EC-Council

Building A Culture Of Security

C|ND

Certified Network Defender

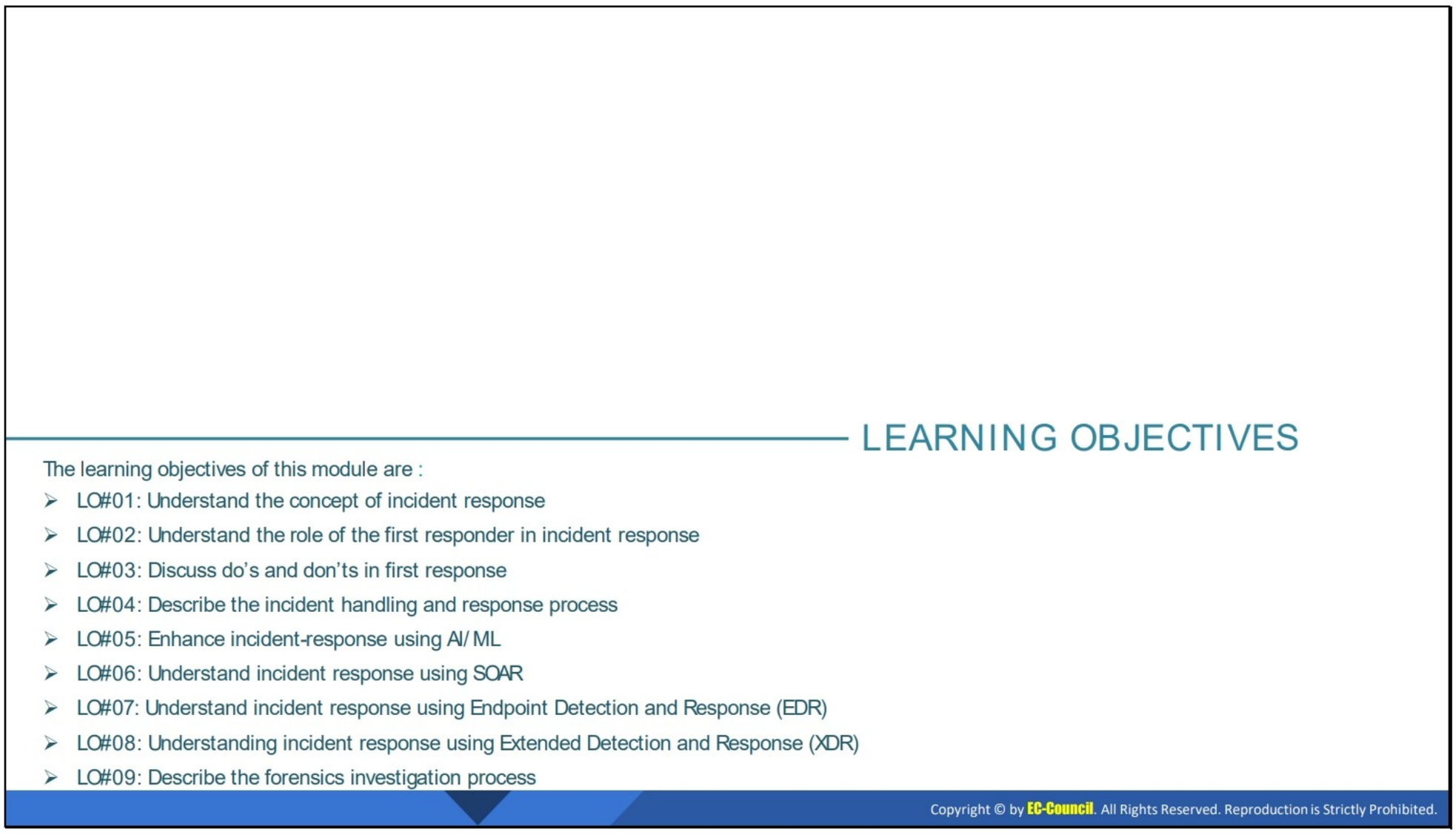
Certified Network Defender v3

MODULE 16

INCIDENT RESPONSE AND FORENSIC INVESTIGATION

EC-Council Official Curricula

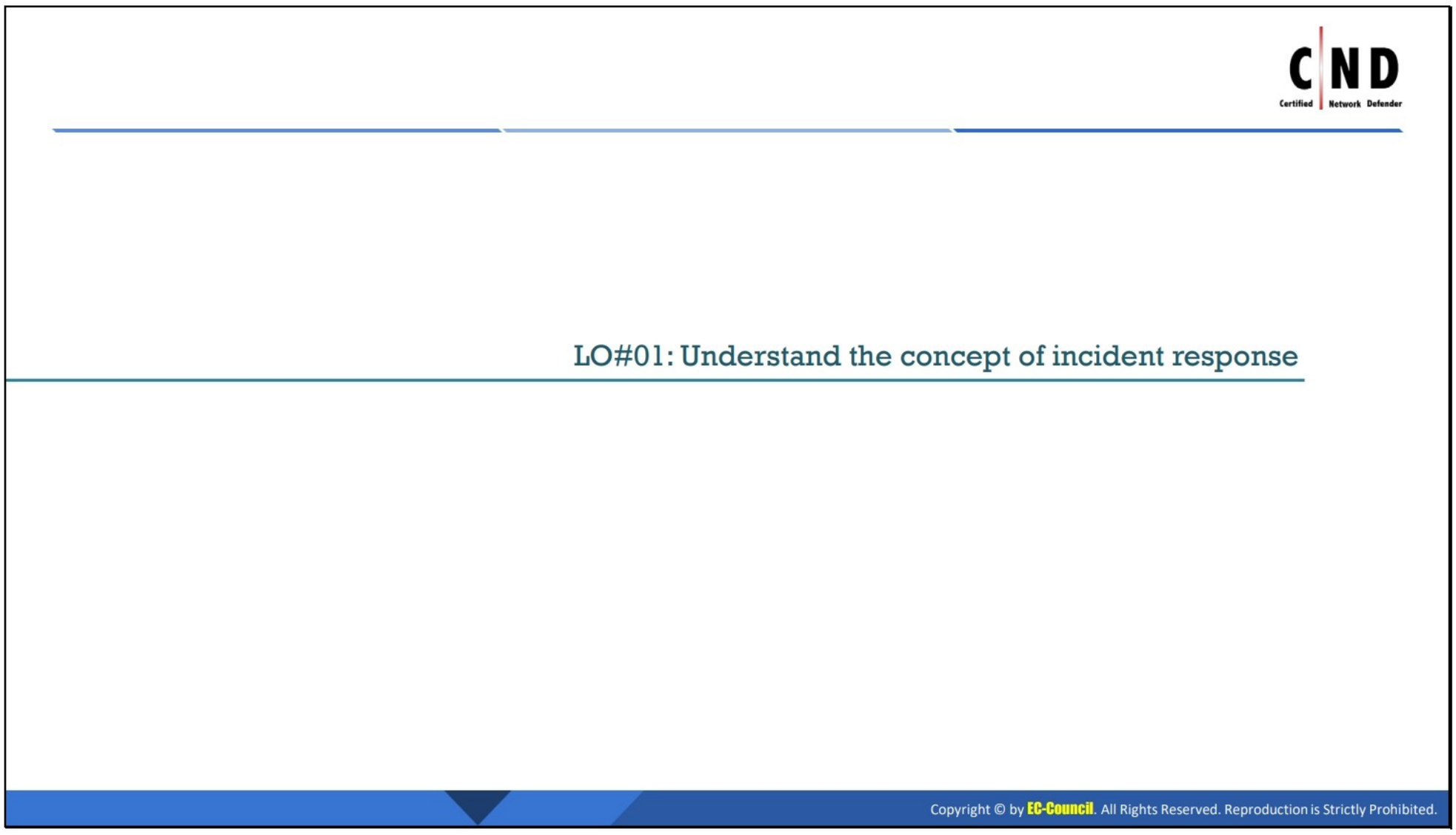
This page is intentionally left blank.



Learning Objectives

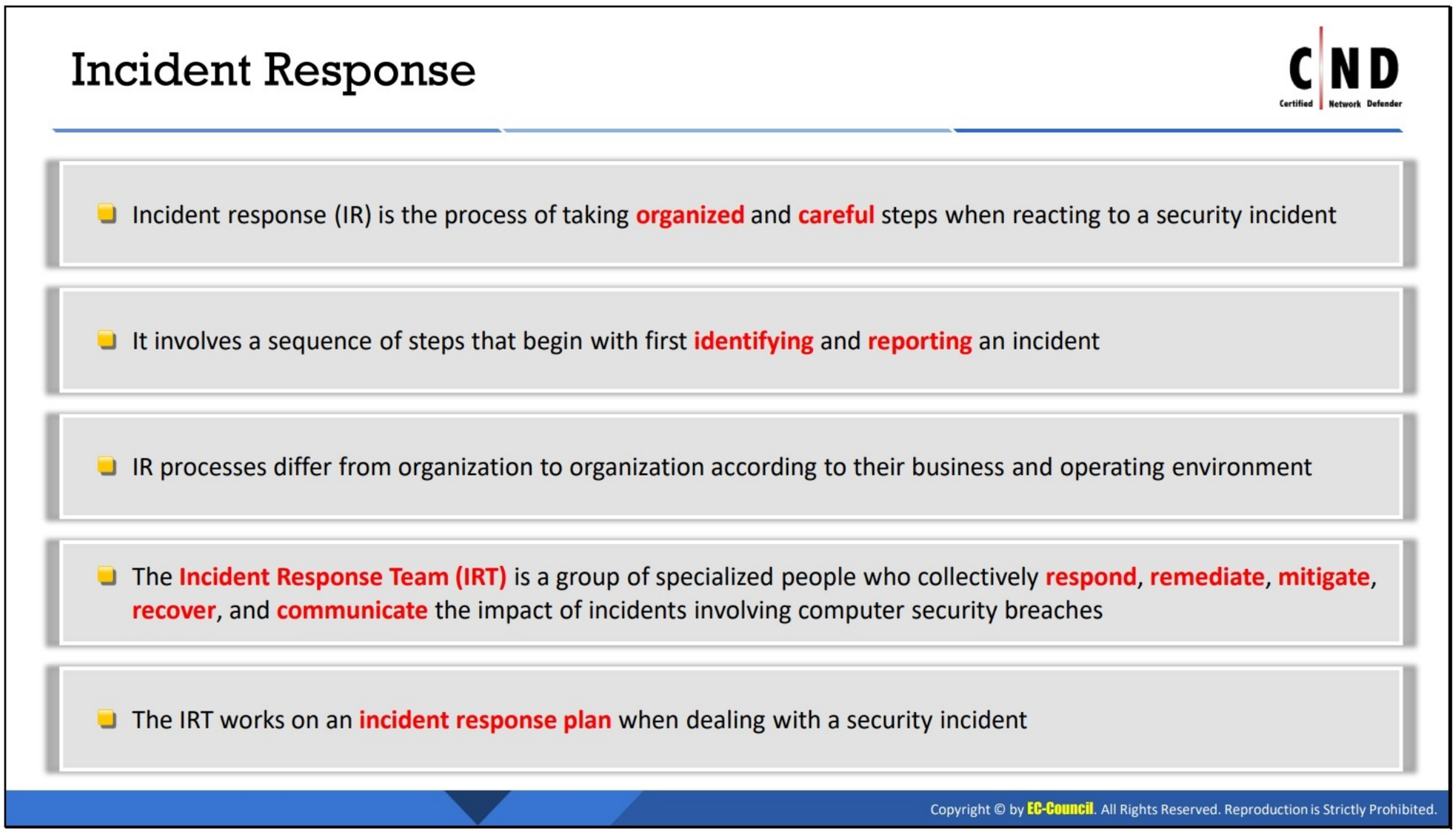
The objective of this module is to discuss the role of incident response and forensic investigation process in an organization's security. The learning objectives of this module are as follows:

- Understand the Concept of Incident Response
- Understand the Role of the First Responder in Incident Response
- Discuss Do's and Don'ts in First Response
- Describe the Incident Handling and Response Process
- Enhance incident-response using AI/ML
- Understand incident response using SOAR
- Understand incident response using Endpoint Detection and Response (EDR)
- Understanding incident response using Extended Detection and Response (XDR)
- Describe the Forensics Investigation Process



LO#01: Understand the Concept of Incident Response

Understanding the concept of incident response (IR) will help handle security breaches effectively and minimize the damages from a cybersecurity attack. The objective of this section is to help you understand the approach, goals, and advantages of IR. It will highlight the roles and responsibilities of an Incident Response Team (IRT).



Incident Response

IR is a systematic approach that is adopted to handle security incidents with minimal damage, recovery time, and costs. In the process of responding to an incident, information such as the vulnerability of the network that caused the attack to occur, who initiated the attack, and the kind of devices and files that are affected are known.

Goals of IR

- To detect if an incident occurred and if it is an actual security incident or a false positive
- To maintain or restore Business Continuity
- To reduce the impact of an incident
- To analyze the cause of an incident
- To prevent future attacks or incidents
- To improve security and incident response
- To prosecute illegal activity

Advantages of IR

- Equips the organization with safe procedures to be followed when an incident occurs
- Saves time and effort, which is otherwise wasted when fixing an encountered incident
- Helps the organization learn from past experiences and recover from losses more quickly
- The skills and technologies required to tackle an incident are determined in advance
- Saves the organization from legal consequences arising from a severe incident
- Helps determine similar patterns across incidents and handle them more efficiently

IRT Roles and Responsibilities

- Depending on the organization, an **in-house** or an **external IRT team** holds different titles, roles, and responsibilities for an incident response

Management	An individual or group of individuals from the management with leadership and decision-making authority
Information Security Team	An individual from the information security team who has experience in discovering and containing incidents
IT Staff	An individual who is aware of the information system and network areas. They may be system or network administrators.
Physical Security Staff	An individual who is responsible for physical security and identifying the extent of any damage
Attorney	An individual responsible for providing legal advice

IRT Roles and Responsibilities (Cont'd)

HR Representative	An individual responsible for handling employee issues for an employee involved in an incident
PR Specialist	An individual responsible for conveying company details after an incident
Financial Auditor	An individual who assesses the financial loss to a company from an incident
IR Officer	An individual responsible for all actions of the IR Team and IR Function. They may be an executive-level employee such as a CISO, or another corporate representative.
IR Manager	An individual who receives the initial IR alerts and leads the IRT in all IR activities
IR Assessment Team	A group of individuals who make decisions on the classifications and the severity of the incident identified. The team comprises representatives from IT, Security, Application, Support, and other business areas.
IR Custodians	An individual responsible for the remediation and resolution of the incident that occurred. They include technical experts and application support representatives.

IRT Roles and Responsibilities

The IRT is a group of specialized people who collectively respond to, investigate, remediate, mitigate, and communicate the impact of incidents involving computer security breaches. The IRT plays a very important role in the organization. However, maintaining such a team separately can involve huge costs and other resources. Therefore, organizations generally use their current

employees who are experts in their fields to constitute the IRT in addition to a few dedicated members.

The IRT can include persons including network and system administrators, managers, stakeholders, employees, and security operations center analysts.

IRT Roles and Responsibilities

Typical roles and responsibilities of IRT members may vary based on the organization's IR activities.

- **Management:** In an organization, the management includes the top-most authoritative decision makers. It may include a single entity or a group of entities who make decisions when an incident occurs. The management should be the first entity to learn about an incident. They decide the steps to be taken after the occurrence of an incident is confirmed.
- **Information Security Team:** The team consists of a group of individuals who possess the skills to detect and analyze security incidents. They can easily identify the nature, category, and scope of the incident.
- **IT Staff:** IT Staff comprises the individuals who are either system or network administrators. They detect the incident by analyzing network traffic, system logs, and service packages and patches, among others, and report it to the management or the IRT. They execute the first response step to avoid further damage.
- **Physical Security Staff:** Physical security staff contribute to the handling of and response to physical security incidents. They can also be the first responders to a physical security incident. They actively report the occurrence of a physical security incident such as fire, theft, damage, and unauthorized access to the management.
- **Attorney:** The attorney is a legal advisor for the organization. Attorneys play a major role in ensuring that any evidence collected is admissible in a court of law. They can also help an organization recover from a financial loss due to an incident.
- **HR Representative:** An internal employee may be involved in a security incident. In these situations, Human Resources (HR) becomes involved when the IRT detects that an internal employee is involved in the security incident. HR provides the IRT with the best possible solution for dealing with any employee involved in an incident.
- **PR Specialist**

  The Public Relations (PR) department serves as a primary contact for the media and informs the media about an event. They update the website information, monitor media coverage, and are responsible for stakeholder communication, including to the following:

  - Board
  - Foundation personnel
  - Donors
  - Suppliers/vendors

- **Financial Auditor**

  Financial Auditors are individuals who assess the financial loss of the organization after an incident. The auditor is responsible for accounting for all losses that occurred as a result of the incident. The auditor is responsible for reporting the financial imbalance in the organization's account.

