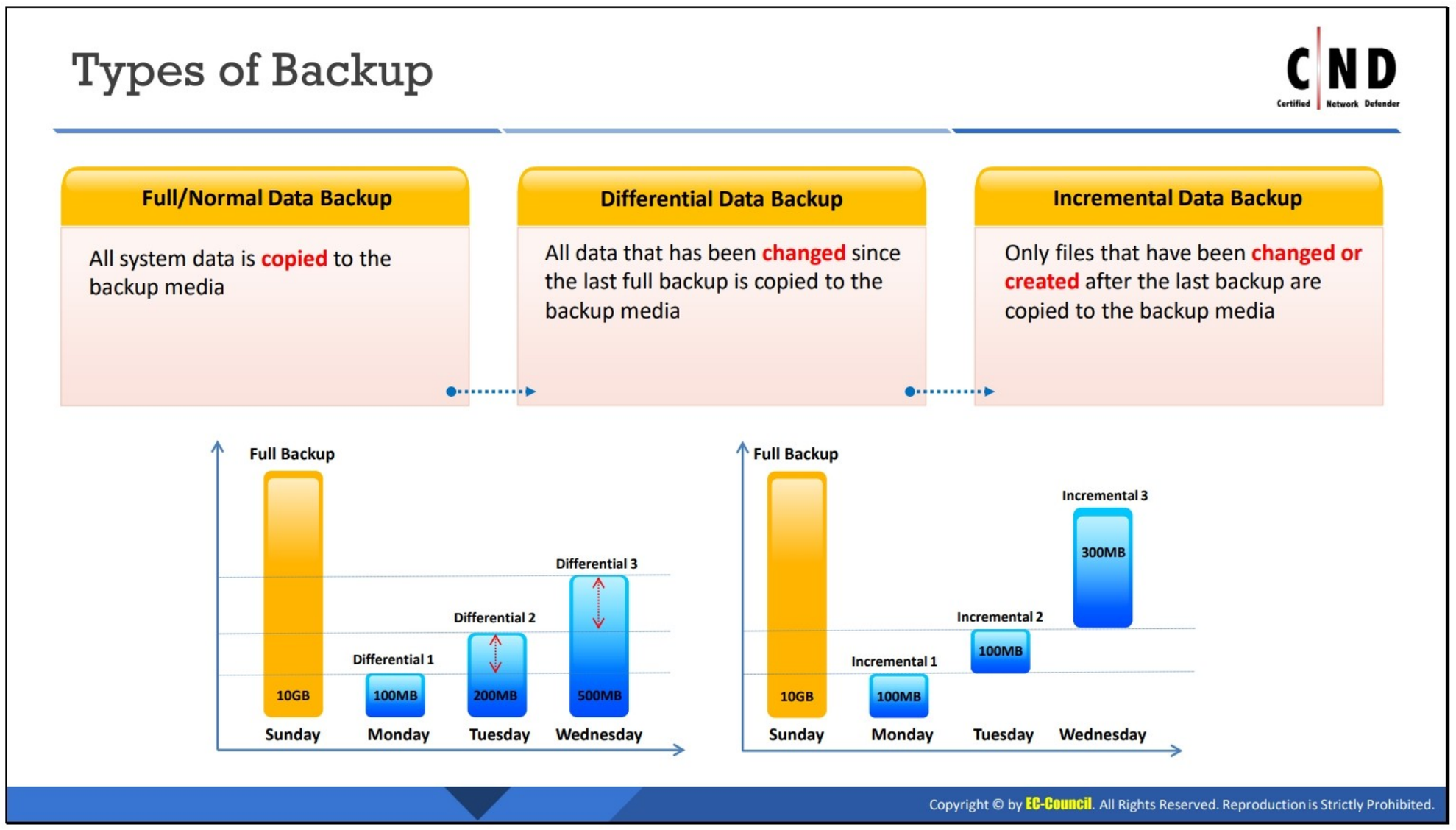
- **Advantages:**
  - Implementing offsite backup creates multiple copies that can be stored in multiple locations.
  - Human error is minimal as the backup process is automated.
  - Data retention is unlimited.
- **Disadvantages:**
  - It is expensive, requiring a third-party service.
  - Requires an Internet connection, and the bandwidth consumption will be higher.
  - The process is lengthy and time consuming.

Cloud Data Backup

A Cloud backup is also known as online backup. It involves storing the backup on a public network or on a proprietary server. Usually, a third-party service provider hosts the proprietary server. The cloud data backup process works according to the requirements of the organization. If the organization needs a daily backup, the proprietary server will run a daily backup. Usually, any noncritical data is archived using a cloud data backup.

- **Advantages:**
  - Cloud data backup is efficient as it uses technologies such as disk-based backup, virtualization, encryption, etc.
  - Many proprietors provide data monitoring and create reports for the organization.
  - The data in a cloud backup is easily accessed through the Internet.
- **Disadvantages:**
  - Data recovery can be time consuming.
  - Cloud data backup proprietors do not give any assurances or guarantees on the completion of a backup. The organization is responsible for checking whether the backup process was successful.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Backup

An appropriate backup type is one that does not have a major impact on bandwidth, cost, time required, and the organization's resources. The three most common backup types are full, differential, and incremental.

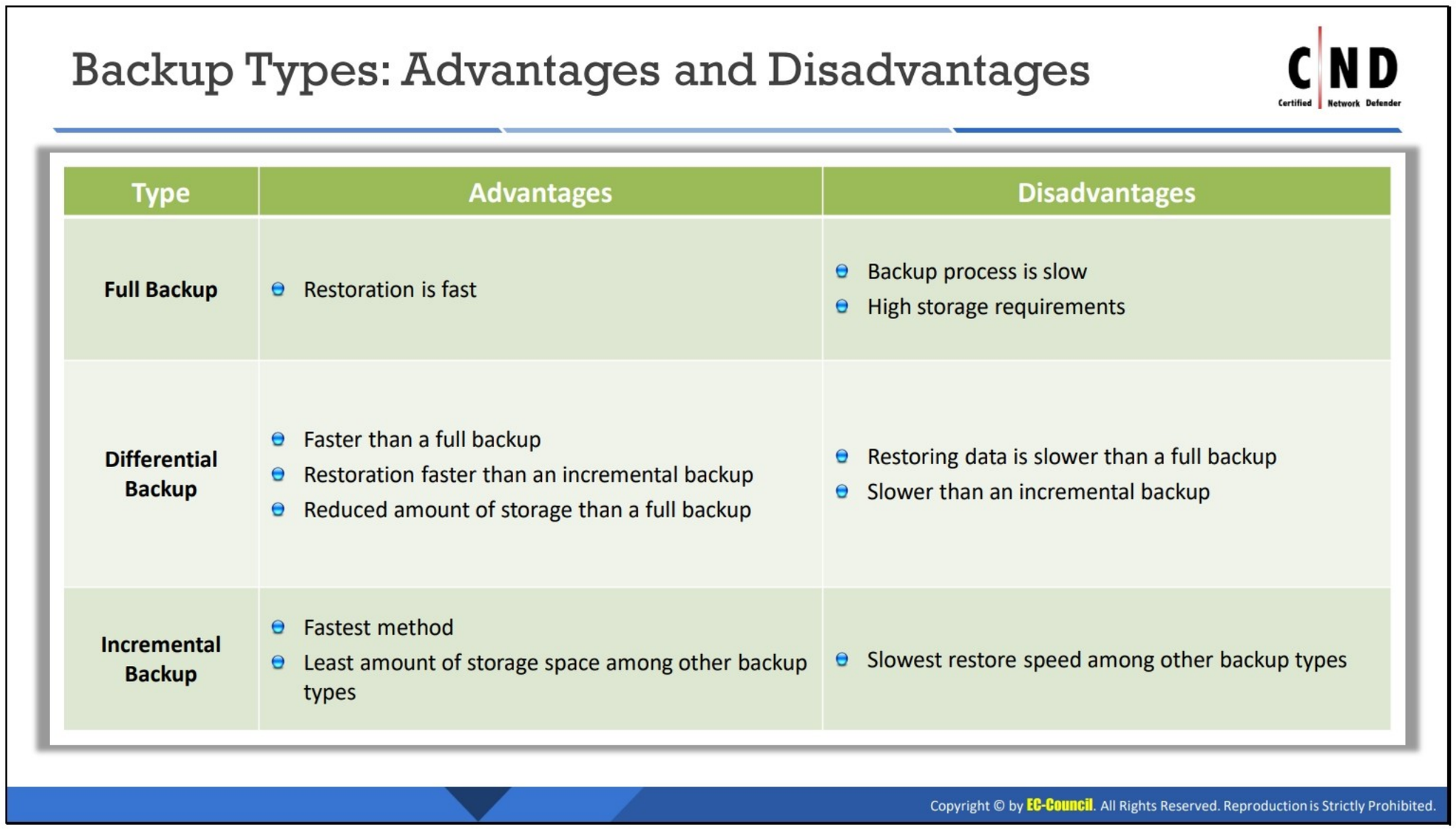
Backup Types

- **Full backup:** This is also called a normal backup. A full backup occurs automatically according to a set schedule. It copies all files and compresses them to save space. A full backup provides efficient data protection for the copied data.
- **Incremental backup:** Backups only the data that has changed since the last backup. The last backup can be of any type. Before an incremental backup is performed, the system should be backed up using a full or normal backup.

  Example: Assume a full backup of the system is scheduled for Sunday, and an incremental backup is scheduled from Tuesday to Saturday. Once the full backup is performed on Sunday, the incremental backup on Monday will only backup the changes that occurred on Sunday. This process will continue until Saturday.
- **Differential backup:** Differential backup is the combination of a full backup and an incremental backup. A differential backup backs up all the changes made since the last full backup.

  Example: Considering the above example, assume a full backup is scheduled for Sunday, and then a differential backup is scheduled to run until Saturday. Once the full backup is completed on Sunday, the differential backup will occur on Monday and the data that was changed will be backed up. On Tuesday, the backup will be for the changes made on Sunday and Monday. Then, on Wednesday, it will include the changes from Sunday, Monday, and Tuesday.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Backup Types: Advantages and Disadvantages

Compare the advantages and disadvantages of each backup type, and then select one that is best suited for the organization.

Full Backup

- **Advantages:**
  - It is easy to restore; the process requires a file name and location.
  - Maintains different versions of the data.
- **Disadvantages:**
  - A time-consuming process because each file is backed up every time a full backup is performed.
  - Large storage requirements.

Incremental Backup

- **Advantages:**
  - Faster than a full backup.
  - Uses storage space efficiently, and there is no data duplication.
- **Disadvantages:**
  - Data restoration is time consuming and a complex process; first, a full backup is done, which is followed by an incremental backup.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Differential Backup

- **Advantages:**
  - Faster than a full backup.
  - Uses storage space more efficiently than a full backup; the backup only contains the changes made at regular intervals.
  - Data restoration is faster than an incremental backup.
- **Disadvantages:**
  - Slower than an incremental backup.
  - Restoration process is slower than a full backup.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Windows Data Backup: Disk, Files, and Folders Backup

Use **File History** to backup and restore in Windows. By default, it backs up the system drive. Other drives can be selected for backup if needed. Regular data and settings back up is recommended to prevent data loss.

Steps to Backup your PC with File History

- Select **Start** > **Settings** > **Update & Security** > **Backup** > **Add a drive** +, and then select an external drive or network location for backups.

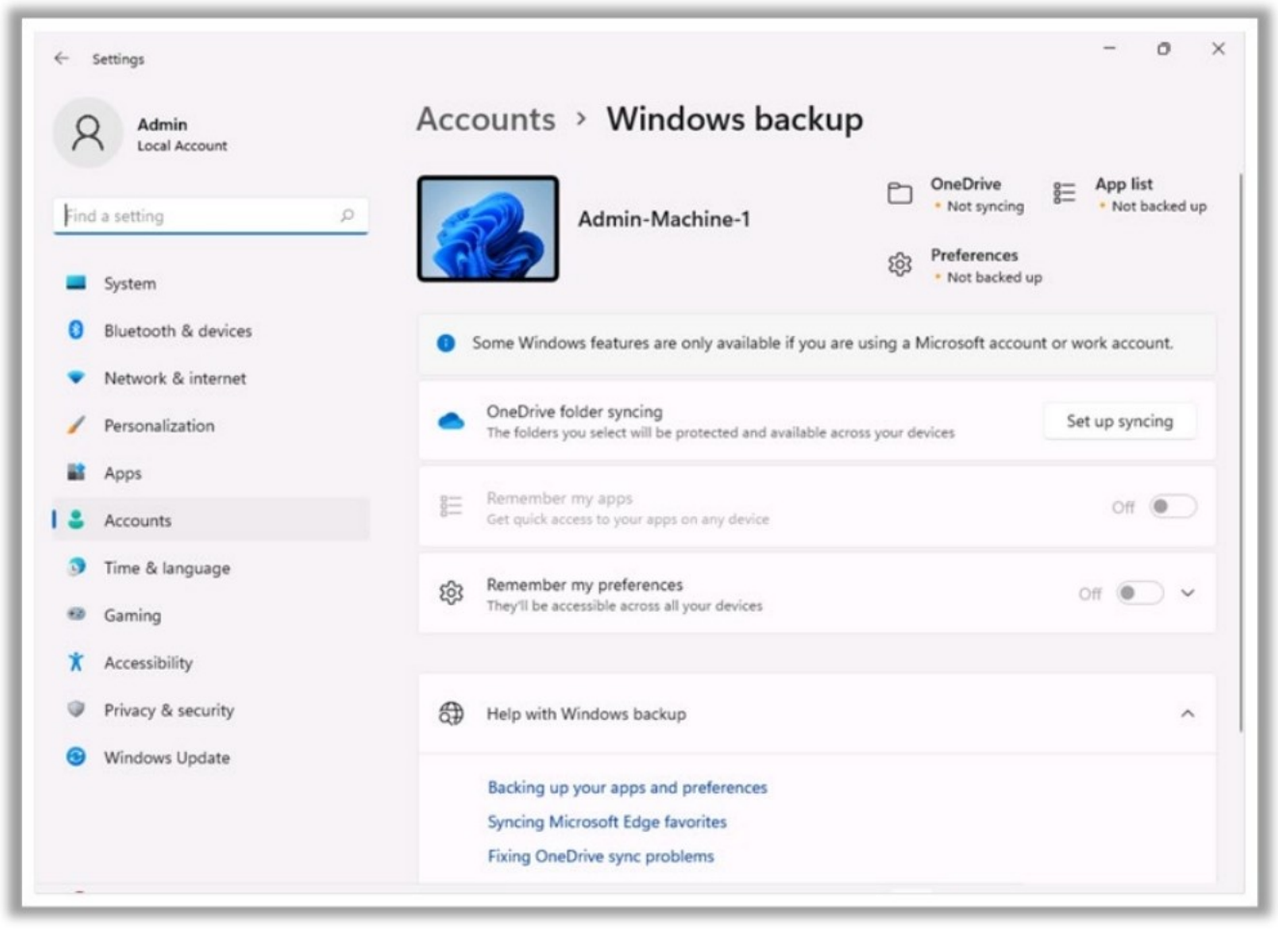


Figure 10.126: Backup PC with File History

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

File History before it is activated in Windows

- Select an external drive. File History is now archiving data. An on/off slider appears under a new heading **Automatically back up my files**.

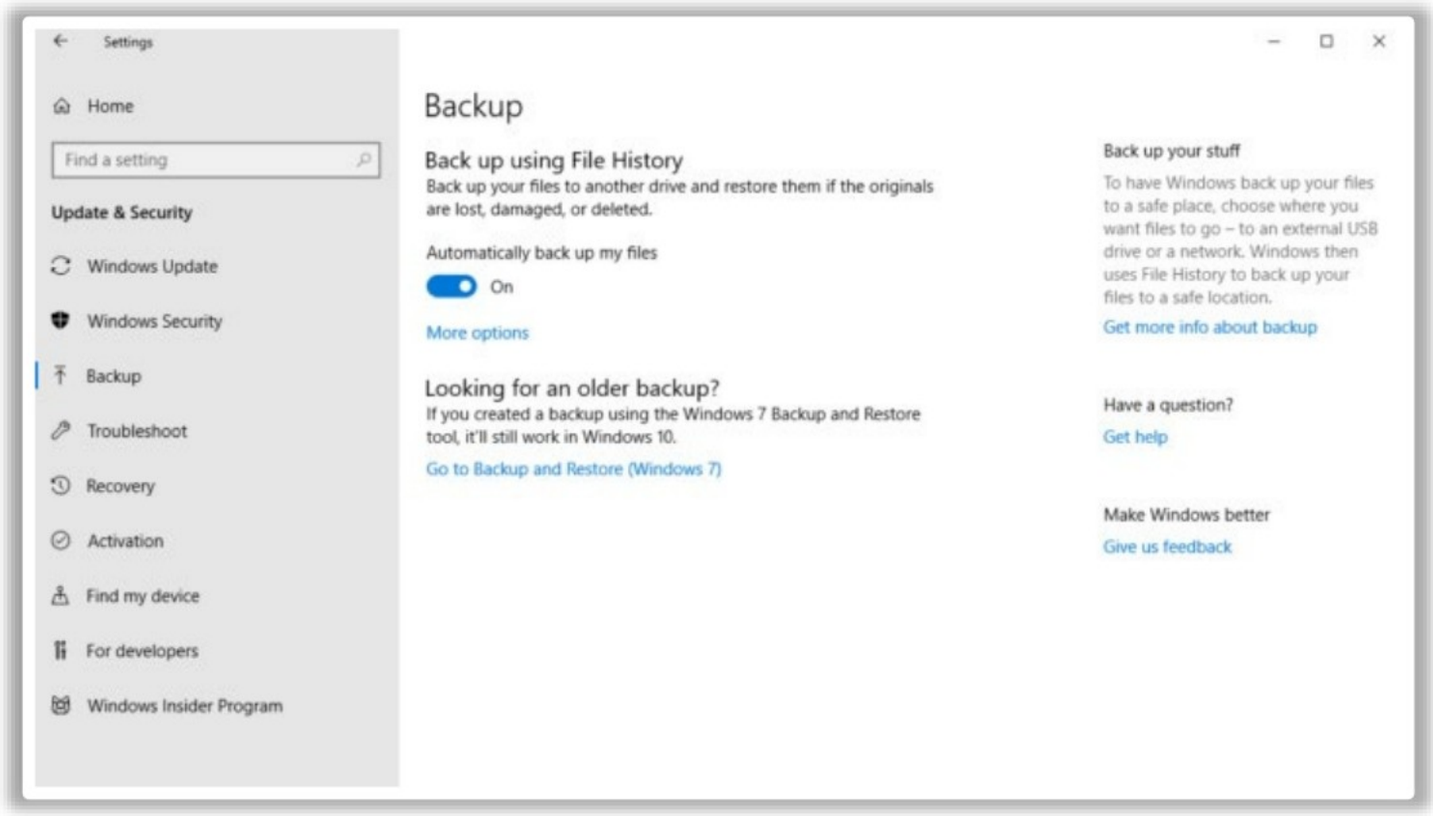


Figure 10.127: Back Up Using File History

- Click **More options** to change the File History defaults.
- By default, Windows File History will back up all folders in the User folder, back up files every hour as long as the backup drive is available, and keep previous copies of the files forever. To change any of these settings, click **More options** under the on/off slider.

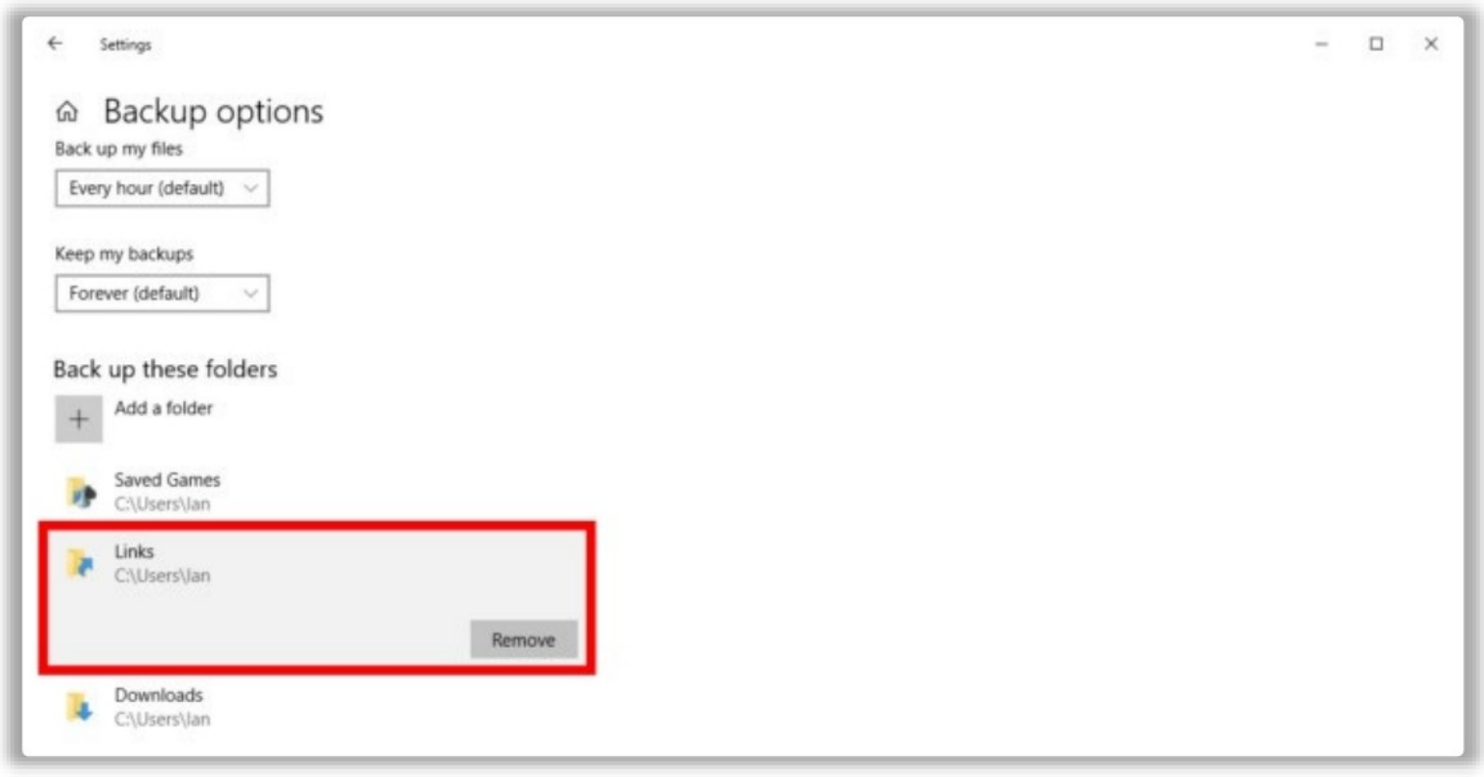


Figure 10.128: Folder Back Up

File History via the Settings app makes it easy to remove folders from your backup list

- In the **Backup Options** window, start a manual backup by choosing the option right at the top.
- Adjust how often to run a backup, with choices ranging from **every 10 minutes** to **once a day**.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- To add a folder to backup, click the "**+**" under **Back up these folders**.
- To remove a folder, scroll down to find it, click on it to highlight, and then click **Remove**.
- Create a list of folders to be specifically excluded, if needed.

(or)

Stop backing up to the currently selected drive and choose another one.

Steps to Restore PC with File History

Follow the steps listed below to retrieve an important file or folder you have backed up.

- In the search box on the taskbar, type restore files, and click **Restore your files with File History**.

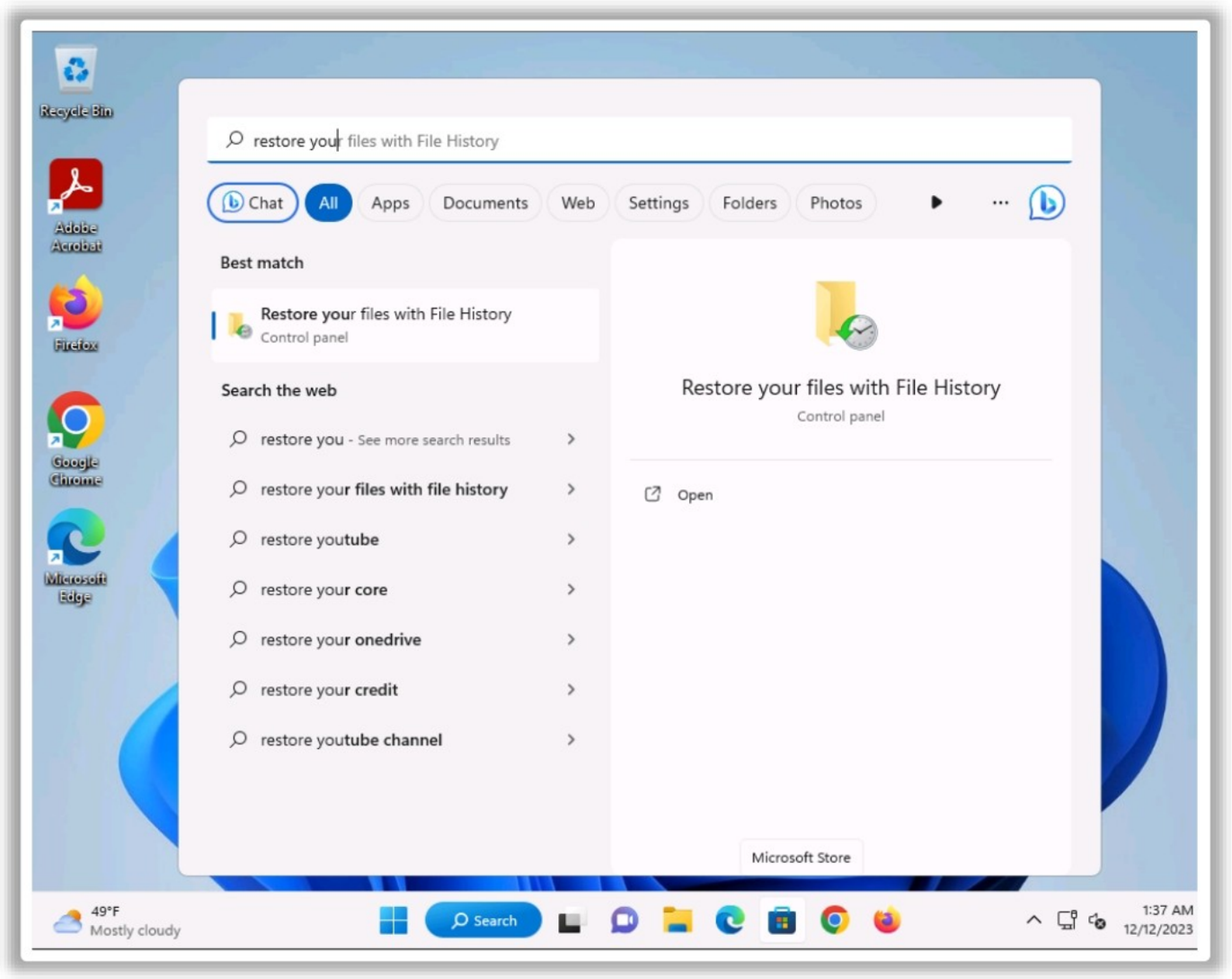
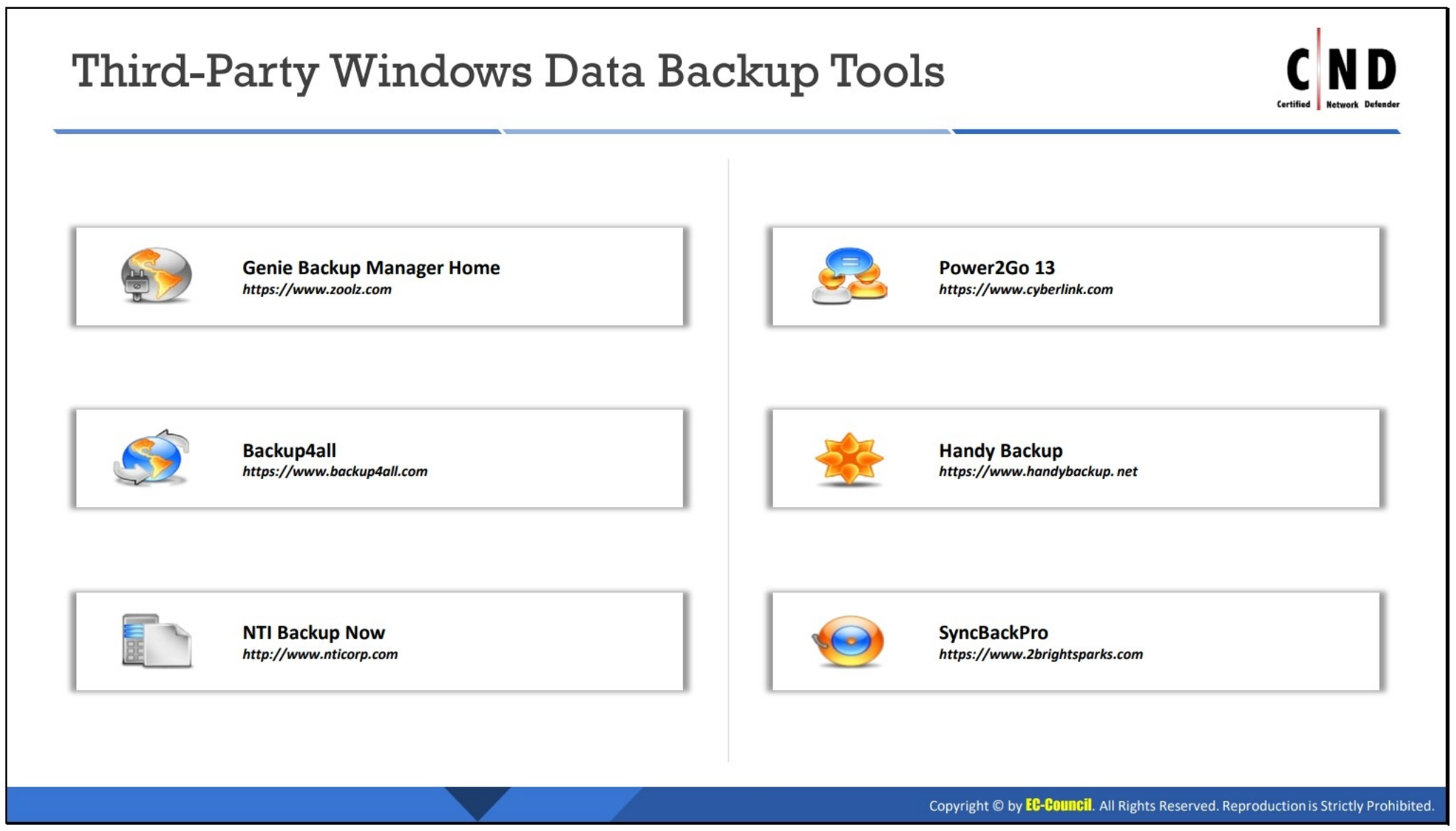


Figure 10.129: Restoring Files with File History

- Search for the file you need, then use the arrows to see all its versions. Upon finding the version you want, select **Restore** to save it in its original location. To save it in a different location, right-click **Restore**, click **Restore to**, and select a new location.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Third-Party Windows Data Backup Tools

Windows data backup tools allow creating copies of files and hard drives to prevent data loss and help restore the original contents in case of data loss. The following are a list of third-party backup tools along with their features.

Genie Backup Manager Home

Source: www.zoolz.com

Genie Backup Manager Home is a tool that provides full control over backup procedures.

NTI Backup Now

Source: www.nticorp.com

NTI Backup Now EZ 6 offers protection for all the digital assets from malicious virus attacks, computer hardware failures, or even a simple human error of deleting an important file by mistake.

Power2Go 13

Source: www.cyberlink.com

Power2Go 13 backups and protects Windows system data to a disk or single USB drive.

Backup4all

Source: www.backup4all.com

Backup4all protects data from partial or total losses. It automates the backup process, compresses the data to save storage space (using standard zip format), and encrypts the backup to protect it from unauthorized use.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Handy Backup

Source: www.handybackup.net

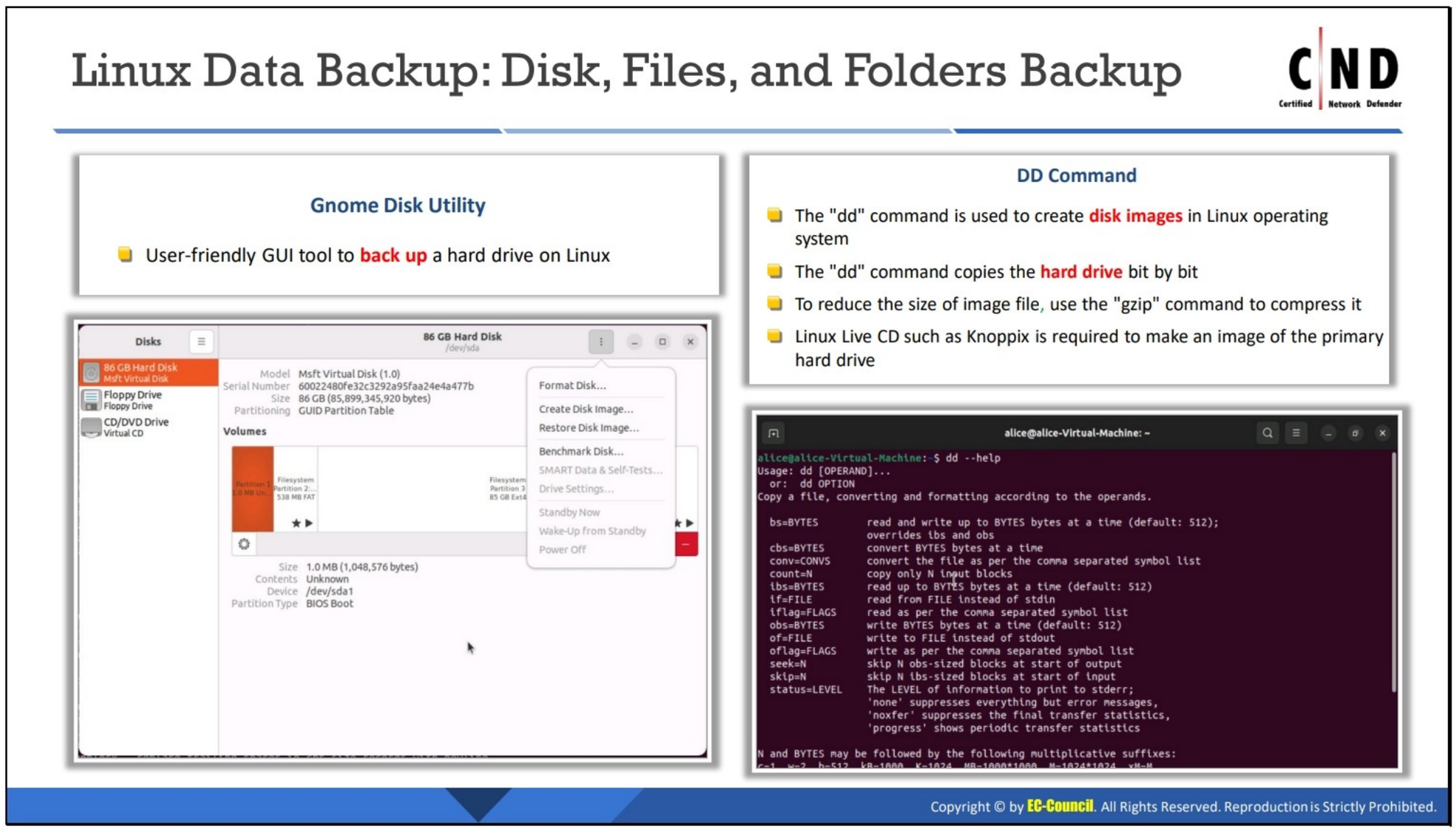
Handy Backup™ is extendable with plugins for backing up popular apps, and offers multiple storage options (backup to external hard drives, USB, FTP, Amazon S3, backup to Google Drive, etc.).

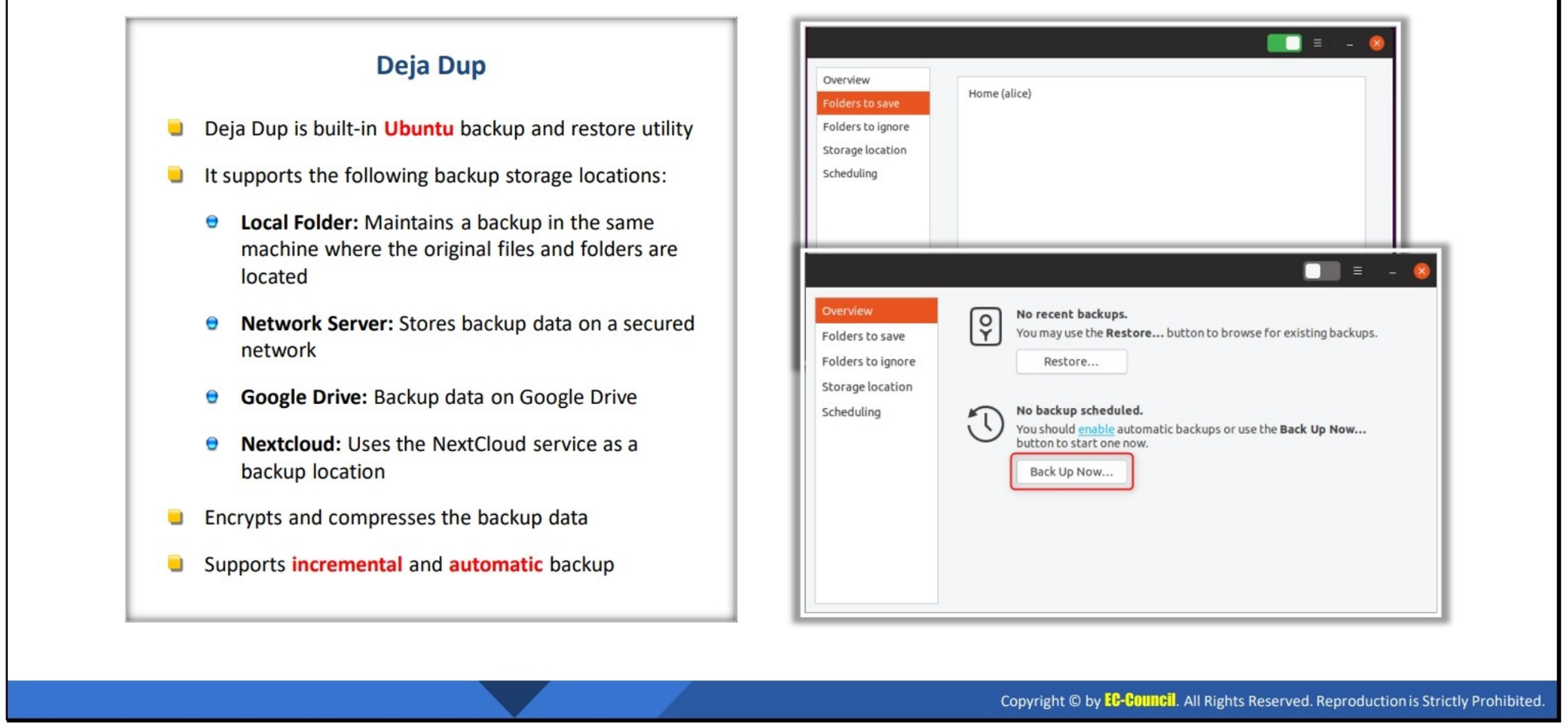
SyncBackPro

Source: www.2brightsparks.com

SyncBackPro is for personal and business users who want a best-in-class backup solution, including scripting and cloud backup support.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.





Linux Data Backup: Disk, Files, and Folders Backup

A user can use the following utilities to back up the entire contents of a hard drive on Linux.

Gnome Disk Utility

Gnome Disk Utility is a tool that comes with most Linux distributions that take advantage of Gnome's desktop and software offerings. Backing up with Gnome Disk Utility is quite simple. You

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

just have to select which hard drive to back up in the form of a raw.IMG file, and select where to save the backup.

Steps to Easily Backup a Hard Drive with Gnome Disk Utility

- Install the gnome-disk-utility package.

  sudo apt-get install gnome-disk-utility

- Open the Gnome Disk Utility tool and select the hard drive you want to back up, click on the menu, and then click the **New Disk Image** option.

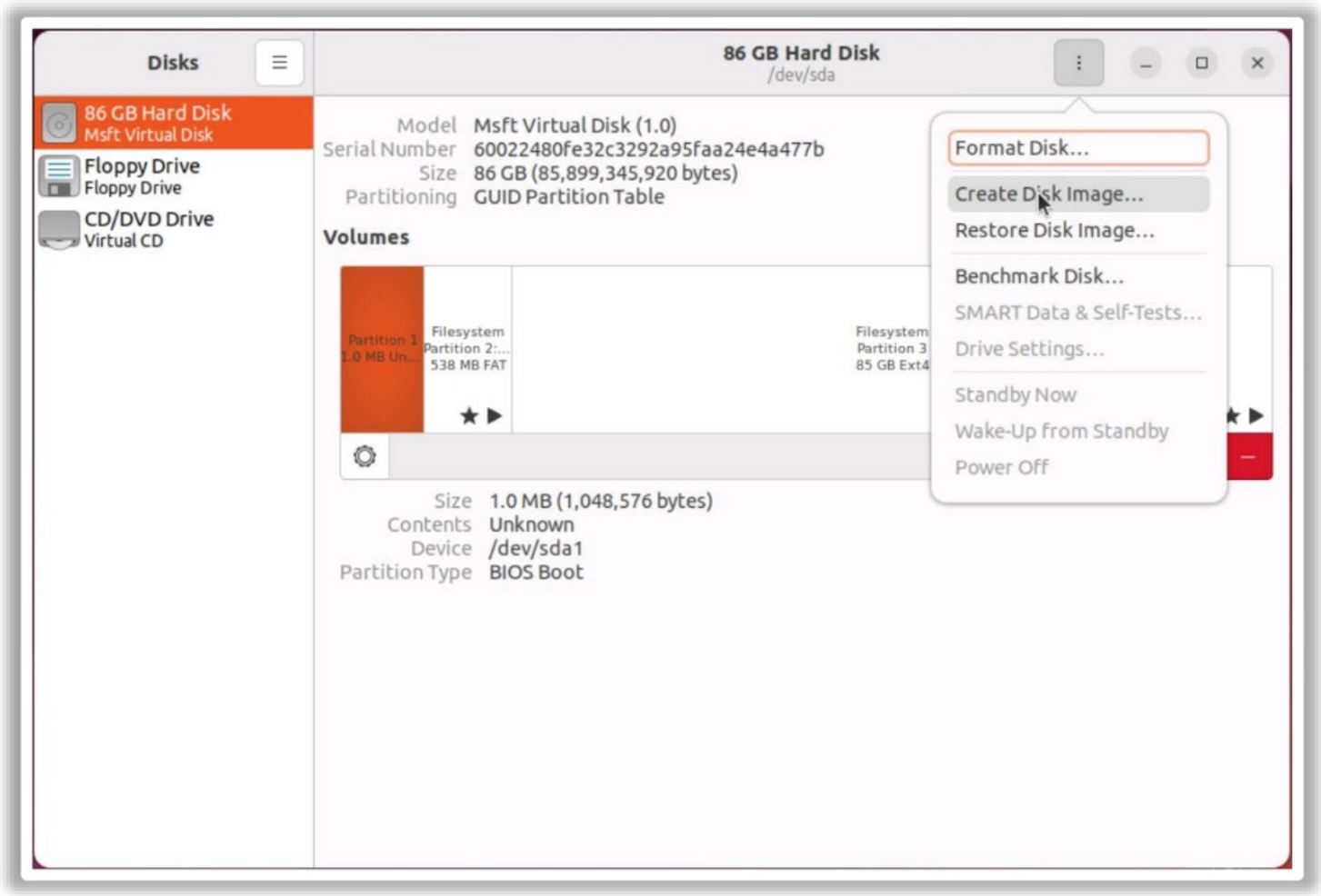


Figure 10.130: Gnome Disk Utility tool

- Enter the .img file name, and select the backup location. Click **Start Creating…** to start the backup process.

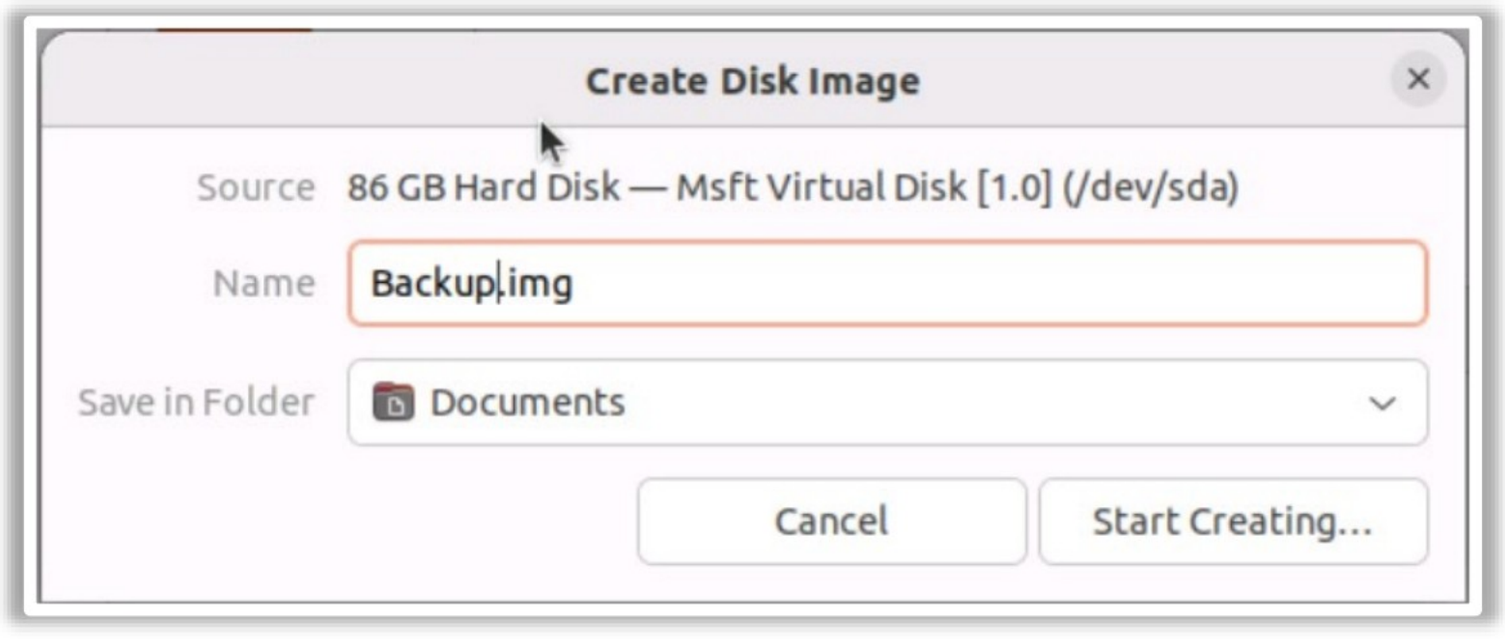


Figure 10.131: Creating Disk Image

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- A .img file will be created in the specified folder.

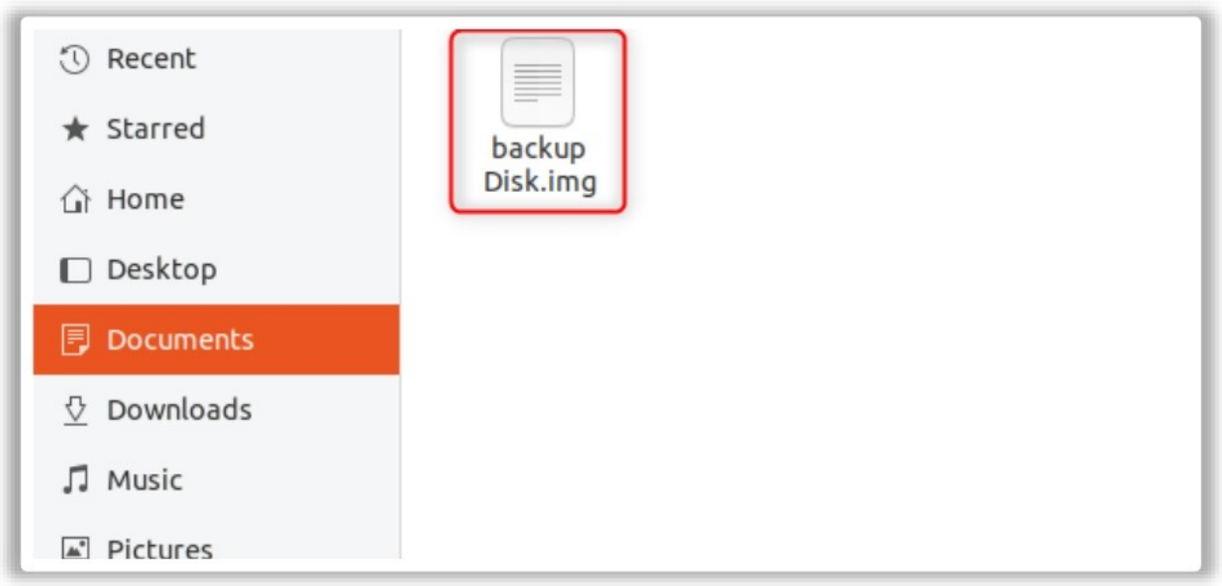


Figure 10.132: A .img file in Special Folder

DD Command

DD command tool is easy to use. The “dd” command is used to create disk images in Linux operating system. This command copies the hard drive bit by bit. Compress the image file using the “gzip” command to reduce its size. A Linux Live CD such as Knoppix is required to make an image of the primary hard drive. The steps for using the DD tool to make a backup of a Linux hard drive are as follows.

- Open a terminal window.
- Select the hard drive to be backed up with the **lsblk** command. For example, use **/dev/sda** and decide where the DD tool will place the backup. For example, **/dev/sdb** (another hard drive).

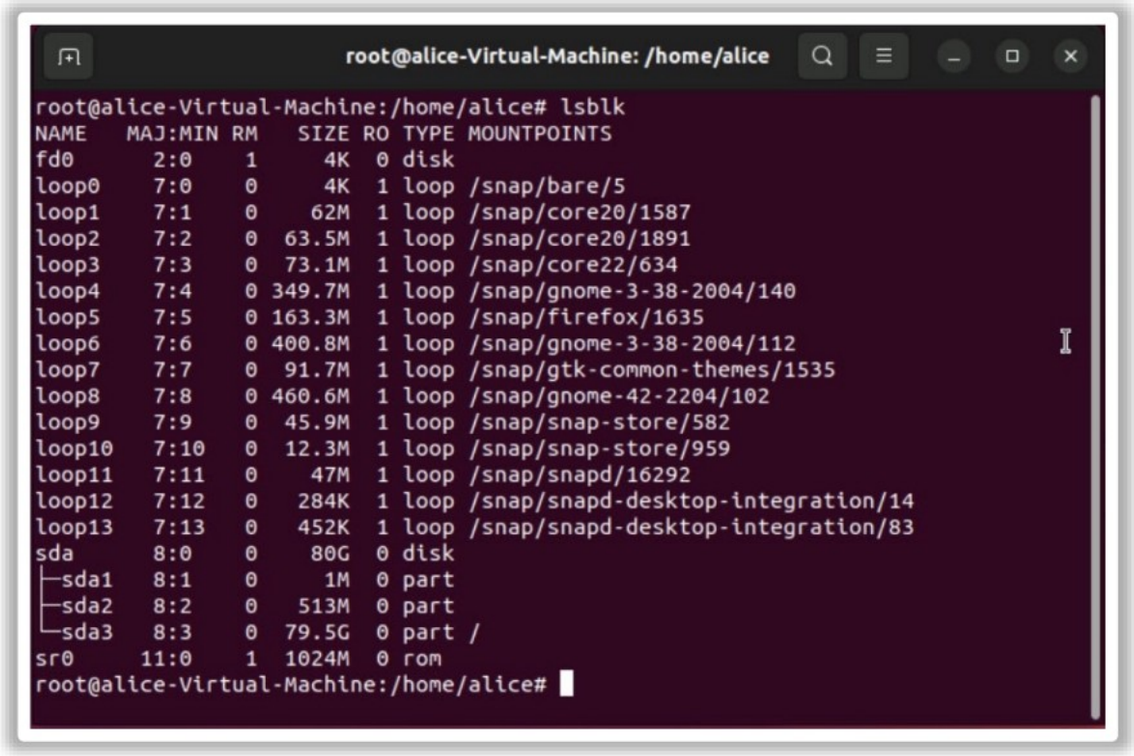


Figure 10.133: Selecting hard drive to be backed up with the **lsblk** command

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

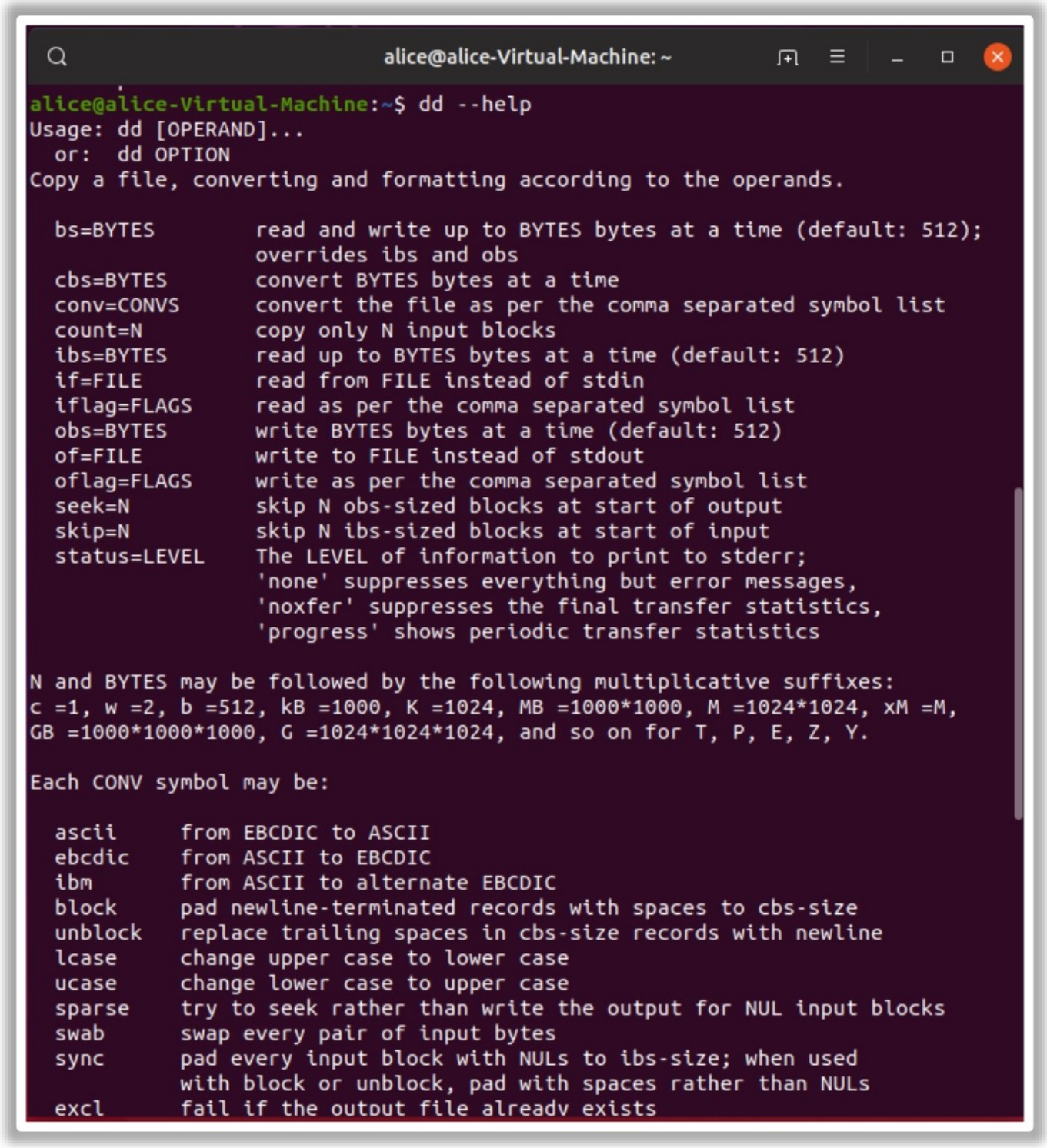


Figure 10.134: Using --**help** option with **dd** command utility

- Enter the following command to run the backup.

  sudo dd if=/dev/sda of=/dev/sdb

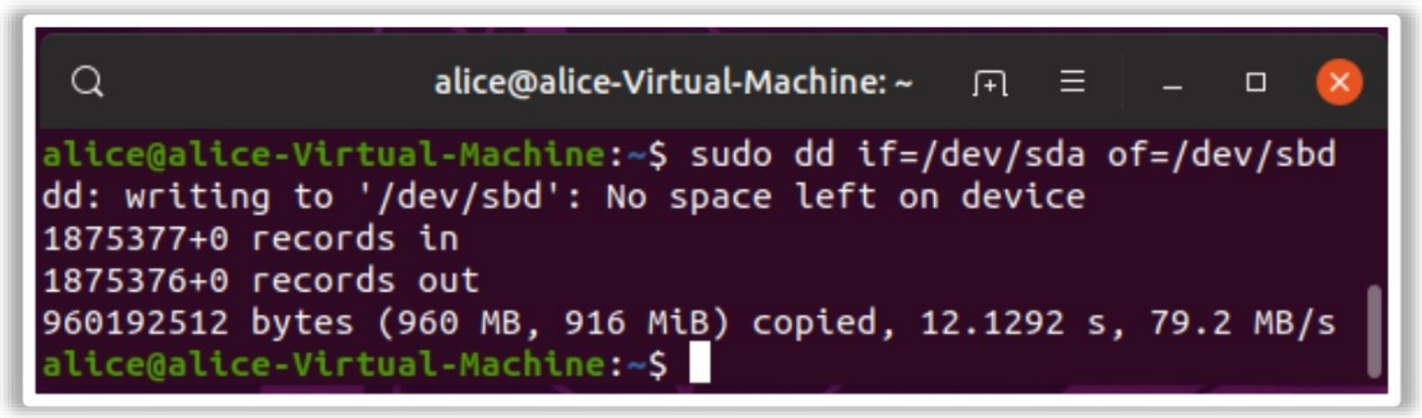


Figure 10.135: Command to run back up

- To back up one partition instead of an entire drive, use the following command.

  sudo dd if=/dev/sda1 of=/dev/sdb1

- To restore the backup, enter the following command and wait patiently.

  sudo dd if=/dev/sdb of=/dev/sda

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- To restore a partition backup, use the following command.

  sudo dd if=/dev/sdb1 of=/dev/sda1s

Deja Dup

Deja Dup with its GUI front-end offers all features the user will need in a simple backup solution. They include

- Support for local, remote, or cloud backup locations (including services like Amazon S3 and Rackspace Cloud Files).
- Built-in encryption and compression support.
- Incremental backups.
- Scheduled backups.
- Integration with Nautilus and other file managers.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Mac OS Data Backup: Disk, Files, and Folders Backup

Time Machine

- Time Machine is a built-in backup solution in Mac OS
- It automatically creates Mac backups on an external drive



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Mac OS Data Backup: Disk, Files, and Folders Backup (Cont'd)

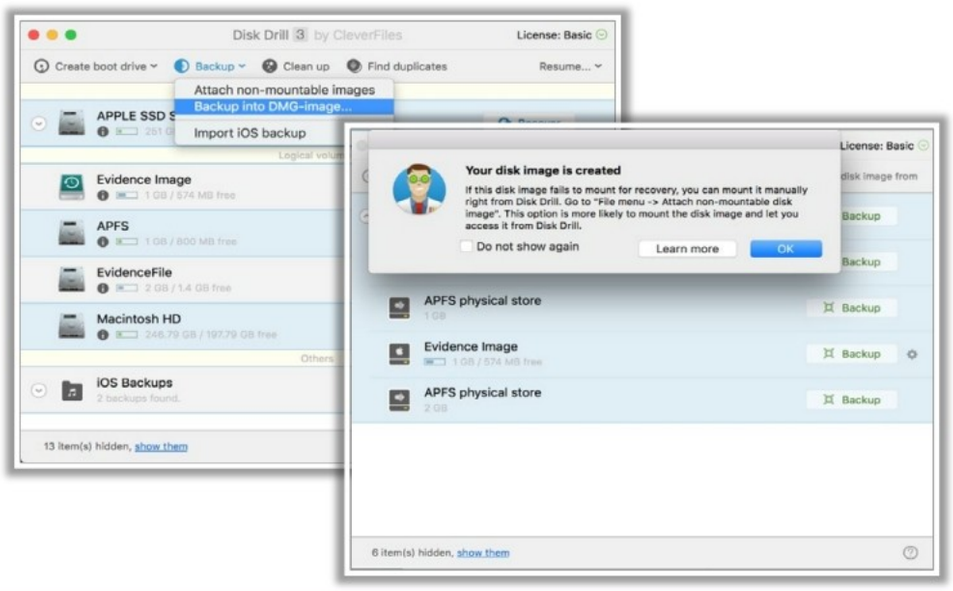
ChronoSync Express

- Backs up **multiple source folders** into a single destination folder on any mounted volume
- Creates a **synchronizer task** to backup multiple selected folders and copy them with their contents to a single destination



Disk Drill

- Disk Drill allows you to backup data on Mac OS X by creating a **byte-to-byte** disk image



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Mac OS Data Backup: Disk, Files, and Folders Backup

Time Machine

Apple's built-in solution for backing up Mac OS, Time Machine allows the connection of an external hard drive over USB or Thunderbolt (or FireWire, for older Macs) for a wired connection, or over a network for a wireless connection. Time Machine backs up every hour, deleting older backups as the backup drive starts running out of space.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Steps to Use Time Machine for Backups on Your Mac

- Enable Time Machine backups on Mac
  - Select **System Preferences** from the Apple menu and select **Time Machine** icon.



Figure 10.136: System Preferences

  - Click **Select Backup Disk**.

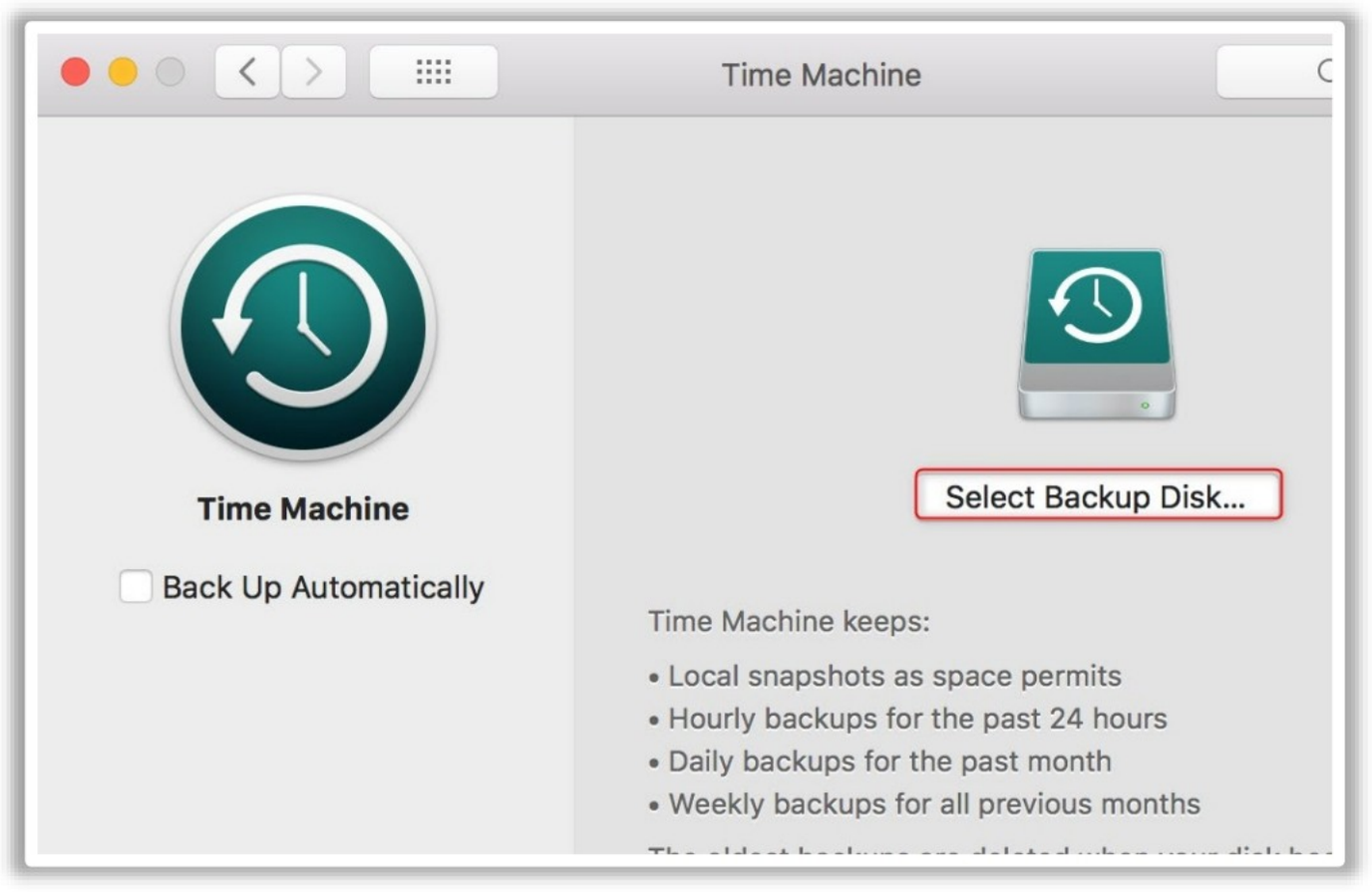


Figure 10.137: Time Machine

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Select which disk the user would like to use as a Time Machine backup, and check the **Back Up Automatically** box to automatically back up your Mac to your chosen disks.

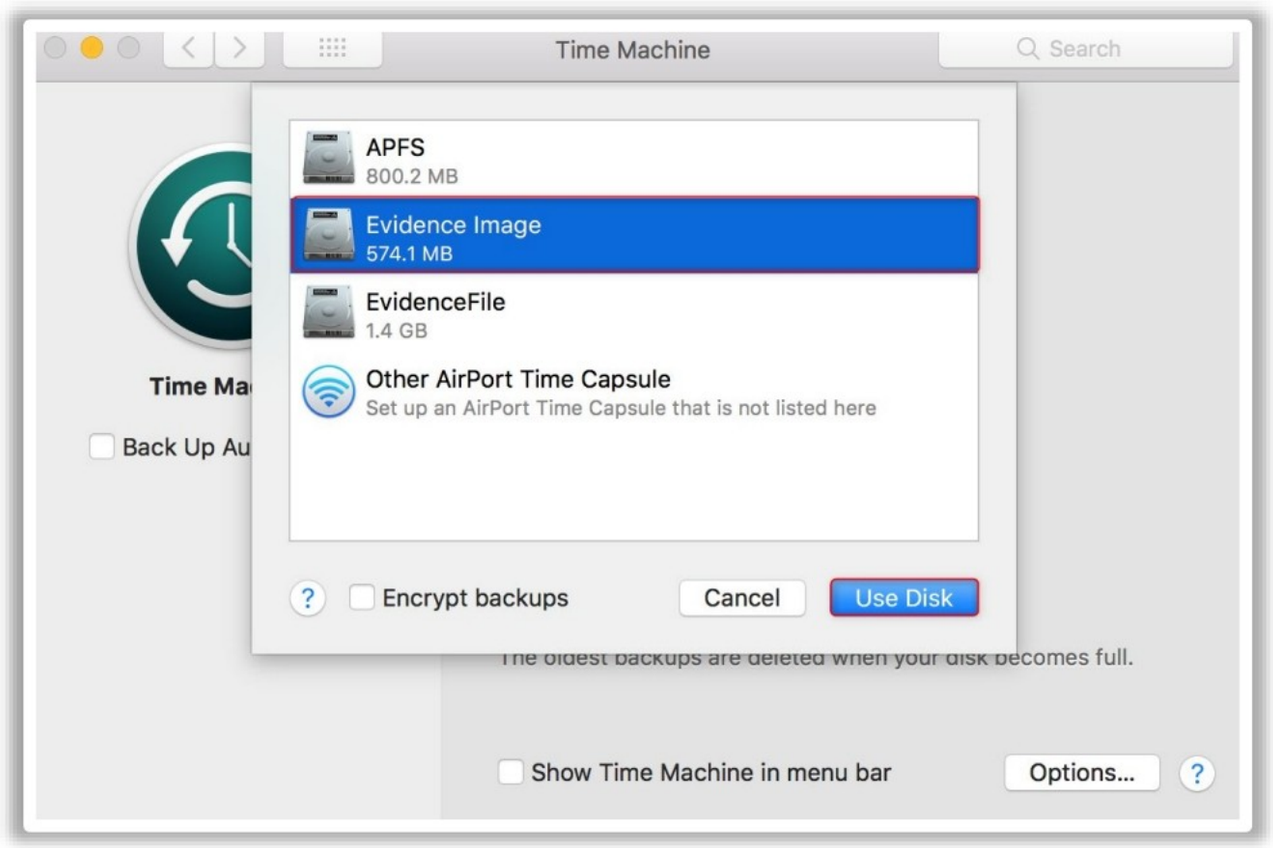


Figure 10.138: Automatically Back Up Mac to Chosen Disks

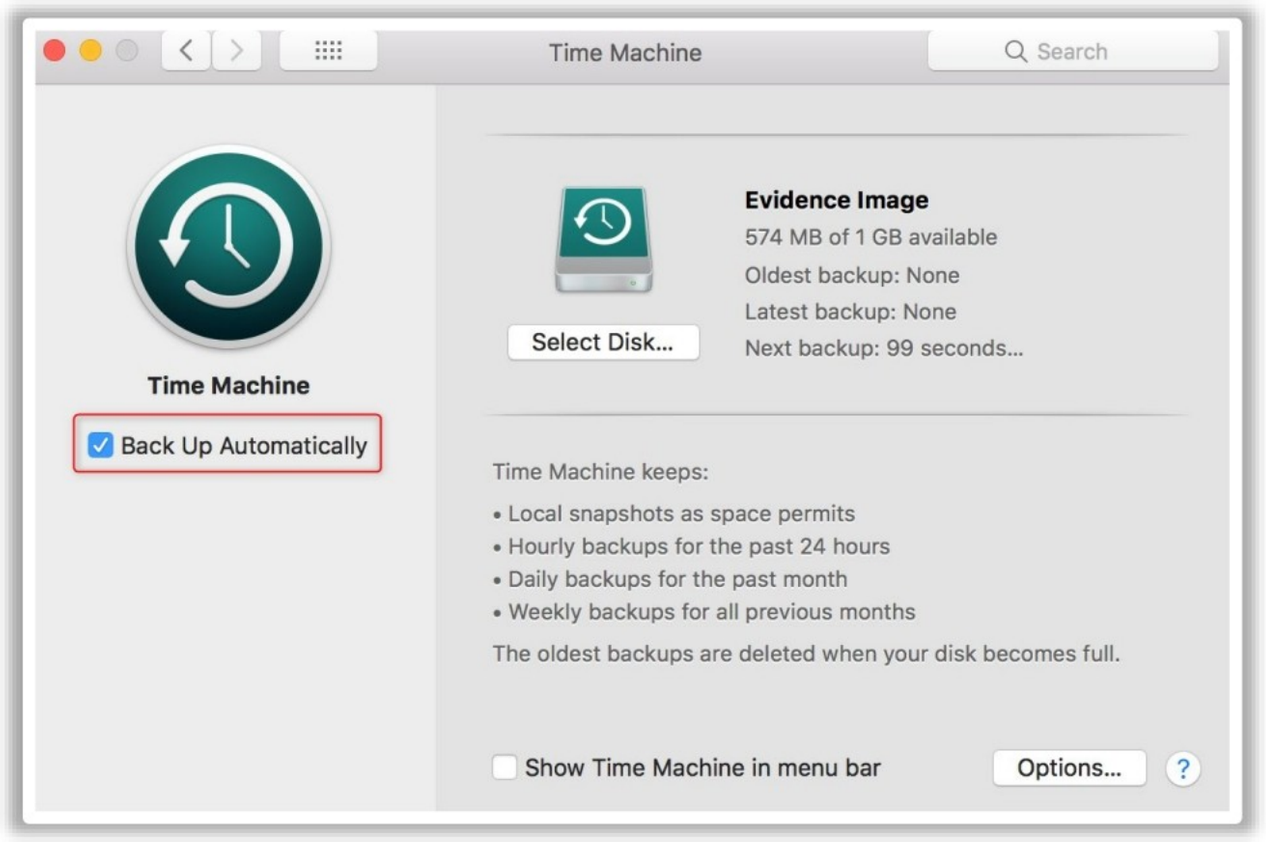


Figure 10.139: Selecting Back Up Automatically

- Hard drive is ready to accept backups through Time Machine.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **How to restore files from a Time Machine backup**
  - Select **System Preferences** from the Apple menu and select the **Time Machine** icon.



Figure 10.140: System Preferences

  - Check the box next to **Show Time Machine in menu bar** and click **Enter Time Machine** after clicking the Time Machine icon in the Menu bar.
  - Find the file or folder in question and click **Restore**.

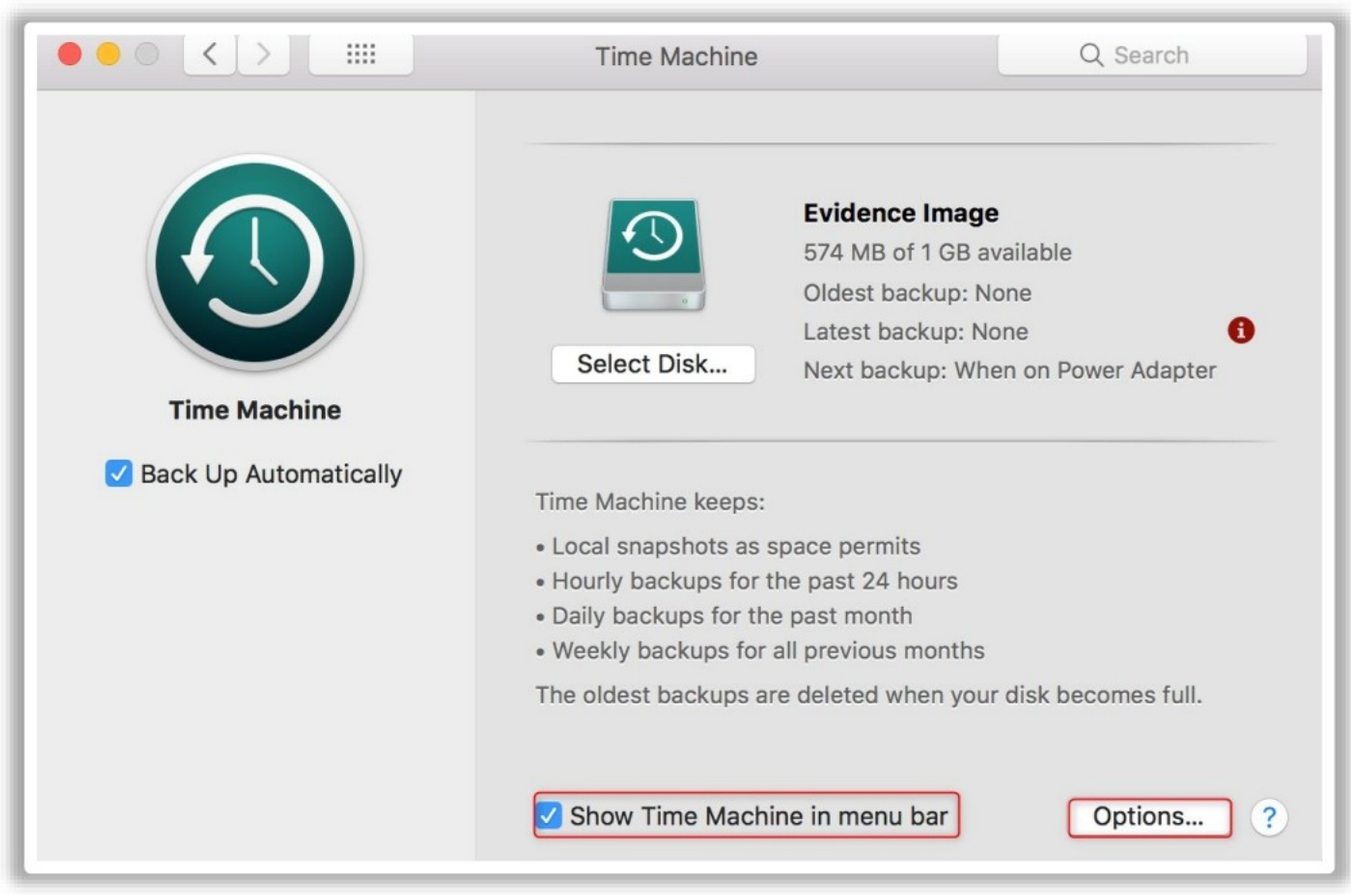


Figure 10.141: Finding Files or Folders

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

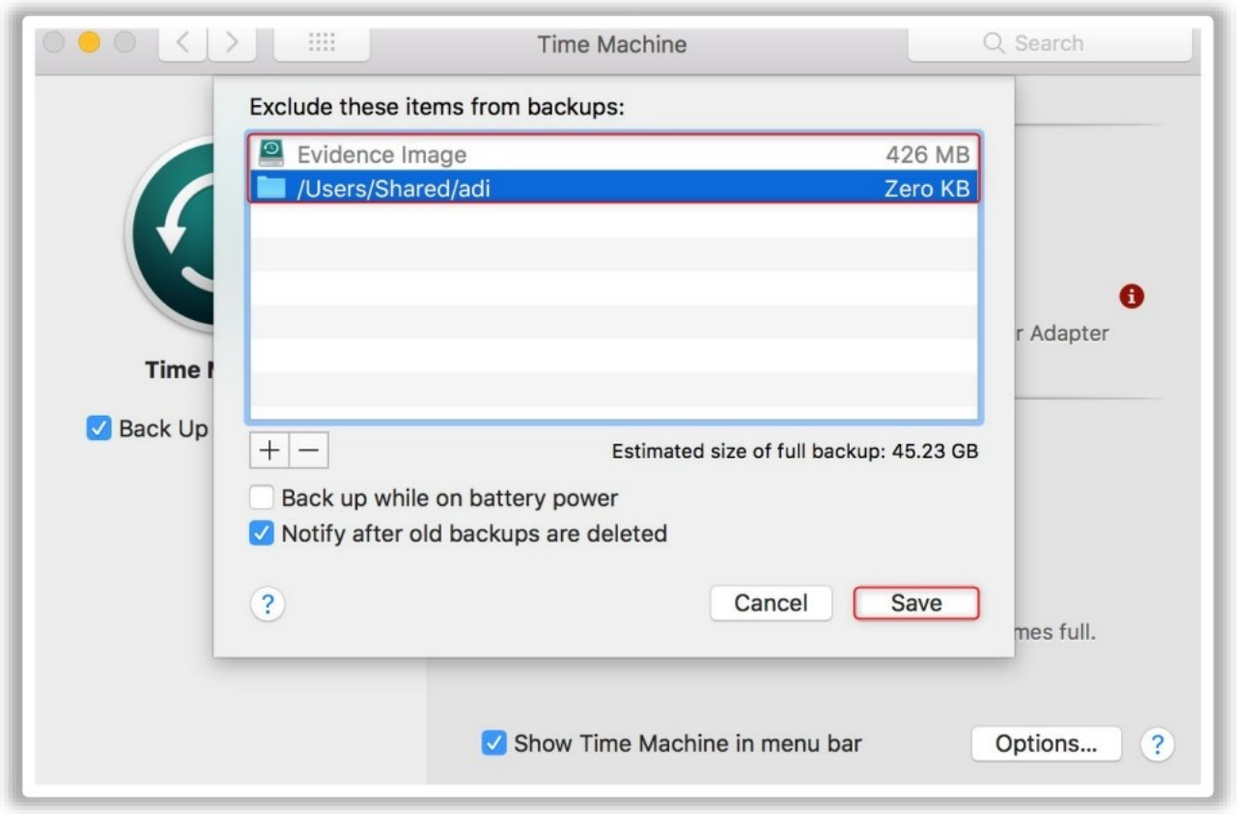


Figure 10.142: Restoring Files from Time Machine Back Up

- Time Machine will copy that file back to its original location on the hard drive.