- **IR Officer**

  The IR Officer is an individual who oversees all IR activities in an organization. IR officers are executive employees who are responsible for how the IRT functions. Every action taken by the IRT is reported back to the IR Officer who further reports to the management of the organization.

- **IR Manager**

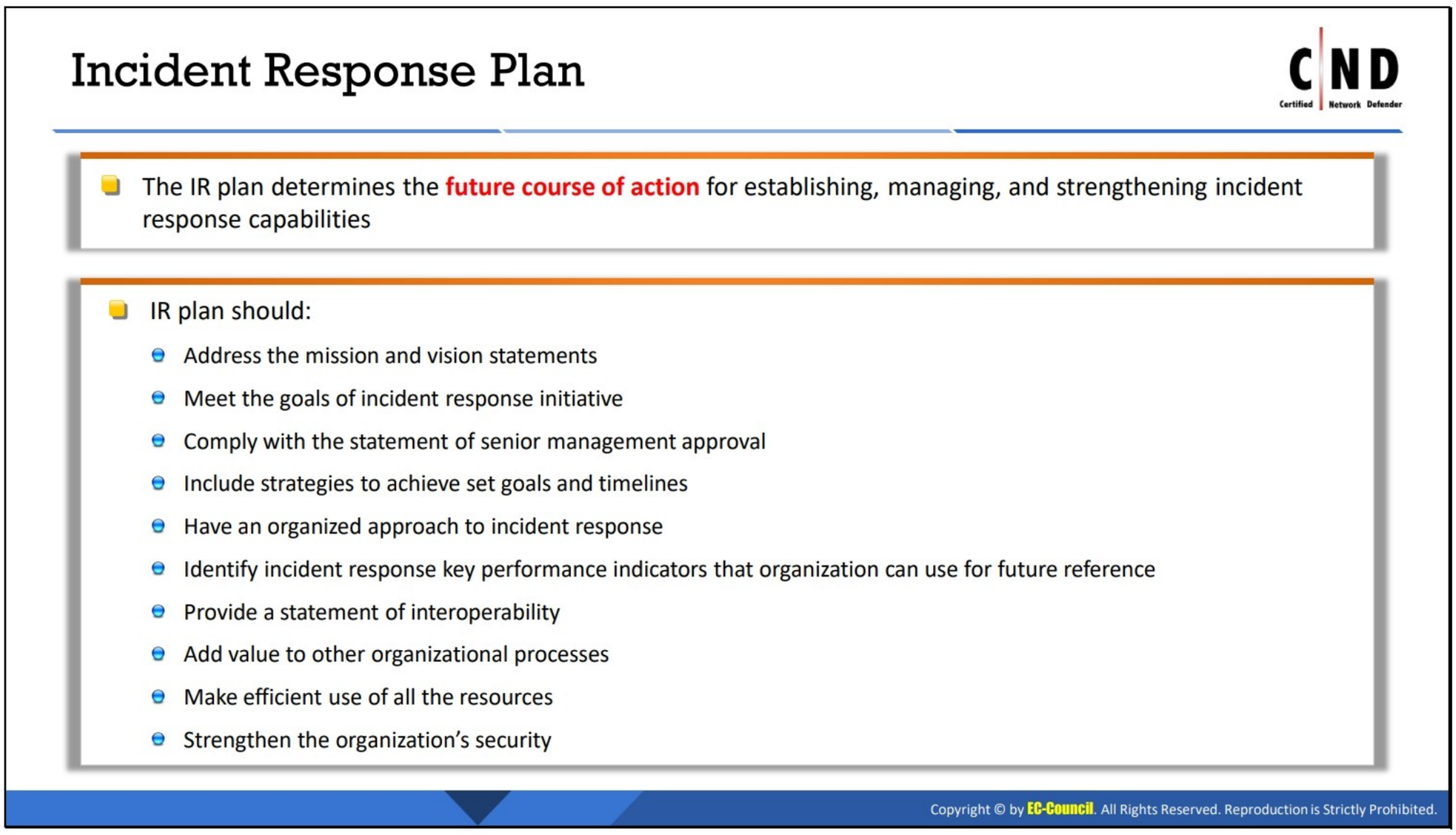
  The IR Manager must be a technical expert who understands security and incident management. The IR Manager focuses on the incident and analyzes how to handle it from a management and a technical point of view. They are responsible for the actions performed by the incident analysts and reporting the information to the IR Officer.

- **IR Assessment Team**

  The IR Assessment Team comprises individuals who prioritize the occurrence of an incident based on the amount of loss it caused to the organization. The team comprises individuals from various domains such as IT, security, application support, and other business areas.

- **IR Custodians**

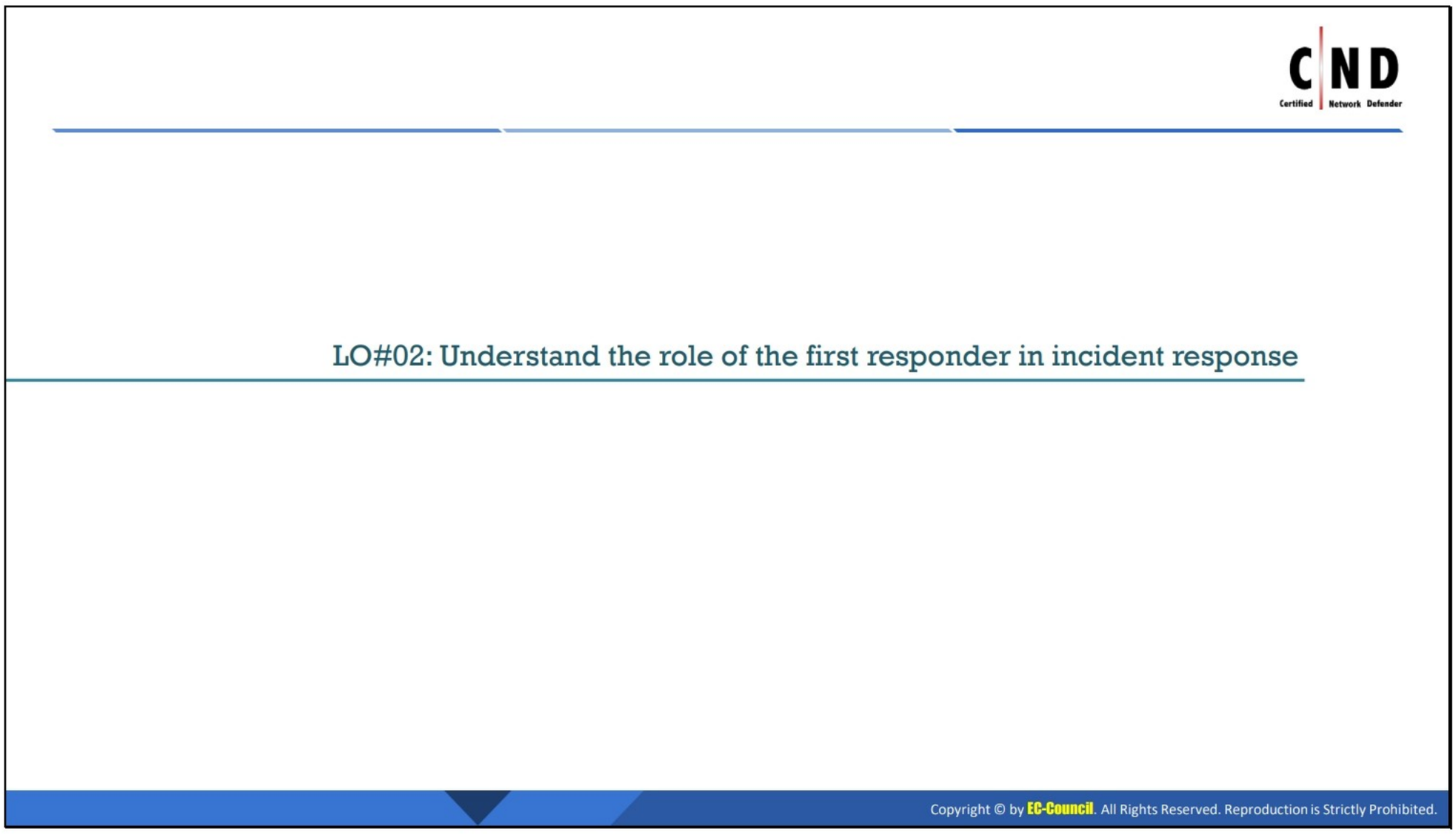
  IR Custodians are either technical experts or application support representatives. They play an important role when an application incident occurs. To respond to the incident, IR Custodians create an action framework that is further shared with the management.



Incident Response Plan

The IRT creates an incident response plan (IRP) before handling and responding to the incidents. An IRP is a set of guidelines that are required when responding to an incident in a dedicated and formal manner. The plan contains the elements required for executing the IR effectively. These plans include response instructions for any detected incidents. The IRP includes the company requirements such as size, structure, and functions. The plan identifies the resources required for managing the incidents.

- An IRP should include the following:
  - Aim of the IRP
  - Objectives and approaches
  - Methodology of the IR
  - Standards to assess IR efficiency
  - Observing the current status of IR
- Components of an IRP:
  - Name and contact information of the IRT
  - System details such as data flow diagrams and network diagrams of the incident
  - The complete process required while recording and handling an incident
  - Report security incidents to the Information Security and Policy (ISP), who appoints a security analyst to handle the incident
  - Respond to the incident in a timely manner



LO#02: Understand the Role of the First Responder in Incident Response

The objective of this section is to understand the role of the first responder in incident response (IR). The first responder plays a crucial role by proving a quick initial response to the incidents of threats or attacks in the organization. This section deals with the roles and responsibilities of the first responder.

First Responder

- A first responder is an individual who arrives first at the crime scene and **brings the incident to the attention of others**
- The first responder could be an end user, network administrator, or any other individual who is involved in the day-to-day network operations, spends a lot of time in **network environments**, and is familiar with the organization's assets, network traffic, performance and utilization, network topology, location of each system, security policy, etc.
- The first responder play a **key role** in incident response and forensic investigation process. He/she can provide great help in early detection of incident, source of the incident, impact of incident, evidence collection and preservation, etc.
- The first responder should aware of the incident response and forensics investigation procedure, otherwise response to the incidents can be **delayed**. The delay in incident response can **increase the potential impact** of incident or even evidence can be corrupted and/or lost

First Responder Roles and Responsibilities

- **Reporting** the incident
- **Alerting** the management and incidence response teams
- **Containing** incident
- **Identifying** the crime scene
- **Collecting** the complete information about the incident
- **Protecting** the crime scene
- **Documenting** all the findings
- **Preserving** temporary and fragile evidence
- **Packaging** and transporting the electronic evidence

First Responder

The Incident Response Team (IRT) works on the pretext of the first responder of the incident. The term "first responder" refers to the individuals who arrive first at the crime scene and gain access to the victim's computer system after the incident report. A first responder may be a user, network administrator, law enforcement officer, or investigation officer. They are responsible for protecting, integrating, and preserving any evidence obtained from the crime scene.

The time gap between the occurrence of an incident and transference of evidence is an important aspect in incident response. It is the responsibility of the first responder to ensure the reliability and liability of the evidence. The method used by any first responder is very important in preserving the evidence and finding the attackers. First responders should be trained to gather evidence without modifying any of the services running at that moment. This is a critical task for the first responders as they have to gather evidence before it is lost. The first responder needs to have a dedicated and well-organized plan when responding to any type of incident as they collect the initial information and determine the extent and impact of the attack or incident. This allows other people involved in handling the incident to effectively determine other courses of action that may be required for investigating the incident.

An experienced first responder can easily apply good forensic techniques when they respond to an incident in the initial stages. They can predict the extent to which any change in the evidence may affect the further investigation. This proficiency is an extra add-on in maintaining the availability, integrity, and reliability of the evidence. The first responder needs to always understand the importance of their role as it highly affects the security and efficiency of the organization.

First Response Rule

- Under no circumstances should anyone except forensic analysts make any effort to collect or recover the data from any computer system or electronic device that holds electronic information.
- Remember that any information present inside the collected electronic devices is probable evidence and should be treated accordingly.
- Any attempts to retrieve data by unqualified individuals should be avoided. These attempts could either compromise the integrity of the files or result in the files becoming inadmissible in legal or administrative proceedings.
- The workplace or office must be secured and protected to maintain the veracity and quality of the crime scene and the electronic storage media.

Things You Should Know before First Response

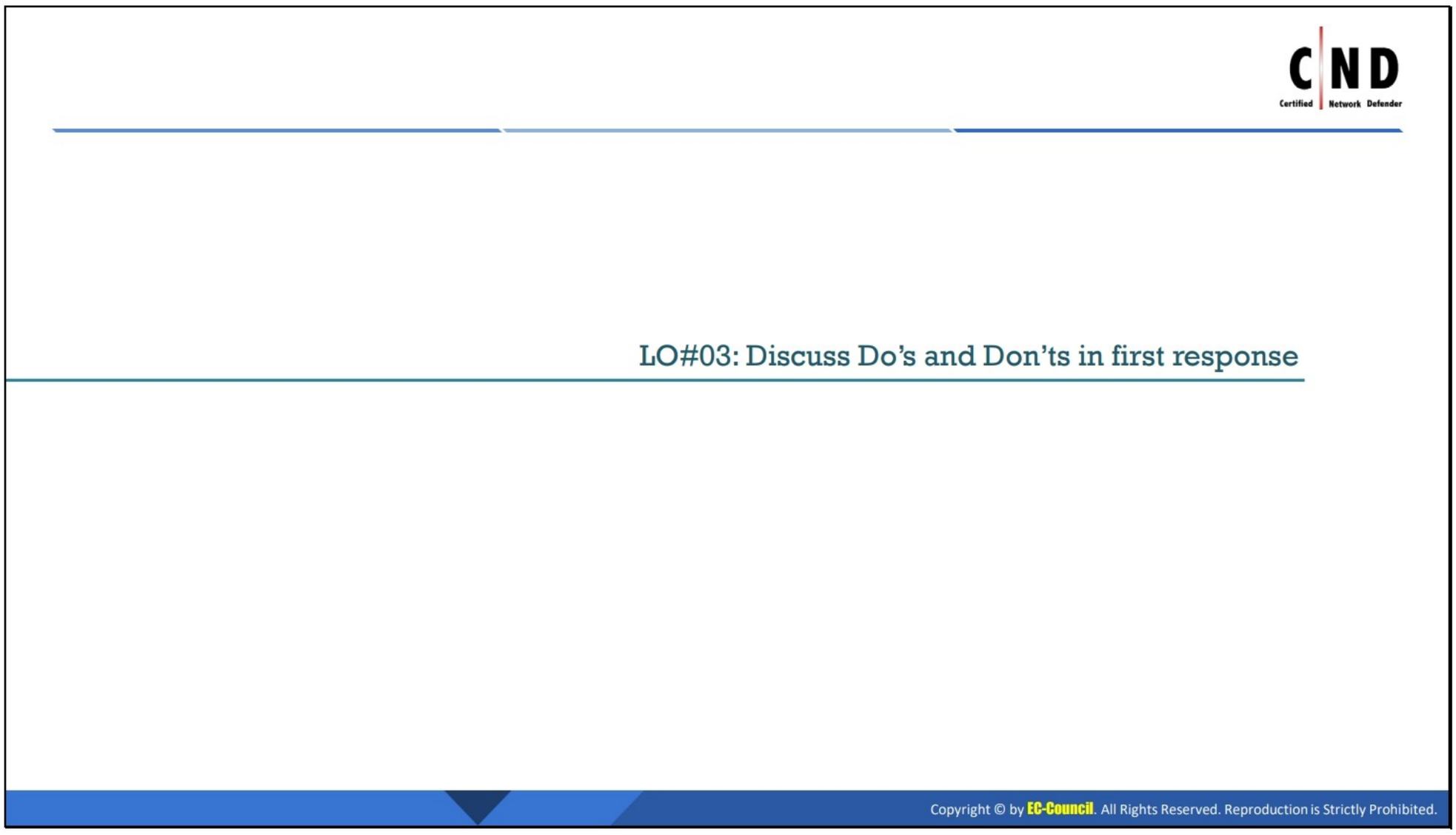
The first responder should review the incident plan of their organization and suggest or implement changes to the incident response plan (IRP) as required.

A typical IRP includes the following:

- **Contacts of IRT:** It will help a first responder to immediately contact the IRT when an incident occurs. Having an IRT immediately on the location of the incident will help minimize any delay in responding to an incident.
- **Escalation procedures:** First responders should know whom to contact and report the incident. There will be certain escalation procedures for the first responder that will help them report the incident without any delay.

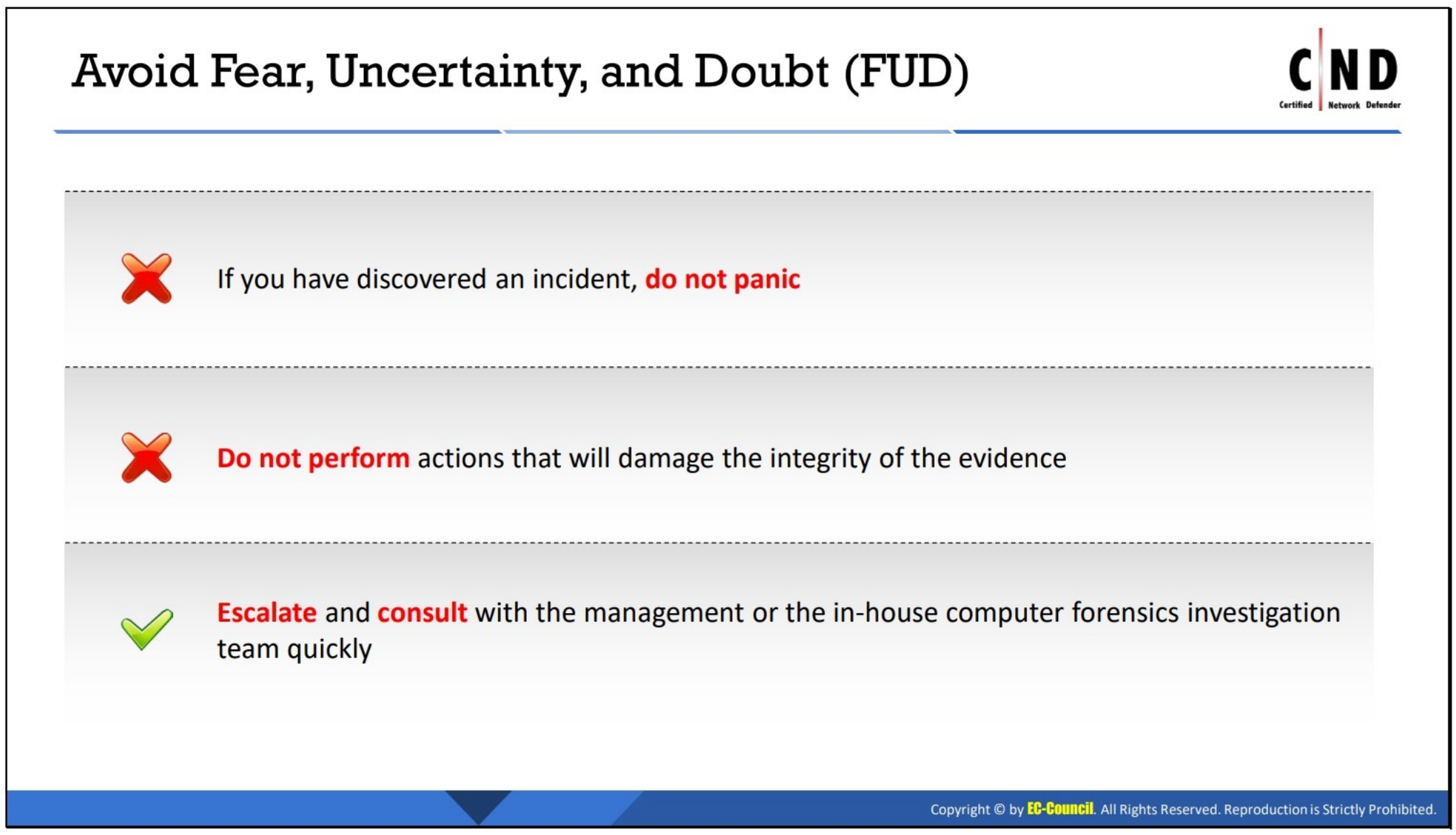
  First responders collect and document the following information before escalating the incident:

  - IP address and physical location of the affected systems
  - Type of data on the systems
  - Timeline of activities the system/user went through before the incident
  - How the incident was detected
  - Number of users affected
- **Procedure for reporting and handling an incident:** First responders should be aware of reporting and IR procedures.
- **Containment actions:** The IRP includes containment actions for all types of security incidents. Different containment actions are required for different types of incidents. The first responder should be aware of the containment actions for various types of security incidents, as it helps prevent further damage to an organization.



LO#03: Discuss Do's and Don'ts in First Response

Any misleading or inappropriate steps for providing a first response could place the organization in undesired situations. This can be due to lack of knowledge or skills required for a first response. The objective of this section is to discuss the Do's and Don'ts in first response to avoid undesired situations.



Avoid Fear, Uncertainty, and Doubt (FUD)

Fear, Uncertainty, and Doubt (FUD) is not a new concept for organizations. Any incident can create an environment of fear and anxiety among the team. A security incident outbreak is often very stressful and brings about a lot of doubt and uncertainty. Decisions made in fear and anxiety will worsen the situation. Usually, small-sized companies do not have an Incident Response Team (IRT). In such scenarios, first responders usually lack the confidence required to deal with an incident.

Providing a first response in a state of fear or uncertainty can forego certain important and resourceful information related to the incident. This could mislead the investigation team and cause delays in identifying why the incident occurred. A decision made while panicking can affect the evidence quality.

A first responder should be confident while providing a first response to an incident. If unsure about the decision to make during a first response, the first responder should consult with the top management, the information security team, or the in-house IRT.

Make an Initial Incident Assessment

- If you find any indications of a security incident:
  - Check whether it is an **actual incident** or a **false positive**
  - Identify the **category** and **severity** of the security incident

Types of Incidents

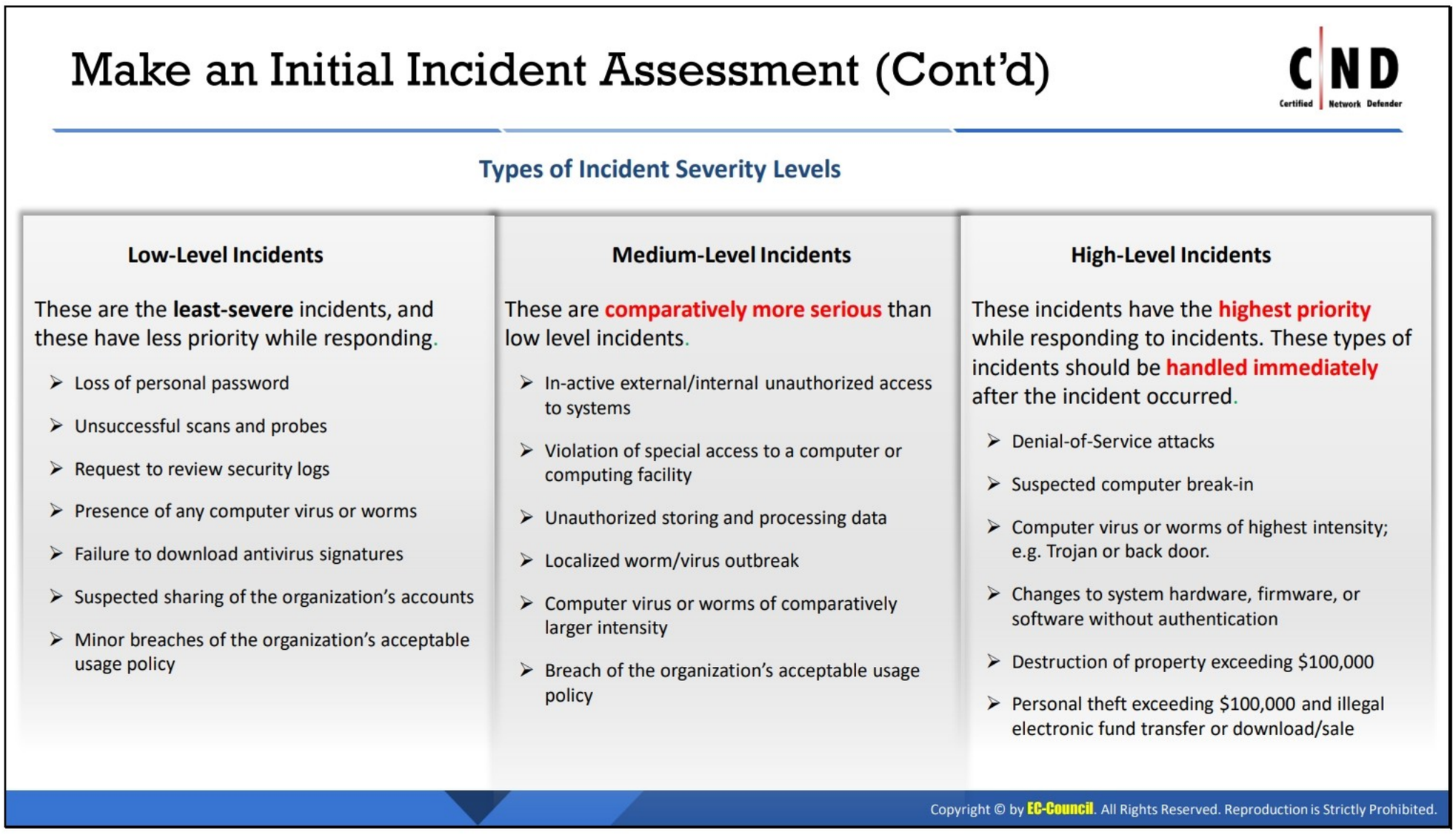
Various types of alerts are produced by security tools, among which only few are related to a **potential security issue**.

- **False Positive:** An alarm is raised when no attack has occurred. Non-malicious activities are identified as dangerous
- **True Positive:** An alarm is raised when an actual attack has occurred
- **False Negative:** No alarm is raised when an actual attack has occurred. Malicious activities are not recognized
- **True Negative:** An alarm is raised when no attack is detected. Non-malicious files are rejected successfully

Make an Initial Incident Assessment (Cont'd)

Category of Incidents

Category of Incidents	Description
Unauthorized Access	An attacker gains unauthorized access to system resources.
Denial of Service (DoS)	An attack resulting in the unavailability of services for authorized network users
Malicious Code	Malware (e.g. virus, worm, Trojan horse, keyloggers, spywares, rootkits, and backdoors) infecting operating systems and/or applications
Improper Usage	Individuals in the organization using system resources against acceptable usage policies
Scans/Probes/Attempted Access	Activities undertaken by attackers to identify open ports, protocols, or services, for exploiting an information system later.
Multiple Component	An incident that encompasses two or more of the incident types mentioned above



Make an Initial Incident Assessment

The first responder should conduct an initial assessment upon the occurrence of an incident that has been identified. An initial assessment helps determine the following.

- Source of the incident
- Whether the incident that occurred is a false positive or an actual incident
- Deciding the severity of the incident helps take immediate actions and minimizes the risk.
- Note down all actions performed during the occurrence of the incident.

An initial assessment provides an outline for the type of attack that occurred. The information recorded in this stage is useful in containing the damage and avoiding risk. Further handling of the incident depends on the facts arrived at in the initial assessment phase.

The first responder should record information such as the following:

- Features of the incident
- Date and time when the incident occurred
- Incident indication list
- Impact scope of the incident
- Nature of the incident or the type of attack

Types of Incidents

An alert is generated when a suspicious event is noticed in the network. Various types of alerts are produced by security tools; among them, only a few are related to a potential security issue.

Based on these alerts, incidents are categorized into four different types.

- **False positive:** False positives are a false result for an activity that never occurred. It is an attack-positive reply for a normal event. An alert raises an alarm when no attack has occurred. This means that non-malicious activities are identified as dangerous. For example, an alert may be generated for a brute-force attack on the network. However, after examining the incident, it might be found that the brute-force attempt was nothing but an authenticated user trying to log in through multiple attempts. Such alerts are known as false positives.
- **True positive:** True positives are true or correct results for an event that has occurred in the network. These are attack-positive replies for an incident that actually occurred in the network. If a true positive is identified, then certain actions are taken immediately to prevent the attack from continuing. By true positives, actual malicious events are identified. For example, if a malicious activity is identified, then it is referred to as an incident. After examining the incident, if it is identified that an actual attack had occurred on the network, then such alerts are known as true positives.
- **False negative:** False negatives are false results for an activity that actually occurred. It is an attack-negative reply for an actual attack. A false negative is a type of alert that actually will not raise an alarm even if an attack is occurring on the network. Not defining the rules properly will result in such kinds of errors in the alerting system. Due to false negatives, actual attacks may not be identified that may lead to a cybersecurity breach in the organization. For example, an attacker tried to gain access to an unauthorized network and succeeded after attempting nine times. If the rule in the security tool is set such that an alert is generated only after 10 login attempts, then the attempts of the attacker may not be noticed. In this way, false negatives can be dangerous for an organization if they are not rectified.
- **True negative:** True negatives refer to no alarms being generated when no attacks have occurred. Such alerts will not raise any alarm because no incident is identified. The security tool has to be designed such that they produce true-negative alerts. For example, if nothing suspicious is occurring in the network, then the security will not raise any alarms. These kinds of alerts where no detection is made are known as true negatives.

Incident Severity Levels

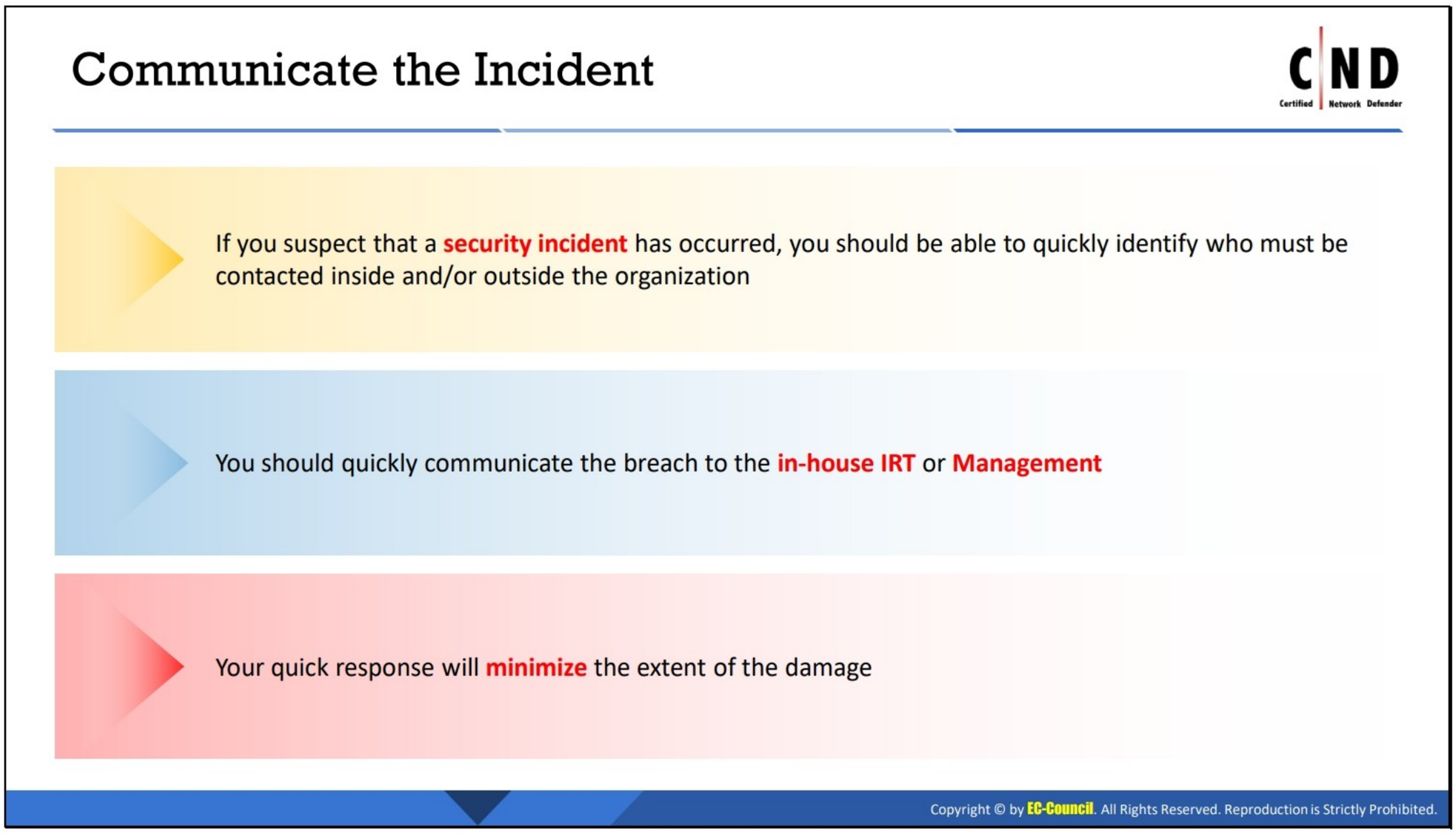
The severity of an incident is an important measure of the impact on the security of an organization. It determines the urgency of handling an incident, level of expertise required in handling the incident, and the extent of the response.

The severity of an incident is determined by the following.

- **Impact of the incident**: Determines the extent of the damage or impact of the incident on the organization.
- **Criticality of the service**: Determines the level of dependency of other services on the affected service.
- **Confidentiality of the information**: The severity of the information stored in the incident service.
- **Probability of spread**: The rate at which other systems or services are affected by the incident.