ChronoSync Express

ChronoSync Express backs up multiple source folders to a single destination folder on any mounted volume. It creates a synchronizer task to backup selected multiple folders and copy them with their contents to a single destination. The destination folder can be a local hard drive, NAS, or mounted file server. ChronoSync Express includes assistants for

- Home folder backup
- Folder backup
- Synchronize two folders
- Multiple folder backup

Steps to Use ChronoSync Express to Create Mac OS Data Backup

- Select **Use a setup assistant** from the ChronoSync Express Organizer window. This takes you to all assistants ChronoSync Express has to offer. Here, select **Multiple Folder Backup**.

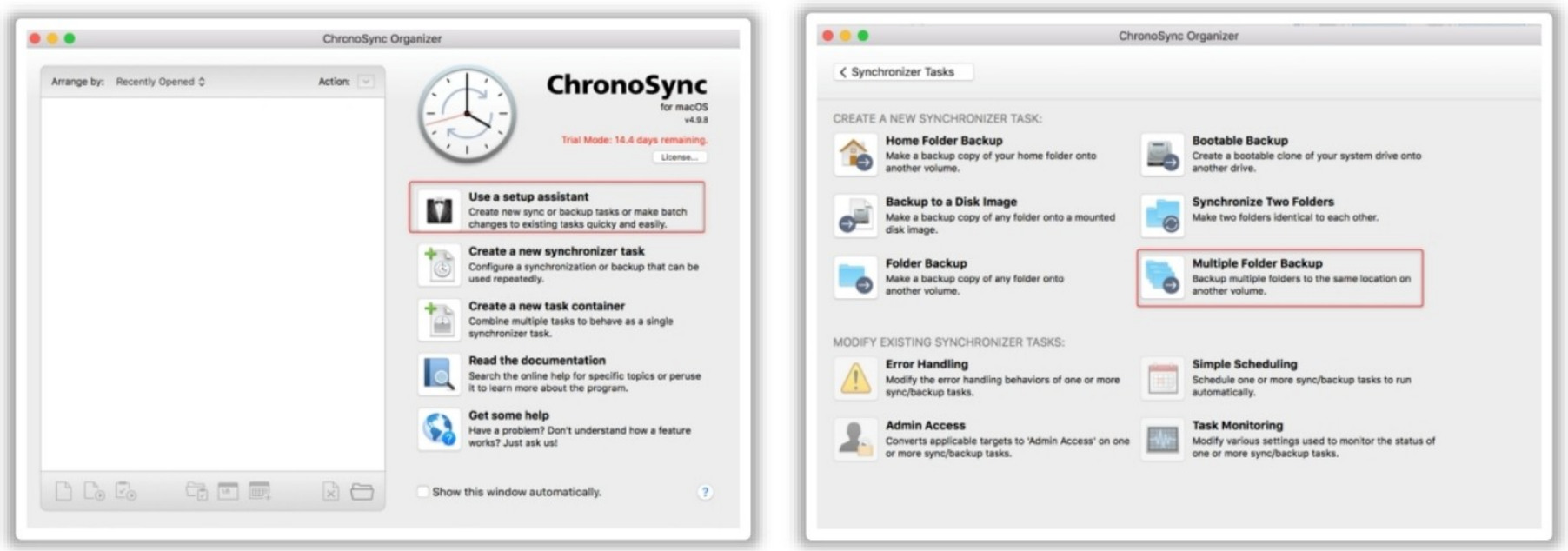


Figure 10.143: ChronoSync Express Window

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Click **Get Started** to set up the assistant in a new window.



Figure 10.144: Multiple Folder Back Up

- Select the folders that contain all data to backup. Then, click **Next Step**.

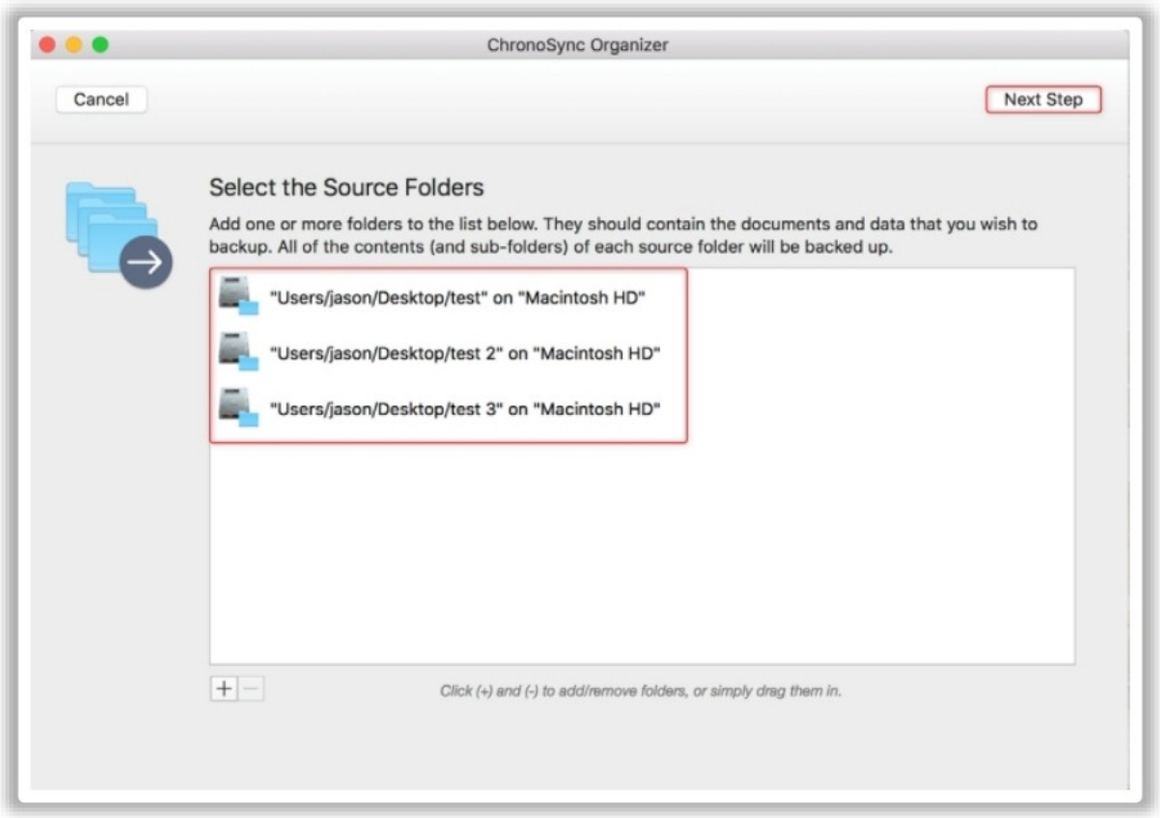


Figure 10.145: Selecting the Source Folders

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Select the folder where the source folders (chosen in the previous step) will be copied. Then, click **Next Step**.

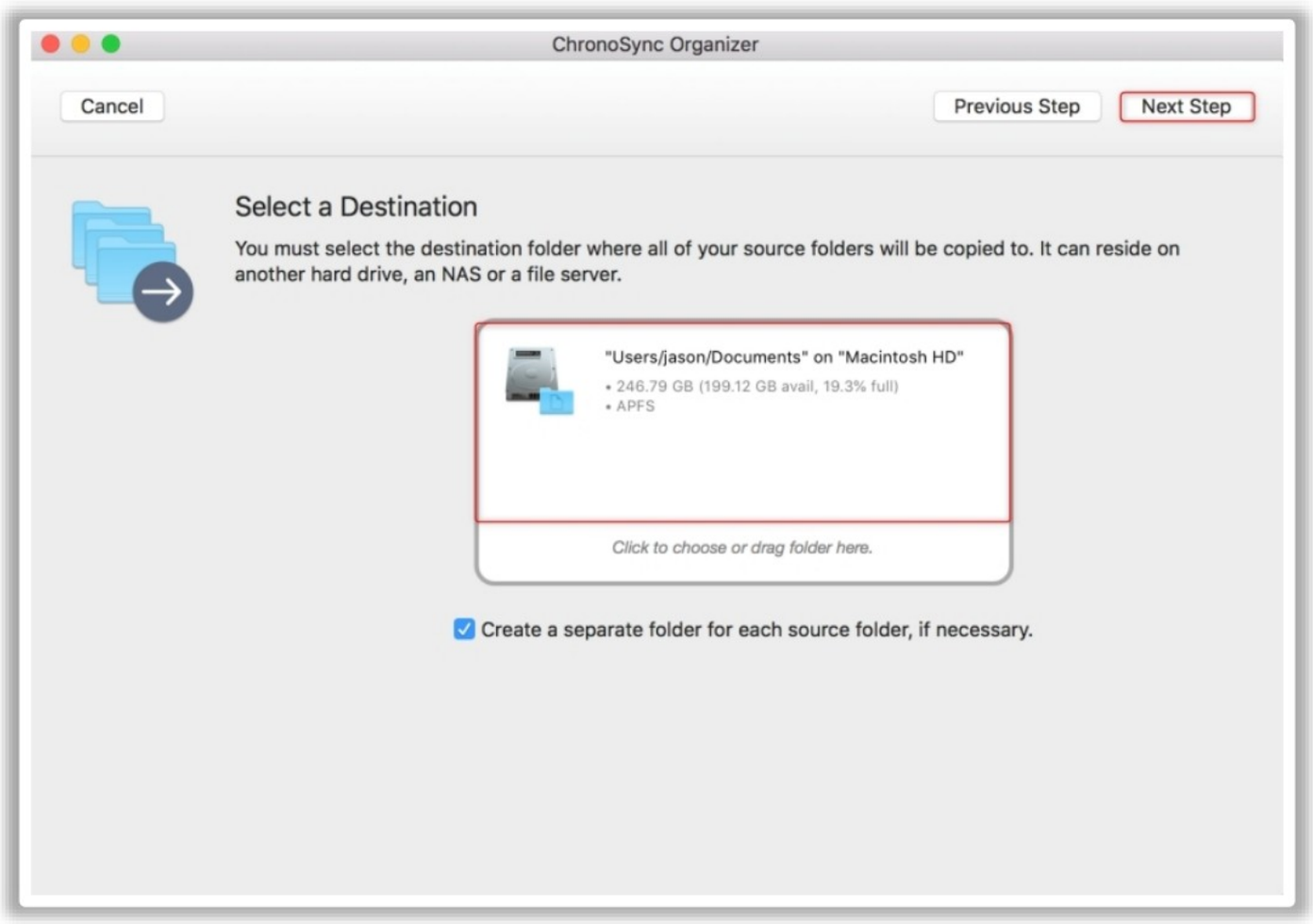


Figure 10.146: Selecting a Destination

- To include only certain types of data, choose only those types on this screen, or keep a default of backing up all data. Then click **Next Step**.

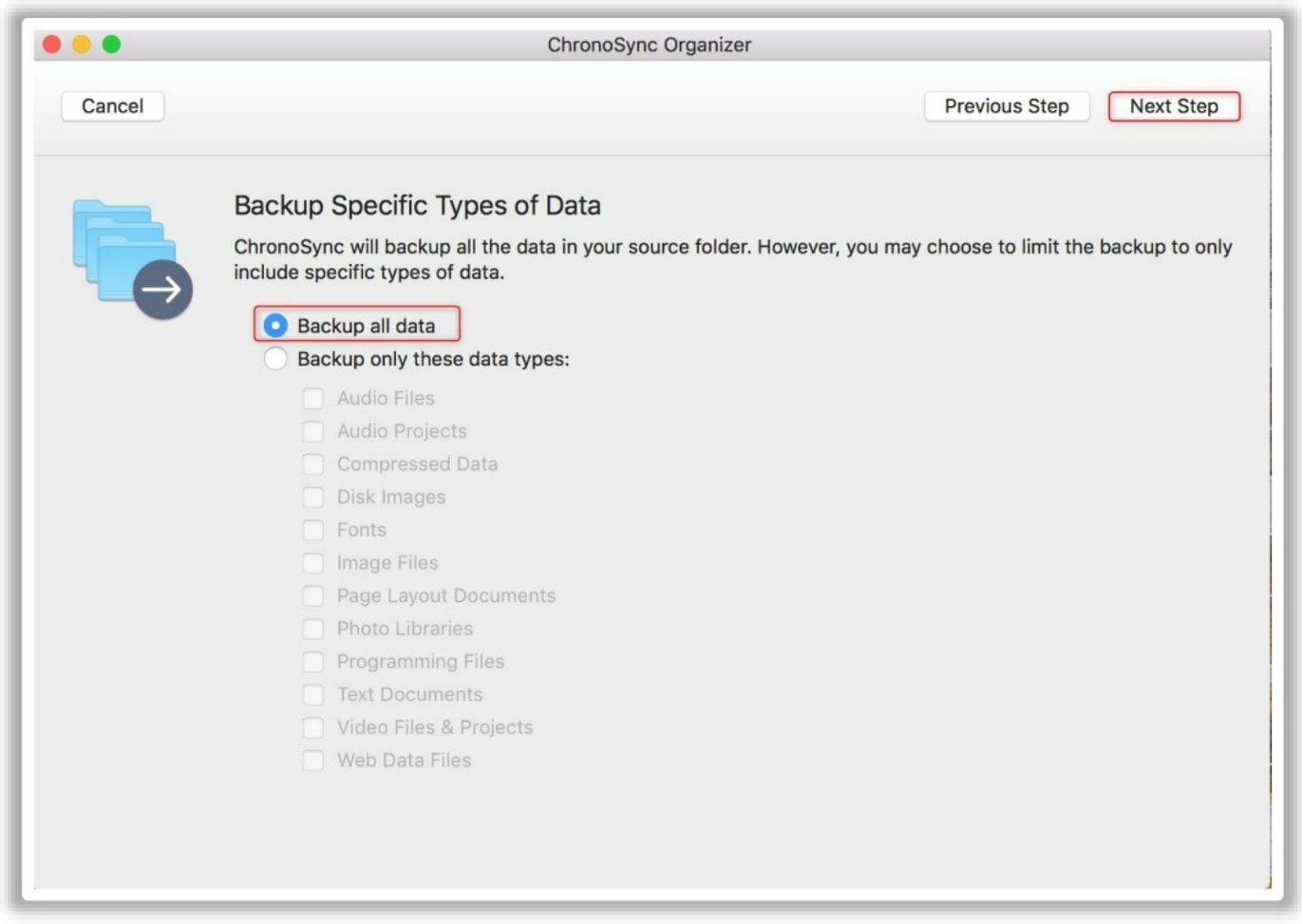


Figure 10.147: Backing Up Specific Types of Data

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Determine whether you need an archive, and then click on **Next Step**.



Figure 10.148: Replaced or Deleted File Handling

- Give **Multi Folder Backup** assistant a unique, meaningful name, and click **Create Task** to complete the assistant setup.

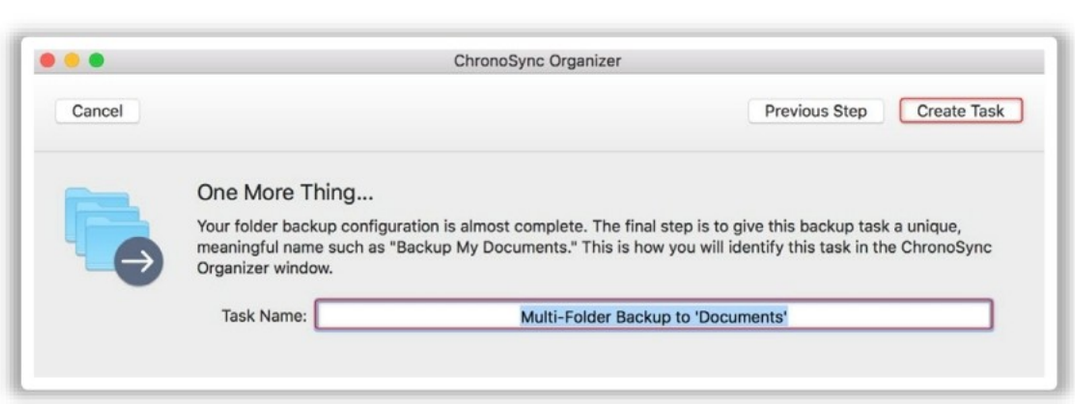


Figure 10.149: Creating Task to Complete the Assistant Setup

- ChronoSync Express has created a new task with the settings specified during the assistant setup.

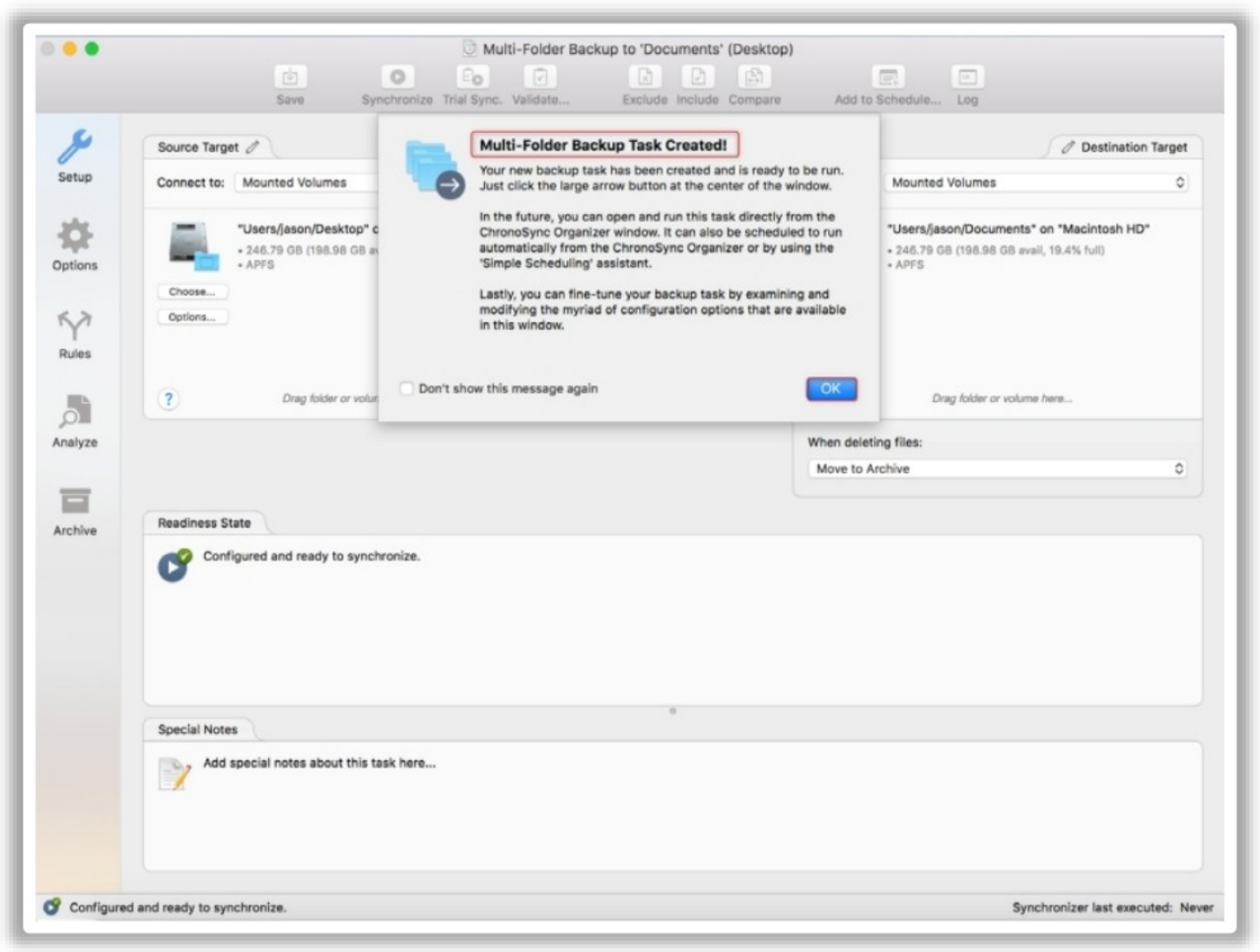


Figure 10.150: Creation of New Task with Specified Settings

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Disk Drill

Disk Drill software for Mac uses a clone to enact data recovery functions. You can also use an exact copy of your original disk as a backup. Disk Drill allows you to backup data on Mac OS X by creating a byte-to-byte disk image.

Steps to Backup Mac with Disk Drill

- Download and install Disk Drill on Mac.
- Open Disk Drill, select **Backup** from the upper menu, and then select **Backup into DMG image**.

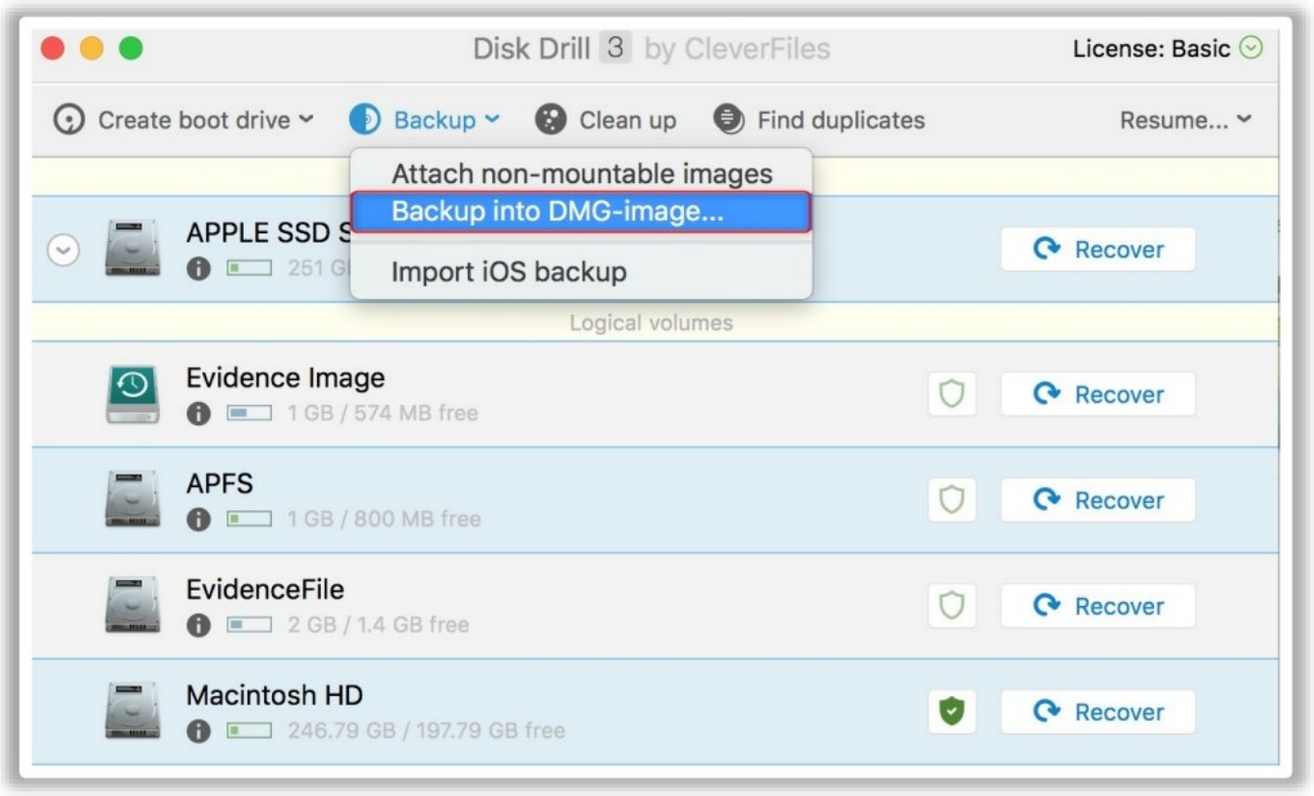


Figure 10.151: Disk Drill Window

- Select a drive to make a byte-to-byte disk image from.

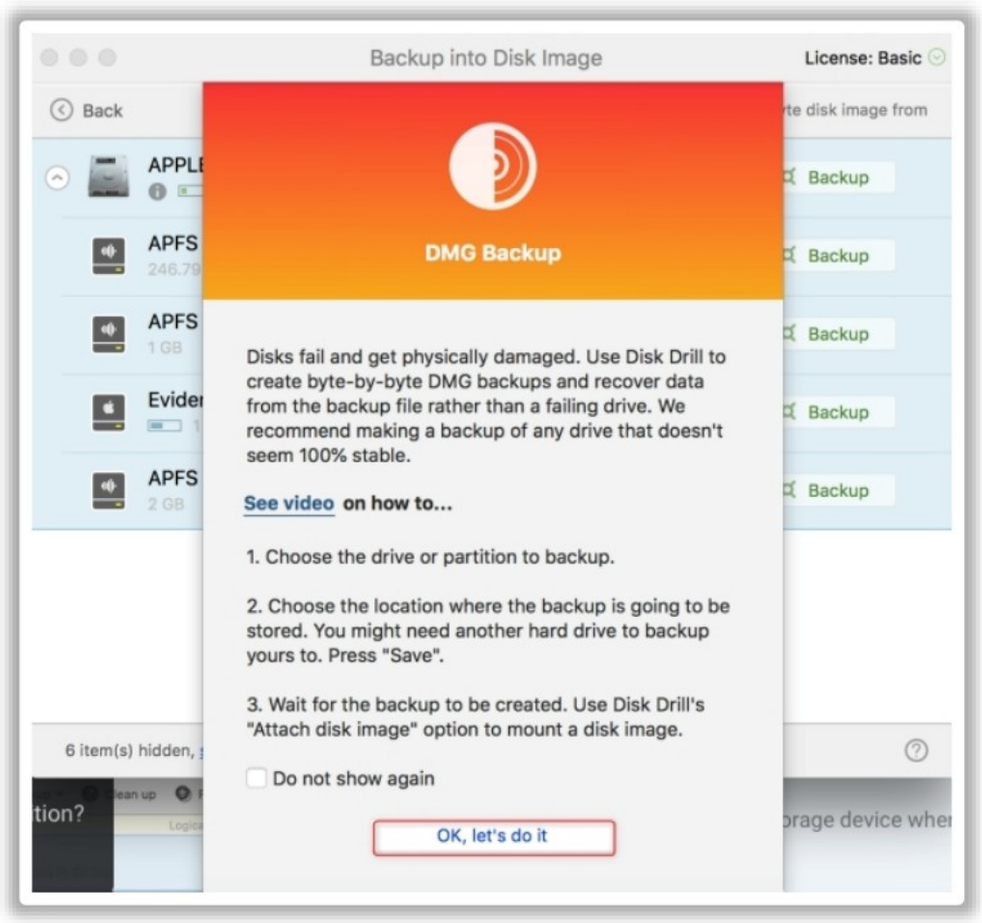


Figure 10.152: Drive Selection

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Connect the external drive to save the clone and click **Save**. The backup program starts creating the clone.

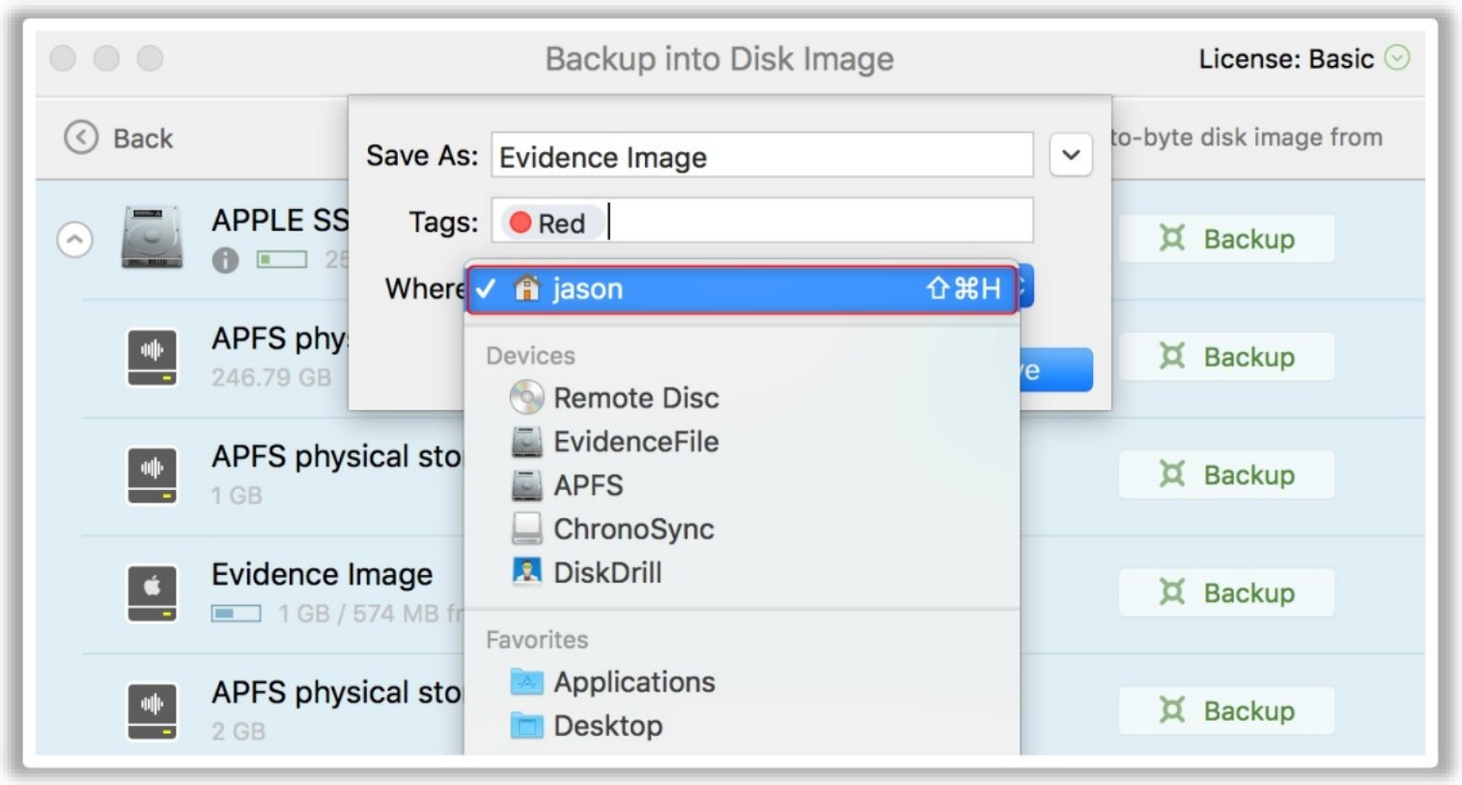


Figure 10.153: Back Up Program Start Creating a Clone

- Wait for the backup to be created.



Figure 10.154: Disk Image is Created

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Database Backup: MS SQL Server

- MS SQL Server supports the following types of **backups**:
  - Full or database backup
  - Differential or incremental
  - Transactional log or log

Create SQL SERVER database backup using T-SQL

BACKUP TYPE	COMMAND	EXAMPLE
Full database backup	Backup database <Your database name> to disk = '<Backup file location + file name>'	Backup database DemoDB to disk = 'D:\DemoDB_Full.bak
Differential backup	Backup database <Your database name> to disk = '<Backup file location + file name>' with differential	Backup database DemoDB to disk = 'D:\demoDB_diff.bak' with differential
Transaction Log backup	Backup log <Your database name> to disk = '<Backup file location + file name>'	Backup log DemoDB to disk = 'D:\DemoDB_log.trn'

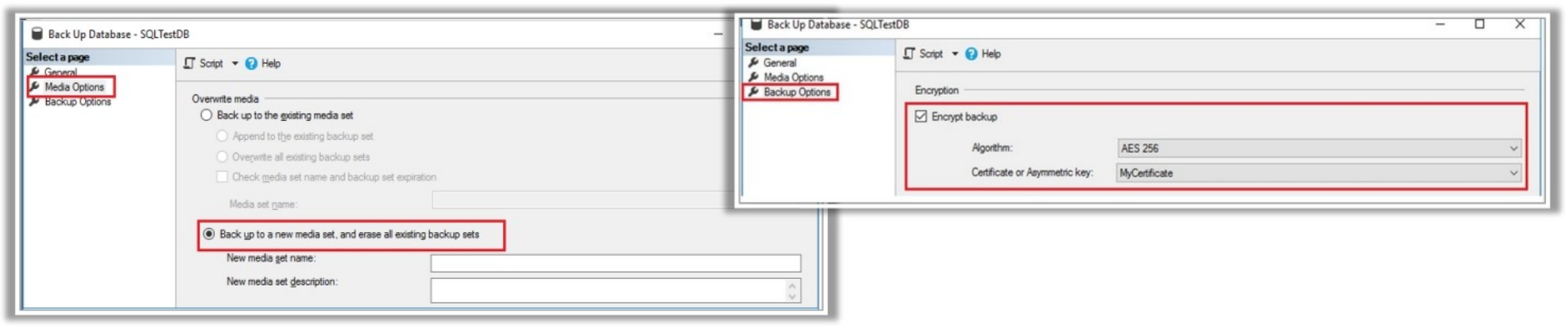
Create SQL SERVER database backup using Powershell Backup-SqlDatabase cmdlet

```
$credential=Get-Credential
Backup-SqlDatabase -ServerInstance Computer[\Instance] -Database SQLTestDB -BackupAction
Database -Credential $credential
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Database Backup: MS SQL Server (Cont'd)

- **Create SQL SERVER database backup using SQL Server Management Studio**
- **Create Encrypted SQL SERVER database backup using SQL Server Management Studio**



Note: To perform a differential or a transaction log backup you need to have at least one full backup of the selected database

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Database Backup: MS SQL Server

Backing up an MS SQL server database can secure its data. There are three types of MS SQL server backups. They are

- **Full or database backup,** which comprises the entire database when the backup is completed.
- **Differential or incremental backup,** which comprises only changes made to the database since its most recent full database backup.

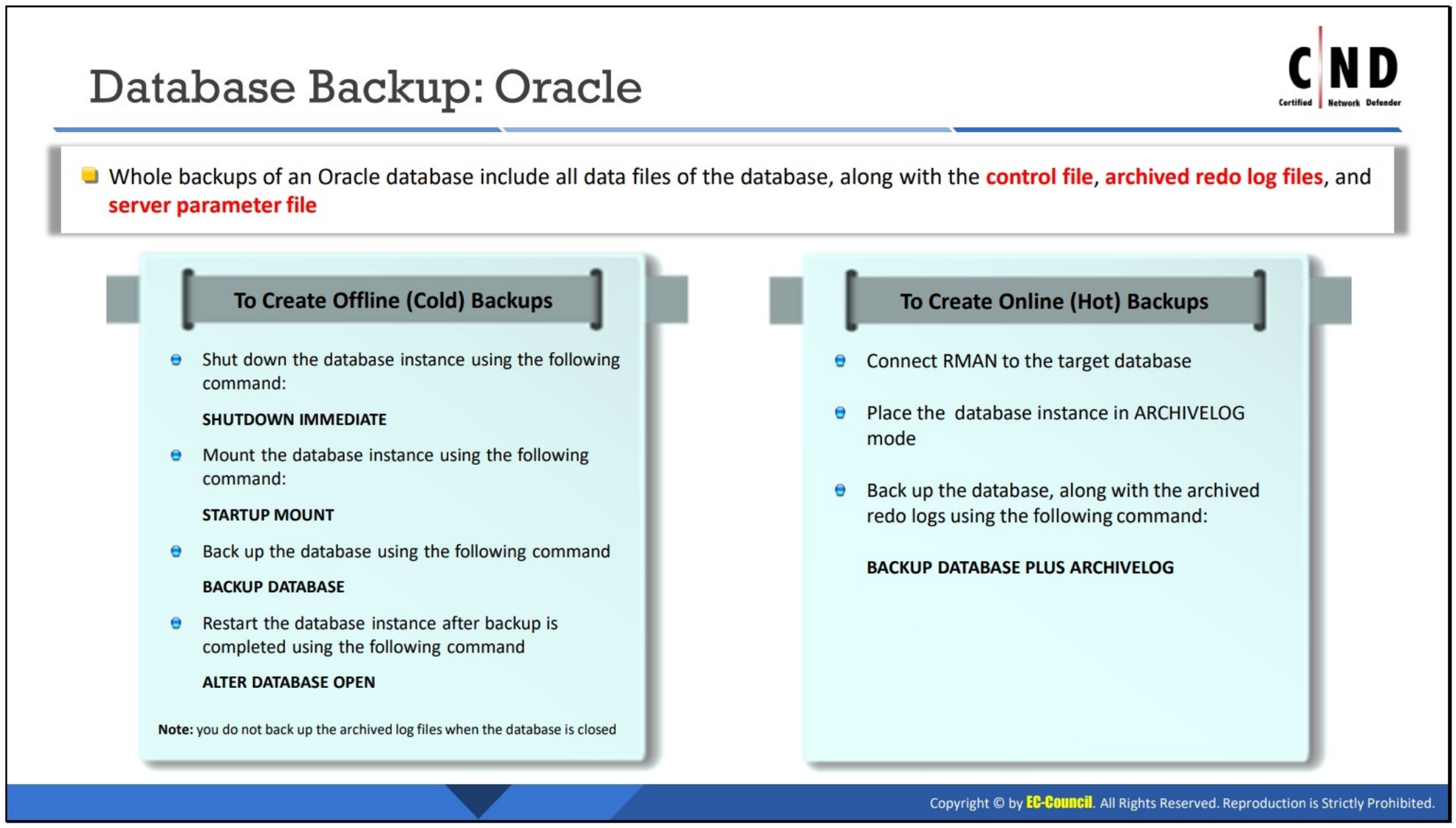
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Transactional log or log backup**, which comprises all log records that were not backed up in an earlier log backup.

  You can take a SQL server database backup using

  - **T-SQL**
  - **Powershell Backup SqlDatabase cmdlet**
  - **SQL server management studio:** SQL server management studio enables the creation of an encrypted database backup.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Database Backup: Oracle

A whole backup of an Oracle database comprises the complete contents of all data files of the database, along with the control file, archived redo log file, and server parameter file. A complete recovery uses all these files while recovering data. It is possible to take a whole backup when the database is shut down (offline/cold backup) or open (online/hot backup). In the case of offline backup, a whole backup taken after a shutdown can be used to recover up to the time of the last full backup. In the case of online backup, a whole backup taken while the database is open is not consistent with a given point in time, and must be recovered before the database is available.

Steps to Create Offline (Cold) Backups

- Shut down database instance using the following command.

SHUTDOWN IMMEDIATE

- Mount the database instance using the following command.

STARTUP MOUNT

- Back up the database using the following command.

BACKUP DATABASE

Note: There is no need to backup the archived log files when the database is closed.

- Restart database instance after backup is completed using the following command

ALTER DATABASE OPEN

Steps to Create Online (Hot) Backups

- Connect RMAN to the target database.
- Keep the database instance in **ARCHIVELOG** mode.
- Back up the database along with the archived redo logs using the following command:

  BACKUP DATABASE PLUS ARCHIVELOG

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Email Backup: Outlook

- Business emails use an **POP**, **Exchange**, or **IMAP** account

Backup and Restore POP3 data

- In POP3 account outlook emails, contacts, calendar, tasks, and notes are stored locally on your PC inside a .pst file
- Copy the .pst file to the backup location when Outlook is closed

Backup and Restore IMAP data

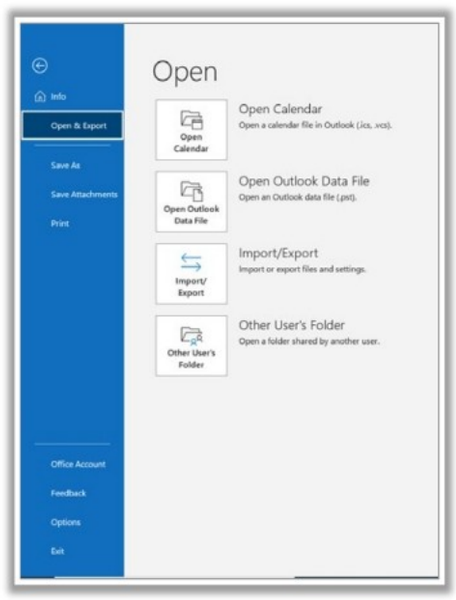
- In IMAP account outlook emails, contacts, calendar, tasks, and notes are stored in a .pst file, an .ost file, or a combination of both
- In Outlook 2013, 2016, 2019, or Office 365, regularly export all folders marked with "This computer only" to a .pst file to backup data
- Make backup copies of your cached .pst or .ost files

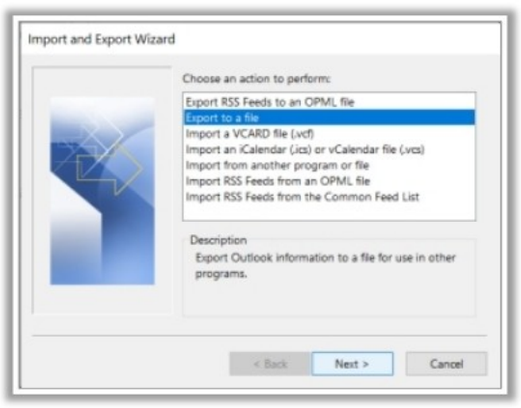
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

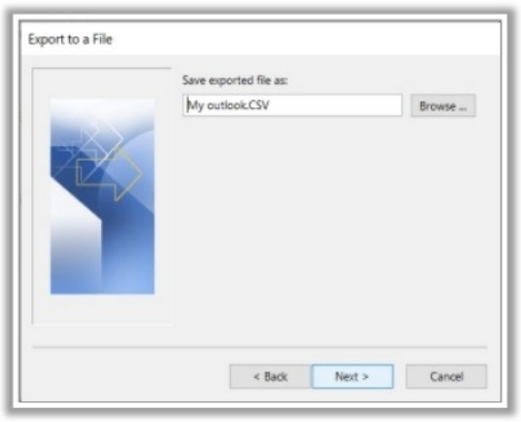
Email Backup: Outlook (Cont'd)

Exporting Data in Outlook

1. Select **File** → **Open & Export** → **Import/Export**
2. Select **Export to a file**, and then select **Next**
3. Select **Outlook Data File (.pst)**, and select **Next**
4. Choose a location and name for your backup file, and then select **Finish**







Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Email Backup: Outlook

Business emails use a POP, Exchange, or IMAP account. Exchange and IMAP servers allow automatic archival of business emails, anytime and anywhere. You have to check with an admin for accessing the archived emails. If only an local email backup is needed, move or delete older items with AutoArchive or export the items to a .pst file. You can then restore the backup (.pst) file when needed.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Steps to Export Data in Outlook

- Select **File** > **Open & Export** > **Import/Export**.

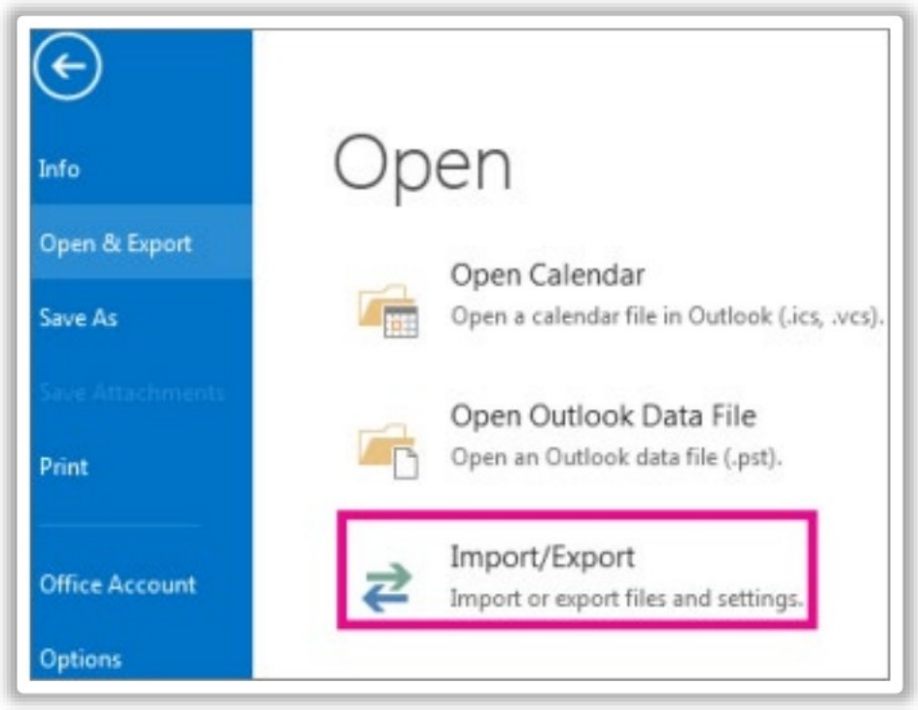


Figure 10.155: Selecting Open and Export Option

- Select **Export to a file**, and then select **Next**.



Figure 10.156: Selecting Export to a File

- Select **Outlook Data File (.pst)**, and select **Next**.

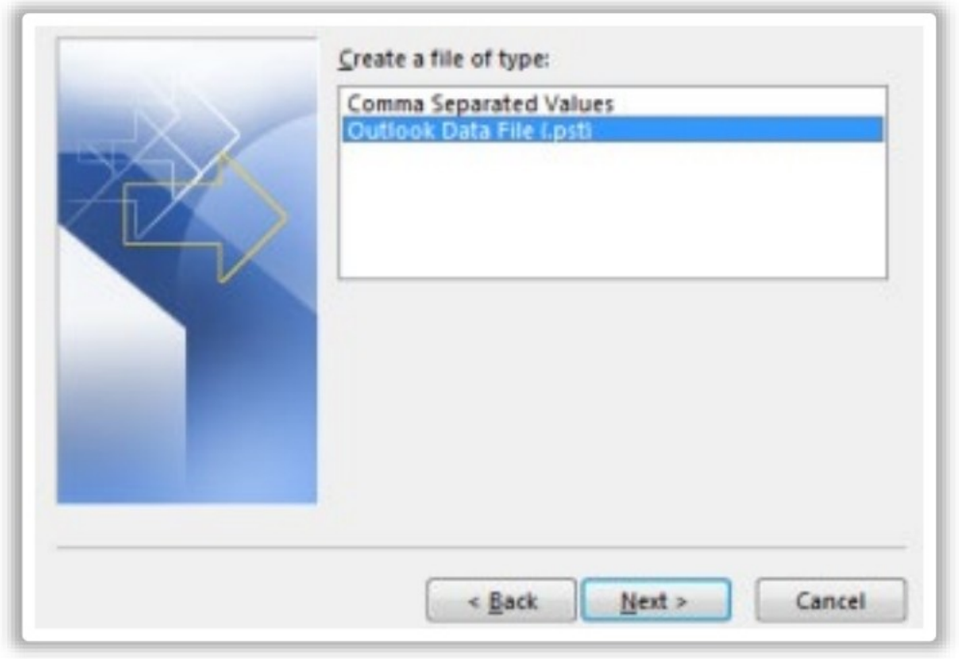


Figure 10.157: Selecting Outlook Data File (.pst)

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Select the mail folder you want to back up and select **Next**.
- Select a location and name for the backup file and select **Finish**.
- Enter and confirm a password to ensure no one has access this file, and then select **OK**.

Backup and Restore POP3 Data

In the case of a POP3 account, all Outlook data such as emails, contacts, calendar, tasks, and notes are stored locally in a.pst file. It is recommended to backup the.pst file regularly to the backup location (by copying the .pst file to a hard drive, USB, CD, DVD, or online storage location) when Outlook is closed. Use the export and import method to backup selected folders only.

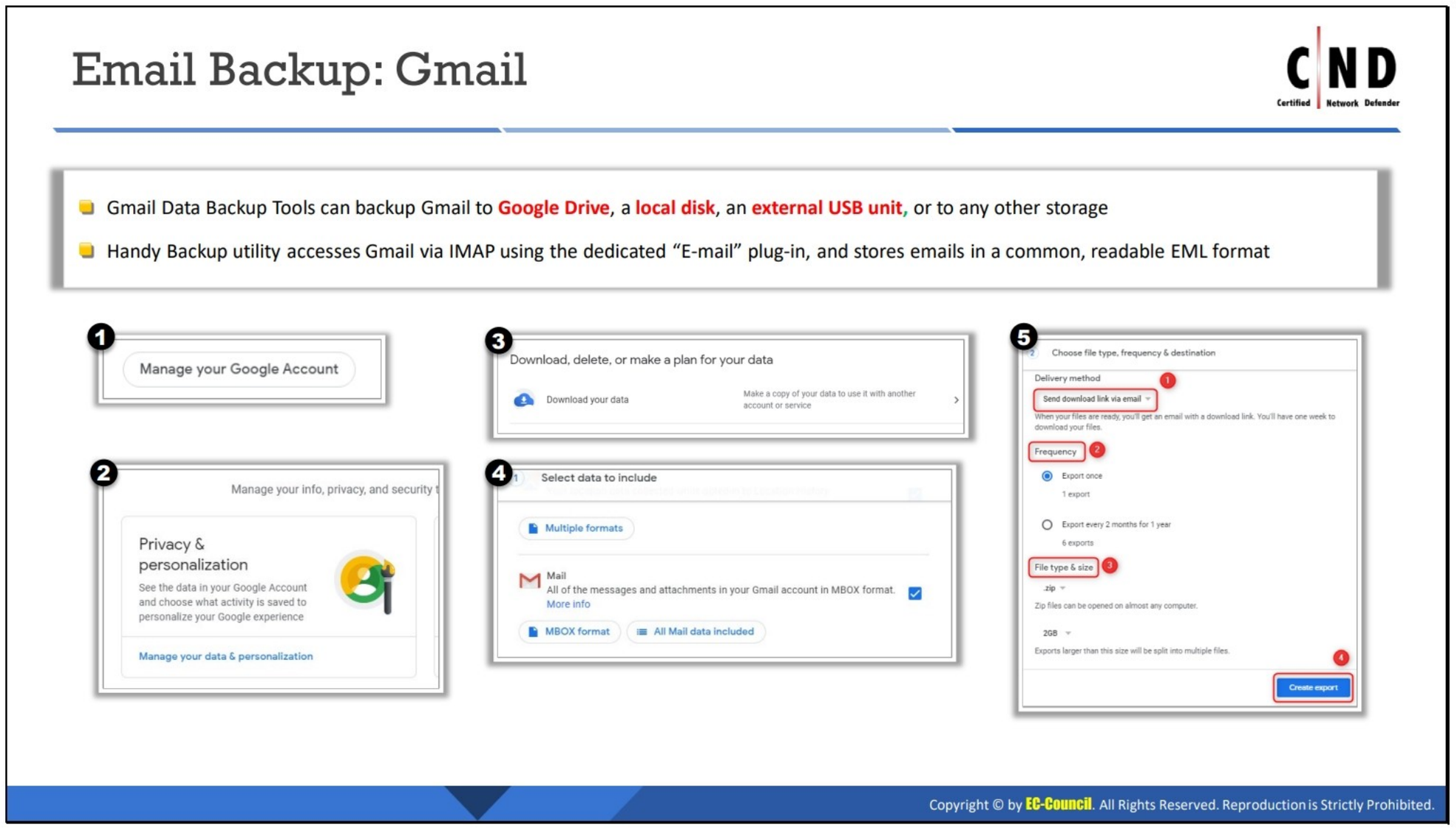
To restore this file, copy it to a location where you would like to work on it. Then, open Outlook and connect to the .pst file by its location: **File**-> **Open**-> **Outlook Data File….**

Backup and Restore IMAP Data

In the case an IMAP account, all Outlook data such as emails, contacts, calendar, tasks, and notes are stored in a.pst file, an.ost file, or a combination of both, which makes a proper backup of both emails and other data in IMAP accounts complex. Regularly export all folders marked with “This computer only” to a.pst file.

To restore IMAP data, rename the .ost and .pst files which comprise the cache of IMAP data to .old when Outlook is closed.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Email Backup: Gmail

Gmail Data Backup Tools can backup Gmail to Google Drive, a local disk, an external USB unit, or to any other storage. Gmail allows data backup to your system using third-party apps. Google allows data backup to a local drive/external hard drive using Google's data tool.

Steps to Backup Gmail

- Open Gmail account.
- Navigate to **Google Account** > **Manage your Google Account**.

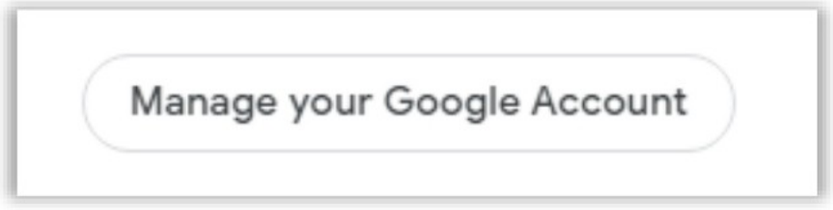


Figure 10.158: My Account/Manage your Google Account Window

- Click **Privacy & personalization**.

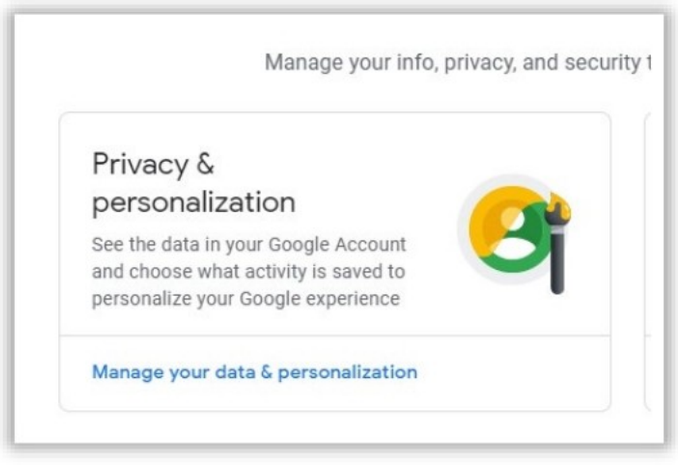


Figure 10.159: Selecting Privacy & personalization

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Click **Download, delete, or make a plan for your data**.

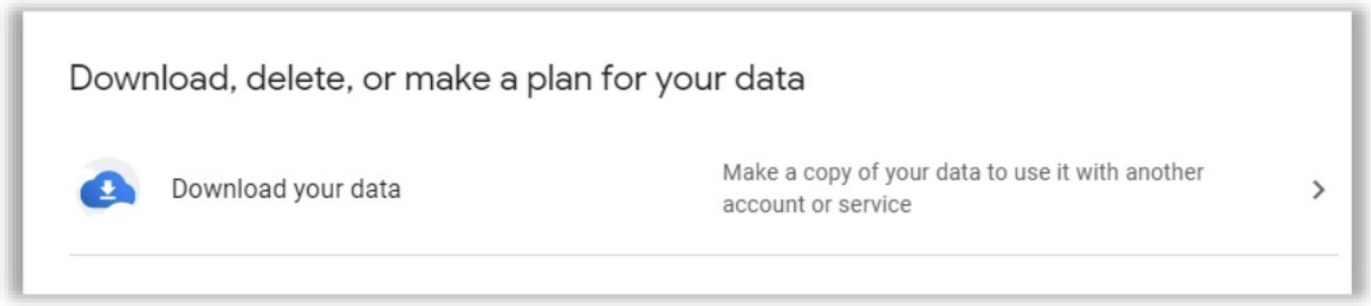


Figure 10.160: Choosing Proper Option for Email Backup

- In the **Download your data** page, see the complete list of the Google products that you can choose and backup. To archive mail, click **SELECT NONE** under **Select data to include**. Scroll down, locate Mail, and check Mail to select it.

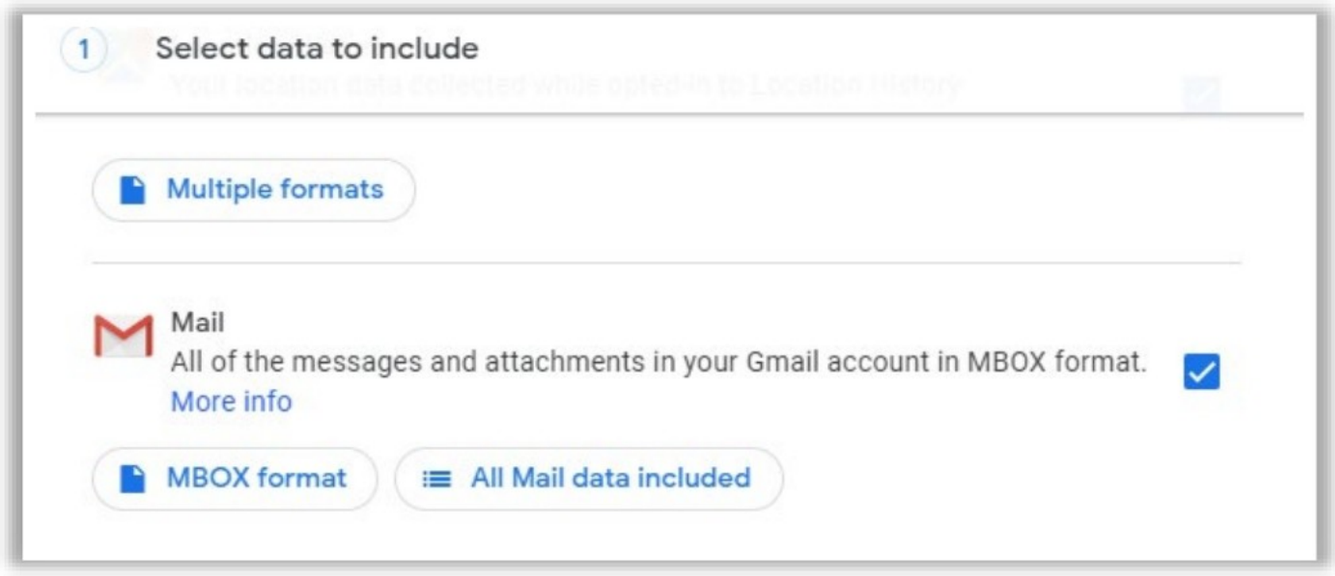


Figure 10.161: Selecting the Data

- Click **Next step** button.
- Select the file type as .zip or .tgz. Select **Delivery method** from the list of options. Select one of the options to **Send download link via** email, Google Drive, Dropbox, or OneDrive.

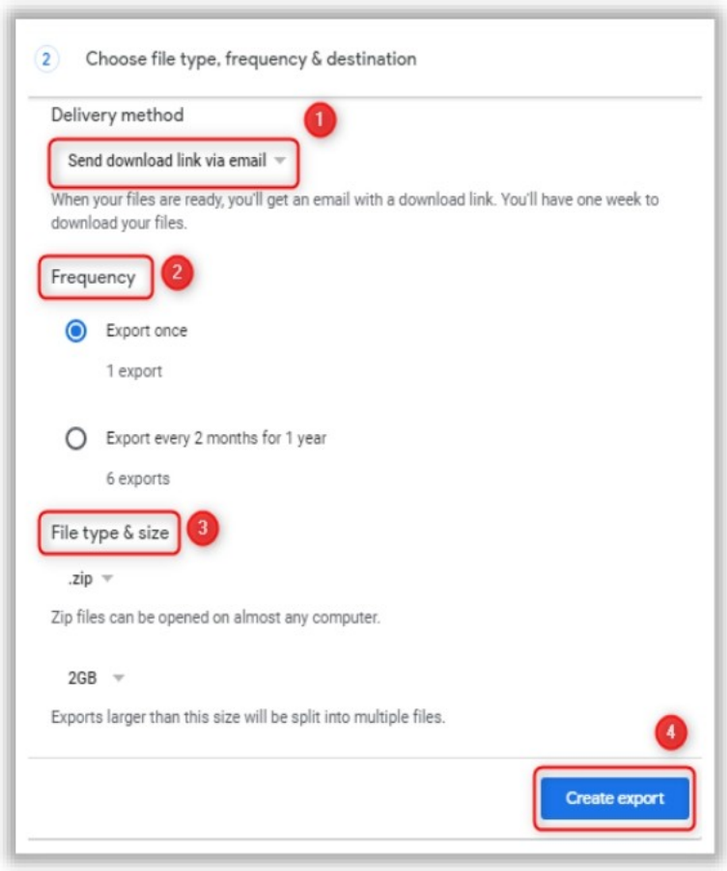
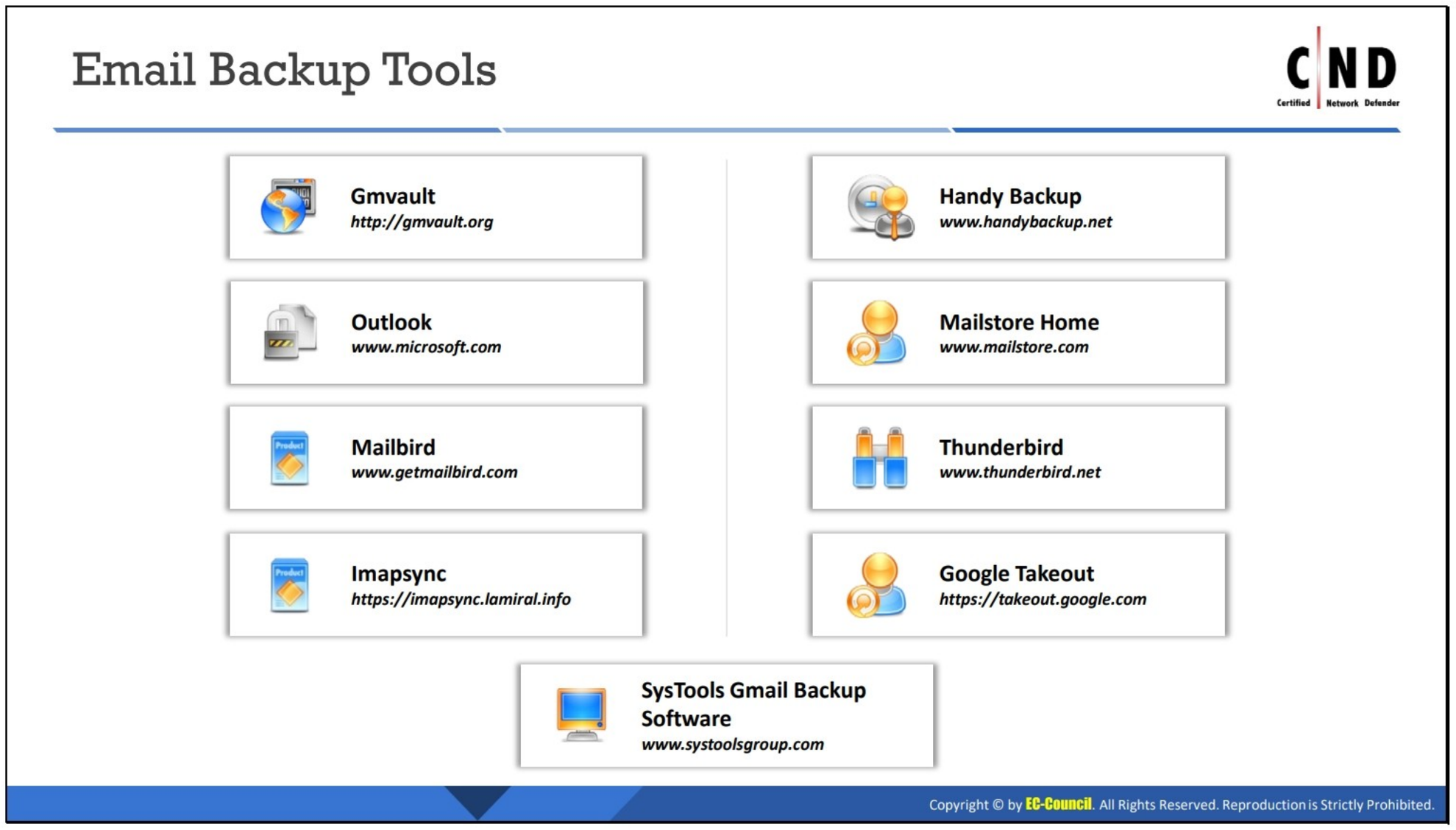


Figure 10.162: Create an export

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Email Backup Tools

The following are some third-party tools offering an email backup facility.

Gmvault

Source: http://gmvault.org

Gmvault with its full sync mode can backup the entire Gmail account in a unique directory. The email backup repository can then be easily moved from one machine to another. Its key features include restoring emails in any Gmail account, updating a backup in minutes, handling all Gmail IMAP hiccups, and encrypting saved emails, along with being highly customizable.

Handy Backup

Source: www.handybackup.net

Handy Backup allows the backup of emails from any server with just a few clicks, provides an easy access to the mail backup from almost any web or local service, and simplifies message export, import, or migration between email services. Its key features include backing up emails using IMAP protocol, migrating an email backup to different mailboxes, backing up local email solutions, etc.

Mailstore Home

Source: www.mailstore.com

MailStore Home archives private emails from almost any source, and searches through them quickly, and keeps them safe and retrievable for years. Its key features include a central archive for all emails, one-click restore. It is also safe for large amounts of data, mobile email archiving, among others.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Outlook

Source: www.microsoft.com

When an Outlook app is installed on a computer, it can be used to move emails, contacts, and calendar items from one email account to another (for example, Gmail account). Items can be exported by creating a .pst file. This Outlook data file contains your messages and other Outlook items, and is saved on system.

Thunderbird

Source: www.thunderbird.net

Thunderbird stores data in a separate location called profile folder, away from the program files. To move data, copy the profile folder to an equivalent location on a destination computer. It allows you to save copies of your emails on your computer as EML files. These files can be opened with a number of email programs.

Mailbird

Source: www.getmailbird.com

Mailbird allows email backup for its users by copying the Mailbird folder "C:\Users\'your user name'\AppData\Local" to a new system. The user only has to install Mailbird in a new system, and overwrite the Mailbird folder in new system with the copied Mailbird folder.

Google Takeout

Source: https://takeout.google.com

Google Takeout can export a copy of the content in your Google account to back it up or use it with a service outside of Google.

Imapsync

Source: https://imapsync.lamiral.info

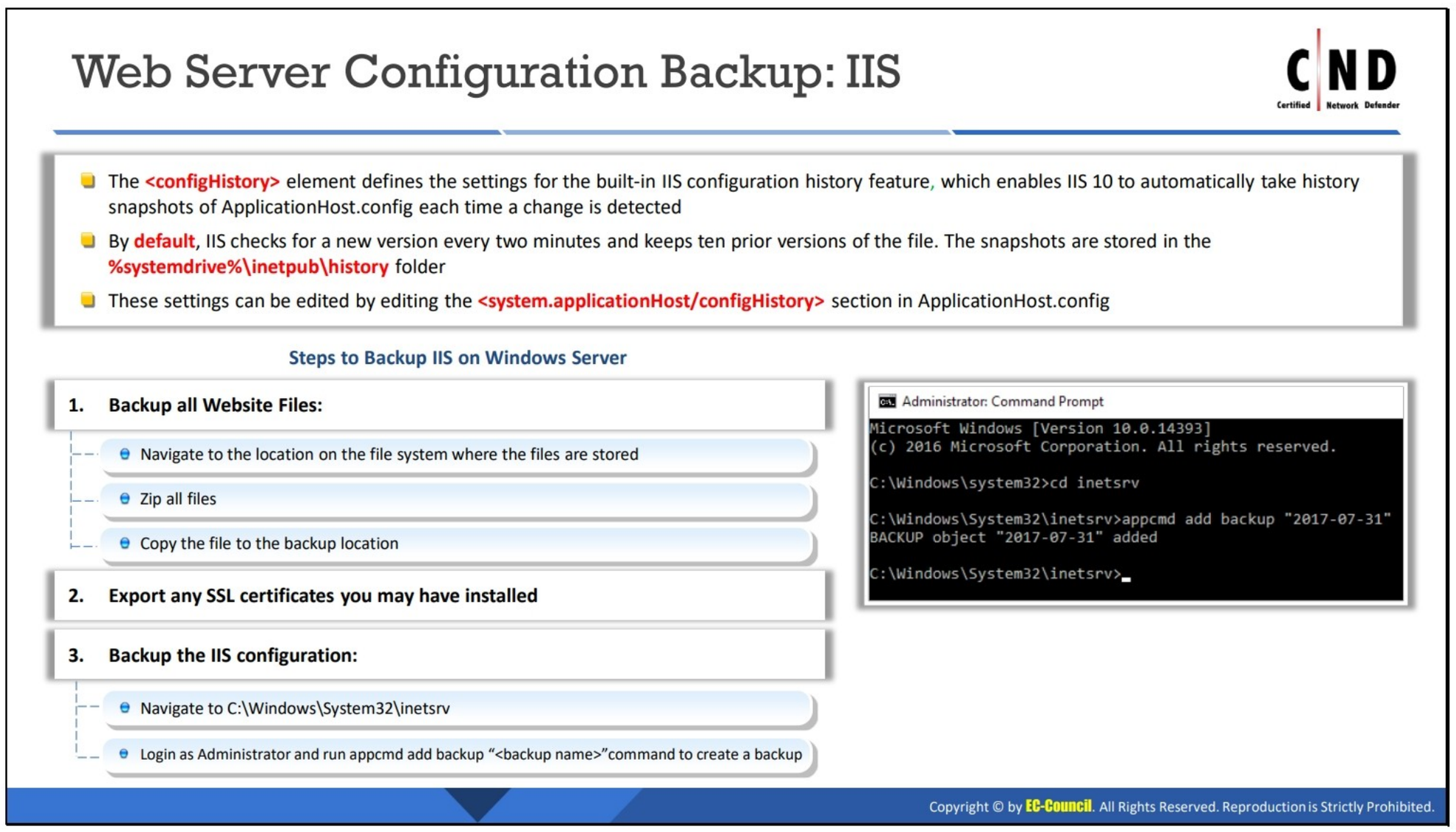
This IMAP transfer tool allows you to migrate or backup IMAP accounts. It is a command-line tool that allows incremental and recursive IMAP transfers from one mailbox to another, both anywhere on the Internet or in your local network.

SysTools Gmail Backup Software

Source: www.systoolsgroup.coms

SysTools MailBakup is a unified tool to backup web-based emails. Other features include backup of multiple web-based emails, varied email preview options, recursive listing of emails, a powerful search to spot emails, multiple email backup formats, complete backup reporting, etc.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Web Server Configuration Backup: IIS

The **<configHistory>** element defines the settings for the built-in IIS configuration history feature, which enables IIS 10 to automatically take history snapshots of **ApplicationHost.config** each time a change is detected. By default, IIS checks for a new version every two minutes and will keep ten prior versions of the file. The snapshots are stored in the **%systemdrive%\inetpub\history** folder. These settings can be edited by editing the **<system.applicationHost/configHistory>** section in **ApplicationHost.config.**

The steps necessary to backup website data and configuration running on the IIS web server are given below.

Steps to Backup IIS on Windows Server

- **Step 1: Backup all website files** (by default, they are stored in %SystemDrive%\inetpub\wwwroot).
    - Navigate to the location on the file system where the files are stored.

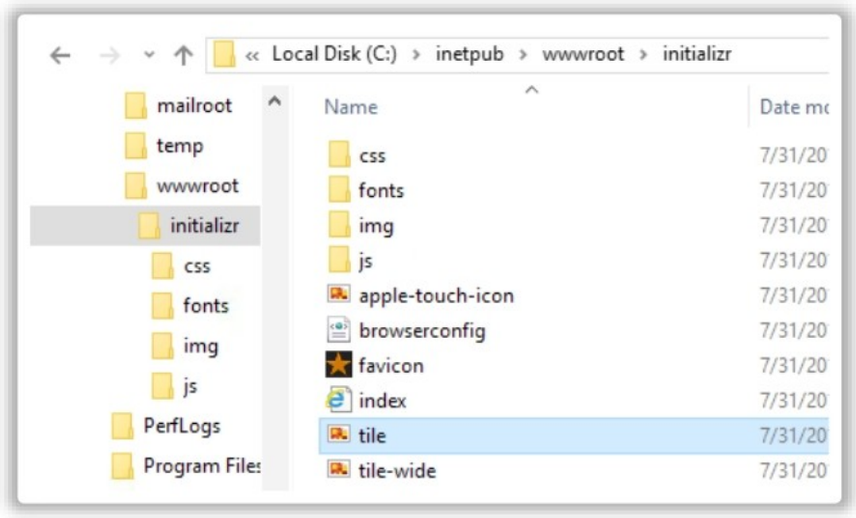


Figure 10.163: Navigating on the File System

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Zip all files.

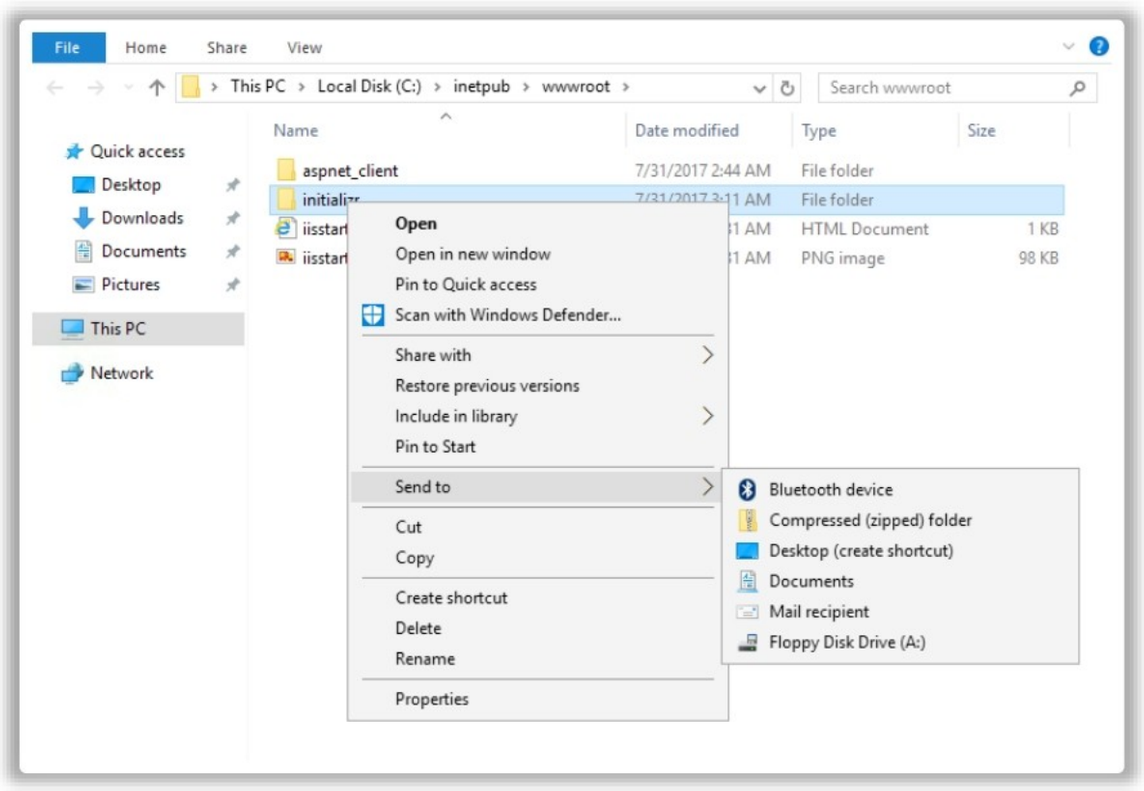


Figure 10.164: Zipping the Files

- Copy the file to the backup location.

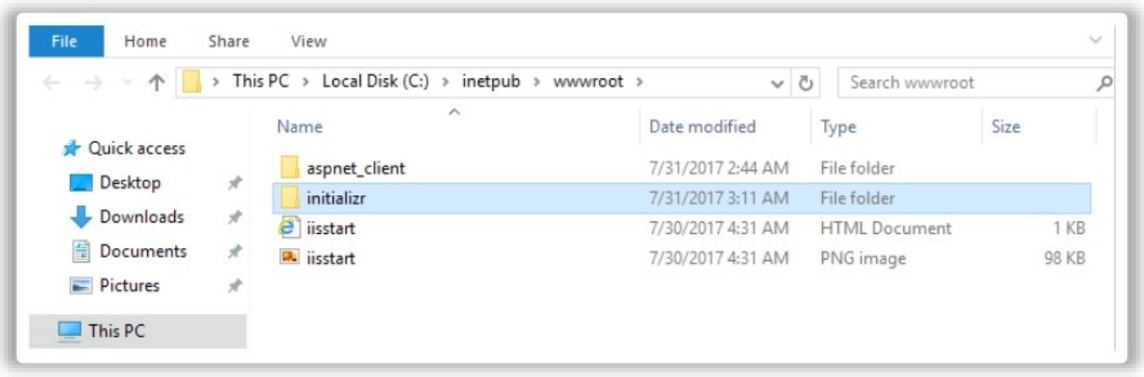


Figure 10.165: Copying File to Back Up Location

- **Step 2: Backup/Export of current IIS certificates**
  - Get the list of SSLs on the server using the following command.

    netsh http show sslcert

- **Step 3: Backup the IIS configuration**
  - Navigate to **C:\Windows\System32\inetsrv** on the source server, and run the following command to create a backup.

    appcmd add backup “<backup name>”

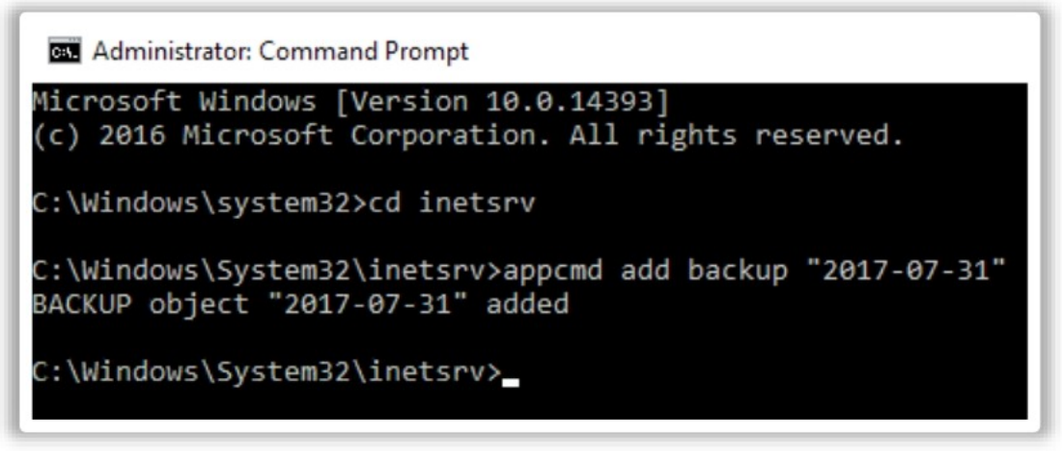


Figure 10.166: Command to Create Backup

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- The backup will be created in **C:\Windows\System32\inetsrv\backup.**

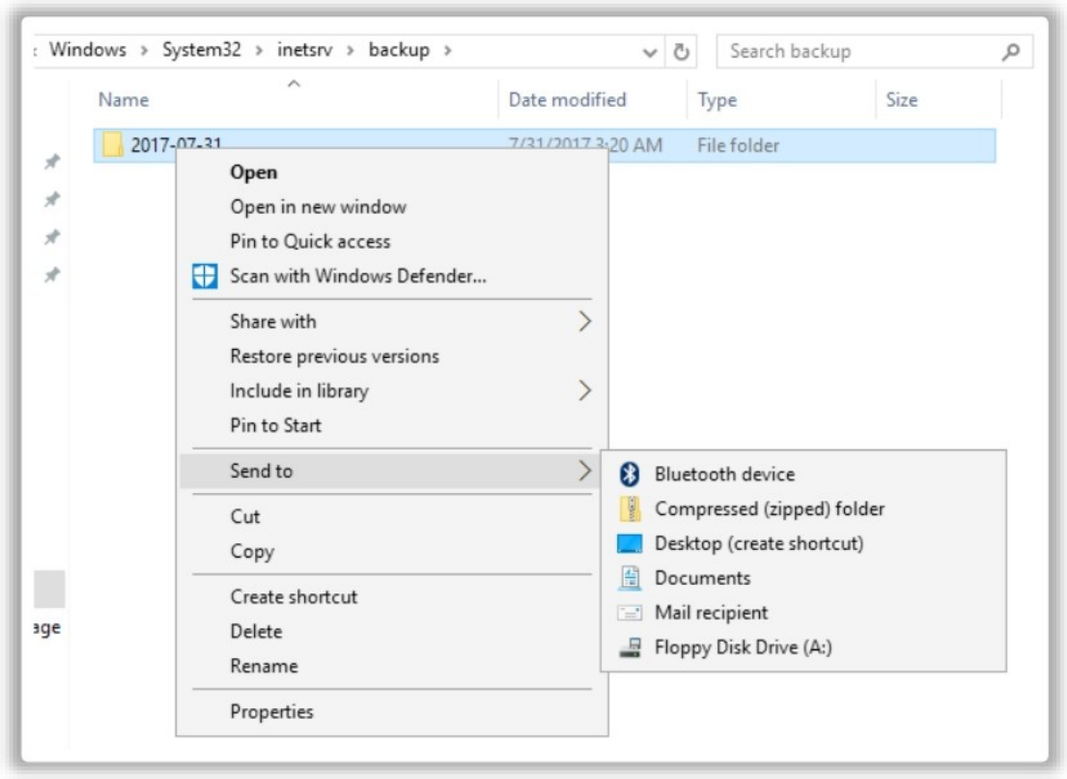
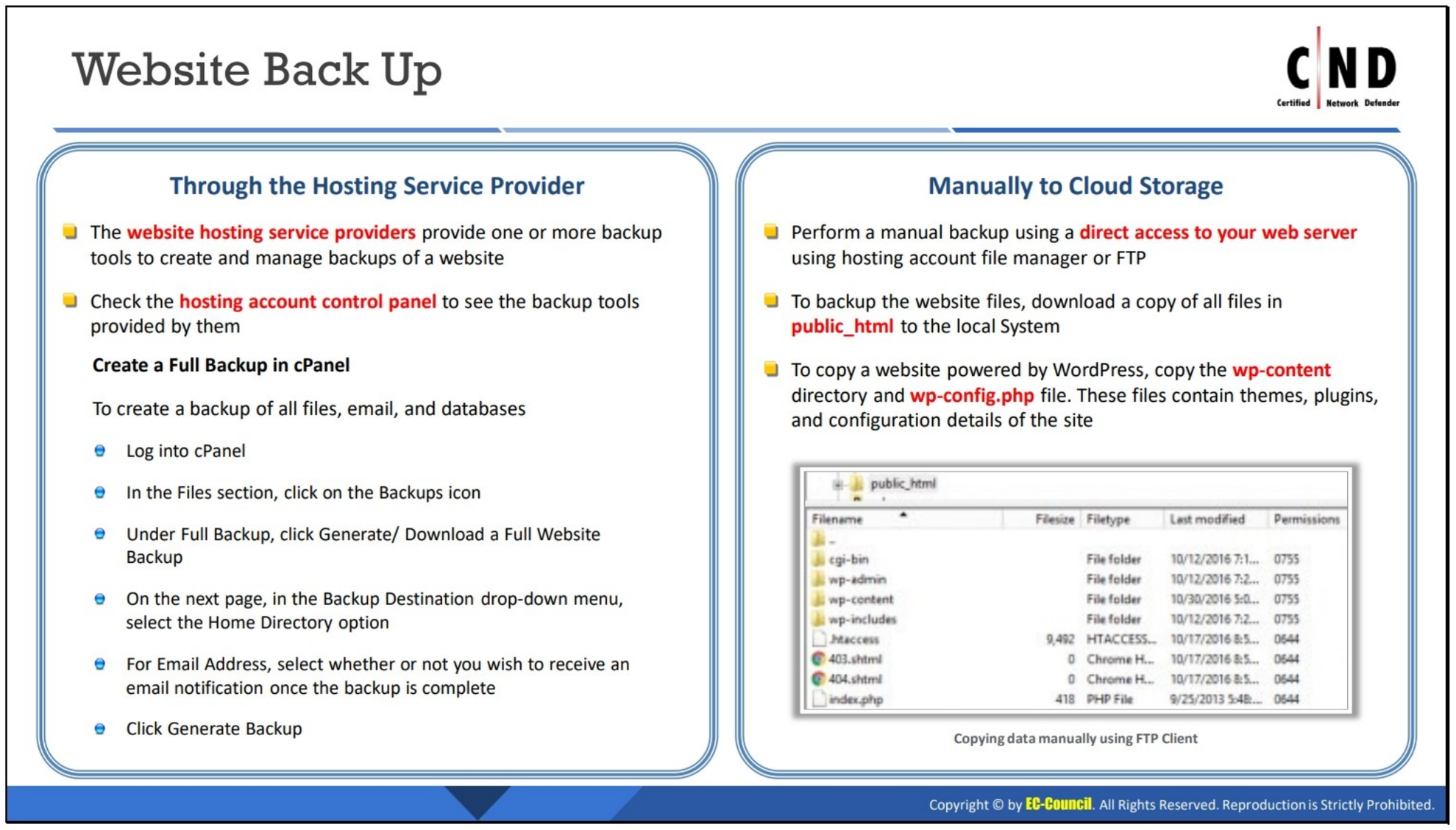


Figure 10.167: Creation of Back Up

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Website Back Up

Choose any one of the following three ways to backup a website.

Through the hosting service provider: The website hosting service providers provide one or more backup tools to create and manage a website backup. Check the hosting account control panel to see the backup tools provided by them. For example, A2 Hosting service provides two options to help you manage backups: backup wizard and server rewind tools.

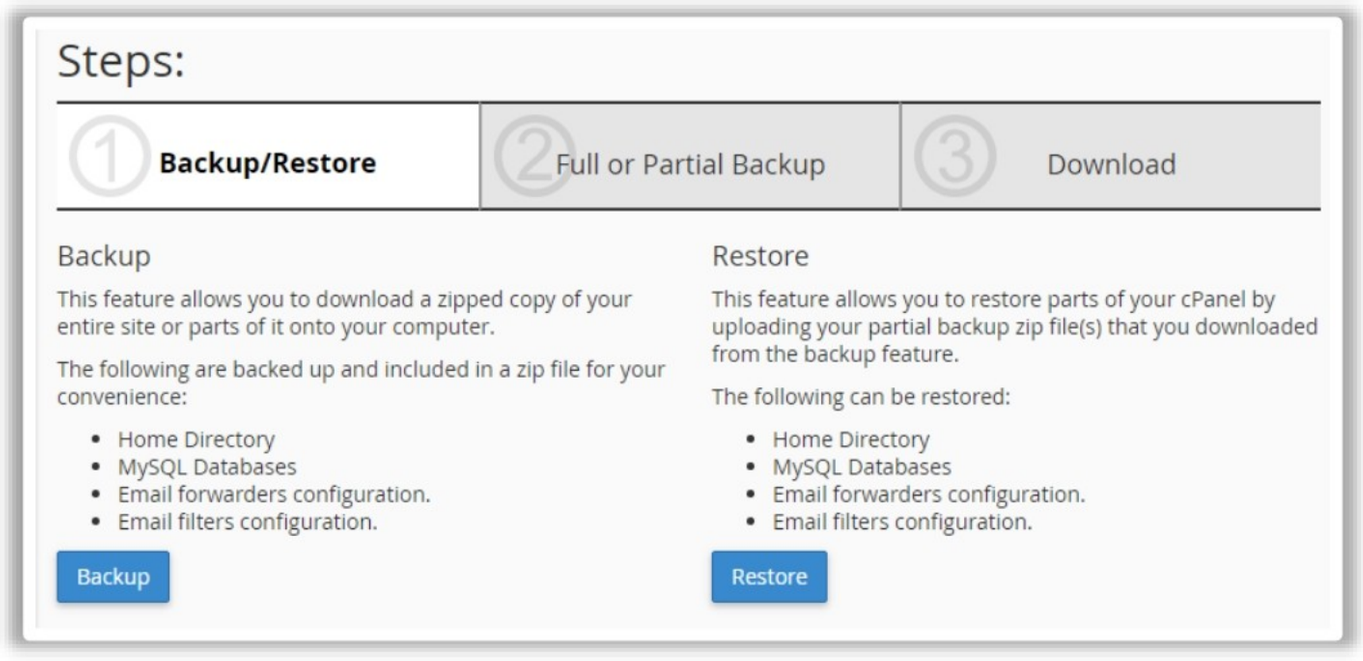


Figure 10.168: Back up Tools in the Hosting Account Control Panel

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

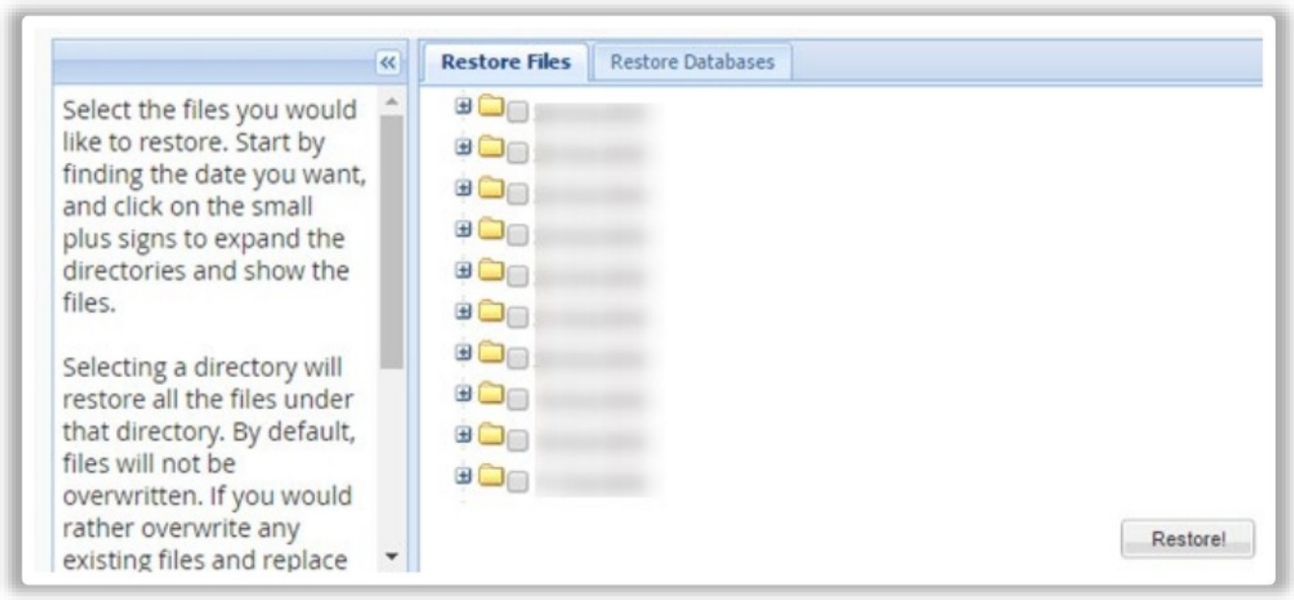


Figure 10.169: Selecting the File that the User Want to Restore

- **Create a full backup in cPanel** to backup all files, emails, and databases.
  - Log into cPanel.
  - Click **Backups** icon in the Files section.
  - Under **Full Backup**, click **Generate/ Download a Full Website Backup.**
  - On the next page, in the **Backup Destination** drop-down menu, select the **Home Directory** option.