Organizations categorize the severity of incidents as high-level, medium-level, and low-level incidents.

- **High – Level Incidents:**
  - The incident has a high probability of affecting a large number of systems or services in an organization.
  - The impact of the incident may lead to a financial crisis.
  - Affects the major functioning and operations of the organization.
- **Medium-Level Incidents:**
  - The incident could affect at least half of the systems or services in an organization.
  - Affects a non-critical system or service.
  - Disrupts the normal working of the organization.
  - The incident has a tendency to propagate to other systems or service.
- **Low-level Incidents:**
  - Affects only a few systems or services in an organization.
  - Low probability of affecting the functional and operational aspects in an organization.
  - Will not propagate to other systems or services.

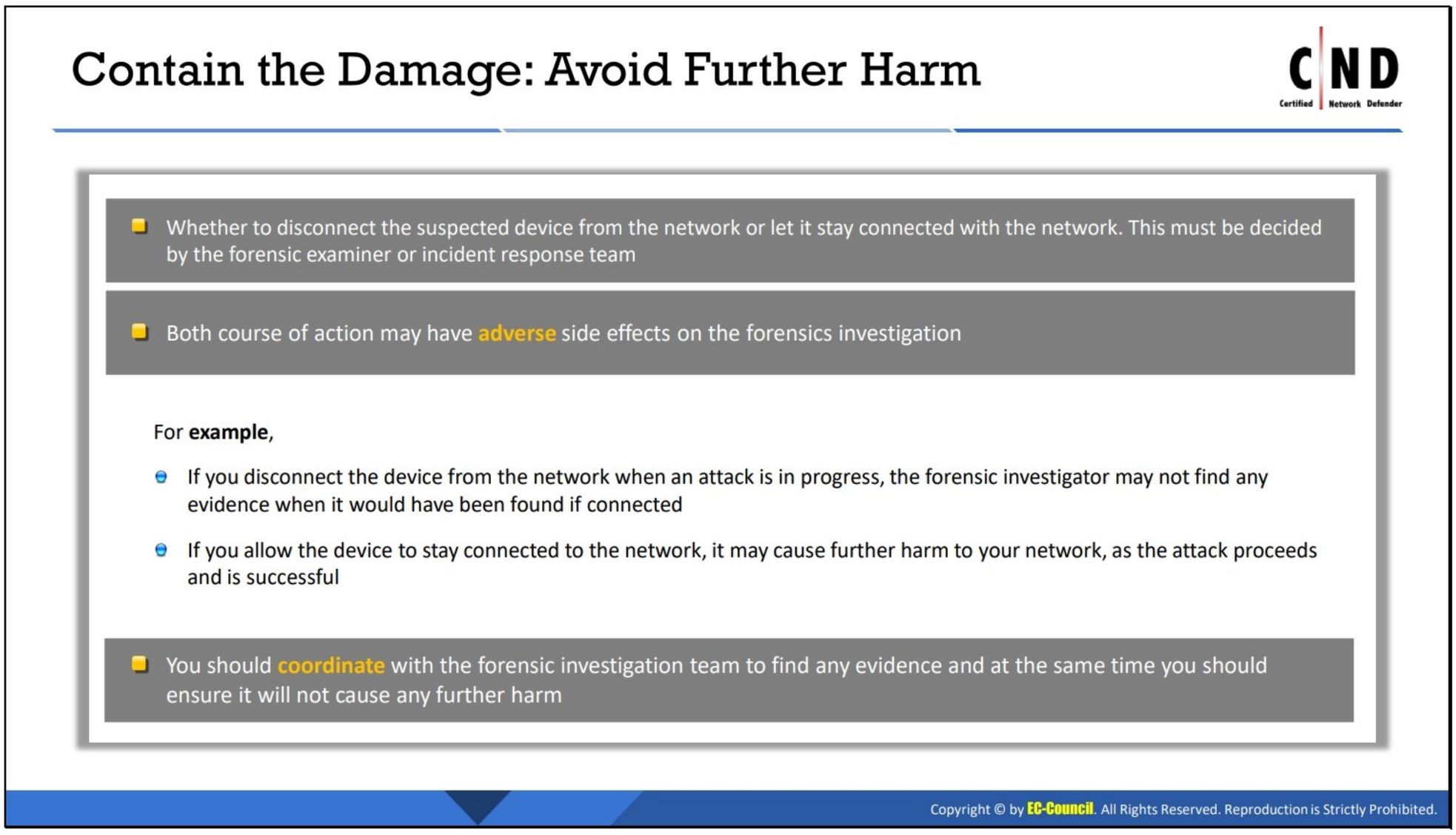


Communicate the Incident

The IRP will include the procedures and point of contact for communicating about the incidents. It may include the following:

- Clear idea of who to contact
- The contact team or person should be an expert in handling the incident.
- A dedicated team for contacting any external team for IR

They contact these people or teams through phone, SMS, or e-mail mentioned for immediate communication.

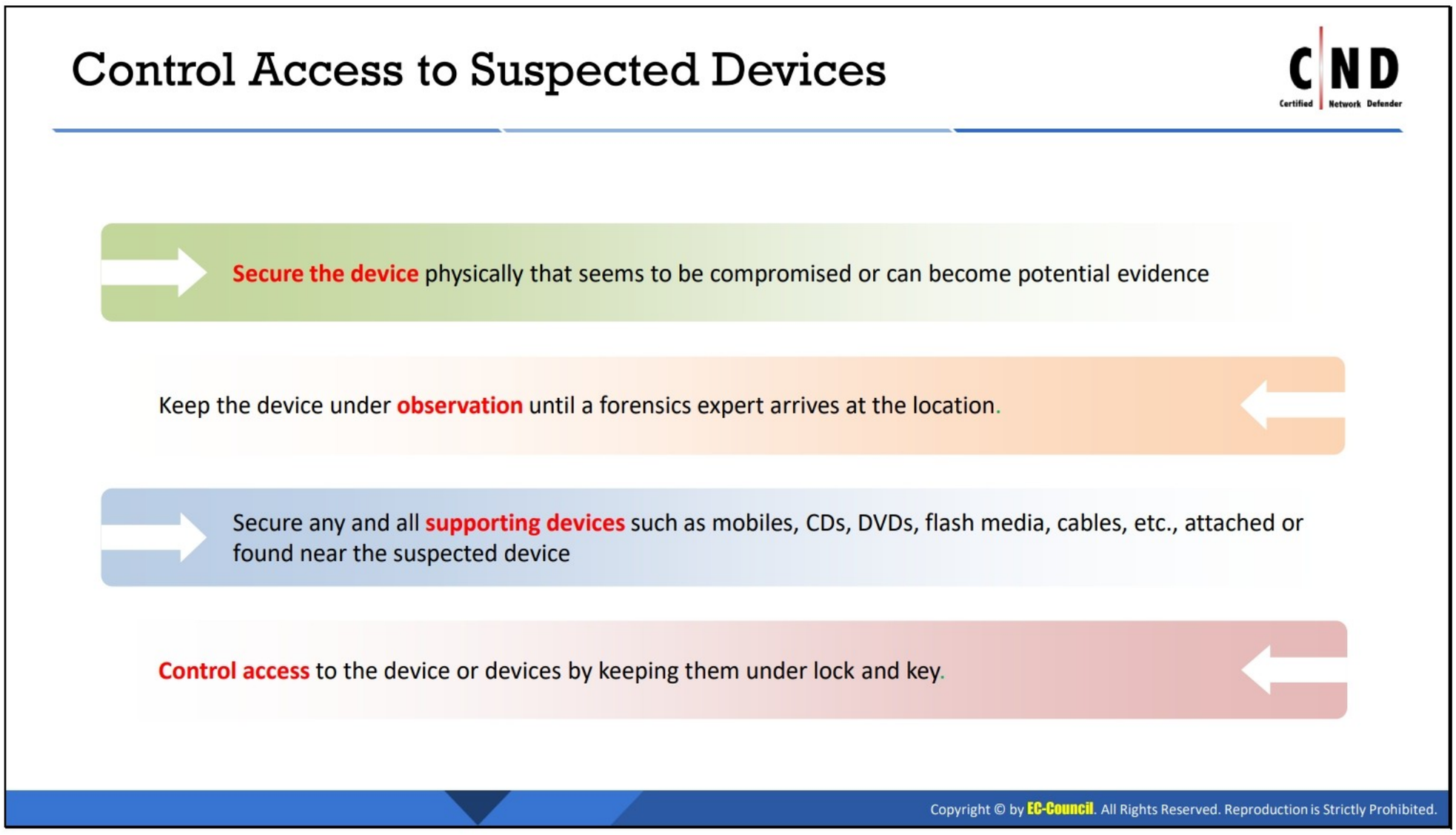


Contain the Damage: Avoid Further Harm

First responders have to take appropriate care while containing the incident. The process for containing the incident may involve different approaches for different types of incidents.

Common actions that help the first responder avoid further harm to the organization include the following:

- Prioritizing components
- Identifying the sensitive data, hardware, and software
- Do not notify all employees regarding the incident.
- Distinguish the instances wherein the incidents need to be handled offline or online.
- Determine all areas that are more likely to be attacked and implement methods to prevent further attacks.
- Build a new system that contains all services and requirements with new administrative and service account passwords.

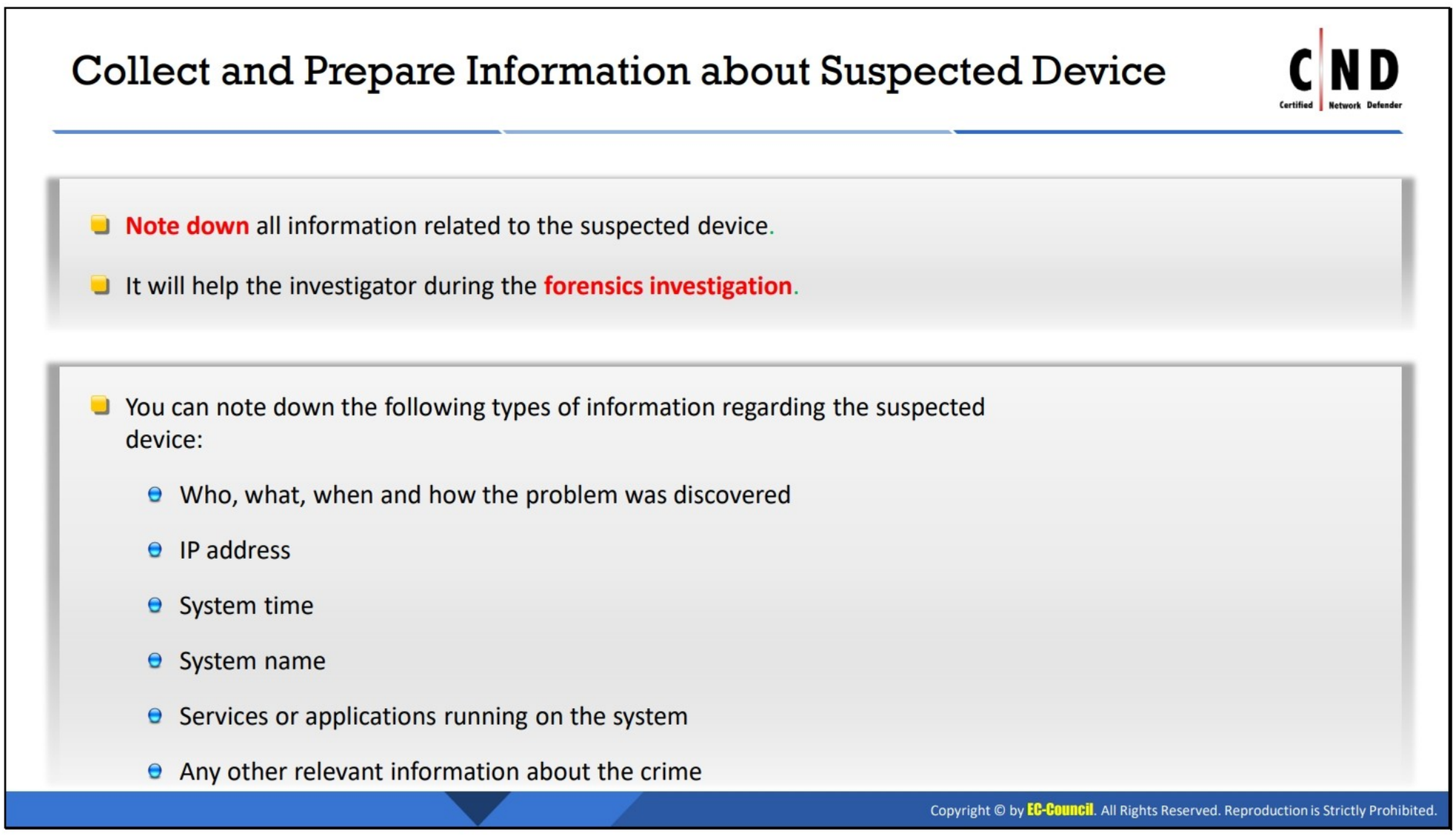


Control Access to Suspected Devices

The first responder should understand the importance of securing the evidence during their first response. They should implement and execute certain preventive measures to control access to a suspected device.

- **Secure the device:** The first responder should securely maintain the devices that were compromised or were the source of the incident. These devices can be potential evidence during an incident investigation.
- **Scrutiny of the devices:** The first responder should keep the device under observation and not tamper with the device until the forensic team arrives. Tampering with the devices can lead to loss of evidence, thus affecting the incident investigation.
- **Secure supporting devices:** Apart from the suspected device, the first responder should also gather all other devices or media that were found near the suspected devices. Leaving any such evidence behind can change the course of an investigation action plan.
- **Control access to the device**: No other user or employee should have access to the suspected or the evidence device.

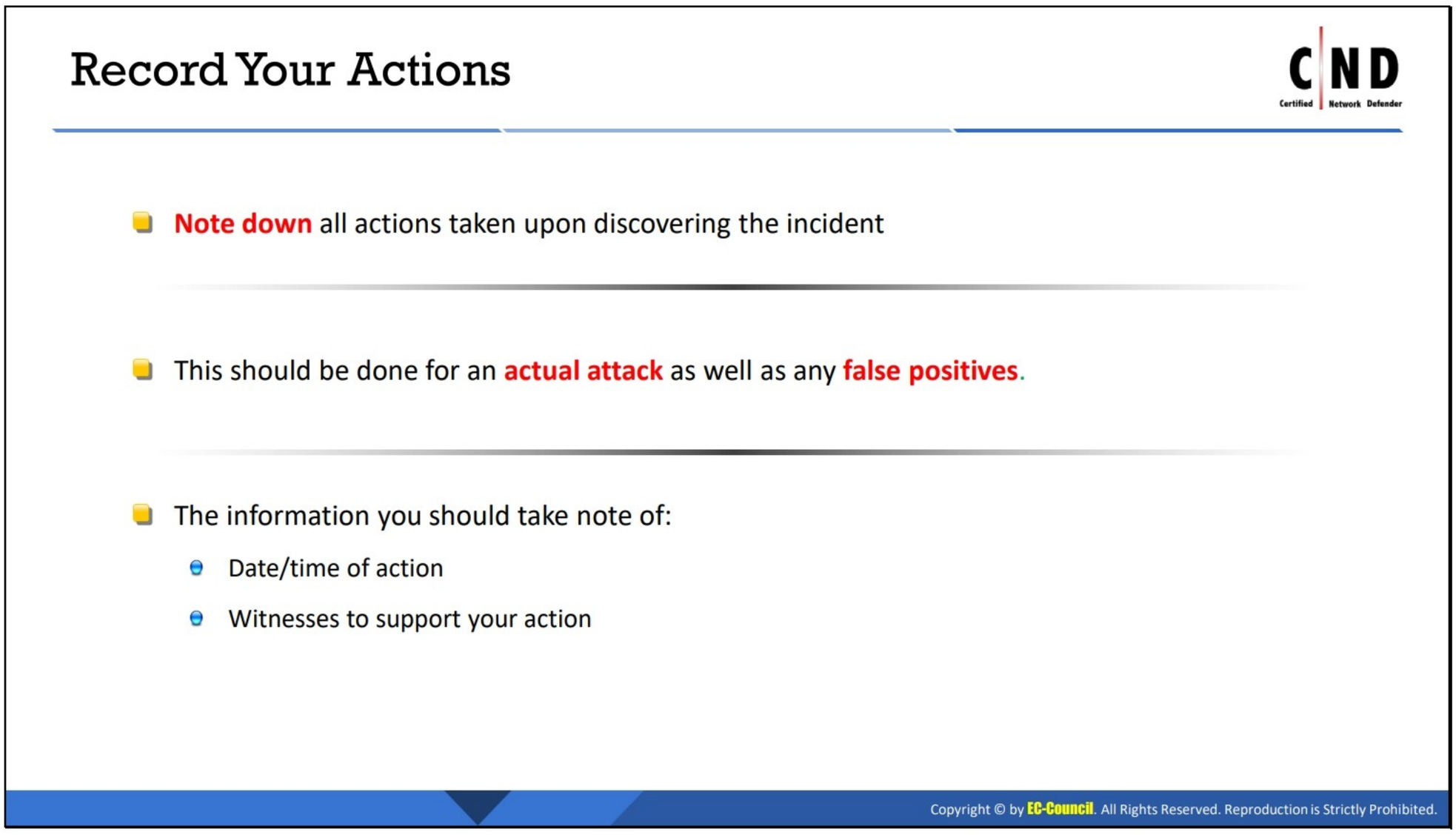
The scrutiny of the devices depends on the first responder; any damage or tampering with the devices can affect the investigation procedure. If the premises can be locked down, the first responder should lock the premises until the arrival of the forensic team.