  - For Email Address, select whether or not you wish to receive an email notification once the backup is complete.
  - Click **Generate Backup**.
- **Manually to cloud storage**
  - Perform a manual backup using direct access to your web server using hosting account file manager or FTP.
  - To backup website files, download a copy of all files in public_html to the local system.

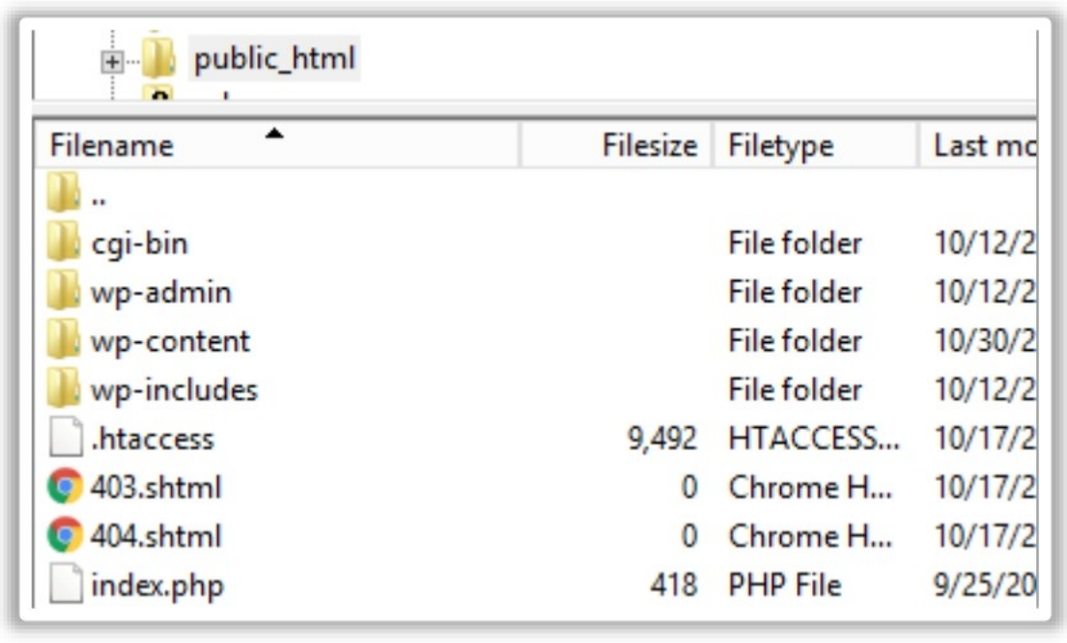


Figure 10.170: Files in public_html

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- To copy a website powered by WordPress, copy the wp-content directory and wp-config.php file. These files contain themes, plugins, and configuration details of the website.

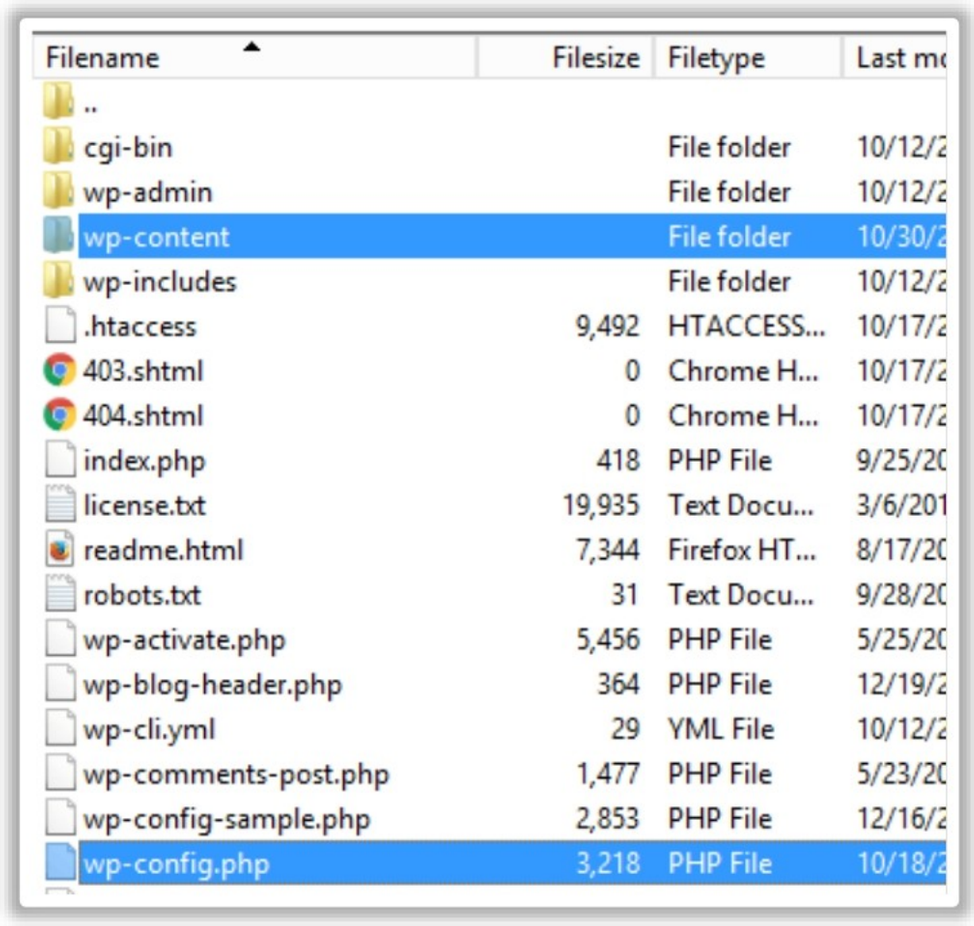


Figure 10.171: Copying the wp-content directory and wp-config.php file

- Right-click and use the Download command to create copies of your selection on a local hard drive, then upload them to any cloud storage service.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Data Backup Retention

Data retention is the process of storing and maintaining important information for meeting compliance and business data archival requirements. It helps organizations in recovering business-critical data in case of data loss.

Every organization should develop a data retention policy to ensure that all important data is satisfactorily stored. The data retention policy is a set of rules for preserving and maintaining data for operational or regulatory compliance requirements. The policy defines the required retention periods for different data types, and also sets the minimum standards for destroying certain information.

A data retention policy is applied to all business units, processes, and systems in all countries where an organization operates. It is applied to an organization's officers, directors, employees, agents, affiliates, contractors, consultants, advisors, or service providers who can collect, process, or have access to different data types. Moreover, it is applied to all documents such as emails, hard copy documents, soft copy documents, audio and video files, etc.

Steps to Create Data a Retention Policy

The following steps are used to create a data retention policy:

1. Build a data retention policy development team

You should build a data retention policy development team that includes the members such as:

- In-house legal counsels
- Departmental managers and supervisors
- Those who receive and manage financial reports

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Those who develop financial reports
- Staff members for managing data retention settings

2. Identify the types of regulatory compliances applicable to your business

Different regulatory compliances specify different data retention durations and data removal conditions. Some of them are listed below:

- The Health Insurance Portability and Accountability Act (HIPAA)
- The Sarbanes-Oxley Act (SOX)
- The Internal Revenue Service (IRS)
- The Children's Online Privacy Protection Act (COPPA)
- The EU's GDPR

3. Specify the types of data to be included in your data retention policy

The following types of data should be included in the data retention policy:

- Documents
- Emails and other electronic documents
- Customer records
- Transactional information
- Spreadsheets
- Contracts
- Correspondence between staff and clients, agents, vendors, shareholders, and the public
- Supplier and partner data
- Employee records
- Customer records
- Sales, invoice, and billing information
- Tax and accounting documentation
- Financial reports
- Healthcare and patient data
- Student and educational data
- Other information produced, collected, and maintained for satisfying regular business activities

4. Develop a data retention policy

Develop a data retention policy considering the following points:

- Purpose

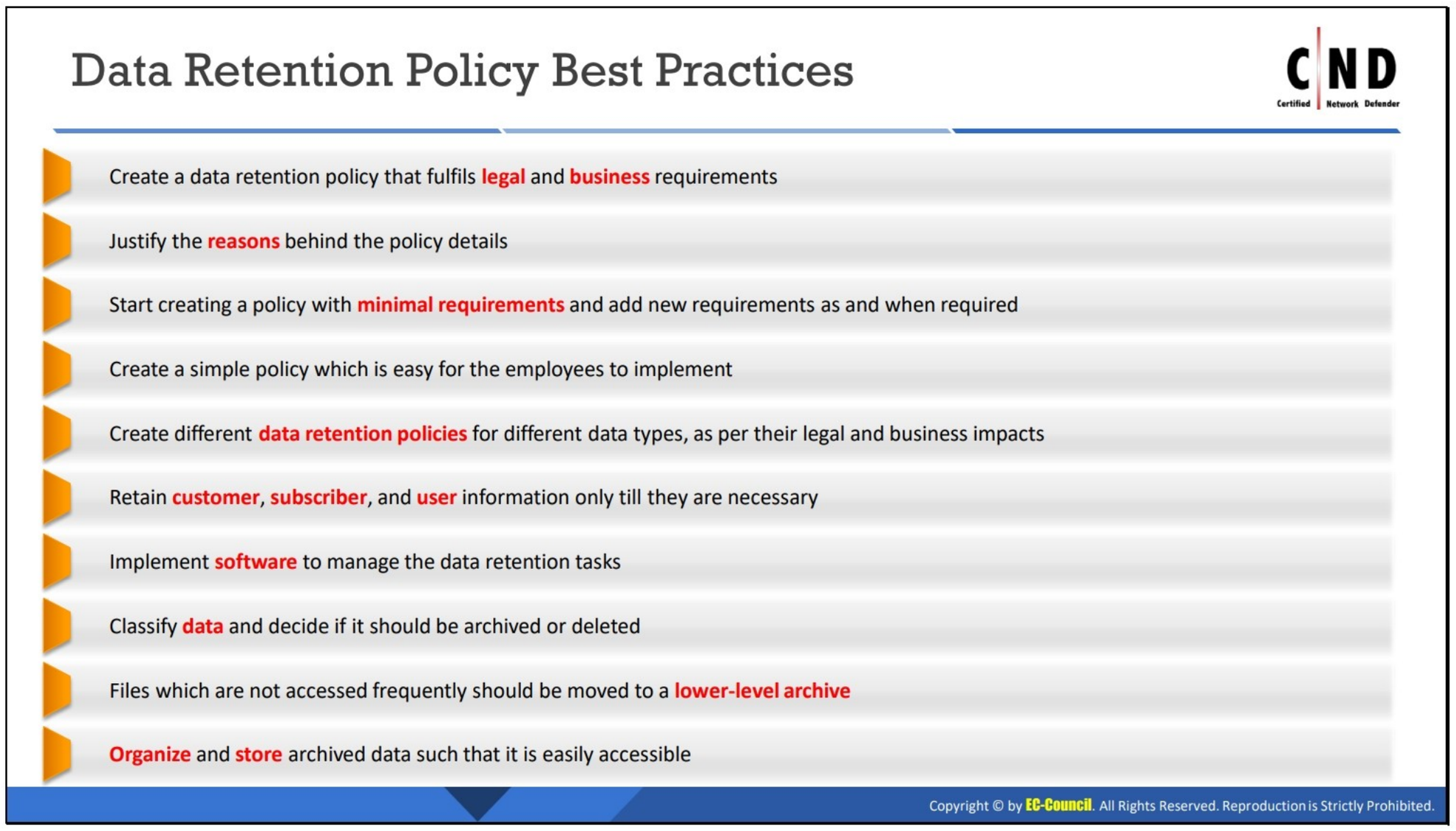
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Applicable laws, regulations, policies, rules, and acts
- Record retention and deletion schedule
- Litigation plan
- Review and update schedule

5. Inform all employees about the data retention policy

All employees should be aware of and comprehensively understand the different aspects of the data retention policy. Provide each employee a copy of the data retention policy and also design training and review sessions to keep them updated.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

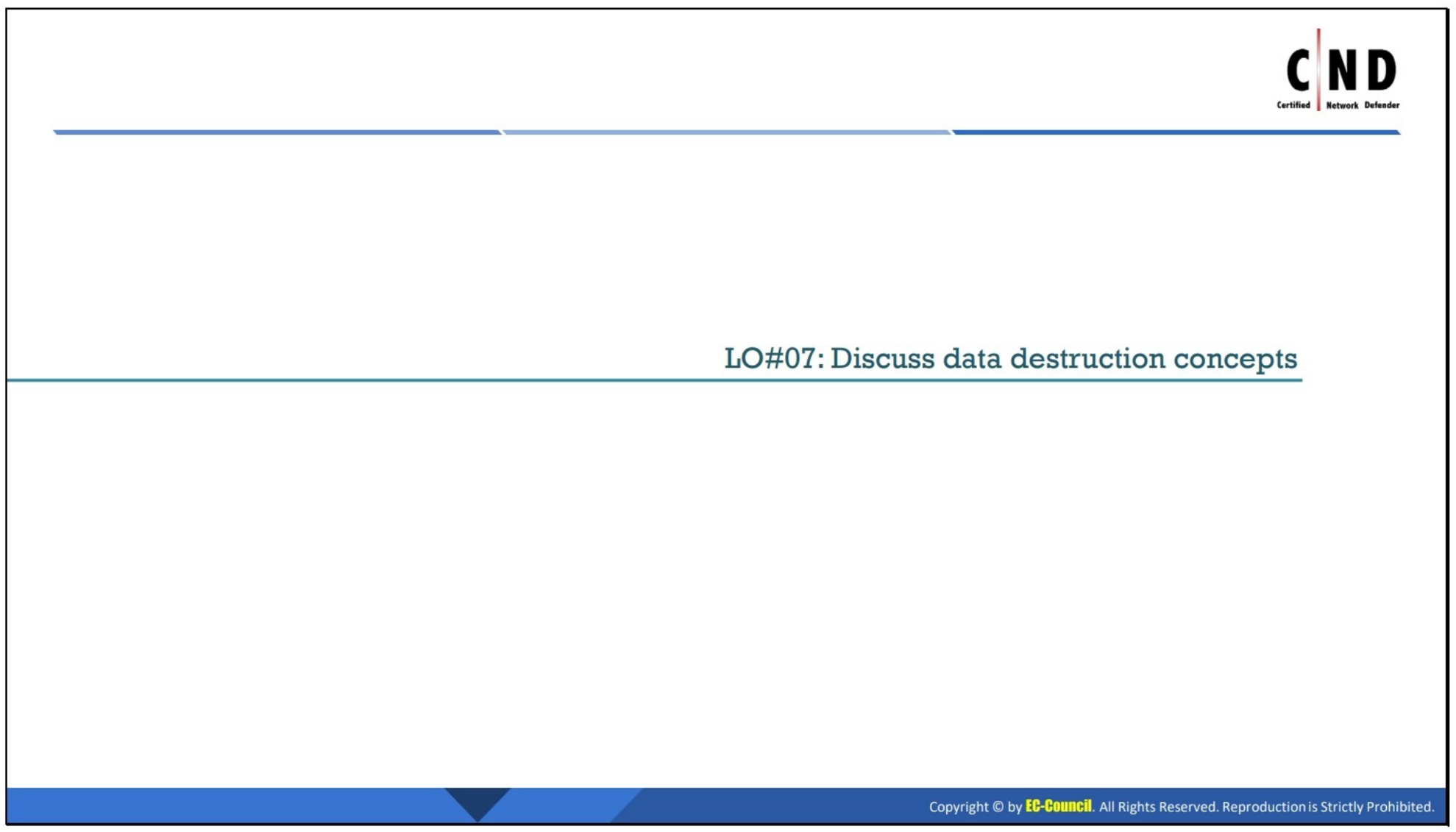


Data Retention Policy Best Practices

The following data retention best practices for an organization can help establish and enforce a more compliant and useful data retention policy suited to their needs:

- Create a data retention policy that fulfills legal and business requirements
- Justify the reasons behind the policy details
- Start creating a policy with minimal requirements, and add new requirements as and when required
- Create a simple policy which is easy for the employees to implement
- Create different data retention policies for different data types, as per their legal and business impacts
- Retain customer, subscriber, and user information only till they are necessary
- Implement software to manage the data retention tasks
- Classify data and decide if it should be archived or deleted
- Files which are not accessed frequently should be moved to a lower-level archive
- Organize and store archived data such that it is easily accessible

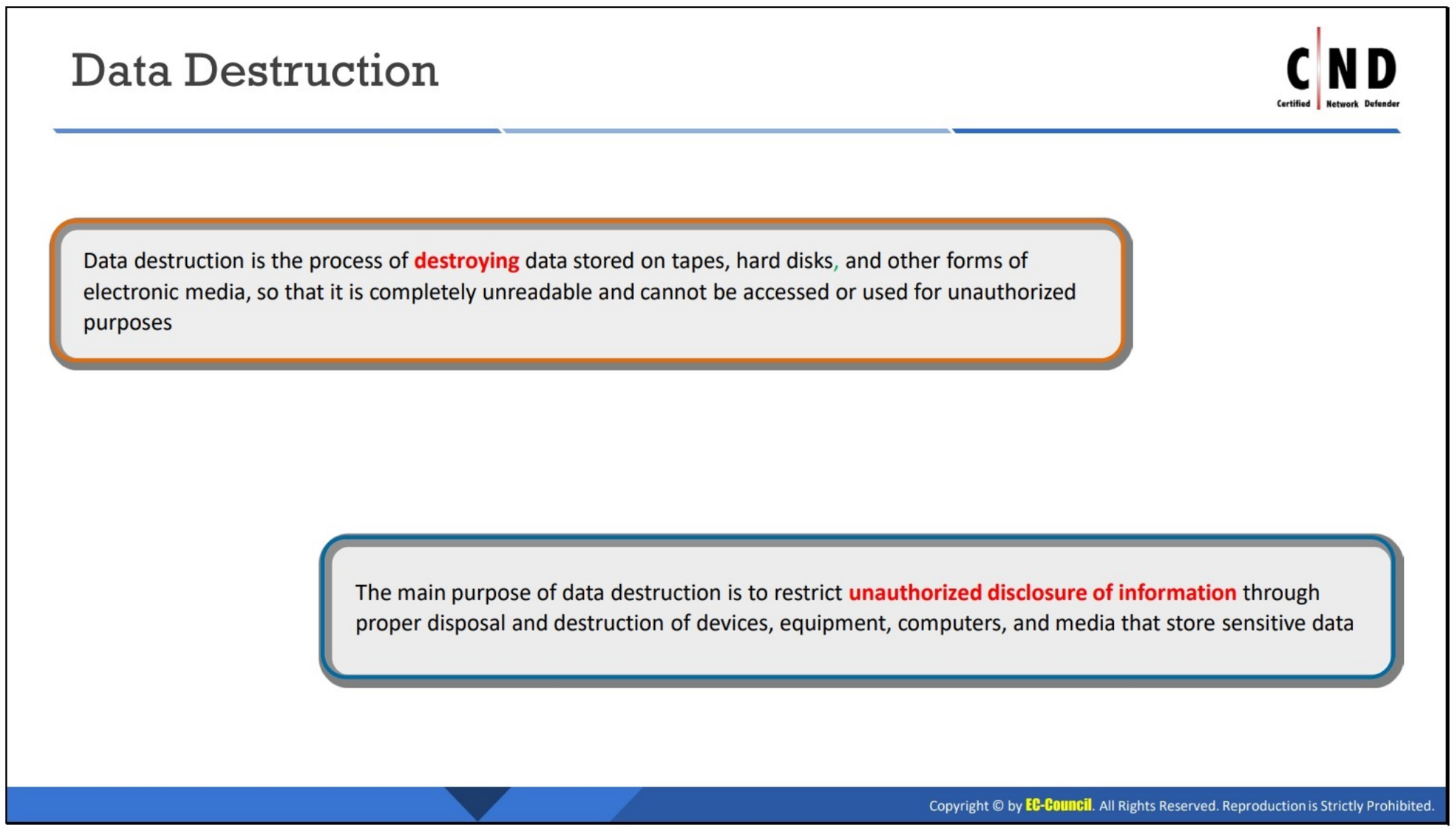
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



LO#07: Data Destruction Concepts

An organization should have a plan to destruct data such that it is not readable and accessible by unauthorized users. The objective of this section is to explain the concept of data destruction and a data destruction policy.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Data Destruction

Computers, smartphones, and other devices store a large amount of information, some of which may be sensitive and critical, such as emails, documents, personal photos, etc. Once not in use, the user deletes the data presuming that the information is deleted and cannot be recovered. If not deleted properly, the information still exists on the hard drive or memory chip, and anyone accessing such a system can recover these deleted files. The best way to permanently delete files or sensitive data is by implementing data destruction methods.

Data destruction is a process of destructing the stored data in electronic media such as hard drives, flash drives, tapes, etc. into an unreadable form that cannot be accessed or exploited for unauthorized purposes. The main purpose of data destruction is to restrict the unauthorized disclosure of information through proper disposal and destruction of devices, equipment, computers, and media that store sensitive data.

The various forms of data destruction are:

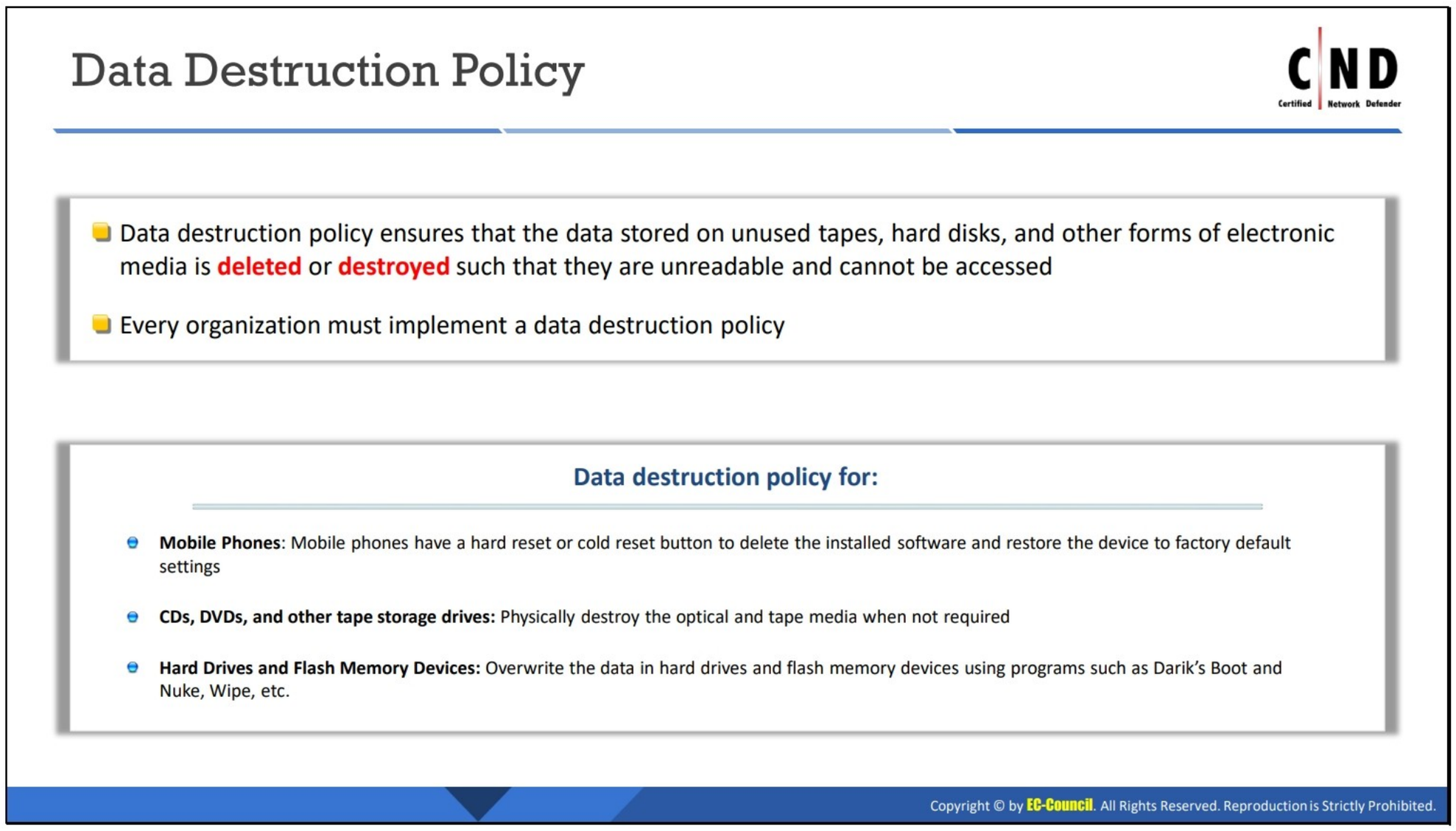
- Delete/Reformat
- Wipe
- Overwriting data
- Erasure
- Degaussing
- Physical destruction
- Electronic shredding
- Solid-state shredding

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Security Benefits of Data Destruction

- Data destruction protects the sensitive information of customers and employees from cybercriminals.
- Hefty fines can be avoided with data destruction as a security breach can lead to various penalties.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



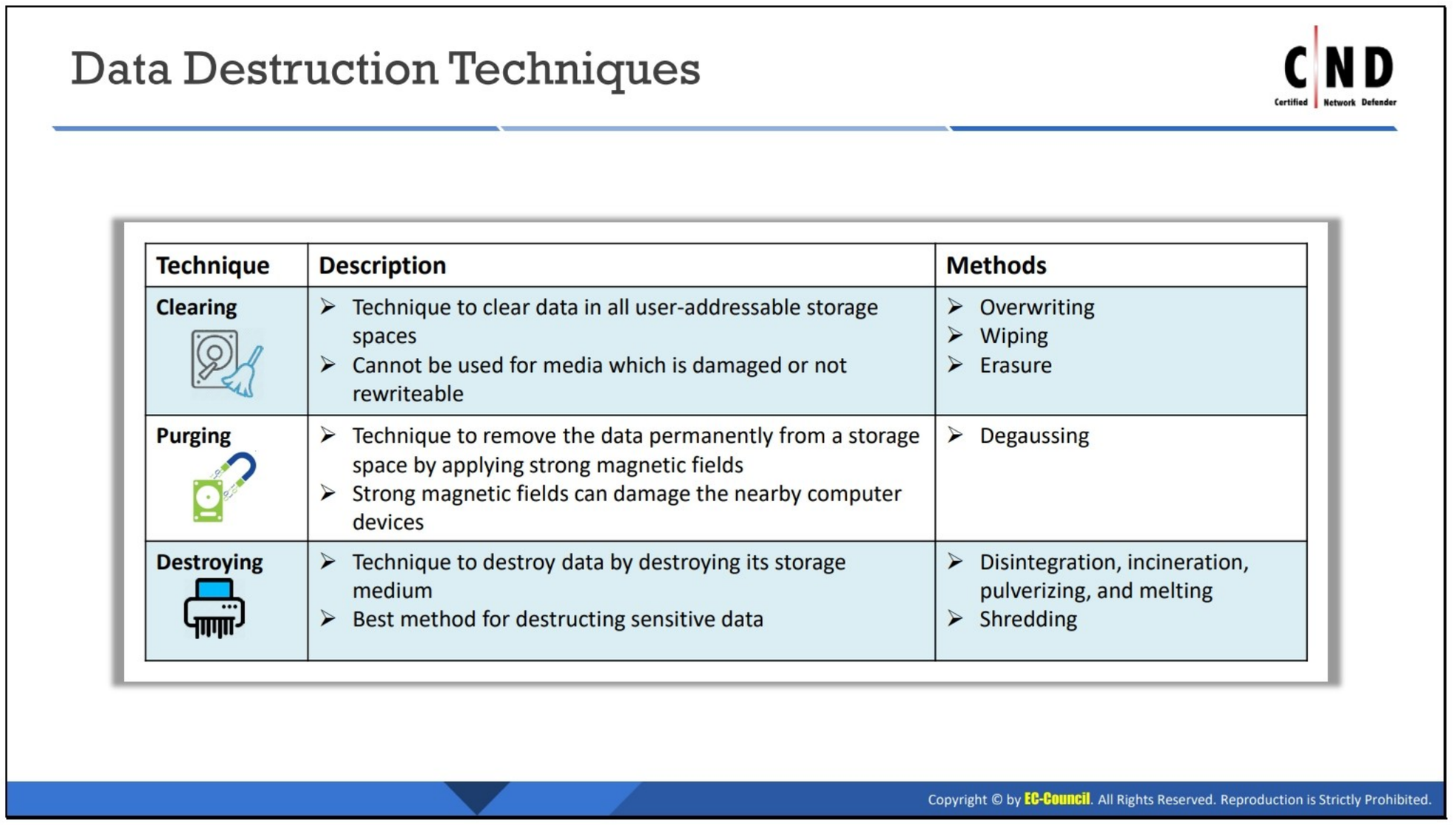
Data Destruction Policy

A data destruction policy ensures that the data stored on unused tapes, hard disks, and other forms of electronic media are overwritten or destroyed such that they are unreadable and cannot be accessed for unauthorized purposes. Implementation of a data destruction policy reduces the chances of a privacy breach. Companies should spend their time and money on a data destruction policy since they have to safeguard their data and prevent a data breach. Every organization must implement a data destruction policy.

Implementation of a data security policy: For implementing a data security policy, all devices and media no longer used by an organization should be securely removed, destructed, or overwritten.

- **Mobile phones - iPhones, Androids, Blackberries, etc.**: Mobile phones have a hard reset or cold reset button to delete the installed software and restore the device to factory default settings.
- **CDs, DVDs, Blu-rays, and other tape storage drives**: Physically destroy the optical and tape media when not required.
- **Hard drives and flash memory devices**: Overwrite the data in hard drives and flash memory devices using programs such as Darik's Boot and Nuke, Wipe, etc.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Data Destruction Techniques

The different data destruction techniques are listed below.

1. Clearing

Clearing is a data destruction technique that protects the sensitivity of information against a keyboard attack. Information eliminated by this method will not be recovered through data, disk, or file recovery tools. This technique is not applicable to media that is damaged or not rewritable. Overwriting, wiping, and erasure are the methods used for clearing information.

- **Overwriting:** Overwriting is a method of writing new data over old data with the purpose of eliminating old data completely. Sometimes, this is accomplished in a single attempt. However, if the medium implements strong security, multiple passes may be required. This ensures that all information is destroyed, and any recovery tool will not be able to recover it.
- **Wiping:** Data wiping is a method of clearing data from an electronic device so that it cannot be read any longer. It is performed by physically connecting an electronic device to a wiping device. Once the information is wiped out from an electronic device, it can be reused without losing storage capacity.
- **Erasure:** Erasure is another method used to delete all data from a hard drive into a form that it can no longer be recovered by anyone. This method is used by businesses that have purchased equipment off-lease or want to reuse hard drives for storing different information.

2. Purging

Purging is a data destruction technique that protects the sensitivity of information against a laboratory attack. A laboratory attack occurs when an unauthorized individual uses signal

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

processing recovery tools in a laboratory environment to recover sensitive information. Degaussing and executing the Secure Erase firmware command are two purging methods.

- **Degaussing**: Degaussing is a method of using high-powered magnets to disrupt the magnetic field of a magnetic media, such as hard drive disks and tapes. This method cannot be implemented on optical media such as CDs and DVDs. Degaussing the hard drive disk will typically make it inoperable, thus making it impossible for a user to check whether all data has been destroyed. This method is effective in destroying storage mediums with large amounts of information, but inappropriate if the user wants to reuse the storage device for storing different information.

3. Destroying

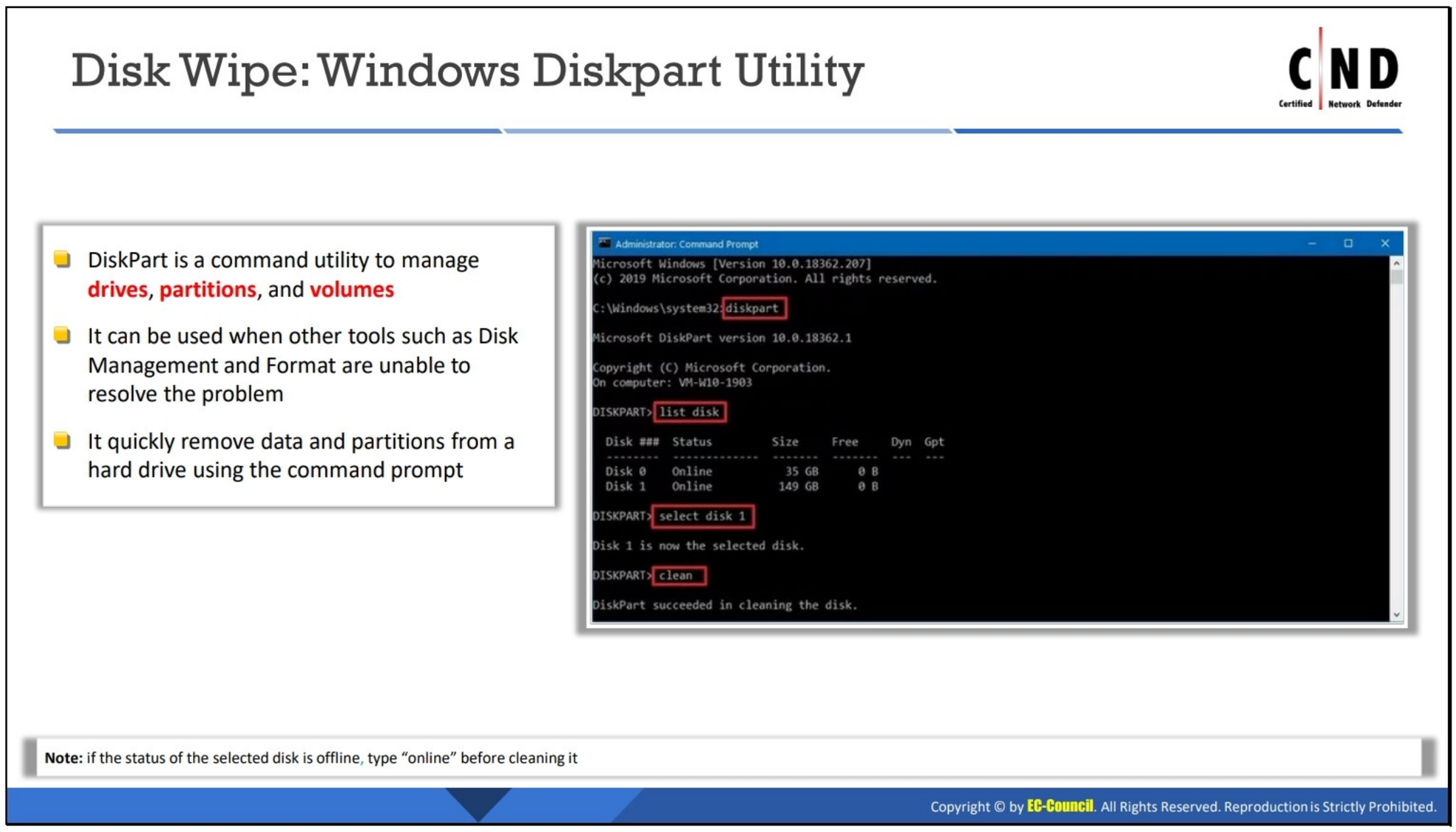
Destroying is a data destruction technique which physically destructs the media through a variety of methods, such as disintegration, incineration, pulverizing, shredding, and melting. This method is used in circumstances where complete destruction of data along with physical media is required.

- **Disintegration, incineration, pulverization, and melting**: These the physical destruction methods not only destroy the information stored in a storage media but also the physical media containing that information, either through outsourced metal destruction or by burning them.
- **Shredding**: This is another physical destruction method used to destroy information stored in any storage media such as hard drives, optical drives, smartphones, tablets, credit card swipe devices, etc. It breaks the electronic media into multiple pieces not larger than two millimeters. This method is specially used to destroy data stored in an organization's data center or in a large stockpile of old hard drives and media.

4. Disposal

Disposal is a technique of eliminating information without considering data destruction. This technique is applied to documents containing nonconfidential information. The disclosure of such information will not affect the organization goals, lead to any financial losses, or harm an individual.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Disk Wipe: Windows DiskPart Utility

- DiskPart is a command utility to manage drives, partitions, and volumes.
- It can be used when other tools such as Disk Management and Format are unable to resolve the problem.
- It quickly removes data and partitions from a hard drive using the command prompt.

Steps to Wipe a Hard Drive with Windows DiskPart

- Open command prompt in Administrator Mode.
- Type diskpart and press **Enter** to launch Diskpart.
- Type list disk for listing all drives connected to the computer, and press **Enter.**
- Type select disk 1 for selecting the drive the user wants to clean, and press **Enter.**
- Type clean to wipe out the drive and press **Enter.**

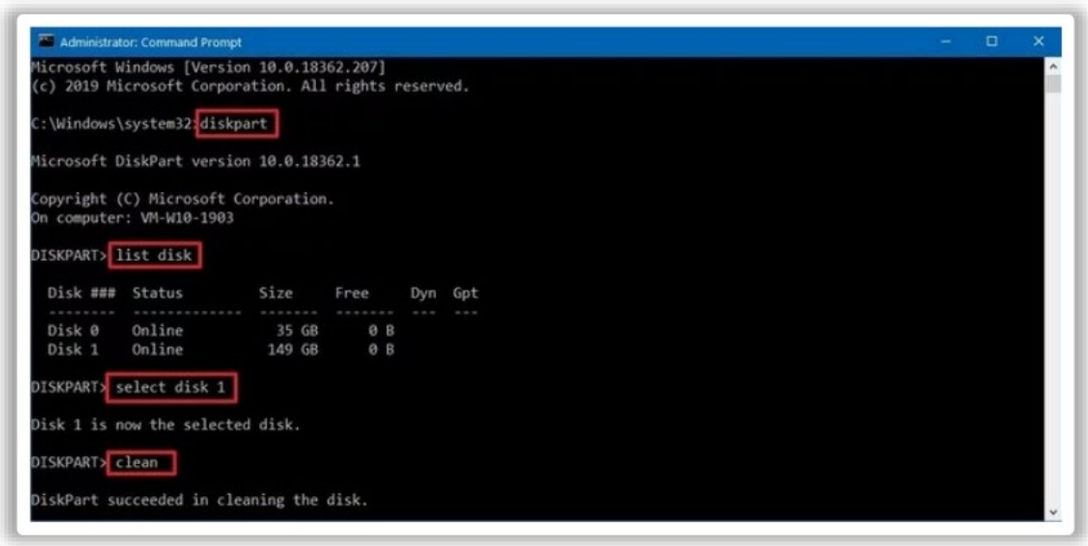


Figure 10.172: Wiping a hard drive with Windows DiskPart

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- Type list disk for confirming the selected drive and press **Enter**.
- Type create partition primary command for creating a new partition on the drive and press **Enter**.
- Type select partition 1 command for selecting the new primary partition and press **Enter**.
- Type active for activating the selected partition and press Enter.

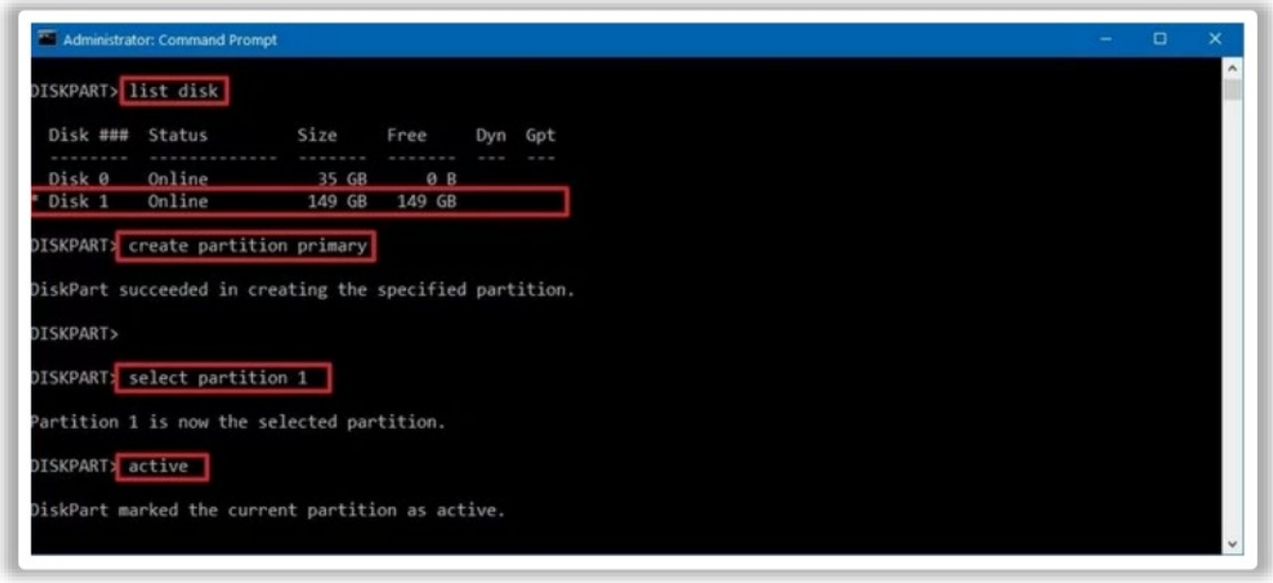


Figure 10.173: Selected partition activation

- Type format FS=NTFS label=Data quick for formatting the partition and setting a drive label, and press **Enter**.
- Type assign letter=w command to assign a letter and make the drive available in File Explorer, then press **Enter**.

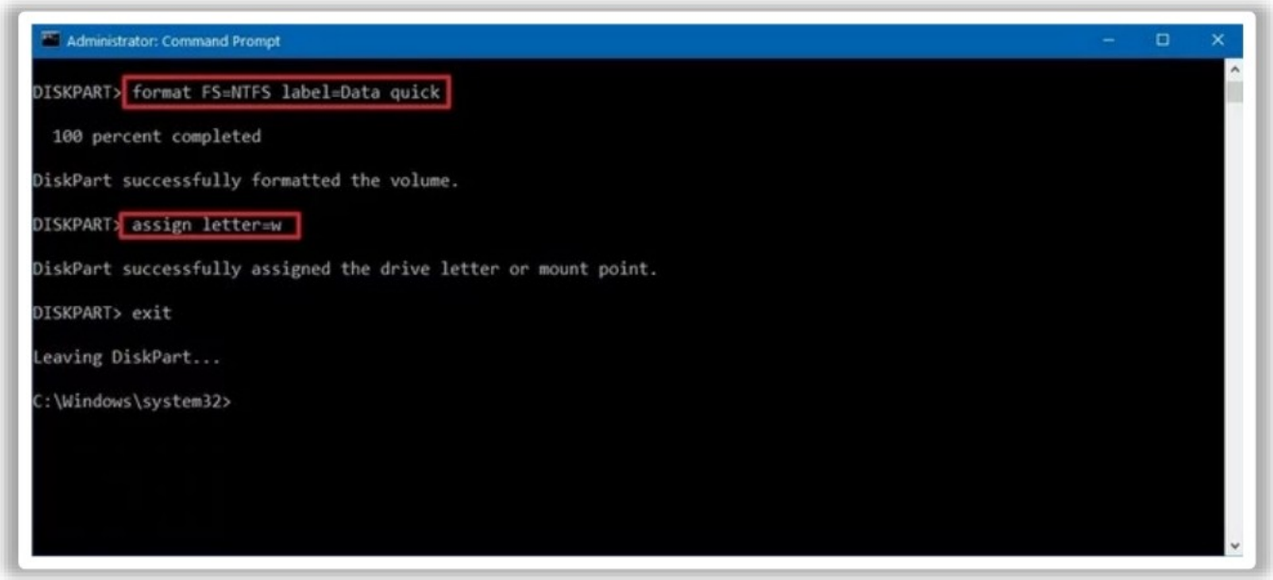
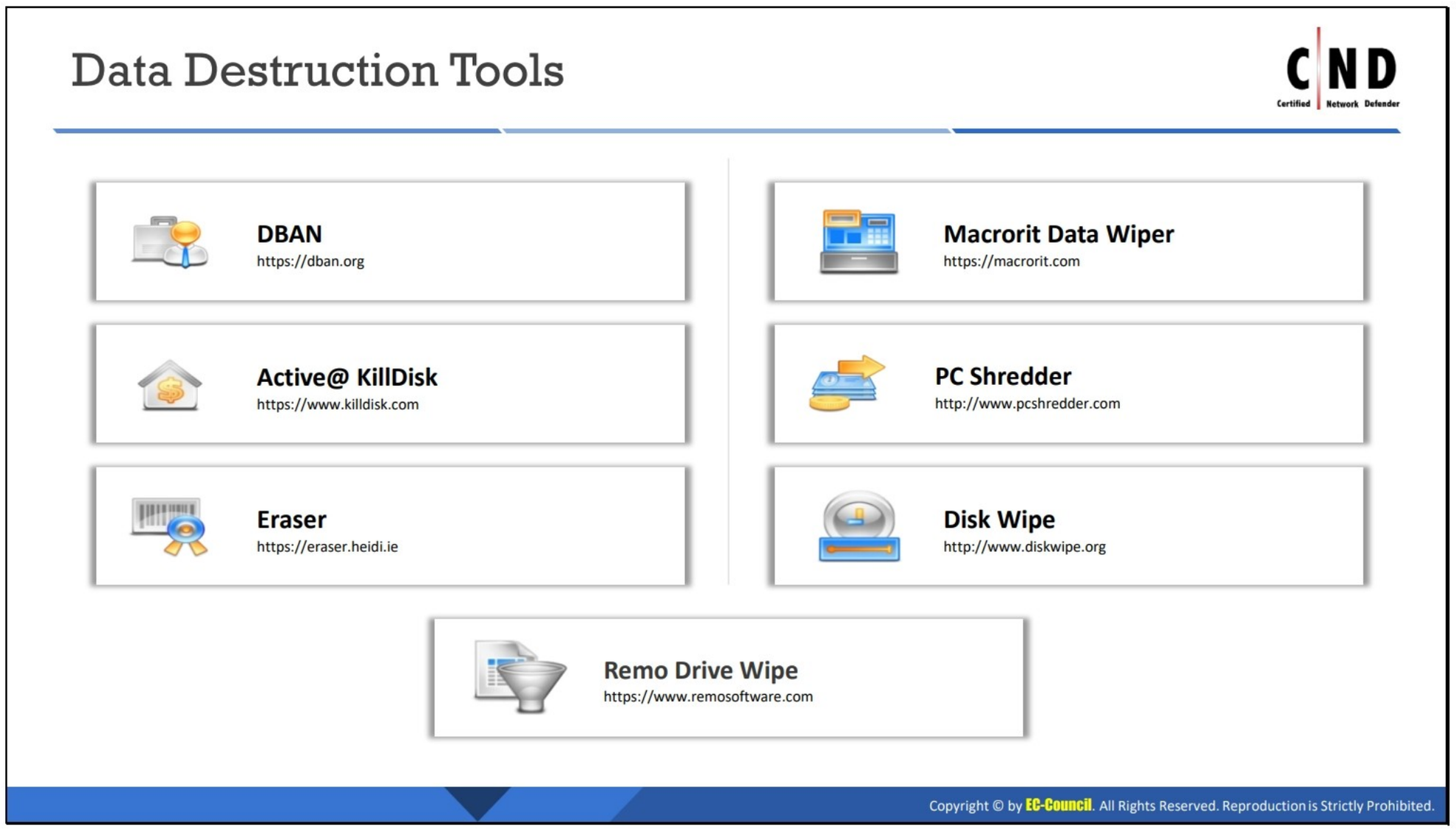


Figure 10.174: Formatting the partition and making the drive available in File Explorer

- Type exit command for terminating DiskPart, and press **Enter**.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Data Destruction Tools

The following are some data destruction tools.

DBAN

Source: https://dban.org

DBAN is a free, open-source data wiping software for personal use. It deletes information stored on HDDs in PC laptops, desktops, or servers, and also removes viruses/spyware from Microsoft Windows installations. But it may not completely sanitize data across the entire drive. It cannot detect or erase SSDs, and does not provide a certificate of data removal for auditing purposes or regulatory compliance.

Macrorit Data Wiper

Source: https://macrorit.com

Macrorit Data Wiper uses a storage-overwriting process to overwrite the sectors on a device. The storage-overwriting process complies with United States government requirements for deleting sensitive user data.

Active@ KillDisk

Source: www.killdisk.com

KillDisk Industrial Desktop is a disk sanitation hardware solution for the consumer market. It supports US DoD 5220-22M erasure and various international sanitizing standards.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Eraser

Source: https://eraser.heidi.ie

Eraser is a security tool for Windows which completely removes sensitive data from a hard drive by overwriting it several times with carefully selected patterns. Eraser is currently supported by Windows XP; Windows Server 2003, Windows Vista; Windows Server 2008; Windows 7, 8, and 10; and Windows Server 2012 and 2016.

Disk Wipe

Source: www.diskwipe.org

Disk Wipe is a free, portable Windows application for permanent volume data destruction. It can erase all disk data and prevent their recovery. It uses a powerful algorithm that fills the volume with useless rubbish binary data multiple times. Disk Wipe is released as a freeware under the EULA license.

PC Shredder

Source: www.pcshredder.com

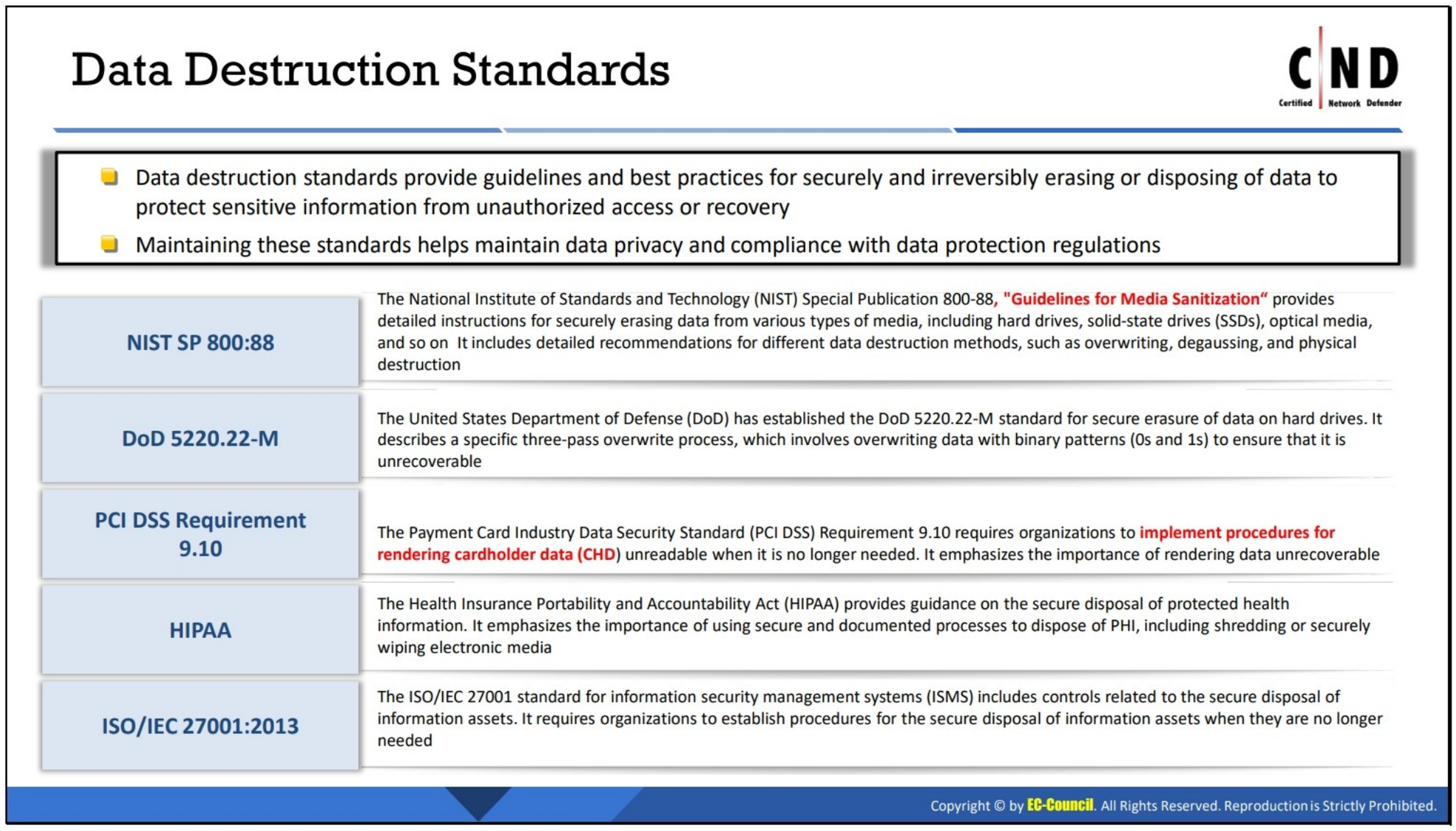
PC Shredder is a free data removal and file shredder software. It can permanently delete files and folders, and make them irrecoverable. It completely shreds the files, make it impossible for anyone to restore the deleted information. It works on Windows NT, Windows 2000, Windows XP, Windows 2003 Server, and Windows Vista. There are no minimum hardware requirements for PC Shredder to run properly.

Remo Drive Wipe

Source: www.remosoftware.com

Remo Drive Wipe is a drive wipe tool (for Windows), which completely removes sensitive data from a hard drive or logical drives by overwriting it several times with carefully selected data shredding patterns and various international disk sanitization standards. It has an intuitive design and a simple user interface, which helps the user safely and easily erase private data from a hard drive.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Data Destruction Standards

Data destruction standards outline regulated procedures for executing physical and logical methods of data destruction, such as shredding, burning, degradation, and data deletion. These standards offer guidelines and best practices for securely and permanently erasing or disposing of data to safeguard sensitive information from unauthorized access or retrieval. Adherence to these standards is crucial in upholding data privacy and complying with data protection regulations.

Data destruction standards are as follows:

- **NIST SP 800:88:** The National Institute of Standards and Technology (NIST) has a set of guidelines for media sanitization that was first published in 2006. It is one of the most popular and widely used sanitization guidelines in today's world. It outlines three ways to attain data destruction in the media. All three of these methods can effectively destroy data on magnetic, flash, and optical media, as well as span devices such as hard drives and SSDs. It provides detailed instructions for securely erasing data from various types of media, including hard drives, solid-state drives (SSDs), optical media, and more.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

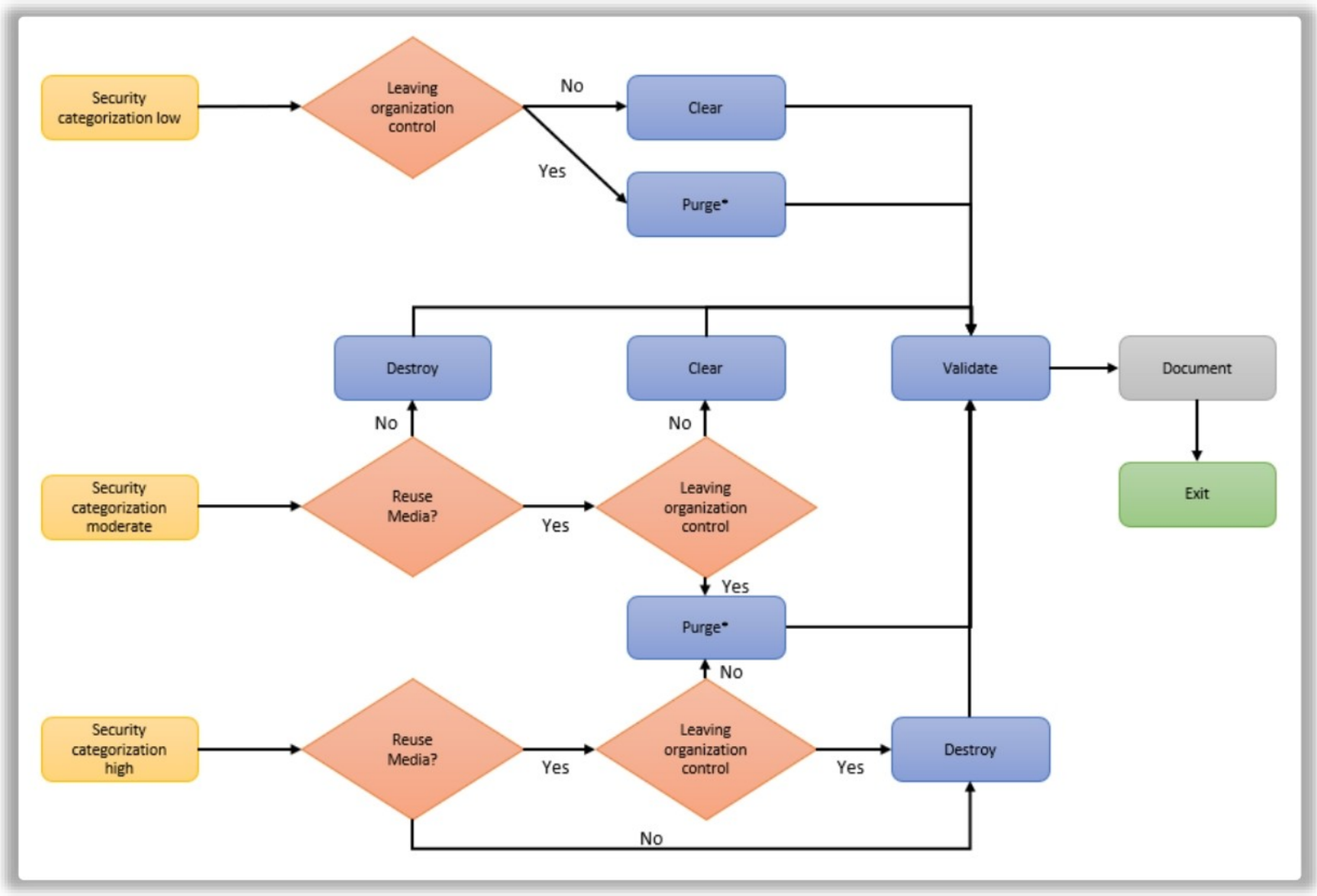


Figure 10.175: NIST SP 800:88 Decision Matrix

Media Sanitization Decision Matrix of NIST SP 800:88

The methods are Clear, Purge, and Destroy.

- **NIST Clear:** This method works by overwriting all the existing data in the user-addressable memory on the media using the standard read/write commands. The data is re-written with a new value so that it is permanently lost and protected from non-destructive data recovery methods. Factory reset of devices also comes under this method.
- **NIST Purge:** This method uses special commands and mechanisms to destroy data on SSDs. It uses vendor-specific commands to sanitize the drive by increasing the voltage on memory blocks and then lowering them to zero. In this manner, the data can be erased electronically.
- **NIST Destroy:** This method uses a bunch of different ways to break down the storage media, such as shredding, breaking it, melting it, burning it, etc. Basically, it physically destroys the storage media, and the data behind it is gone forever.

- **DoD 5220.22-M:** This standard outlines a procedure for the deletion of data on specified addressable memory locations using specified binary patterns, such as zeroes, ones, and random bit patterns. It involves a three-stage overwrite process, with verification after each stage. This ensures secure erasure of data on hard drives.
  - **Pass 1:** Overwrite all addressable memory locations using binary zeroes.
  - **Pass 2:** Overwrite all addresses with binary ones.
  - **Pass 3:** Overwrite with a random bit pattern; the final overwrite pass is verified.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Storage media	Clear	Sanitize
Magnetic tape	Degauss	Degauss or destroy
Magnetic disk	Degauss or overwrite	Degauss, destroy or overwrite
Optical disk	Overwrite	Destroy
DRAM	Overwrite or remove all power	Overwrite, remove all power, or destroy
EAPROM/EEPROM	Full chip eraser	Overwrite or destroy
Flash EPROM	Full chip erase	Overwrite then full chip erase or destroy
Programmable ROM (PROM)	Overwrite	Destroy
Nonvolatile RAM (NOVROM)	Overwrite or remove all power	Overwrite, remove all power, or destroy

Table 10.3: DoD 5220.22-M Clearing and Sanitization Matrix

- **PCI DSS Requirement 9.10:** The Payment Card Industry Data Security Standard (PCI DSS) Requirement 9.10 mandates organizations to establish procedures to make cardholder data (CHD) unreadable once it is no longer required, underscoring the necessity of making data irretrievable.

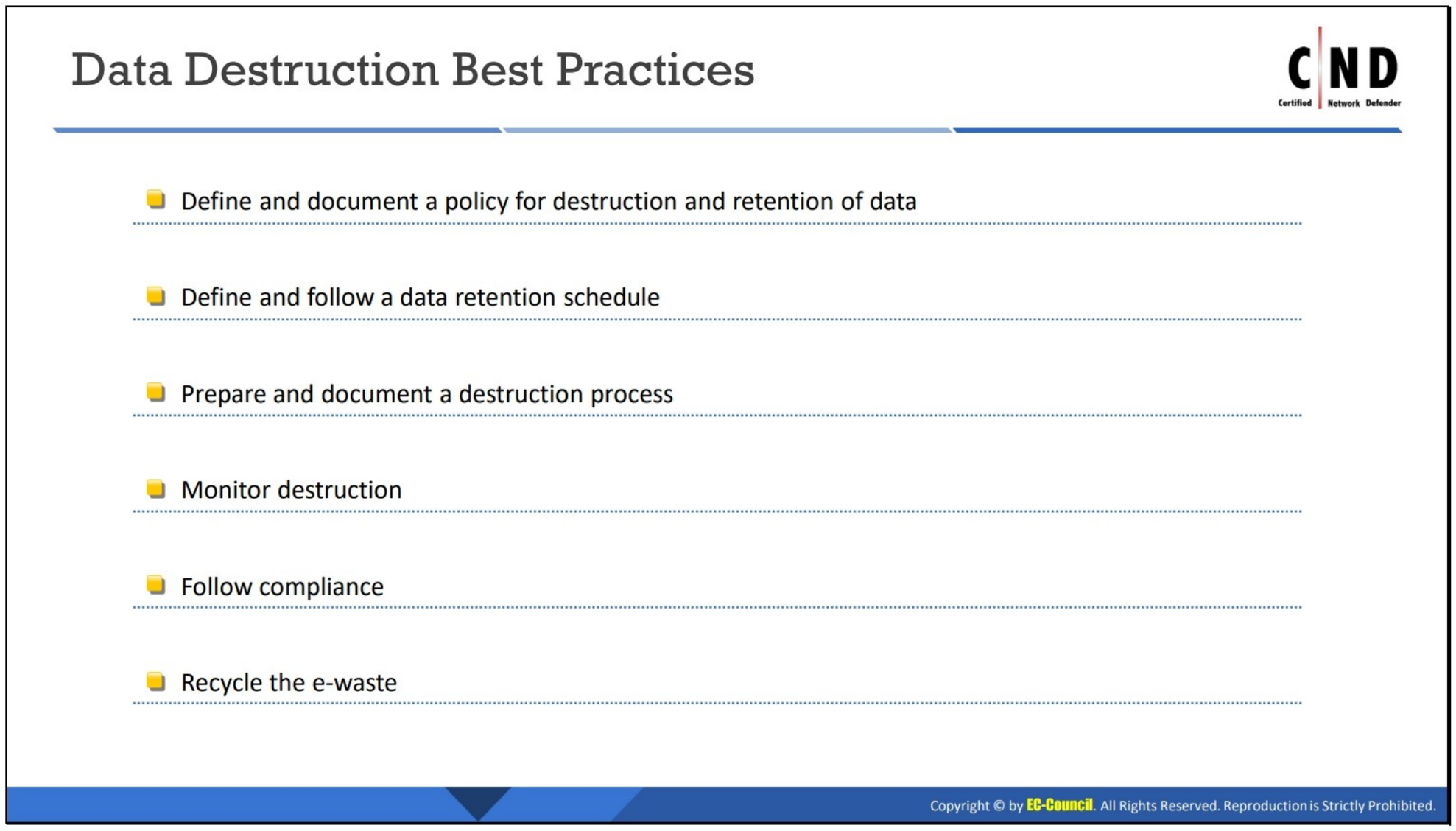
  This requirement also dictates that security compliance and operational procedures, which restrict physical access to cardholder data, be well-documented. Moreover, it is essential that these policies are actively implemented, not merely documented for audit's sake. The framework necessitates that all relevant parties are familiar with and adhere to these procedures. Non-compliance with PCI Requirement 9.10 exposes cardholder data to vulnerabilities.

- **HIPAA Guidance on Data Destruction**: The Health Insurance Portability and Accountability Act (HIPAA) provides guidance on the secure disposal of protected health information (PHI). While HIPAA does not prescribe specific methods, it emphasizes the importance of using secure and documented processes to dispose of PHI, including shredding or securely wiping electronic media. HIPPA ensures that policies and procedures are implemented to address the disposition of hardware or electronic media on which it is stored. Some methods for the disposal may include:

  - For hardware records, burning, pulping, shredding, or pulverizing the record.
  - For electronic media, purging (degaussing), clearing (overwriting media with non-sensitive data) or destroying the media (melting, incinerating, disintegration).

- **ISO/IEC 27001:2022**: The ISO/IEC 27001 standard for information security management systems (ISMS) includes controls related to the secure disposal of information assets. It requires organizations to establish procedures for the secure disposal of information assets when they are no longer needed. This standard enables organizations understand whether the asset includes any information and licensed software; if so, it must be permanently erased. The methods used should prevent unauthorized access or disclosure.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Data Destruction Best Practices

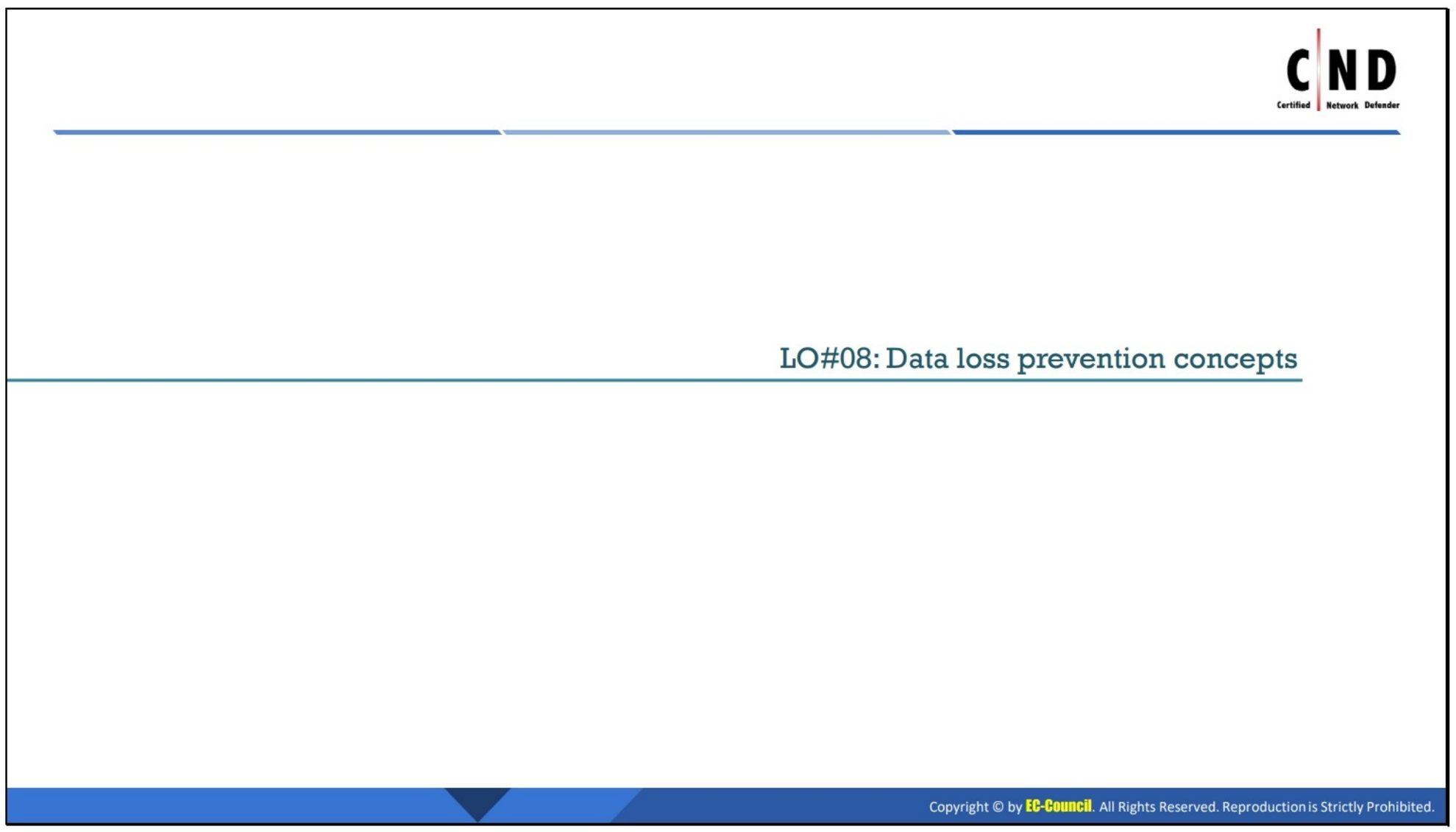
1. **Define and document a policy for destruction and retention of data:** The policy for retaining data will be based on the record retention schedule. Upon completion of the retention period, the data should be destroyed.
2. **Define and follow a data retention schedule**: A data retention schedule sets the guidelines on how long the data should remain accessible for future use or reference, and destructs the data when not in use.
3. **Prepare and document a destruction process:** Accessibility to the confidential information of an organization poses a serious threat; thus, the organization should safeguard its confidential information, recognize the security loopholes, and take measures to avoid them. Best practices in document destruction are divided into three key guidelines for securing customer, employee, and business information, as follows:
    - Shred all and shred regularly.
    - Shred before recycling.
    - Shred using a professional service.
4. **Monitor destruction**: Depending on the growth and evolution of the organization, the destruction needs will change. Hence, monitor the destruction process to meet the current and future needs.
5. **Follow compliance**: The company should be in compliance with the laws and regulations pertaining to classified equipment destruction. If there are policies pertaining to the destruction of classified equipment, then they should be complied with. Disposition of

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

classified equipment requires ethical and legal obligations; therefore, if a company does not dispose equipment properly, they may have to face a number of legal issues.

6. **Recycle the e-waste**: e-waste recycling prevents the reuse or recovery of sensitive information from corporate computers and devices. The proper recycling of e-waste keeps the environment safe.

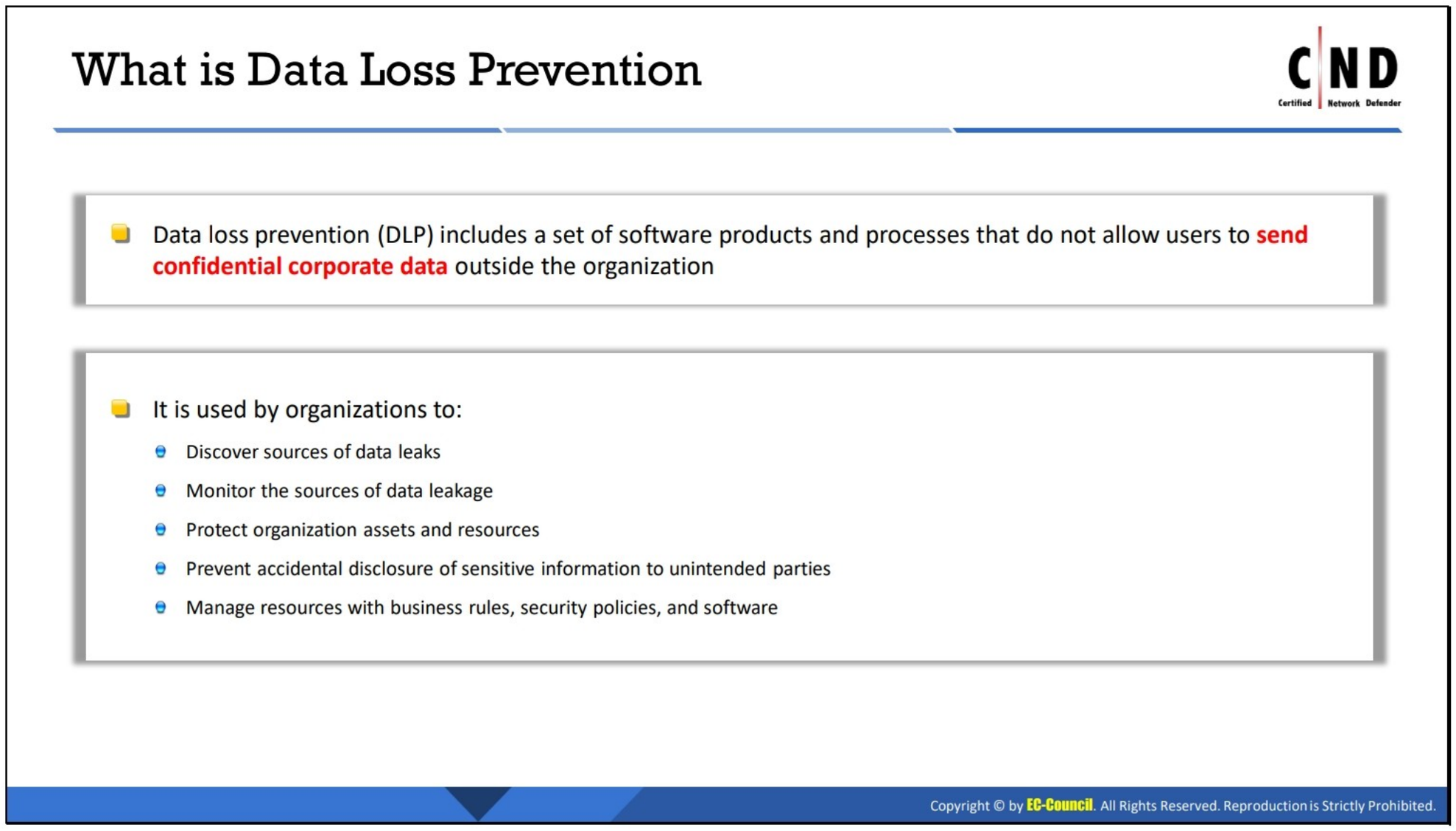
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



LO#08: Data Loss Prevention Concepts

The objective of this section is to explain the importance of data loss prevention (DLP) in data security.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



What is Data Loss Prevention

Data loss prevention (DLP) includes a set of software products and processes that do not allow users to send confidential corporate data outside the organization. These software products help network defenders in controlling what data end users can transfer. DLP rules block the transfer of any confidential information across external networks. They control any unauthorized access to company information, and prevent anyone from sending malicious programs to the organization.

DLP software are implemented according to the organizational rules set by the management. This prevents accidental/malicious data leaks and losses. If an employee tries to forward or even upload company data on cloud storage or on a blog, the access will be denied by the system.

A DLP policy is adopted by the management when internal threats to a company are detected. A DLP policy ensures that none of its employees send sensitive information outside the organization. New emerging DLP tools not only prevent the loss of data but also monitor and control irregular activities from occurring on the system.

Different DLP products are available to help network defenders determine what data users can transfer. DLP products are also known as data leak prevention, information loss prevention, or extrusion prevention products.

DLP is used by organizations to:

- discover sources of data leaks
- monitor the sources of data leakage
- protect organization assets and resources
- prevent accidental disclosure of sensitive information to unintended parties

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

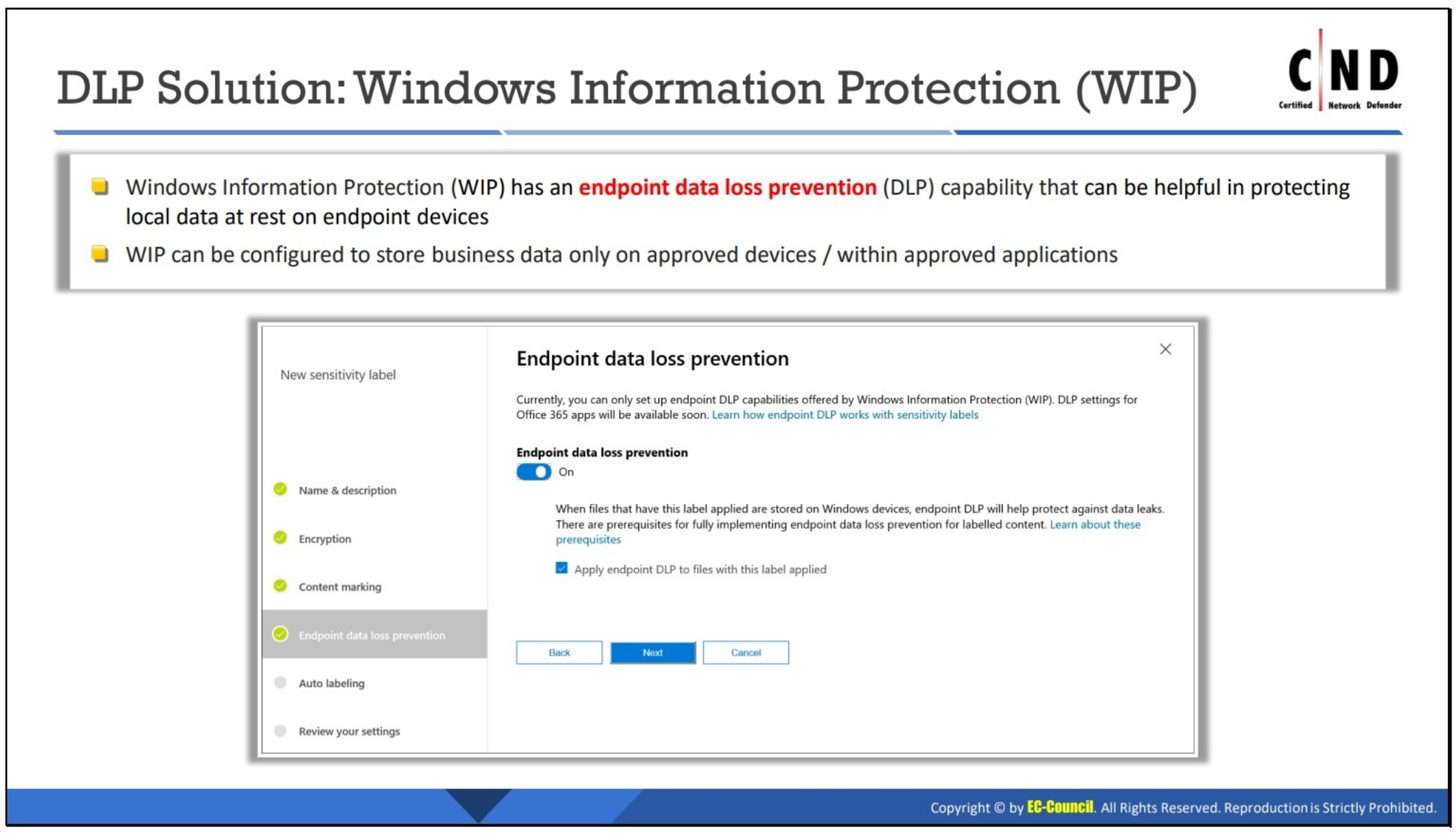
- manage resources with business rules, security policies, and software

Types of DLP Solutions

There are various types of DLP solutions that function differently with the same objective, that is, to prevent data leakage.

- **Endpoint DLP:** Endpoint DLP is a solution that monitors and protects PC-based systems such as tablets, laptops, etc. It is used for preventing data leakage through clipboards, removable devices, and sharing applications. The solution includes an agent that monitors specific user operations such as sending an email, copying a file to removable media devices, printing a file, etc. Endpoint DLP protects data in use.
- **Network DLP:** Network DLP is a solution that monitors, protects, and reports all data in transit. It is installed at the "perimeter" of an organization's network. It helps the network defender in scanning all data moving through the ports and protocols within the organization. It may analyze email traffic, social media interactions, SSL traffic, instant messaging, etc. The solution maintains reports containing information such what data is used, who is using the data, and where the data is sent. Thus, it helps in controlling the flow of data over the organization's network, and meets regulatory compliance. Data collected by a Network DLP is stored in a database for retrieval later.
- **Storage DLP:** Storage DLP is a solution that monitors and protects data at rest, that is, the data stored in an organization's data center infrastructure such as file servers, SharePoint, and databases. It identifies the location where sensitive information is stored, and helps users in determining whether it is stored securely. It allows authorized users to view and share sensitive files in the organization's network.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



DLP Solution: Windows Information Protection (WIP)

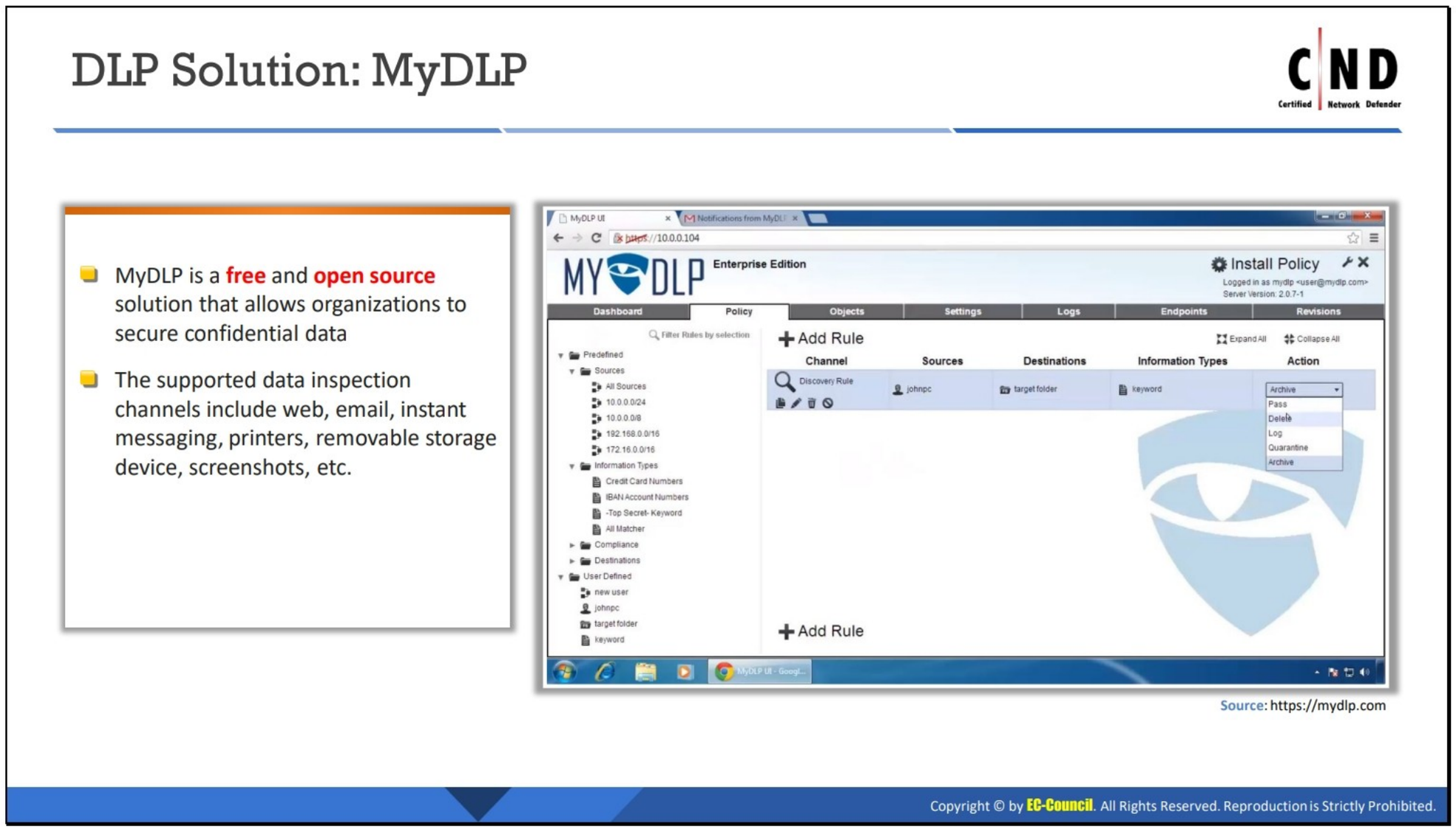
Windows Information Protection (WIP) has an endpoint DLP capability that can be helpful for protecting local data at rest on endpoint devices. WIP can be configured to store business data only on approved devices/within approved applications.