Collect and Prepare Information about Suspected Device

The first responder should collect and prepare all information relevant to the incident during their first response. Gathering first-hand information about this time will aid the forensics investigation. It will be helpful for the investigators if the first responder documents the changes to the affected system from the time the incident occurred until the arrival of the forensic team. If the system is still on, the first responder should note down all information gathered related to the incident. This information can help the forensic team during their investigation.

- **Who, what, when and how the problem was discovered:** Noting this information will help the investigator investigate the initial findings of the incident.
- **IP address:** The investigator is required to keep records of all IP addresses for all affected machines. Such machines should not be connected to the network to avoid data replication.
- **System time:** Knowing the system time when the incident occurred is vital to an investigator. Using this information, they can monitor the changes that the system underwent across the entire timeframe.
- **Running services or applications:** Incidents can be caused because of running applications or services on the system. It is, therefore, necessary to maintain a record of the services and applications as a result.
- **Any other relevant information about the crime:** The first responder should save any findings relevant to the incident. If any handwritten notes were found near the suspected device, the first responder should preserve them and record the content as a copy according to the IR procedures.

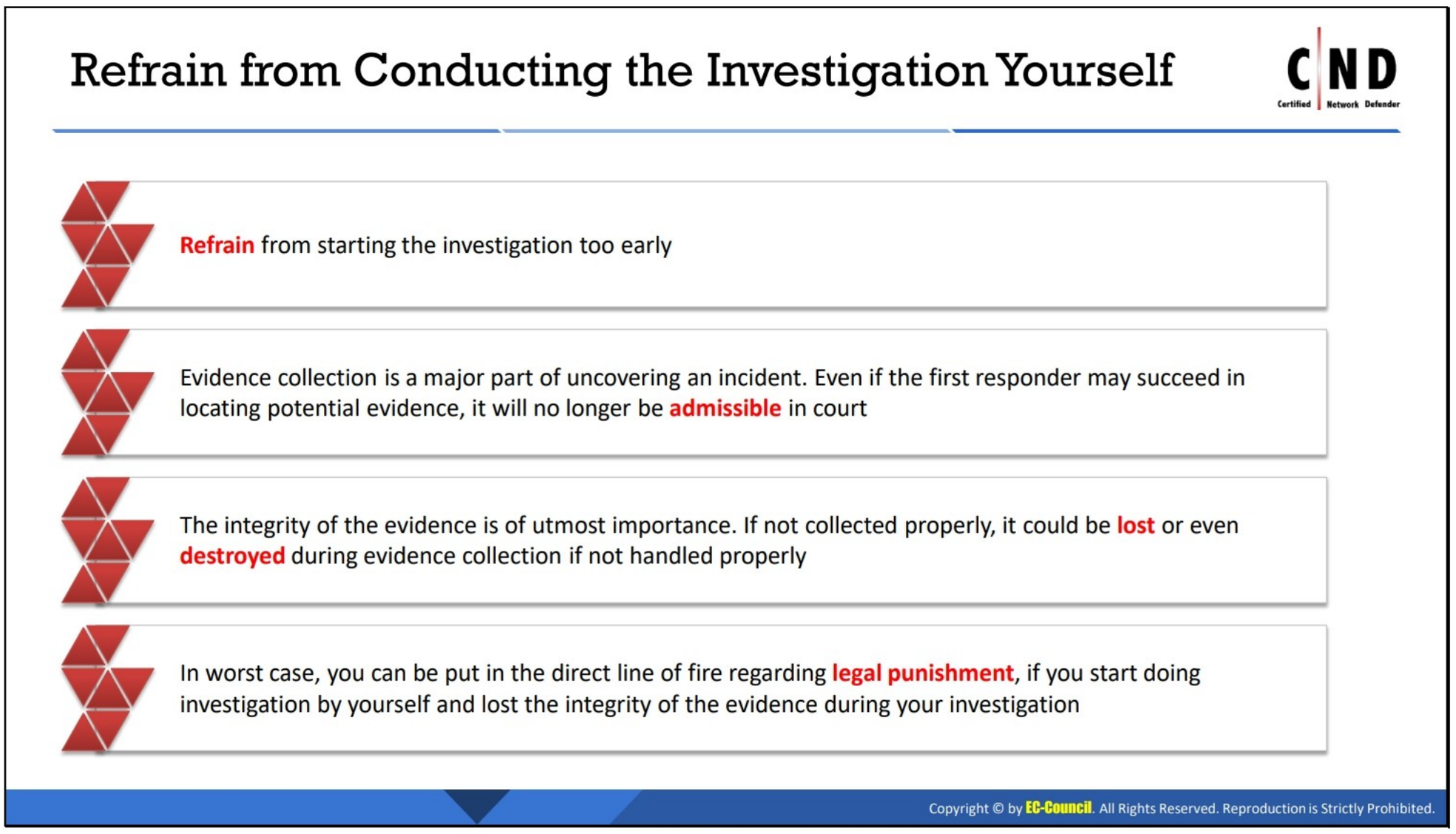


Record Your Actions

The logs of the first responder should be contain descriptions. The responder should record the actions in a series. If the actions are not listed in chronological order, it confuses the investigator. Responders should avoid writing any speculations in their record. Only facts should be noted, as these are the most vital for understanding the incident.

The record should contain details that can assist the investigator. For example, instead of documenting the action as "The web browser started receiving various popups after the attack," an ideal record of the action should be, "Unknown popups were displayed on a Google Chrome browser for thirty minutes after the incident occurred."

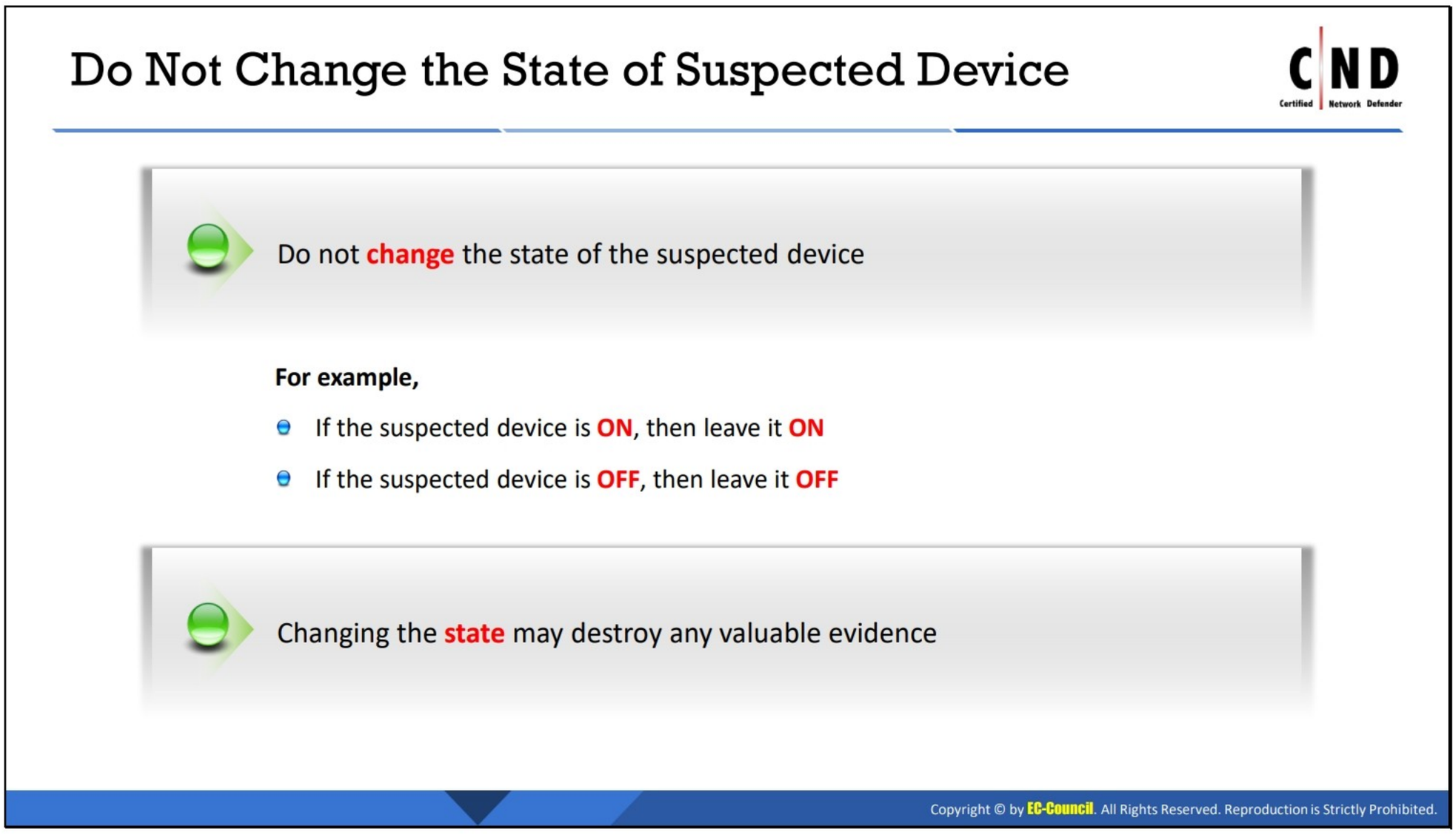
If a network device or an external drive is also affected, the responder should note down the serial number or part number of the device. The first responder should also record the statements of the users whose systems were affected by the incident.



Refrain from Conducting the Investigation Yourself

First responders should refrain from investigating the incident themselves. If the first responder is not well-versed in the forensics investigation process or not trained in forensics investigation techniques, any attempt towards engaging in forensics can and most often leads to the damage of any potential evidence. Even though the first responder might be aware of the reason for the incident, they should not proceed on their own. First responders should wait till they are authorized by the forensic team or management.

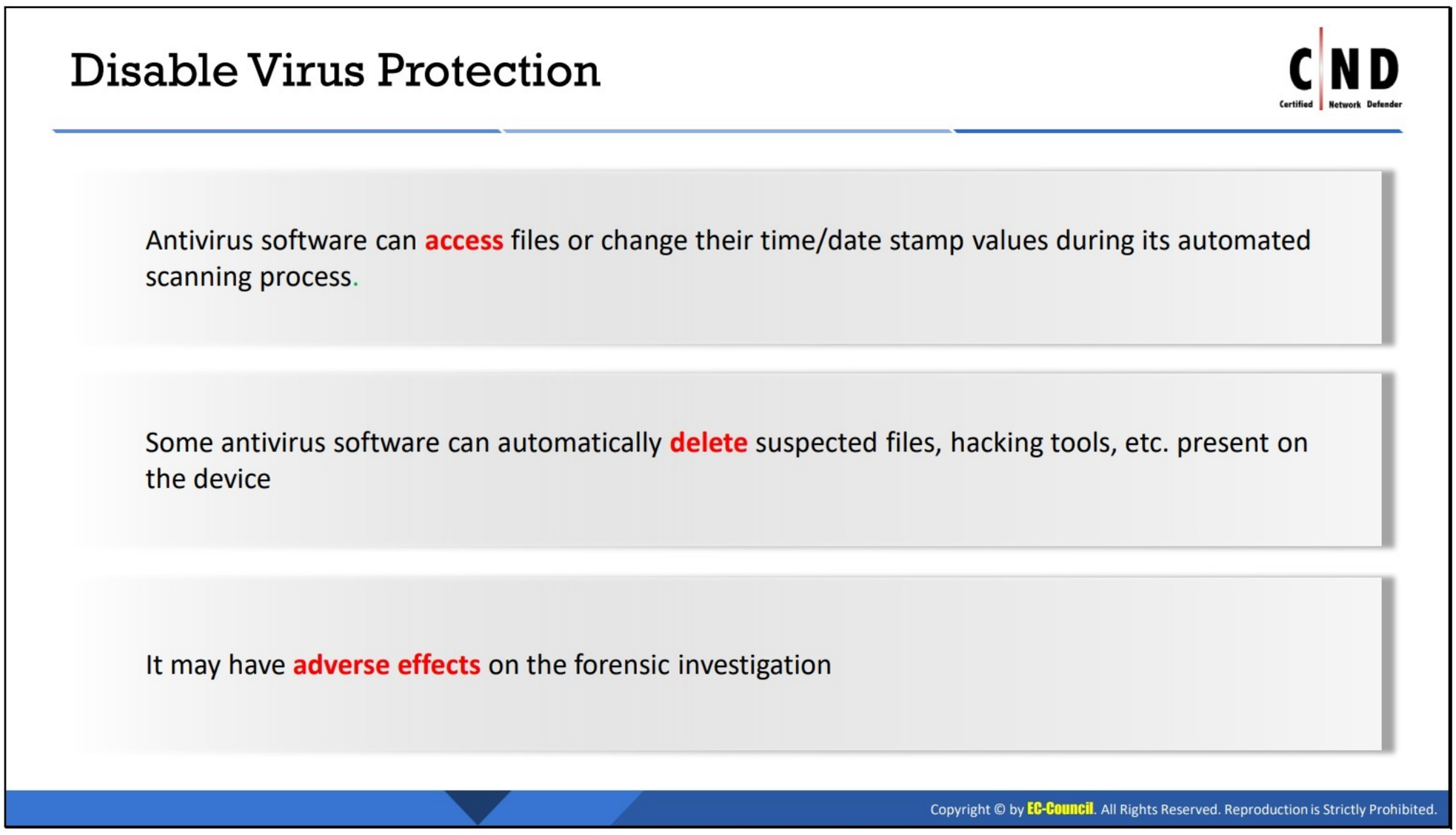
Even if the first responder conducts the forensics investigation and collects the evidence, the integrity of the evidence will no longer be valid in the court. This is because a first responder is not an expert in performing a forensics investigation. The evidence collected might not be accepted in court if it is not collected by an expert forensics investigator who ensures that the evidence is collected in a forensically sound manner. Moreover, if first responders do conduct an investigation that results in evidence tampering, the organization might take legal action against them.



Do Not Change the State of Suspected Device

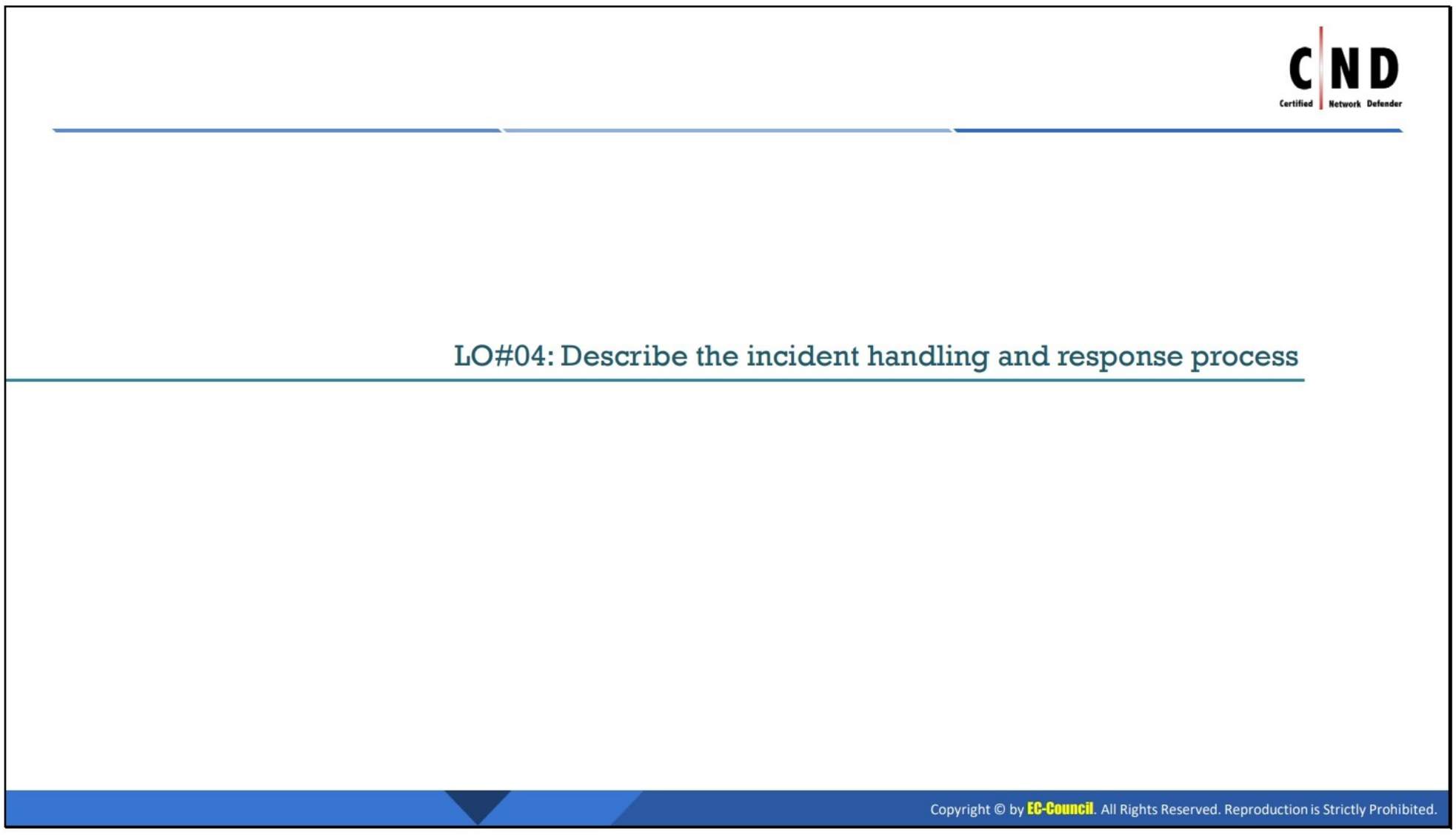
The first responder must not tamper with the state of the suspected device. Altering the state of a system leads to massive changes in the collected evidence. Actions such as system restart and system shutdown force the system to make internal changes, thereby making it difficult for the investigators to appropriately investigate the incident. Any changes made to the state of the suspected device have adverse effects on the quality of the evidence or can completely destroy it. The first responder should always ensure that the system is left in the same state as when the incident occurred.