If the user creates a file on a Windows 11 device, the Windows Defender ATP evaluates its content for sensitive or customized information. In case of file matches, Windows Defender ATP applies DLP at its endpoints. For data discovery, Windows Defender ATP integrates with Azure Information Protection (AIP) and reports the detected sensitive data. Files with sensitive information and sensitivity labels are aggregated by AIP.

Advantages of WIP:

- As WIP separates corporate and personal data, there is no need for an employee to switch the applications or environments.
- It reinforces the data protection for existing line-of-business applications.
- WIP can remove the corporate data from Intune MDM enrolled devices.
- For configuration, deployment, and management, WIP integrates with Microsoft Intune, System Center Configuration Manager, or the current mobile device management.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



MyDLP

Source: www.mydlp.com

- MyDLP is a free and open-source solution that allows organizations to secure confidential data.
- The supported data inspection channels include web, email, instant messaging, printers, removable storage devices, screenshots, etc.
- MyDLP allows the user to monitor, inspect, and prevent all outgoing confidential data without any hassle. With its painless deployment and configuration, an easy-to-use policy interface, and great performance, IT administrators and security officers are able to effectively combat data leakage.

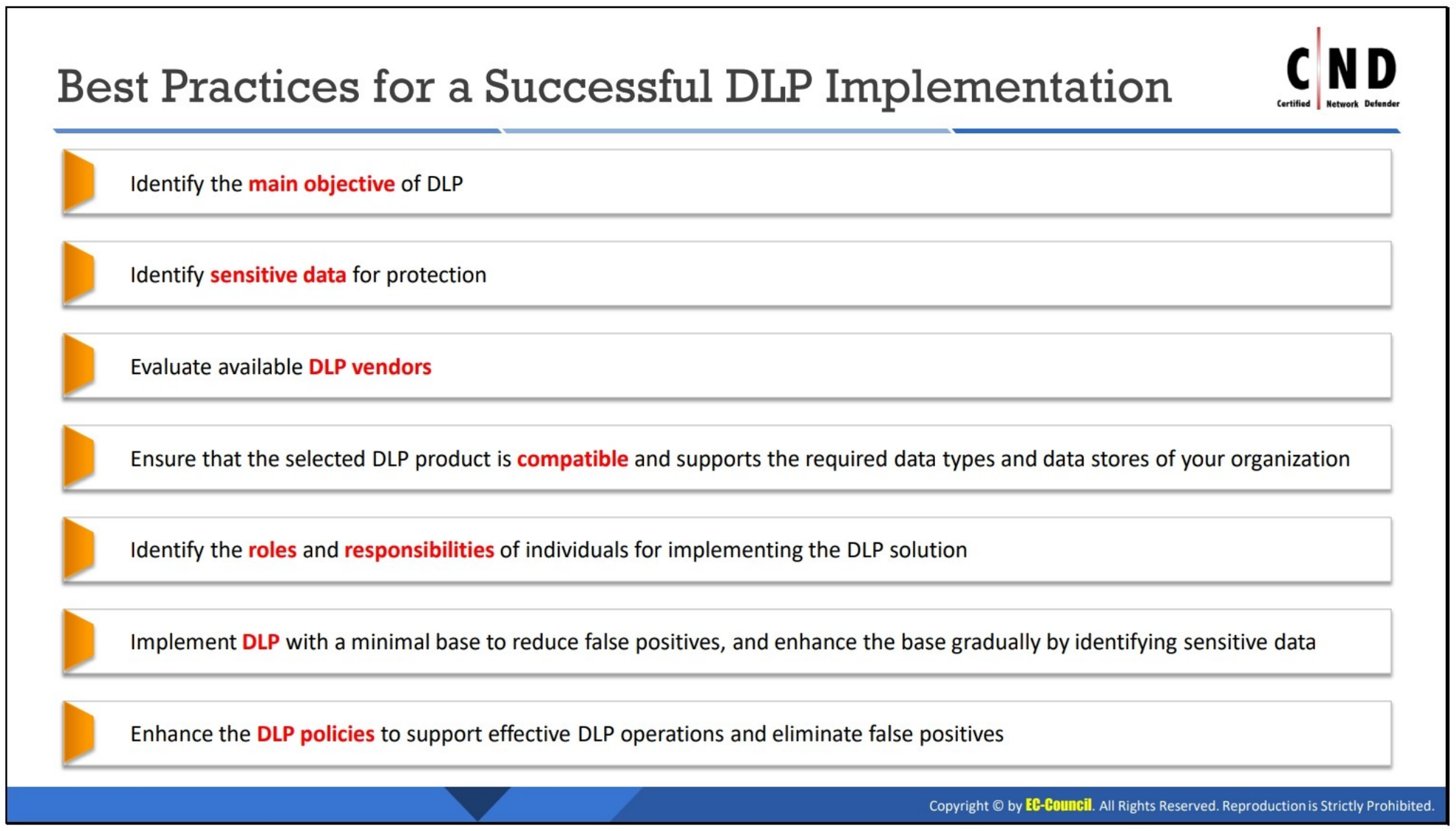
Centralized management: MyDLP provides central data management features. Using MyDLP, the user can:

- manage all MyDLP components with a user-friendly interface.
- define a single rule for all, or different rules for different sources (AD Group, TCP Network Rage, etc.) and different destinations (websites, email domains, etc.)
- administer DLP policy affecting thousands of agents and all network traffic with a few clicks.
- monitor all events in logs in the user dashboard and collect reports.
- make Google-like full-text searches in quarantined or archived suspicious files to see related event details and users.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- restrict different management roles for configuration and audit functions for users and groups with Microsoft Active Directory integration.
- allow executives and other nontechnical staff with a classifier management role to mark documents as confidential without alerting IT staff or breaking DLP policy easily

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Best Practices for a Successful DLP Implementation

DLP safeguards sensitive information in an organization. Implementation of DLP not only prevents the leakage of sensitive data, but also allows the network defender to monitor and control the data accessed and shared by an end user. Some best practices for a successful DLP implementation are as follows:

- Identify the main objective of DLP.
- Identify sensitive data for protection.
- Evaluate the available DLP vendors.
- Ensure that the selected DLP product is compatible and supports the required data types and data stores of the organization.
- Identify the roles and responsibilities of individuals for the implementation of DLP solution.
- Implement DLP with a minimal base to reduce false positives, and enhance the base gradually by identifying sensitive data.
- Enhance the DLP policies to support effective DLP operations and eliminate false positives.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



DLP Solution Vendors

Symantec Data Loss Prevention (DLP)

Source: www.broadcom.com

Symantec Data Loss Prevention (DLP) tracks and secures your confidential data, and ensures its safety, wherever it lives: in the cloud, on the premises, or on mobile devices. It helps you keep data safe on Windows and Mac endpoints by performing local scanning and real-time monitoring. It monitors confidential data that is being downloaded, copied, or transmitted to or from laptops and desktops through emails or cloud storage. It uses a single web-based console to define data loss policies, review and remediate incidents, and perform system administration across all of your endpoints, mobile devices, cloud-based services, and on-premise network and storage systems.

McAfee

Source: www.mcafee.com

McAfee Total Protection for DLP safeguards intellectual property and ensures compliance by protecting sensitive data wherever it lives: on-premises, in the cloud, or at the endpoints. McAfee Total Protection for DLP is delivered through physical or virtual low-maintenance appliances and the McAfee ePolicy Orchestrator platform for streamlined deployment, management, updates, and reports.

Quantum Data Loss Prevention (DLP)

Source: www.checkpoint.com

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Quantum Point DLP pre-emptively protect your business from an unintentional loss of valuable and sensitive information. It monitors data movement and empowers employees to work with confidence while complying with regulations and industry standards.

Trustwave

Source: www.trustwave.com

Trustwave DLP helps enterprises discover, monitor, and secure data at rest, in motion, and in use to prevent exfiltration and ensure regulatory compliance. It analyzes all web-based communication and attachments, including email, instant messenger, P2P file sharing, blogs, social media, FTP, and Telnet, for violations of an organization's governance, compliance, and acceptable-use policies. It automatically blocks HTTP, HTTPS, and FTP traffic that violate compliance policies. It can investigate data at rest to find and protect sensitive information residing in the stored data. Discovery of sensitive data allows security teams to focus their initiatives on specific users and systems, and then implement the appropriate measures to meet compliance requirements.

Digital Guardian

Source: https://digitalguardian.com

Digital Guardian DLP provides visibility and audit reporting of potentially unsecured data.

It uses a patent-pending Database Record Matching™ detection to accurately locate and identify sensitive data at rest on endpoints and servers across your networks and cloud storage.

Automatic and configurable scanning of local and network shares using discovery-specific inspection policies ensure sensitive content is discovered wherever it is located. Detailed audit logging and reports provide you with the information needed to demonstrate compliance, protect confidential information, and reduce data loss risk.

Forcepoint Enterprise DLP

Source: www.forcepoint.com

Forcepoint Enterprise DLP addresses human-centric risks with visibility and control everywhere the employees work and everywhere the data resides. Security teams apply user-risk scoring to focus on events that matter the most, and to accelerate their compliance with global data regulations.

DriveStrike

Source: https://drivestrike.com

DriveStrike is a data and device protection solution for devices that are lost, stolen, missing, or retired. It empowers you to locate, lock, and wipe devices that have escaped your control to prevent data compromise.

From personal accounts to Fortune 500 organizations in healthcare, legal, financial services, government, e-commerce, and entertainment, DriveStrike prevents data breaches to secure their confidentiality, compliance, and competitive advantage.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Retrospect

Source: www.retrospect.com

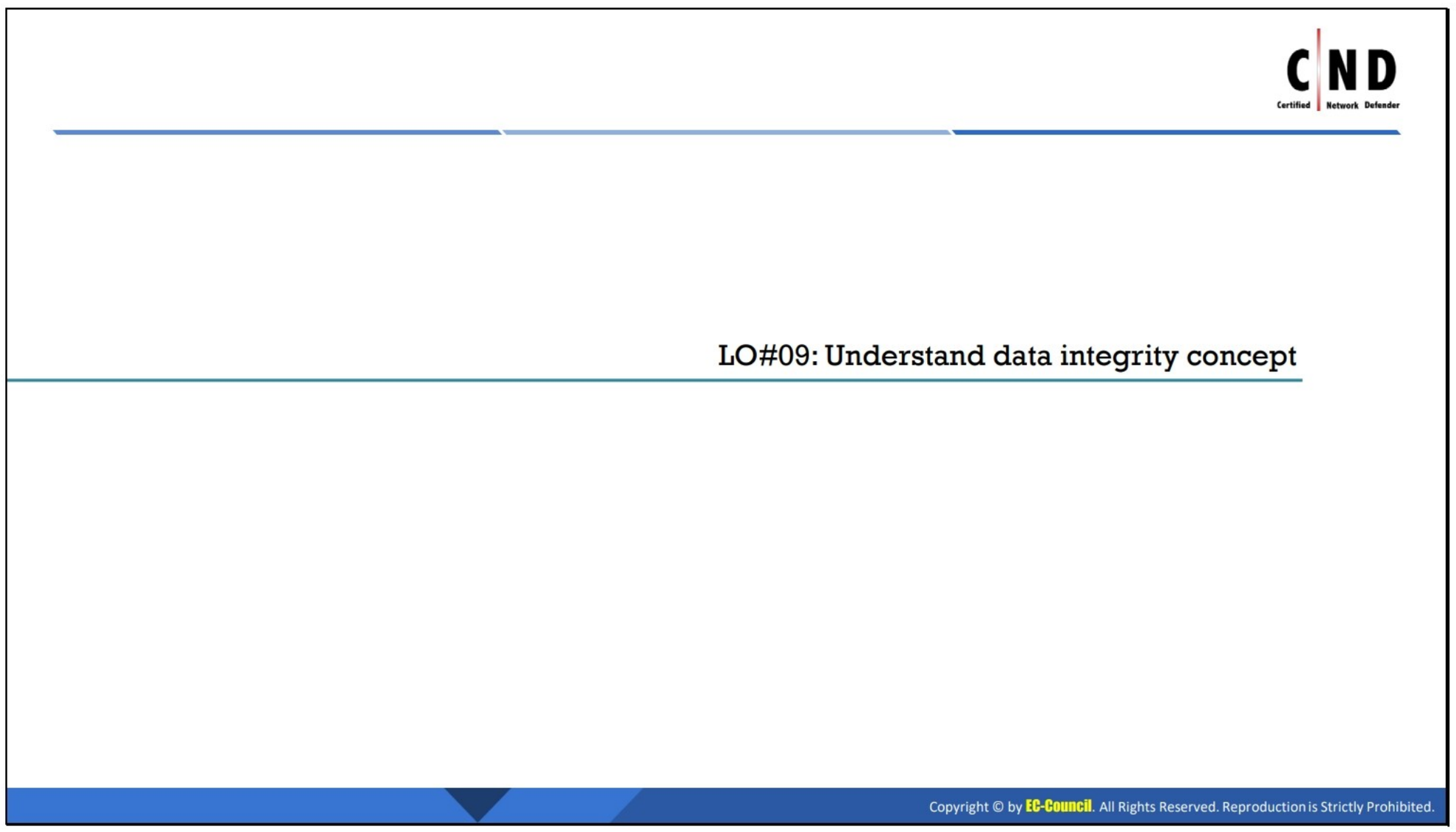
Retrospect Backup provides a complete protection for every major operating system, virtual environment, application, and email services with its built-in backup, archive, and duplicate features.

Safend

Source: www.safend.com

Safend Data Protection Suite (DPS) protects sensitive data before its transfer via comprehensive data encryption, port, device restriction and control, and content inspection. By addressing major compliance requirements such as EU GDPR, SOX, HIPAA, PCI, FISMA, or UK DPA, Safend has already been successfully integrated into critical industries, government agencies, municipalities, educational facilities, financial services, healthcare organizations, law enforcement agencies, and countless other organizations worldwide.

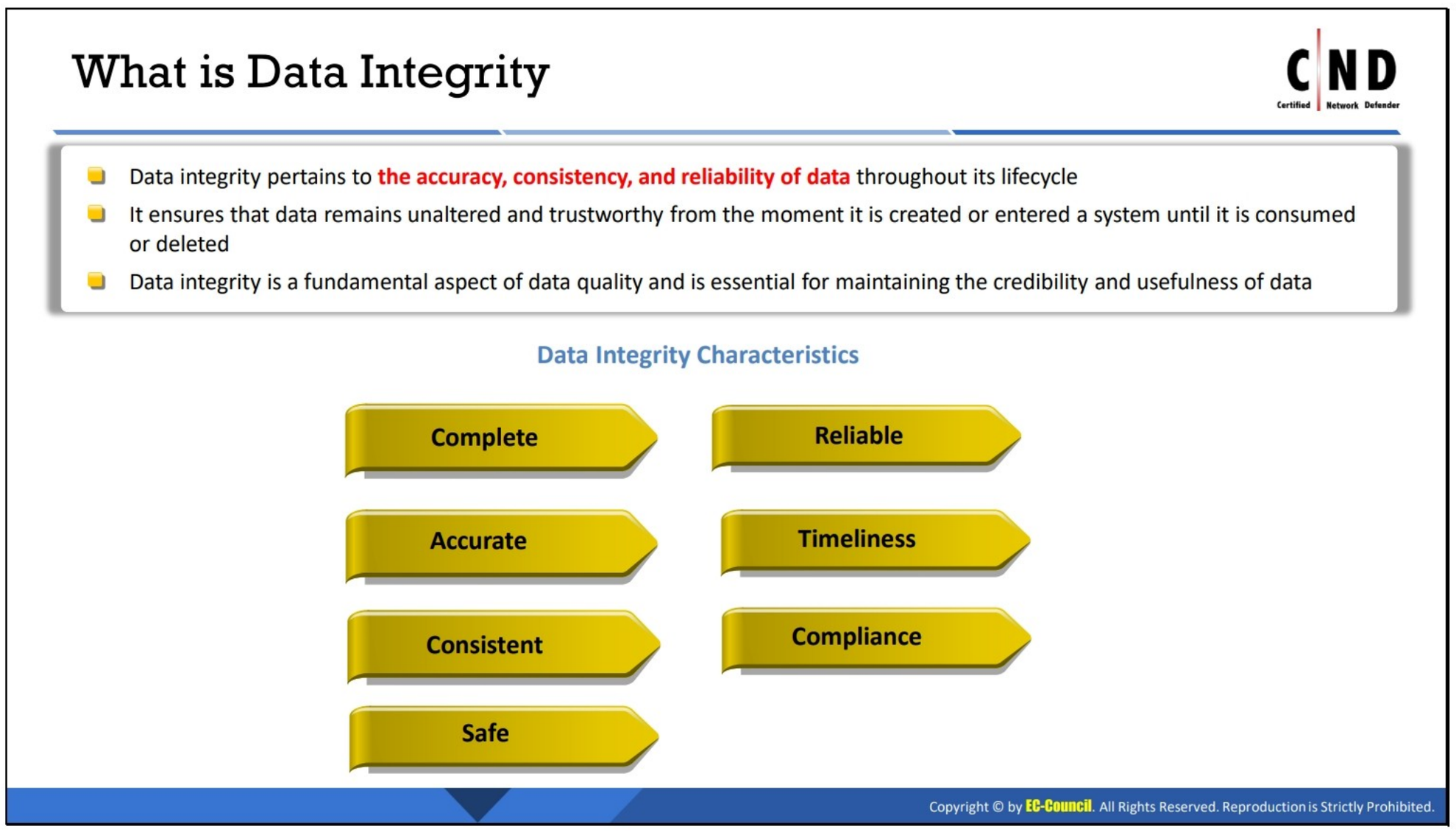
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



LO#09: Understand Data Integrity Concept

This section aims to explain the importance of data integrity and its types. It also explains how to maintain data integrity using various methods, techniques, and tools. It specifies various secure ways to preserve data integrity.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



What is Data Integrity

Data integrity guarantees that data remains intact and uncorrupted, free from unauthorized modifications. It ensures that data is consistently accurate, secure, and reliable throughout its lifecycle. Upholding data integrity aids organizations in complying with regulatory standards, including GDPR, prevents data corruption, and preserves the overall integrity of systems and processes. Data corruption can arise from hardware malfunctions, malicious activities, transfer errors, cyber-attacks, unauthorized data collection, or human mistakes. Organizations committed to upholding data integrity not only safeguard their data's integrity but also ensure its accuracy within their databases.

Characteristics of Data Integrity

Data integrity encompasses the following characteristics:

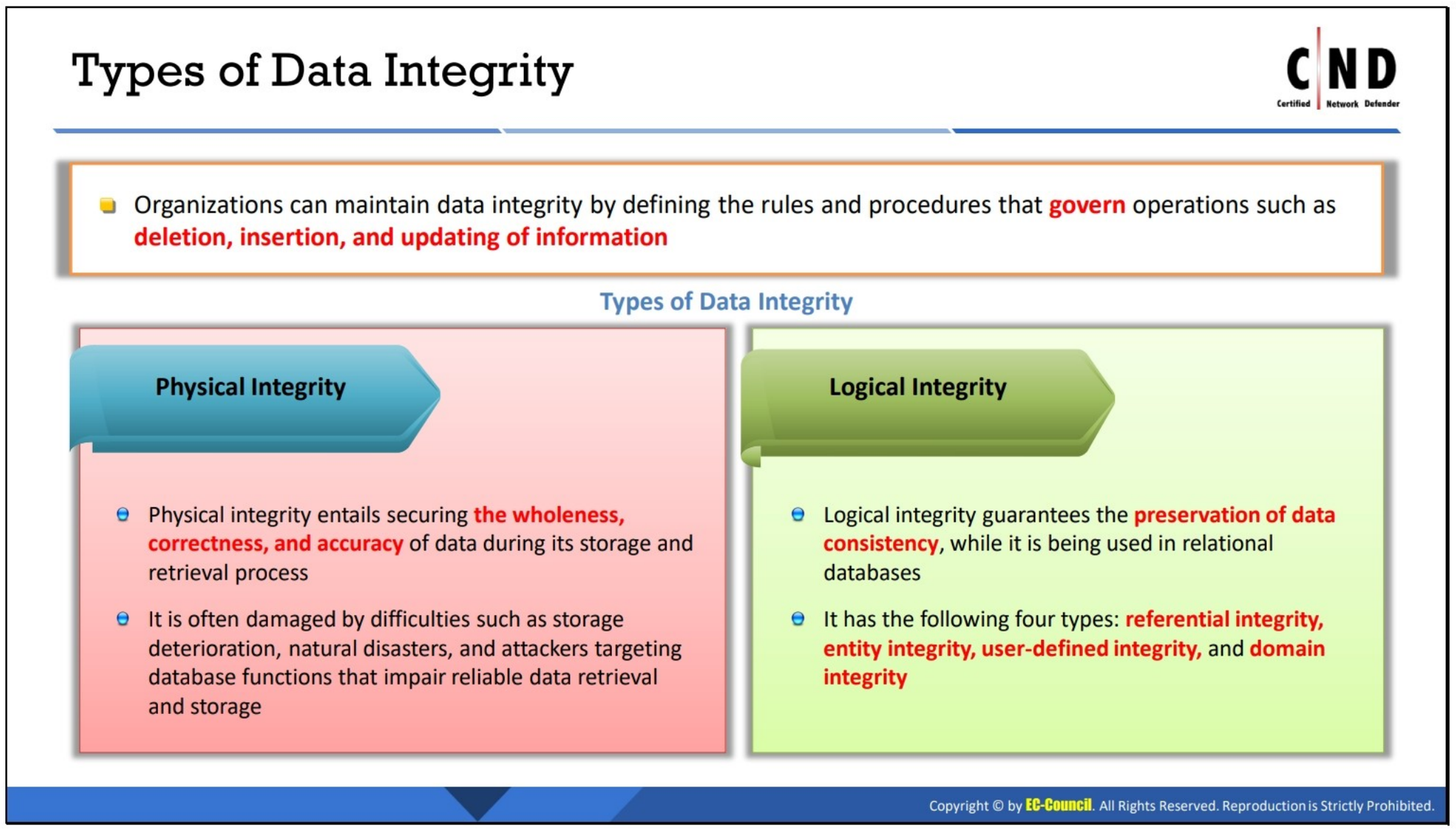
- **Complete**: It signifies the extent to which the available data is comprehensive and inclusive.
- **Accuracy**: It refers to the extent to which a data item accurately represents an object within the real-world context.
- **Safe:** It refers to the data that is maintained in a secure approach and it can only be accessed by authorized users.
- **Compliance**: It ensures that data meets the compliance standards like privacy rules and regulations.
- **Consistent:** It assesses the similarities between data items representing identical objects, based on particular information requirements. Data can be evaluated for consistency

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

either within the same database or when compared to other datasets with similar specifications.

- **Reliable:** The data is consistently accurate and unaltered, ensuring trustworthiness and consistency for users and systems.
- **Timeliness**: It refers to the extent to which data is up to date and accessible within an acceptable time window, duration, and timeline.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Types of Data Integrity

Maintaining data integrity involves two main categories, each comprising a set of methods and procedures. These categories are described below:

- **Physical integrity:** It refers to protecting the accuracy and correctness of data when it is stored or retrieved. It includes issues related to storage devices, memory components, and hardware. The threats that affect the physical integrity of data are as follows:
  - Natural disasters
  - Natural deterioration
  - Hardware failures
  - Radiation or extreme temperatures and pressures
  - Power outages and disturbances

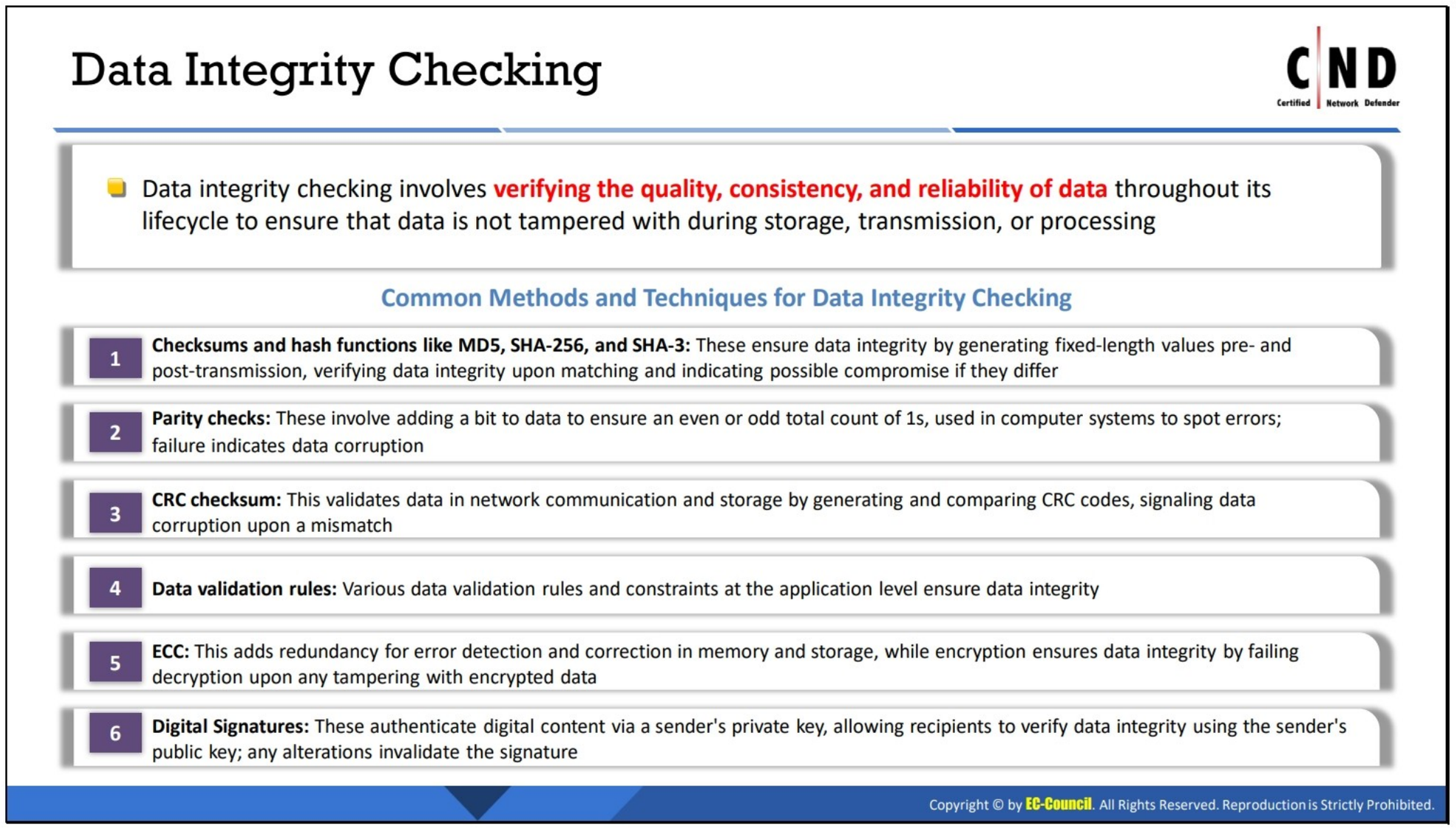
  To improve the physical integrity of data, use advanced error-correcting memory devices, battery-protected write cache, and implement redundant storage subsystems such as redundant array of independent disks (RAID).
- **Logical integrity**: It refers to ensuring that data remains intact even when it is used in different ways through relational databases. It has four types, as described below.
  - **Entity integrity:** It is a feature of a relational database, and it ensures that data is not duplicated and no important data entry is kept null or blank.
  - **Referential integrity:** It refers to a set of rules that define how data is stored and used. It makes sure that only authorized changes, deletions, and additions can

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

occur. By following these rules, it prevents duplication of data, elimination of irrelevant data, and ensures data accuracy.

- **Domain integrity:** It refers to the accuracy of data present in a domain. A domain is a collection of values that a column can accept. It reflects the type, amount, and value range of acceptable data values within a database. If the data is defined as numeric, only numeric values are accepted.
- **User-defined integrity:** It refers to the rules and constraints of data created by the user to meet the needs of an organization and those that are not specified in the entity, referential, or domain integrity.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Data Integrity Checking

Data integrity checking typically involves verifying the quality, consistency, and reliability of data throughout its lifecycle to ensure that data is not tampered with during storage, transmission, or processing.

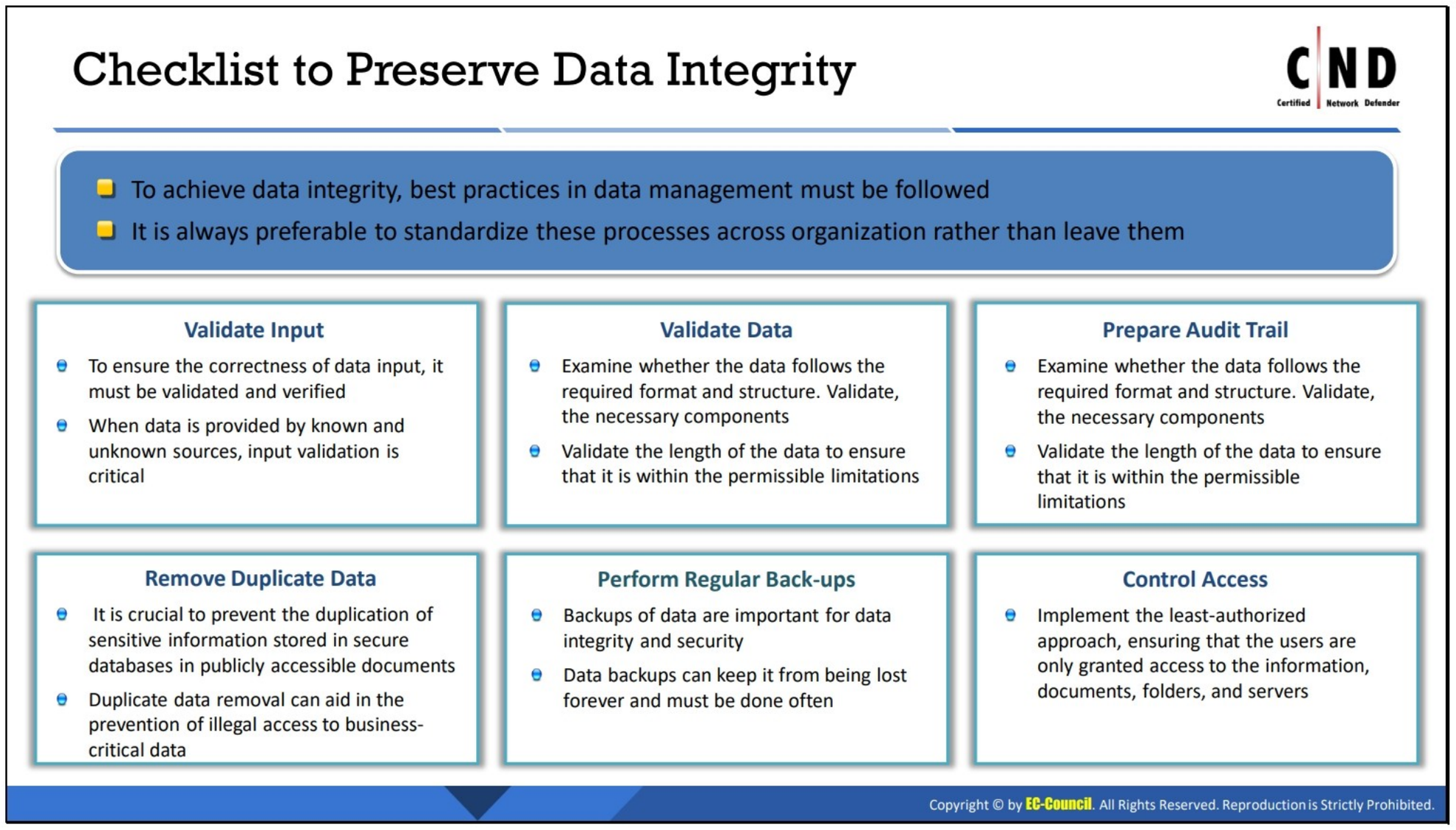
Common methods and techniques for data integrity checking:

- **Checksums and hash functions:** Checksums and cryptographic hash functions, such as MD5, SHA-256, and SHA-3, generate fixed-length values before and after data transmission or storage. When these checksums or hashes are compared, a match indicates that the data remains unaltered, whereas a discrepancy suggests potential data integrity issues.
- **Parity Checks:** This method adds an extra bit to data to ensure that the total number of 1s, including the parity bit, is either even (even parity) or odd (odd parity). Commonly utilized in computer memory and storage systems, it detects errors. If there's a mismatch in the expected parity, it signifies a data error. The sender tallies the number of 1s in the data frame and sets the parity bit accordingly: 0 for even counts of 1s and 1 for odd counts. Upon receipt, the receiver recounts the number of 1s. If the parity matches expectations, the data is accepted; otherwise, it's rejected.
- **Cyclic Redundancy Check (CRC) checksum:** This is utilized in network communication and storage systems to identify errors during data transmission. A CRC code is generated based on the original data and is compared to a received CRC code. When data enters the system, it is accompanied by a brief check value derived from the remainder of a polynomial division of its contents. Upon retrieval, the calculation is performed again, and the values are compared. Any discrepancy suggests data corruption.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Data validation rules**: Various data validation rules and constraints at the application level ensure data integrity. These rules specify the requirements and limits that data must meet to be considered valid and reliable. Potential errors, inconsistencies, or malicious inputs can be recognized and prevented by applying data validation rules, preserving the data's integrity. It can be done through range checks, format checks, input validation, and constraint validation.
- **Error-correcting codes (ECC):** ECC algorithms add redundancy to data so that errors can be detected and sometimes corrected during data retrieval. It is used in computer memory and storage devices to detect and correct errors.
- **Digital signatures**: Digital signatures are used to verify the authenticity and integrity of digital documents or messages. A sender signs the data with their private key, and the recipient can use the sender's public key to verify the signature. If the data has been altered, the signature will not match.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Checklist to Preserve Data Integrity

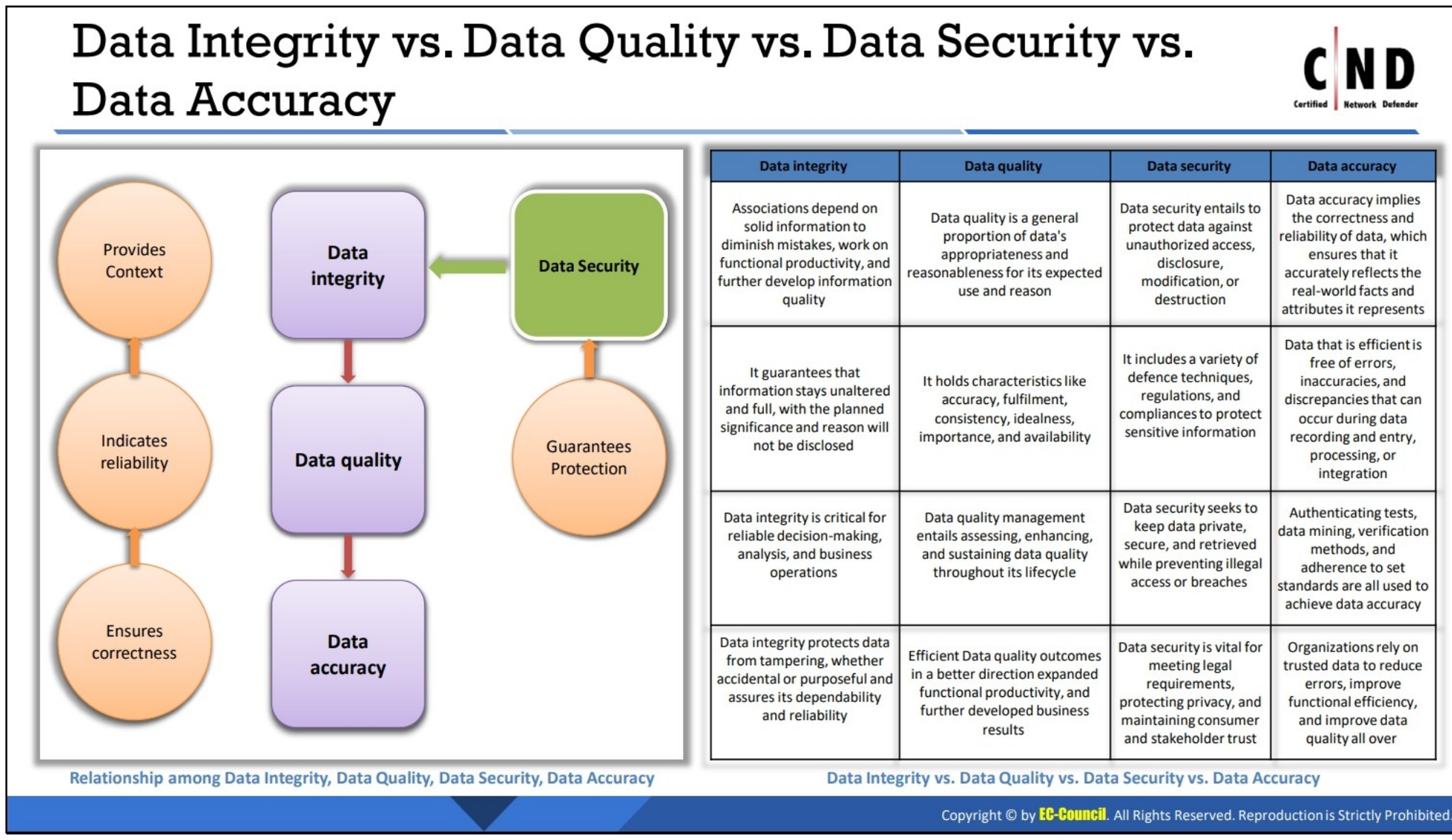
Follow to best practices in data management to achieve data integrity.

- **Validate input:** To ensure the correctness of data input, it must be verified and validated. Input validation is of utmost importance when dealing with data from both known and unknown sources.
- **Validate data:** Data Validate Input verification is the process of verifying the accuracy of data entry. It is necessary when data is inputted from both known and unknown sources such as end-users, malicious users, and apps**.**
- **Remove duplicate data:** The deletion of duplicate data can help to prevent unauthorized access to essential business information or personally identifiable data (PII). It is essential to ensure that confidential information stored in secure systems cannot be copied and pasted onto public documents, emails, folders, or tables.
- **Perform regular backups:** Backup is important for organizations affected by ransomware attacks, as it allows them to restore up-to-date versions of databases and documents. It is essential for data security and data integrity prevents data loss and should be performed as often as possible.
- **Control access:** It is important to implement appropriate access controls to ensure the integrity of data. This is achieved through the implementation of a least-authorized approach to access, which ensures that users are only granted access to the information, documents, folders, and servers necessary for them to carry out their duties effectively and eliminates the possibility of hackers posing as users and restricts unauthorized access to the data.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

- **Prepare audit trail:** An audit trail enables organizations to monitor the occurrence of a breach, identify the circumstances surrounding it, and ultimately locate the perpetrator of the attack. It is essential for organizations to be able to identify the source of a breach in a timely manner.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Data Integrity vs. Data Quality vs. Data Security vs. Data Accuracy

Data integrity is often confused with data accuracy, data security, and data quality. The differences among them are as follows.

Data integrity	Data quality	Data security	Data accuracy
Organizations rely on robust data to reduce errors, enhance operational efficiency, and improve data quality.	Data quality is a measure of the data's suitability reliability intended purpose and use.	Data security involves protecting data against unauthorized access, disclosure, modification, or destruction.	Data accuracy implies the correctness and reliability of data, ensuring that it accurately reflects the real-world facts and attributes it represents.
It ensures that data remains intact and complete, preserving its intended meaning and purpose without unauthorized disclosure.	It exhibits characteristics such as accuracy, fulfilment, consistency, idealness, importance, and availability.	It involves a variety of defence techniques, regulations, and compliances to protect sensitive information.	Efficient data is free of errors, inaccuracies, and discrepancies that can occur during data recording and entry, processing, or integration.
Data integrity is critical for reliable decision-making, analysis, and business operations.	Data quality management entails the assessment, enhancement, and sustenance of data quality throughout its lifecycle.	Data security seeks to keep data private, secure, and retrieved while preventing illegal access or breaches.	Authentication tests, data mining, verification, and adherence to set standards are methods used to ensure data accuracy.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Data integrity safeguards data from tampering, whether unintentional or deliberate, ensuring its consistency and trustworthiness.	Good data quality leads to better decision-making, enhanced operational efficiency, and improved business outcomes.	Data security is vital for meeting legal requirements, protecting privacy, and maintaining consumer and stakeholder trust.	Organizations depend on trusted data to minimize errors, enhance operational efficiency, and elevate overall data quality.

Table 10. : Data Integrity vs. Data Quality vs. Data Security vs. Data Accuracy

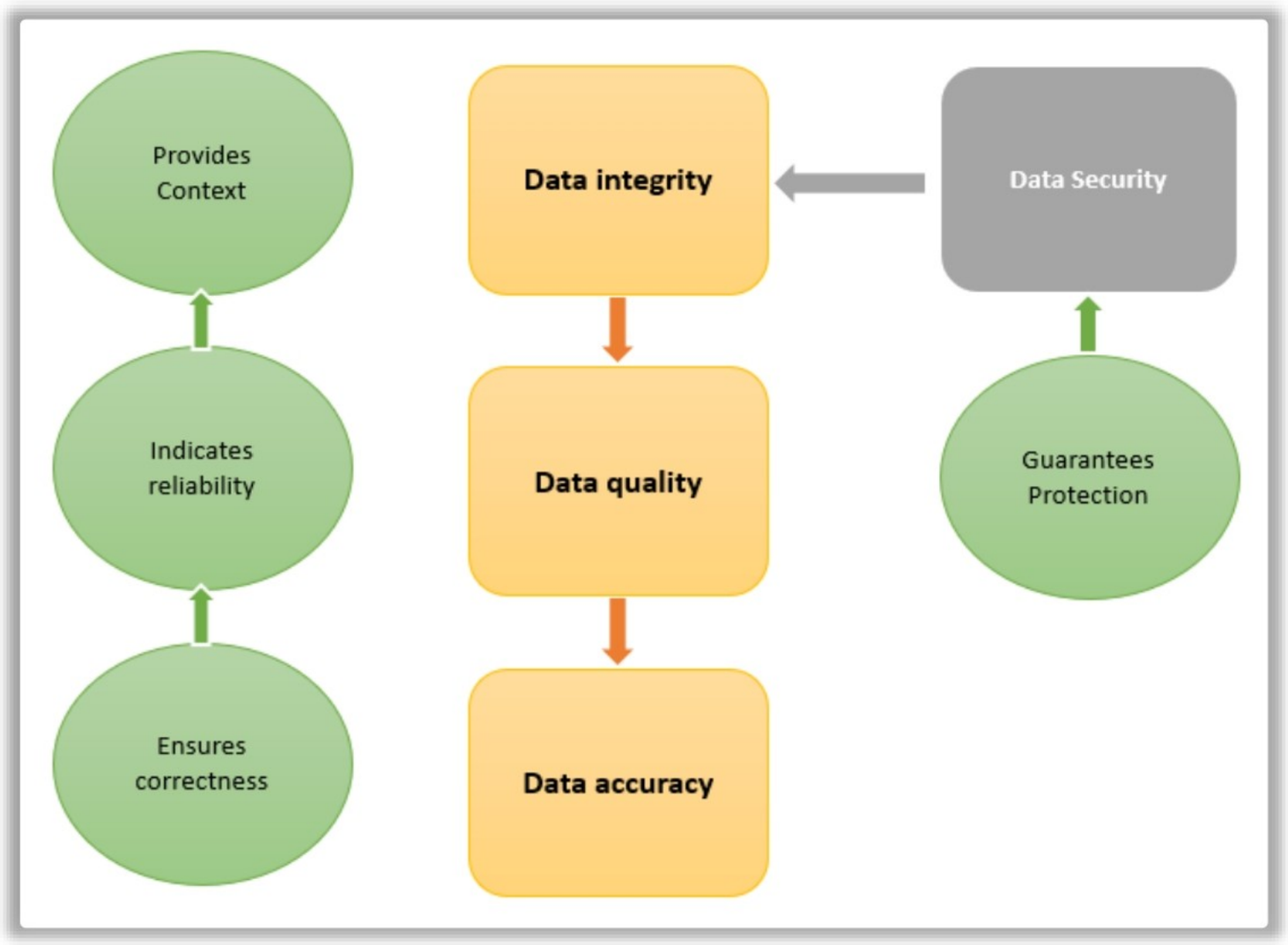


Figure 10.176: Relation among Data Integrity, Data Quality, Data Accuracy, Data Security

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Role of Data Integrity in Terms of GDPR Compliance

- Many key principles and requirements of GDPR are inter-related with data integrity. To comply with GDPR, organizations must maintain records of their data processing activities; **data integrity** is essential in ensuring the **accuracy and completeness** of the records

GDPR REQUIREMENT	ROLE OF DATA INTEGRITY
GDPR requires that personal data be accurate and up to date	Data integrity help maintain the accuracy of personal data by preventing errors, omissions, or unauthorized alterations
Personal data must be collected for specific, explicit, and legitimate purposes and not processed in a manner that is incompatible with those purposes	Data integrity helps ensure that data remains consistent with its intended purpose and is not altered or misused for other purposes
GDPR mandates that data protection should be integrated into systems and processes from the outset	Implementing data integrity measures to prevent data corruption, unauthorized changes, or data breaches
Organizations are required to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk	Data integrity measures, such as encryption, access controls, and auditing, are vital for protecting personal data from unauthorized access and alterations
In the event of a data breach that could result in a risk to individuals' rights and freedoms, organizations must notify the supervisory authority and affected data subjects without undue delay	Data integrity helps prevent and detect breaches, ensuring that data is not compromised
Data subjects have various rights under GDPR, including the right to access, rectify, and erase their personal data	Data integrity ensures that organizations can accurately respond to data subject requests and make necessary corrections if data is inaccurate
When obtaining consent for data processing, organizations must provide clear and accurate information about the processing activities	Data integrity ensures that consent records accurately reflect the data subjects' choices and preferences
GDPR restricts the transfer of personal data outside the European Economic Area (EEA) to countries that do not provide an adequate level of data protection	Data integrity practices help ensure that data remains secure and unaltered during transfers

Role of Data Integrity in Terms of GDPR Compliance

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Role of Data Integrity in Terms of GDPR Compliance

Many of the fundamental principles and requirements of the GDPR revolve around data integrity. For GDPR compliance, organizations are mandated to keep records of their data processing activities. Ensuring data integrity is pivotal to guaranteeing the accuracy and completeness of these records. A lapse in data integrity can subject enterprises to significant penalties. By upholding data integrity, organizations can ensure data safety, regardless of who accesses it.

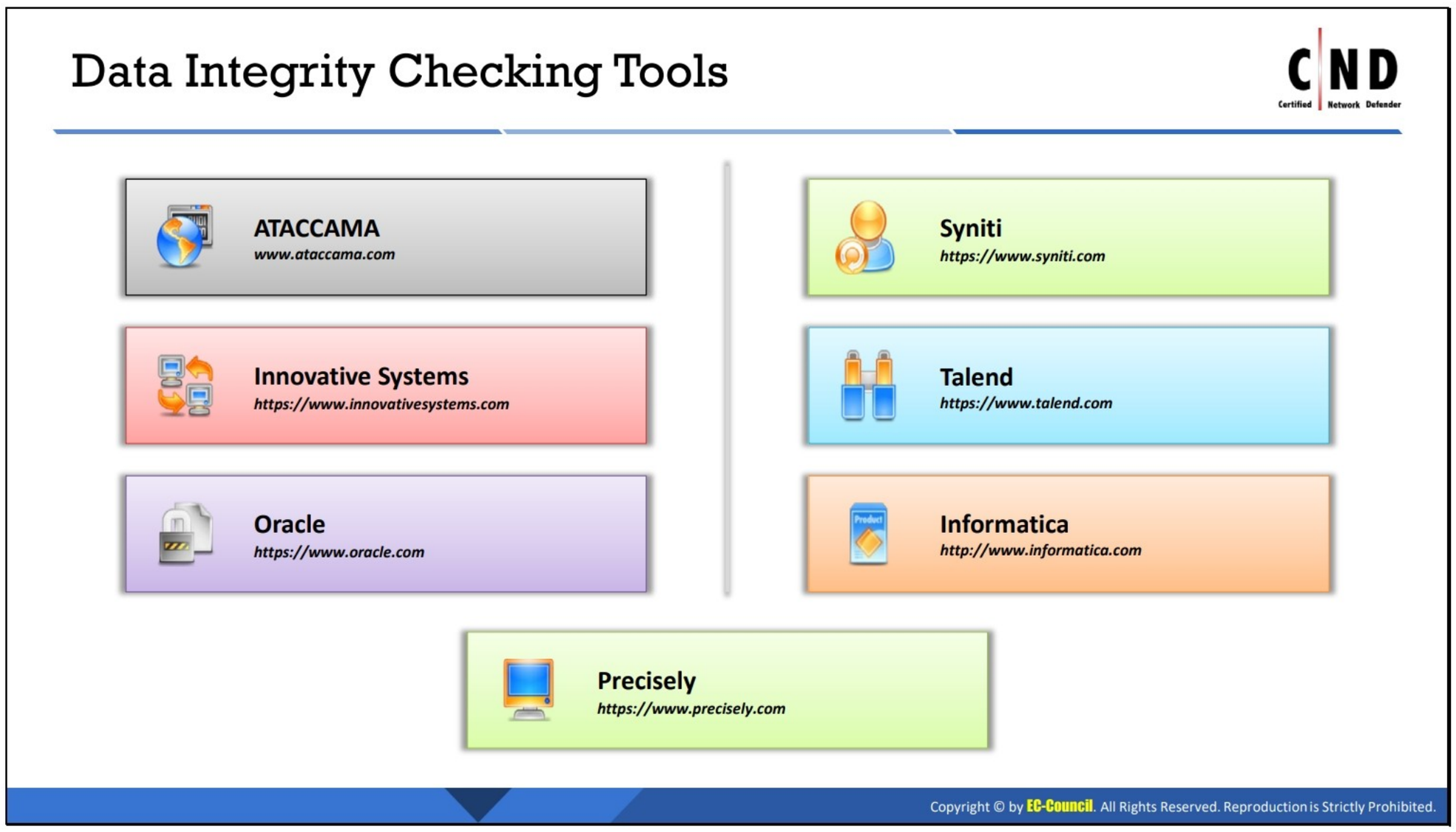
GDPR requirement	Role of data integrity
GDPR mandates the accuracy and currency of personal data.	Data integrity ensures the accuracy of personal data by mitigating errors, omissions, or unauthorized changes.
Personal data should be collected for clear, explicit, and valid purposes and must not be processed contrary to these intentions.	Data integrity guarantees that data aligns with its designated purpose and isn't misused or altered.
Data protection must be a foundational aspect of systems and processes.	Data integrity strategies safeguard against data corruption, unauthorized amendments, and breaches.
Organizations must adopt fitting technical and organizational methods to provide security commensurate with the risk.	Essential data integrity tools like encryption, access limits, and audits protect personal data from unsanctioned access and changes.
If a data breach poses a risk to individual rights, immediate notification to the supervisory authority and affected individuals is mandatory.	Data integrity facilitates the early identification and thwarting of breaches, ensuring data remains secure.
Under GDPR, data subjects are granted rights, including accessing, amending, and deleting their data.	Data integrity ensures prompt and accurate organizational responses to data subject queries, including making any needed corrections.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

When seeking data processing consent, clear and precise information about the processing must be provided by organizations.	Data integrity ensures that consent logs are an accurate reflection of data subjects' decisions.
Transferring personal data outside the EEA to nations lacking adequate data protection is restricted by GDPR.	Data integrity ensures data's security and consistency during such transfers.

Table 10.1: Role of Data Integrity in terms of GDPR

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Data Integrity Checking Tools

The various data integrity checking tools are as follows:

- **ATACCAMA**

  Source: www.ataccama.com

  Ataccama offers enterprise data management solutions. Their single AI-powered platform consolidates data governance, data quality, and master data management tools, optimized for both hybrid and cloud environments.

- **Innovative Systems**

  Source: https://www.innovativesystems.com

  Informatica, is an ETL-based data integration solution provider. Informatica offers data integration solutions and services for a wide range of businesses, industries. And governmental entities, including telecom, healthcare, financial, and insurance.

- **Syniti**

  Source: https://www.syniti.com

  SAP MDG (Master Data Governance) helps organizations consolidate and manage their master data. It also provides other data management features, such as hierarchical processing, bulk processing, integration, data quality assessment, data quality management, and process analytics.

- **Oracle**

  Source: https://www.oracle.com

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

Oracle Cloud Infrastructure (OCI) Data Catalog is a metadata management service designed to facilitate the discovery of data-by-data professionals and facilitate data governance. It is specifically designed to integrate seamlessly with the Oracle environment, offering a comprehensive asset inventory, a business dictionary, and a standard megastore format for data lakes.

- **Talend**

  Source: https://www.talend.com

  Talend is an open-source data integration platform. It provides various software and services that assist users in integrating their data, managing enterprise applications, ensuring data quality, storing data, store it in the cloud, and handling Big Data.

- **Precisely**

  Source: https://www.precisely.com

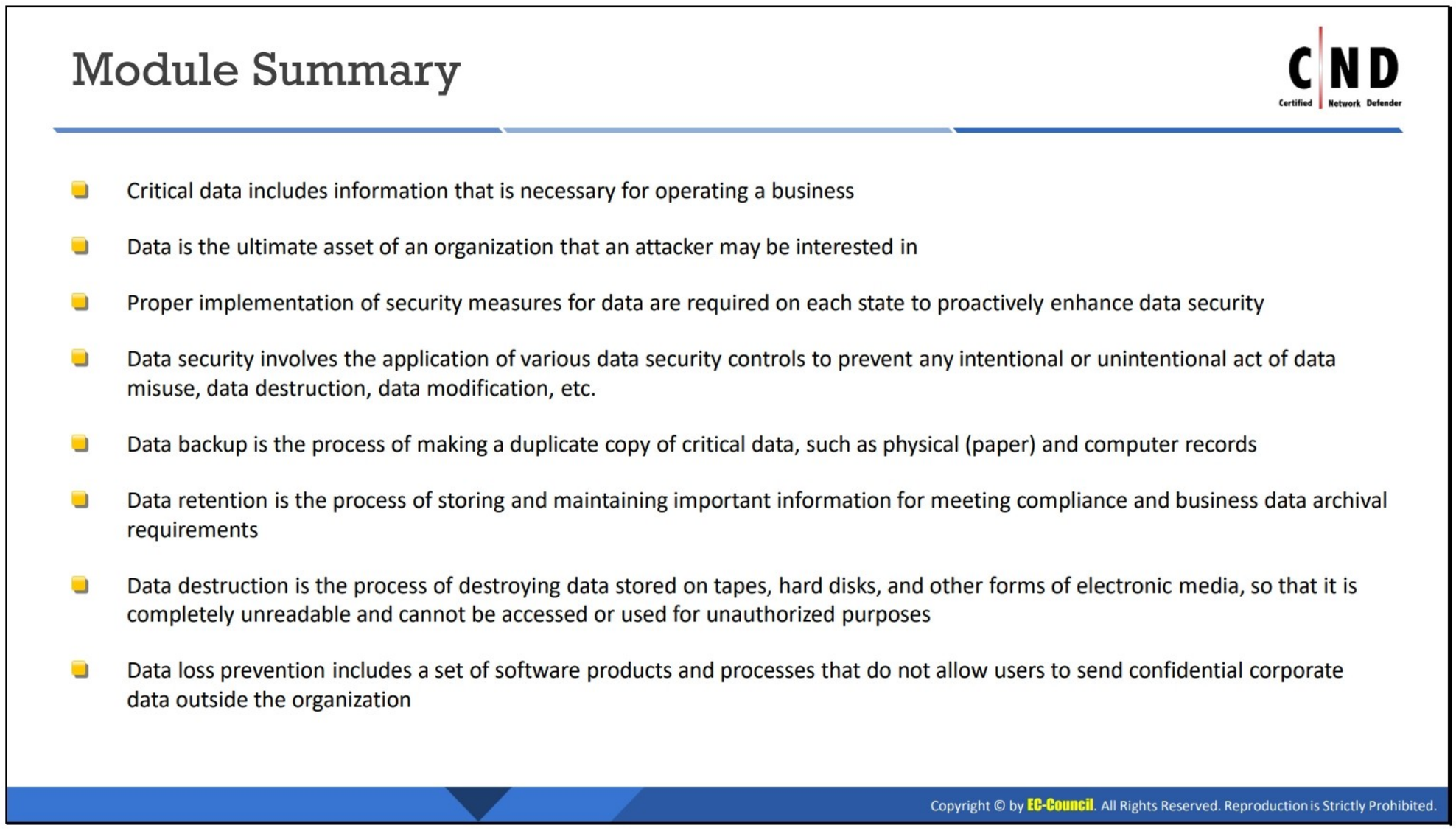
  Trillium Quality provides a comprehensive, robust data quality solution to meet user's ever-evolving business requirements, data sources, and enterprise environments – including the cloud.

- **Informatica**

  Source: http://www.informatica.com

  Informatica is an ETL-based data integration solution provider. Informatica offers data integration solutions and services for a wide range of businesses, industries, and governmental entities, including telecom, healthcare, financial, and insurance.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.



Module Summary

This module discussed the implementation of various data security techniques: data access controls, encryption, data masking, data backup and retention, data destruction, and DLP.

The key points highlighted in this module are:

- Critical data includes information that is necessary for operating a business.
- Data is the ultimate asset of an organization that an attacker may be interested in.
- Proper implementation of security measures for data are required on each state to proactively enhance data security.
- Data security involves the application of various data security controls to prevent any intentional or unintentional act of data misuse, data destruction, data modification, etc.
- Data backup is the process of making a duplicate copy of critical data, such as physical (paper) and computer records.
- Data retention is the process of storing and maintaining important information for meeting compliance and business data archival requirements
- Data destruction is the process of destroying data stored on tapes, hard disks, and other forms of electronic media, so that it is completely unreadable and cannot be accessed or used for unauthorized purposes
- DLP includes a set of software products and processes that do not allow users to send confidential corporate data outside the organization.

Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

This page is intentionally left blank.