For example, if the suspected device is ON, the first responder should not turn it off till the time advised by the forensic investigator. If the suspected device is in a shut-down state, the first responder should not turn it ON.



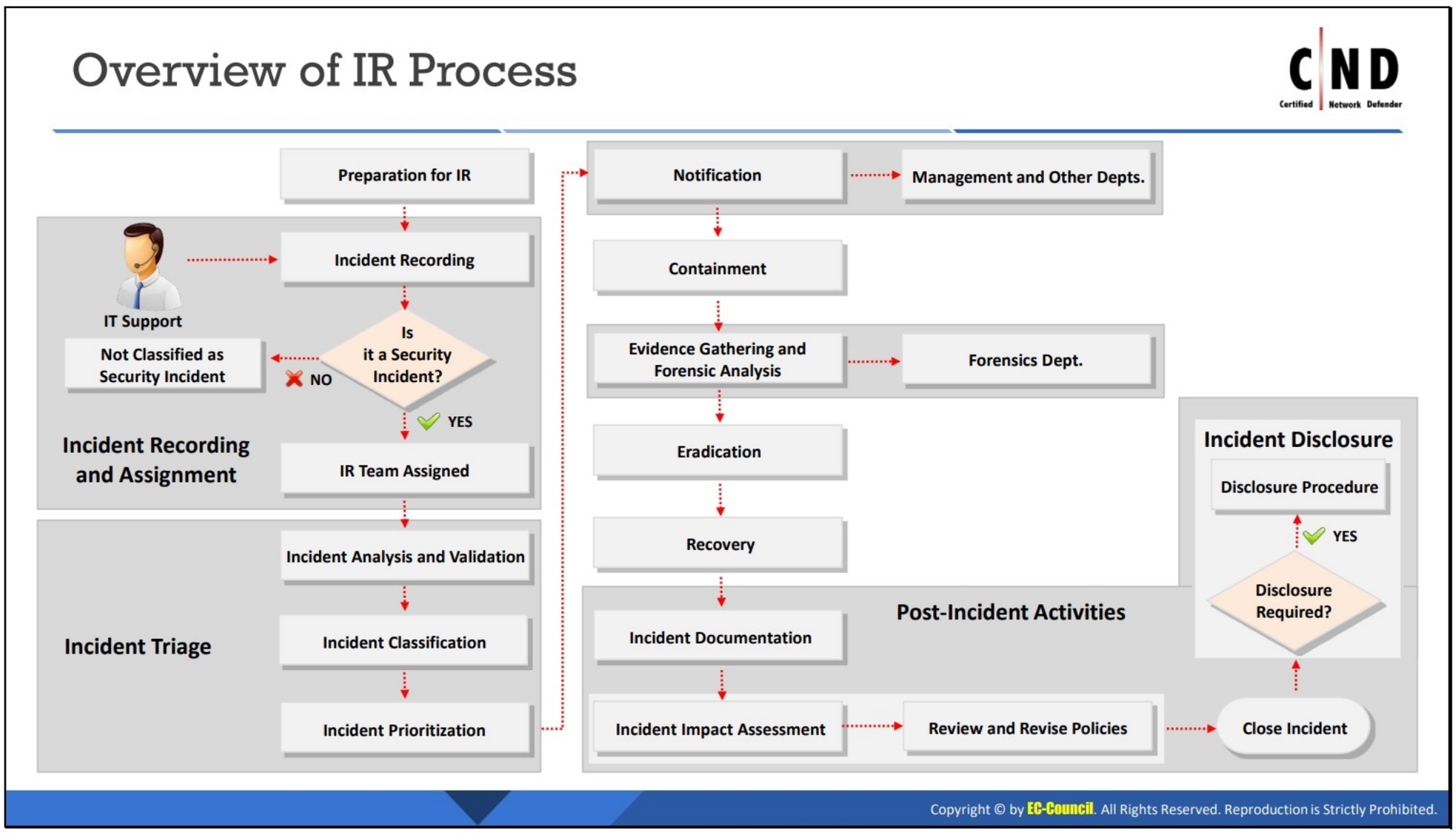
Disable Virus Protection

Anti-virus software installed on a suspected system may create problems when collecting evidence during a forensics investigation. Anti-virus software running on the system may delete or change the state of the evidence as it accesses each file and alters its timestamp. It may even remove the files that offer potential evidence. Hence, security experts suggest that a first responder should disable the virus protection systems as soon as they encounter an incident.



LO#04: Describe the Incident Handling and Response Process

The objective of this section is to introduce you to the complete incident response (IR) process.



Overview of IR Process

The IR process varies across organizations according to their business and operating environments. A pre-defined framework can be utilized to create a sound incident response for the organization.

Each IR process clearly defines some of these rules. Some of them are as follows:

- Restore the normal state of the system in the shortest possible time
- Minimize the impact of the incident on other systems
- Avoid further incidents
- Identify the root cause of the incident and try to rectify it in a short time
- Assess the impact and damage of the incident and try to recover the corrupted or deleted data
- Update security policies and procedures as needed
- Collect evidence to support the investigation to follow

Determining the Need for IR Processes

Cyber-attacks have increased in number as well as in diversity and have become more damaging and disruptive. Since these types of attacks can be harmful and can gather all personal and business sensitive data, it has become necessary to respond to these incidents in an effective and timely manner.

Organizations determine the need of an IR processes based on the current security scenario, risk perception, business advantages of having such processes, legal compliance requirements, other organizational policies, and previous incidents, among other factors.

The IR process will allow the organization to design preventive activities based on the results of risk assessments, but cannot prevent the occurrence of all such incidents. IR processes are necessary for detecting the incidents, reducing any loss and destruction, mitigating the exploited weaknesses, and restoring IT services.

Inputs, complaints, and queries from all stakeholders involved in the organization's business processes affect the decision to establish an IR process. The organization's IRT development project team, executive manager, head of the information security department, or any other person exclusively designated by the management can initiate the IR process.

The main purposes of the IR management and process are as follows:

- **Protect systems**

  It is difficult to ensure high levels of security and place special access controls on various computing resources due to high costs and other constraints. The best strategy for computer systems and network protection is to quickly detect and recover from the security incident. An efficient IR procedure ensures that critical business operations run as they usually would before, during, and after an incident.

- **Protect personnel**

  A swift IR helps in ensuring that no physical damage occurs to human resources due to any workplace incident.

- **Efficiently use resources**

  The resources available for handling an incident used by both technical and managerial personnel are always limited. The best way to utilize these resources is to respond to the incidents as quickly as possible. Information gained from the IR process helps prevent incidents or better handle future incidents and implement strong security for systems and data.

- **Address legal issues**

  IR is also necessary for legal compliance with different laws and acts such as the Health Insurance Portability and Accountability Act (HIPAA) and the Federal Information Security Management Act (FISMA). Efficient incident procedures ensure that the organization remains safe against legal and public liabilities. It is necessary to adhere to the legal principles and practices while responding to incidents. According to the US Department of Justice, it is illegal to use certain monitoring techniques for identifying the incident. The procedures to respond to an incident should guarantee non-violation of legal statutes.

Defining the IR Vision

The IR vision includes the purpose and scope of the planned IR capabilities. This vision features a set of instructions to detect, manage, and respond to an incident. It defines the areas of responsibility and the procedures for handling various security incidents.

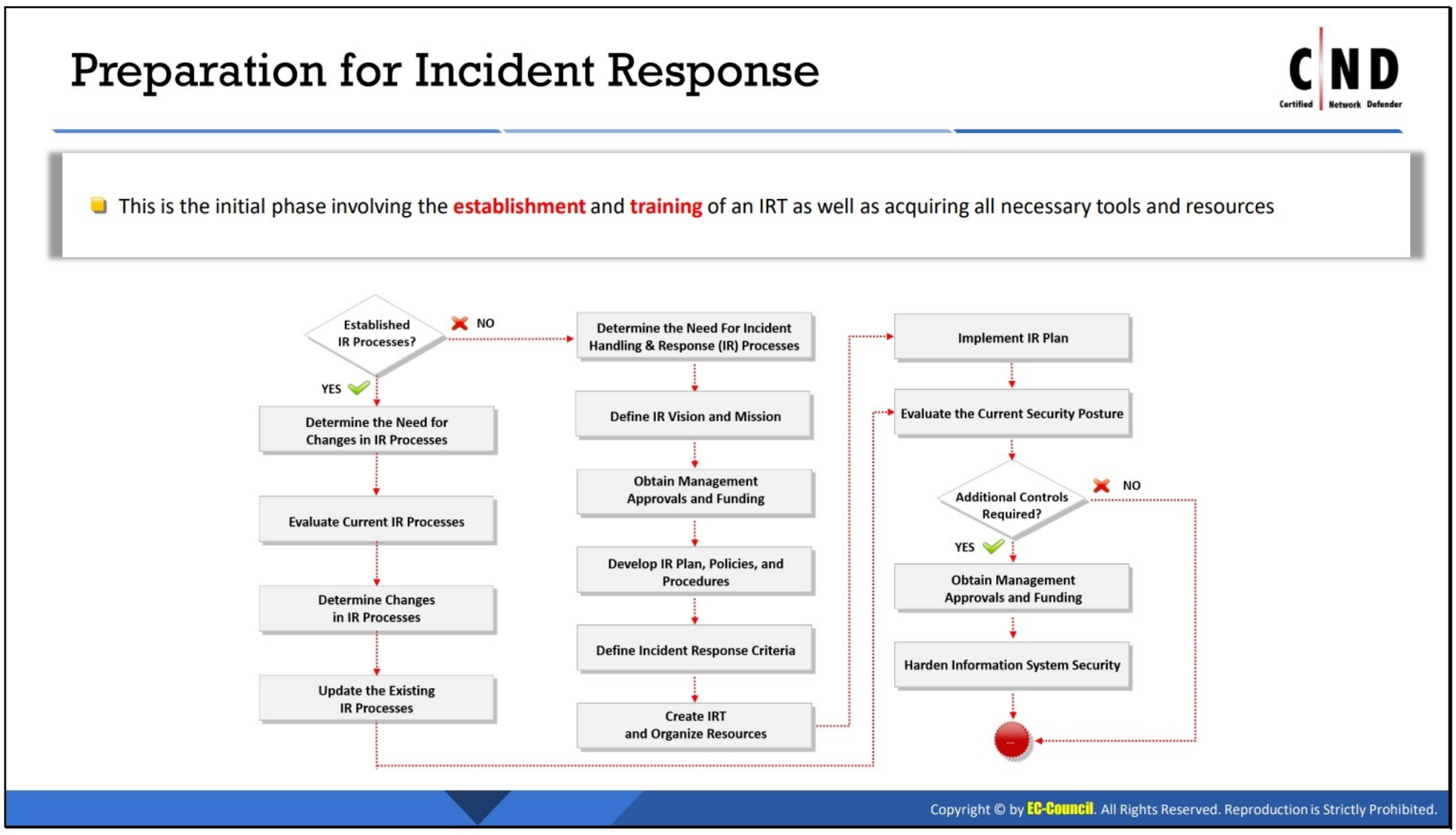
The vision includes the preparation of appropriate documentation and outlines a well-defined approach for handling incidents by taking the necessary preventive actions against any potential threats that may affect the information system. The IR plan covers the following:

- How does information pass to the appropriate personnel?
- How should an incident be assessed?
- Incident containment and response strategy
- How should systems and resources be restored in case of an incident?
- Documentation of the incident
- Preservation of the evidence
- How should the incident be reported to the appropriate personnel?

Key elements in the IR vision statement include the following:

- What IR capability is it aiming to protect?
- What are the short and long-term goals of the IRT?
- What are the services the IRT will offer?
- How will IR capabilities ensure business continuity?
- What are the required resources, and how can the cost be justified with an effective return-on-investment?

Communicate the vision to all stakeholders, and ensure that it is published in an easily accessible repository after the appropriate approvals.



Preparation for Incident Response

Preparation is the readiness to respond prior to the actual occurrence of an incident event. Requirements for preparation include the following.

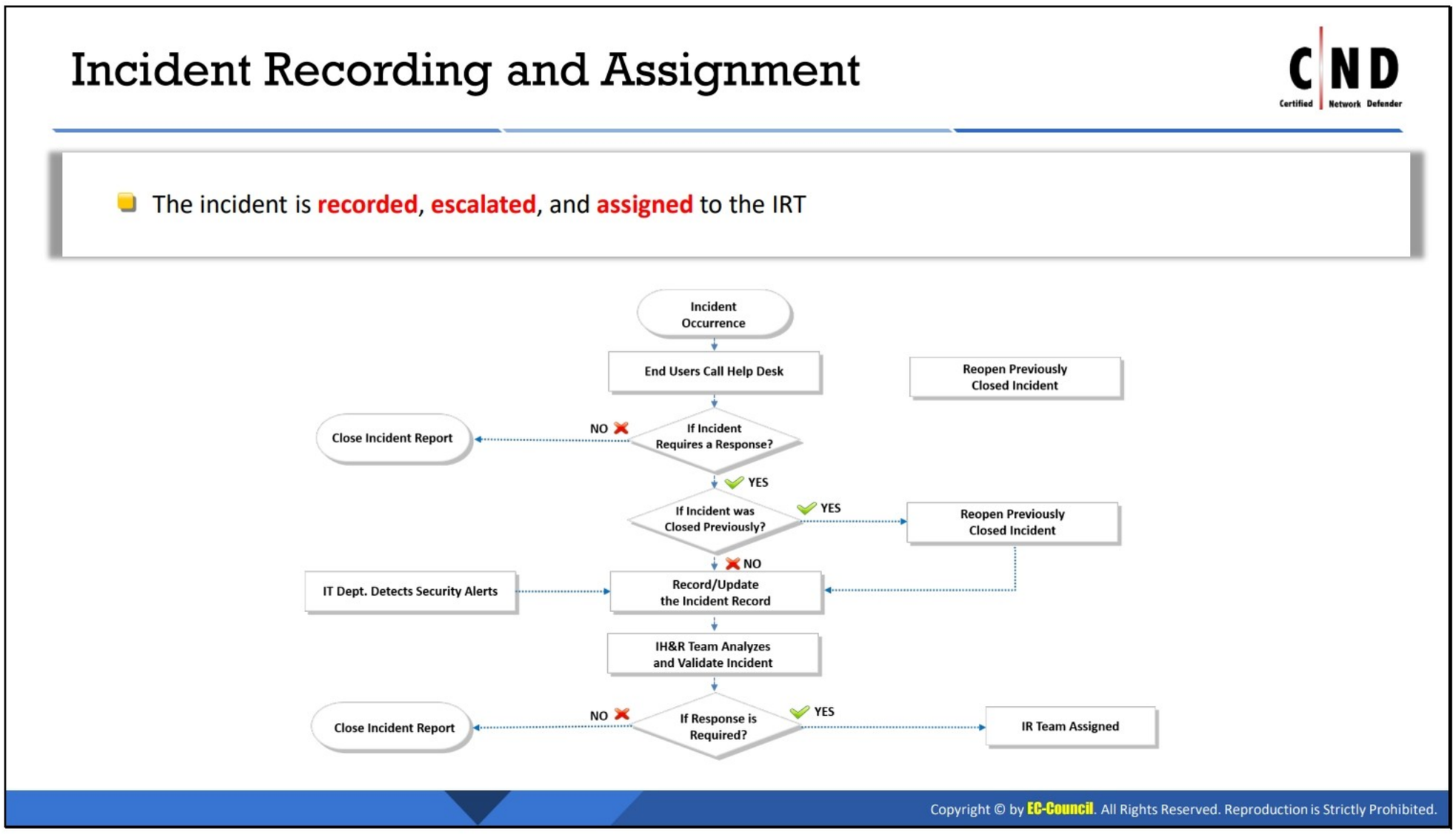
- Establishing a reasonable group of defense/controls depending on the threats posed on the following:
  - Open systems that are vulnerable to attacks
  - Secured systems with no IR
  - Systems dealing with incidents that are to be secured
- Developing a group of methods to deal with incidents:
  - Measures to be considered in different situations by the staff
  - Contact information
  - Keeping information from other neighboring organizations
  - Assigning people to participate in the IR effort
  - Determining risk levels and limits
- Acquiring resources and people to solve problems:

  Monetary resources are required for hardware, software, training, and special equipment for analysis and forensics. Examples of resources include PDAs, safe vaults, Intrusion Detection System (IDS) software, and database server software.

- Developing an infrastructure that supports IR:

  The overall business strategy should be developed to incorporate mechanisms into processes in order to respond to incidents.

  - Line of authority and management should be in place.
  - Defenses/controls specifically matching the resources of the network must be chosen.
  - IR procedures must be followed effectively.
  - Resources should be provided with proper finances.
  - Contact details should be maintained.
  - Evidence of IRs are to be stored.
  - Legal issues should be appropriately addressed.
  - System administrators are responsible for the preparation stage. Their responsibilities include the following:
    - Ensuring password policies
    - Disabling default accounts
    - Configuring appropriate security mechanisms
    - Executing and enabling system logging and auditing
    - Patch management
    - Ensuring proper backups
    - Ensuring the integrity of file systems
    - Identifying abnormal behavior in the system



Incident Recording and Assignment

In an organization, the incident is recorded by IT support personnel who raise an appropriate ticket after a user or employee finds an abnormal change or indicators of an incident on his/her system.

At times, incidents are recoded through Security Information and Event Management (SIEM), IDS, antivirus, and integrity checking software, among others. However, there are certain incidents that are recorded because they are clearly noticeable.

When is an incident recorded?

- Detection of anomaly in data packets sent across the network through the alarm generated by the IDS and firewall
- Antivirus alert being displayed while scanning a computer system
- System and network logs show repeated, unsuccessful login attempts.
- Data are unexpectedly corrupted or deleted.
- Unusual system crashes can indicate attacks. Attackers or intruders can damage the system that contains important data for the network.
- Audit logs show suspicious activity on the systems or network.
- System and security log files log suspicious activity either on the network or security devices.
- A staff member identifies unusual or suspicious activity on a computer system.

- A staff member identifies content on a colleague's computer that violates the organization's security policy.
- Phishing emails are received, or the company's website is defaced.
- History of activities during non-working hours shows that unauthorized access to systems has occurred.
- Social engineering attempts

When an employee of the organization finds abnormal issues pertaining to systems, network, or applications, then they immediately call IT support to inform them about the issue. IT support records the call and tries to identify the issue using the preempted questionnaire that is based on the type of incident. If IT support suspects that the issue is a security incident, then they will assign it to the IR team using a ticketing system.

The tech support or help desk personnel should analyze the event by enquiring for more details and interviewing the victim or the person who reported the incident. This will help in assessing the incident type and whether the victim had accessed some triggers accidentally.

The help desk sends all report and interview details through a ticketing system to the incident handler who assigns a first responder from the IRT members for analysis and validation. The first responder also analyzes the compromised systems, network, databases, and other devices to validate the incident. This helps identify the compromised systems, applications, services, and devices. The first responder lists the compromised elements and updates the incident handler about all incident details through the same ticketing system.

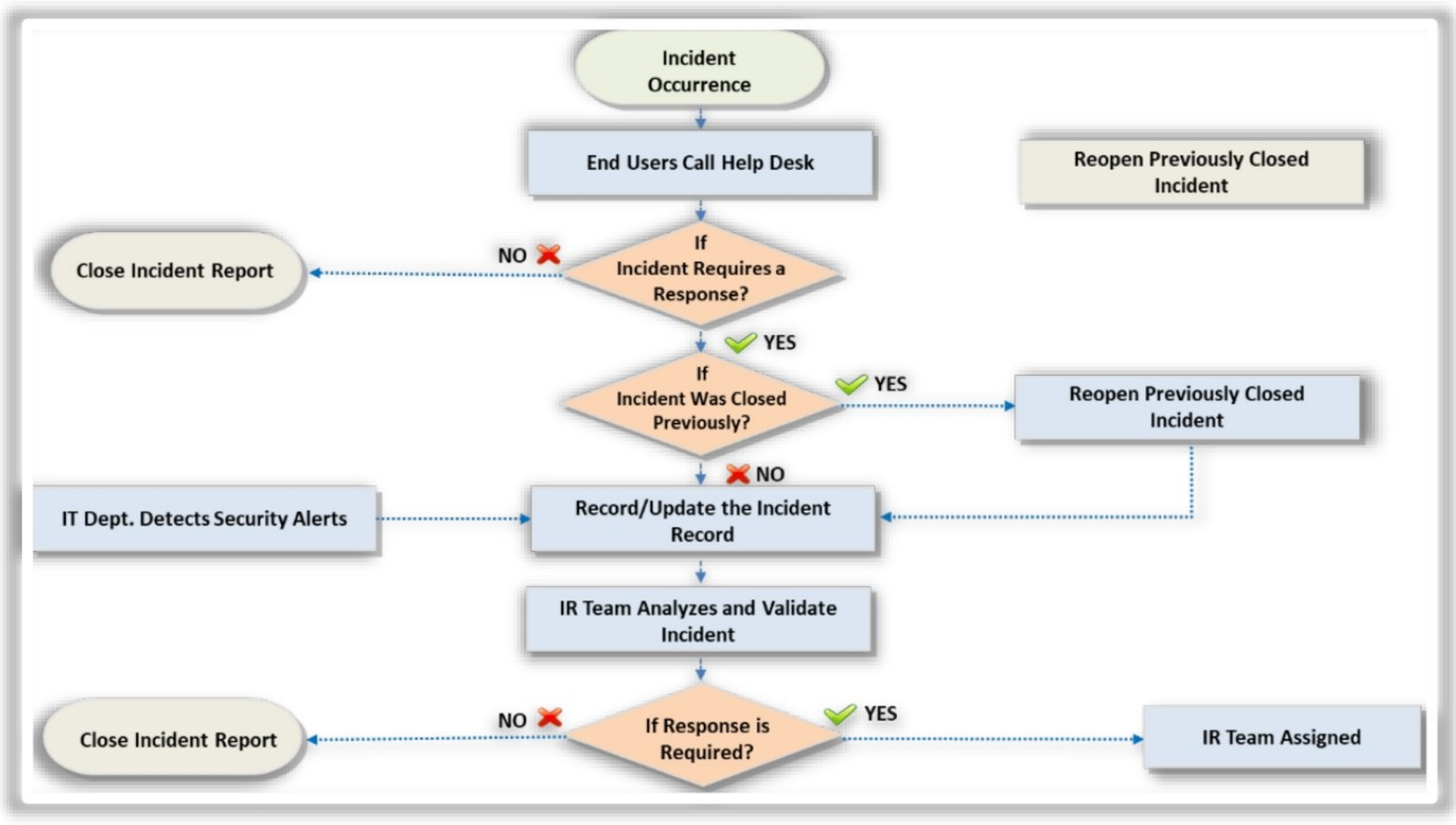
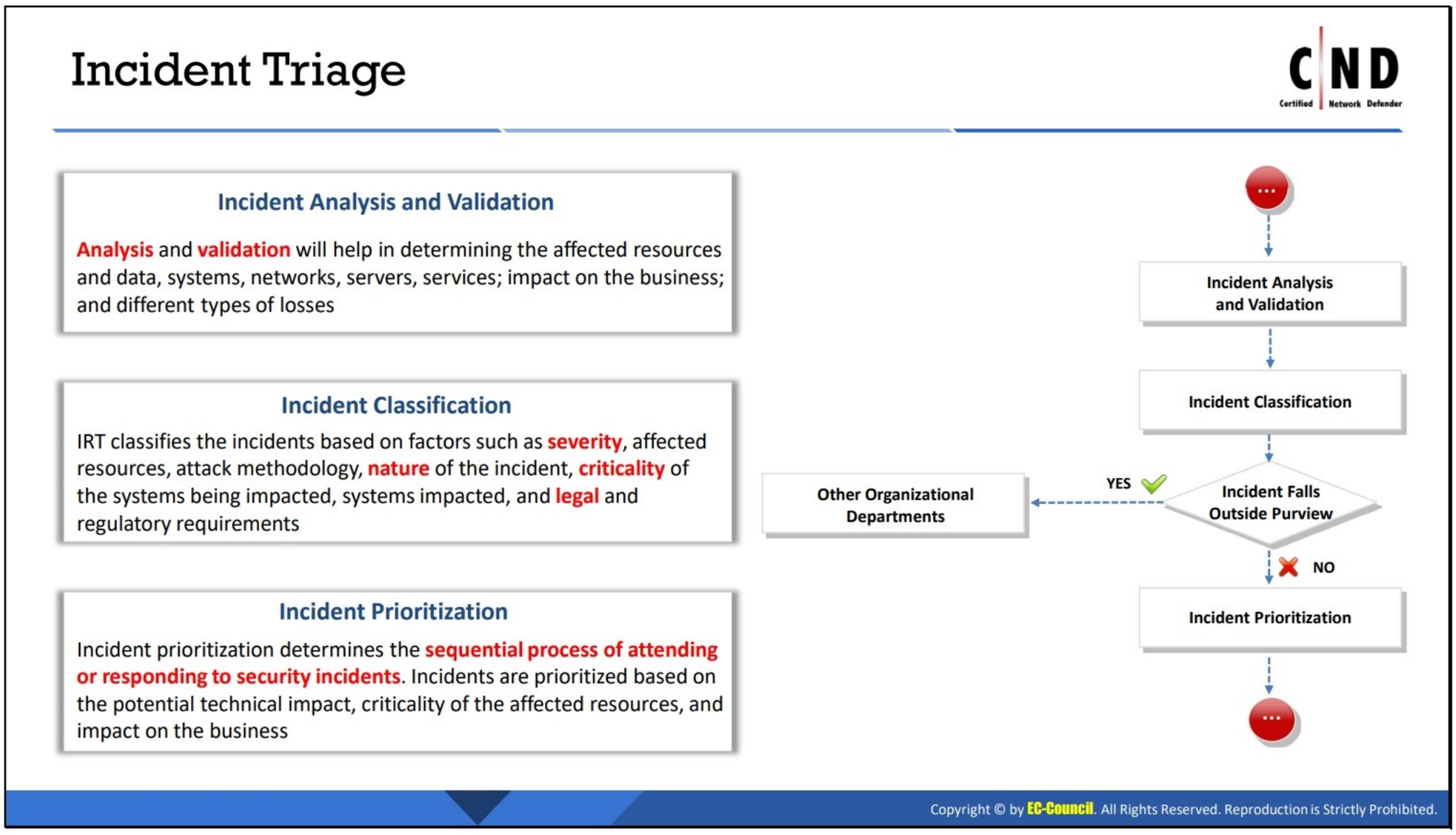


Figure 16.1: Incident Recording at the System

The tech support or help desk personnel try to determine whether the incident is the reflection of any previous incidents and conduct further examination. If it is found to be a previous incident, then they reopen the previously closed incident to update in the IR. Otherwise, they create a record by collecting information about the incident such as security alerts and indicators from

the IT department. This incident record is sent to the IR department to analyze and validate the incident. If they find the incident to be validated, then they immediately assign the IRT for further analysis.

The IRT is responsible for taking over and analyzing the incident with fine sense of judgement making and critical reasoning. The IRT should have a structured approach to efficiently respond to an incident. The IR team manager should classify and prioritize the incidents based on the level (high, medium, or low). The team should classify and attend to the high-priority incidents first, followed by medium- and low-priority incidents, respectively.



Incident Triage

The incident triage consists of three steps: incident analysis and validation, incident classification, and incident prioritization. IRT will first assess the incident details and correlate the indicators with logs and other system files to validate the incident and determine the impacted systems, networks, devices, and applications. They then classify the incident depending on the type of incident. Some of the classification methods include comparing the standard criteria such as networks performance, system behavior, logs, event correlation, data packets, network traffic, files, and applications before and after the incident. Depending on the impacted resources or source of compromise or tools used to attack, the IRT also classifies the incident into types such as endpoint, network, malware, application, and browser incidents. Then the IRT manager prioritizes the incidents based on the level (high, medium, or low). The team attends to the high-priority incidents first, followed by medium- and low-priority incidents, respectively. The prioritization depends on the severity of impact and its effect on the business. Other factors that impact classification include the nature of the incident, criticality of the systems impacted, the number of systems impacted, as well as legal and regulatory requirements. If the incident falls outside the IRT's purview, the IRT contacts other organizational departments. The complete process flow of the incident triage is displayed in the following figure.

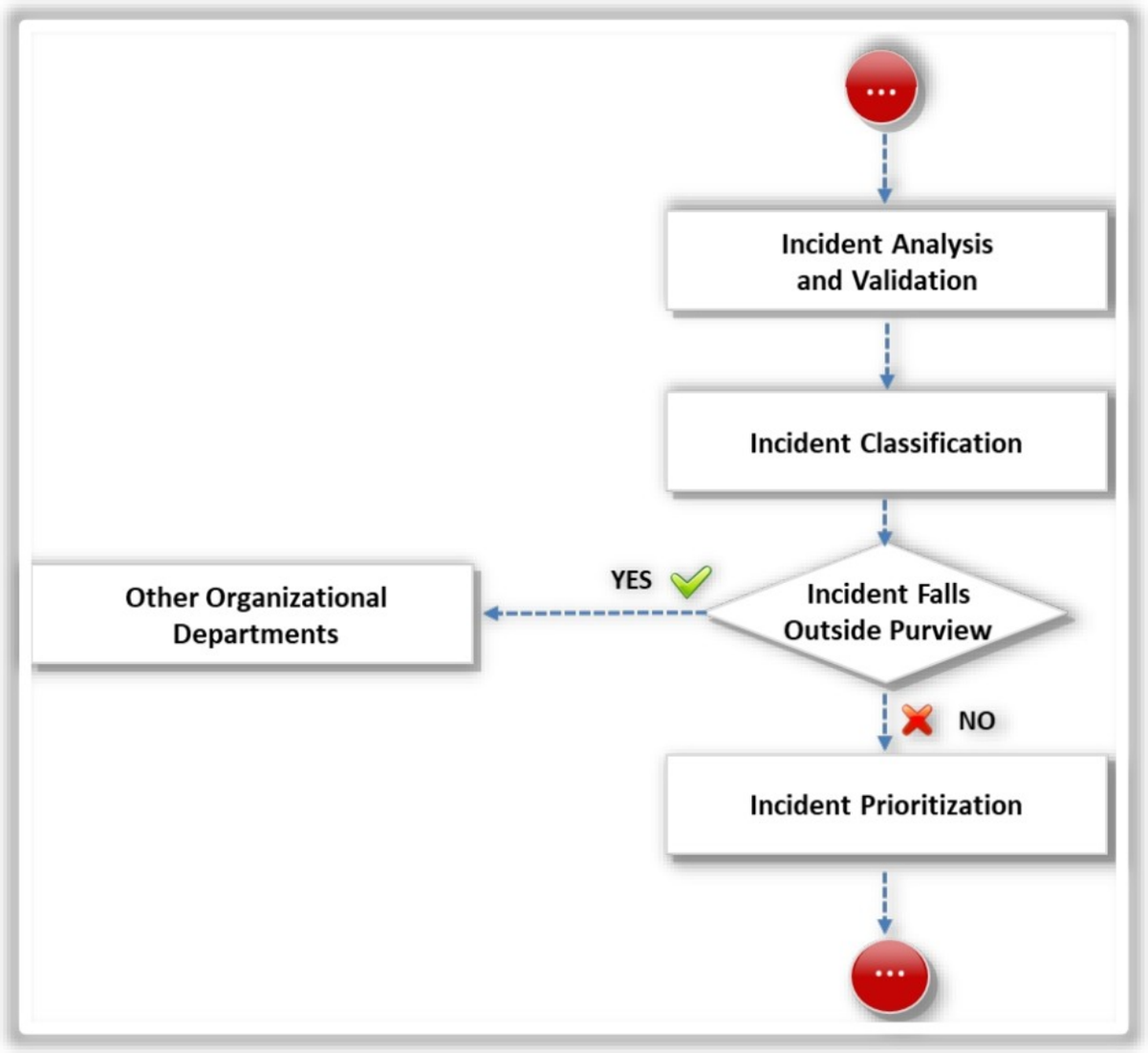


Figure 16.2: Process Flow for Incident Triage

Incident Analysis and Validation

Incident responders need to analyze the indicators of a reported issue to verify if it is an information security incident or an error in the hardware or software components. The IRT should ideally evaluate each indication to determine if it is legitimate. They must find the different sources of indicators, examine the security solutions, verify the system and device logs, and identify the incident and its vectors. Even if an indication is accurate, it does not necessarily mean that an incident has occurred. All incidents cannot be security incidents; some incidents such as web server crash and modification of sensitive files could result from human errors. The incident analysis will help determine if the IRT needs to handle the incident, register the issue and take no further action, or pass it to other teams for processing.

The IRT must perform various validation activities to determine the attack details such as type, vectors, duration, source, and evidence. Analysis and validation will help determine the affected resources and data, systems, networks, servers, services; impact on the business; and different types of losses. The IRT can use this data to classify and prioritize the incidents.

Incident Classification

The classification of an incident depends on the potential targets and the severity of its impact. The purpose of incident classification is to gather all required information to determine its category, time required for resolving, and other criteria.

The role played by the IRT and their activities in this stage are as follows:

- The IRT evaluates the incident details and correlates them with indicators.

- The IRT classifies the incidents based on their severity, affected resources, and attack methodology.

Classifying the information security incident depends on several factors, including the following:

- Nature of the incident
- Criticality of the systems impacted
- Number of systems impacted
- Legal and regulatory requirements

- If the incident falls outside the IRT's purview, the IRT contacts other organizational departments.

The advantages of an effective incident classification are as follows:

- Every incident is correctly forwarded to the respective department.
- Enhances response times as the incidents are routed to the respective department
- Aids in the development of an effective knowledge base
- Increased customer satisfaction

Incident Prioritization

Prioritization of the incident is the most critical decision in the IR process as incidents must not be responded to on a first-come, first-served basis. Incident prioritization determines the sequential process of attending or responding to security incidents. The IRT needs to prioritize the incidents with the highest business impact so that the organization can continue to offer business services with minimal financial losses. The prioritization must depend on the severity of impact, importance of the compromised resources, disrupted operations, and losses incurred due to the incident. The incident responder is responsible for prioritizing the compromised elements and sorting them according to the most important devices or applications required for business continuity. The incident responder then assigns a team to respond to the incident by evaluating the impact and suggesting methods of detection and containment.

Prioritization will also help the incident responder manage the available IR staff and resources. The incident responder assigns the level of priority, predefined criteria and requirement, and urgency in restoring the compromised resource. Working on the most severe incidents will also help the organization minimize business disruption and help reduce financial and reputational loss. It can also reduce the amount and time spent on IR functions such as containment, eradication, and recovery. It will help in scheduling the tasks and increasing the ease of the process of reporting the status to stakeholders and customers.

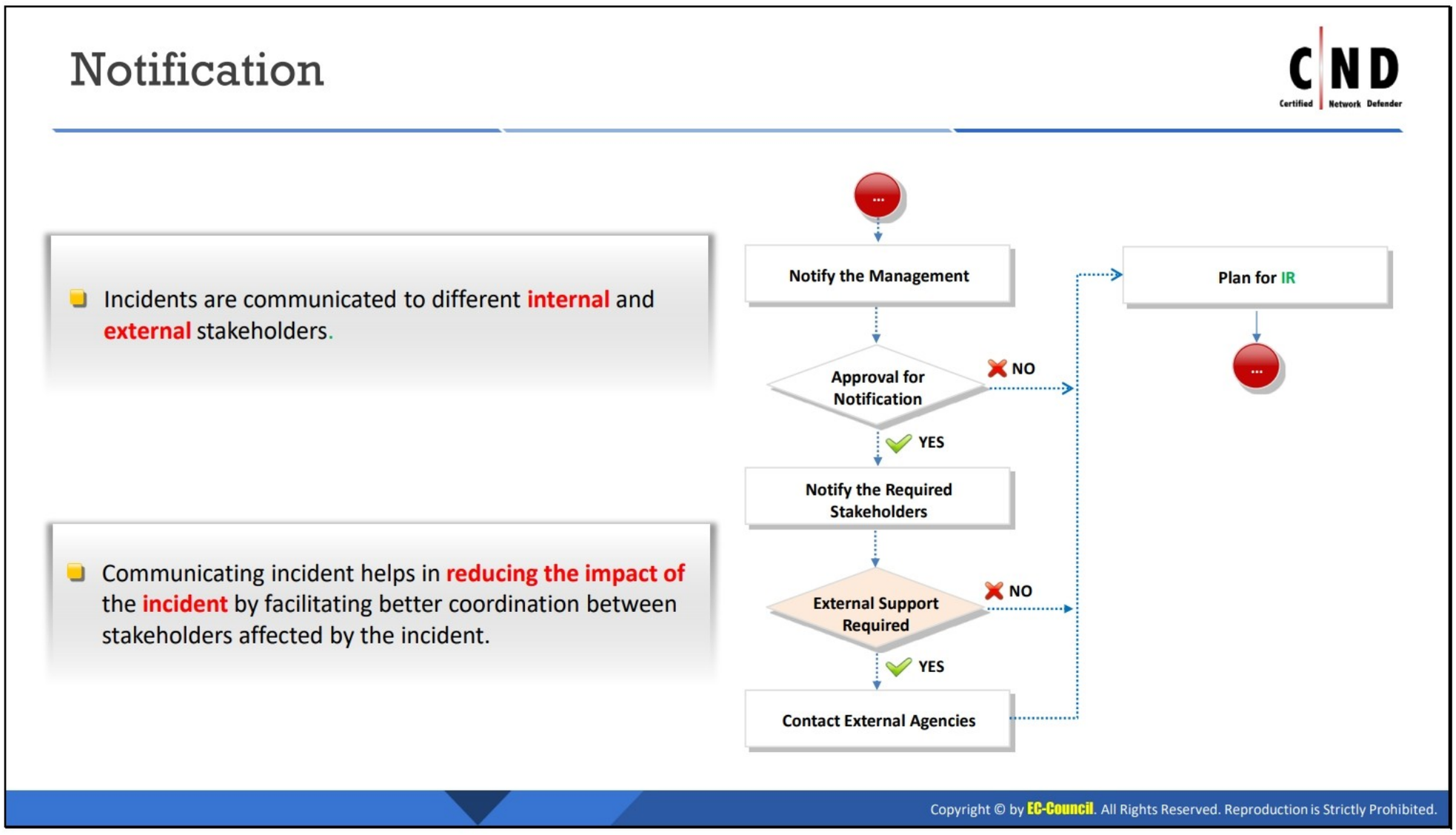
With the emerging number of diverse cyber security incidents, assigning a category to an incident has become an essential step of the incident management process in order to prioritize the incident. Once the incident is identified in an organization, the incident responder will categorize it. Organizations adopt a common set of terminology and categorize the incidents to clearly communicate security incidents and events across different departments in an organization or to

members of an IRT. Incident categorization enables the team to prioritize the incidents and focus on the incidents that require more attention.

The IRT should consider two basic elements in prioritizing incidents.

1. **Impact:** Offer an account of how severe an incident can be for the organization. It is measured in terms of the number of systems impacted by the incident, which increases the number of idle employees and, in turn, directly affects the organizational productivity.
2. **Urgency:** Usually defined in terms of the service level agreement (SLA). If an incident is raised within an organization, it should be resolved at the earliest opportunity.

The importance of impact and urgency vary across organizations. However, generally, both impact and urgency have three levels, namely, high, medium, and low.



Notification

Communication plays a major role in swiftly responding to an incident. It helps in reducing the impact of the incident by facilitating better coordination between different stakeholders affected by the security incident. Communicate the IR process and results to the IRT members, so that they can understand the type of response and their responsibilities when responding to the incident. The detailed process flow of notification is displayed in the below figure:

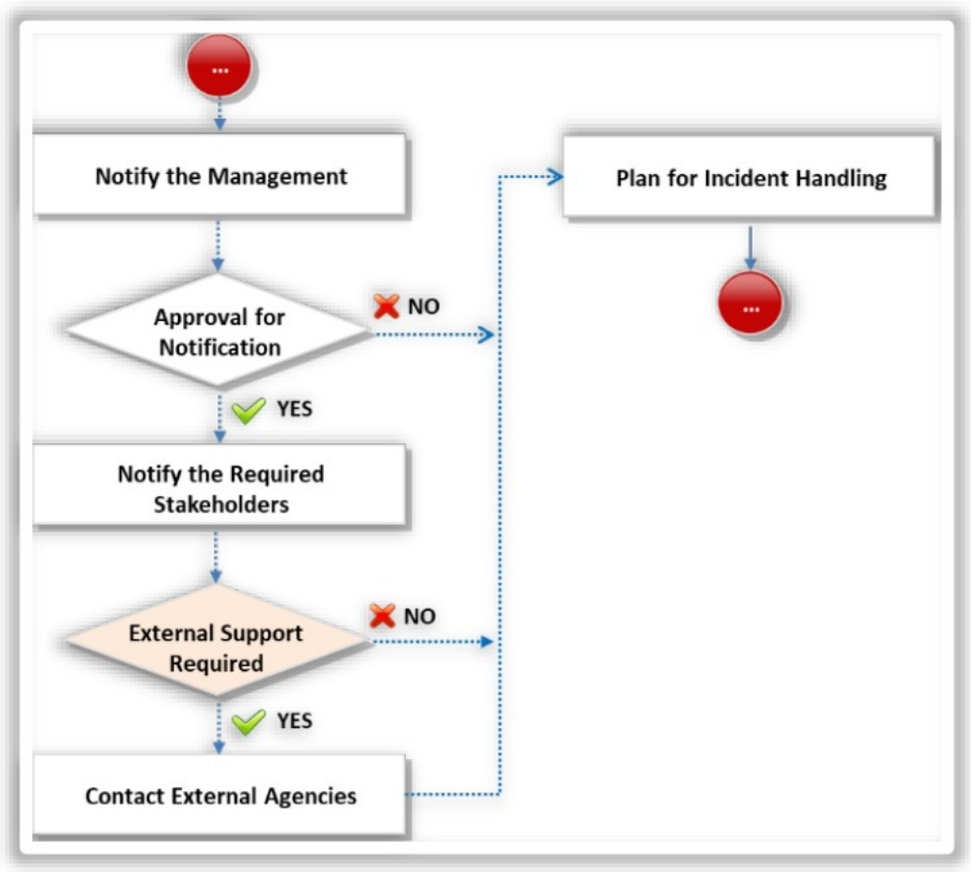


Figure 16.3: Process Flow of Notification

Incident responders must communicate about the severity of the incident with the management or authorized persons to gather relevant approvals for performing IR procedures. The

communication would include the first report, initial processes performed to assess the situation, detection methods applied, impacted resources, and management strategy. The IRT should discuss the incident with a legal representative to file a lawsuit against the perpetrators.

After obtaining the approval, the IRT will communicate the relevant matters about the incident with the necessary stakeholders. All employees and other stakeholders must communicate with the IRT whenever they suspect a security breach. The IRT lead should discuss the breach with core team members and other members of the organization to respond to the incident effectively.

Incident responders can communicate a part of the situation to an external party after approvals from management if they need external support for responding to the incident.

After controlling and mitigating the incident, the IRT can disseminate the details of the incident and lessons learned in the organization and media to create awareness. Depending on the circumstances of the incident, the goal of the response strategy is to examine the most appropriate response procedure. The response plan should consider the political, technical, legal, and business factors of the incident. A response strategy generally depends on the circumstances of the incident.

The factors that affect the resources required to investigate an incident include the following:

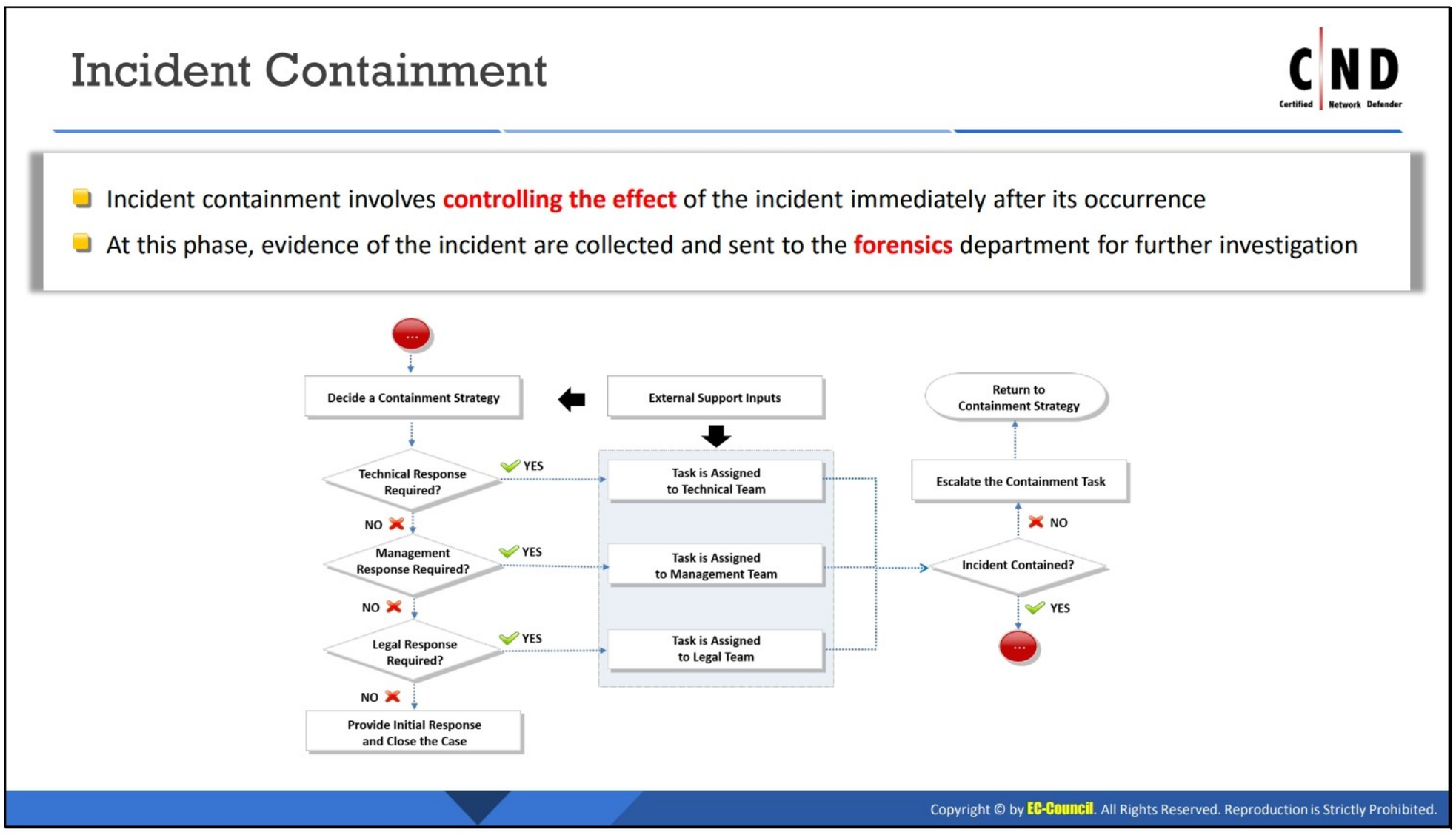
- Forensic duplication of the related computer systems
- Criminal referral
- Civil litigation
- Other aspects
  - What is the range of impact of the incident on systems?
  - How sensitive is the compromised or stolen information?
  - Who are the attackers?
  - Is the public aware of the incident?
  - What unauthorized access level have the attackers gained?
  - What skills do the attackers have?
  - What is the total downtime for the system and the user?
  - What is the total loss in dollars?

The information gathered during the initial response is important for selecting a response strategy. Before selecting the response strategy, reinvestigate the details of the incident.

An organization that is suffering from a security incident needs to notify the appropriate internal and external IRT to minimize any repercussions of the security event.

The IRT's role in the notification and planning includes the following.

- **Notifying management**: The IRT is responsible for notifying the management about the incident that occurred. The management should also be informed about the effects of the incident.
- **Communicating the incident**: Before communicating any information about the incident, the IRT should obtain documented approval from the management. The incident information should not be hidden from the stakeholders and other people. People that are likely to be affected by the incident need to be informed about the incident.
- **Disclosing the details of the incident**: Apart from broadcasting about the incident, the IRT should also seek approval for disclosing the details of the incident. Disclosing the details of an incident is important, as certain stakeholders of the organization need to be aware of these details.
- **Approval denied:** If the management does not provide their approval for disclosing the incident details, the IRT should proceed with the procedure of IR.
- **External support:** Before proceeding with an in-depth investigation of the incident, the IRT checks if external support is required to handle the case.
- **External support required:** If external support is required, the IRT contacts external agencies for input.
- **IRT and external support:** Once the external support joins the investigation of the incident, the IRT and the management team proceed with handling the incident and the response plan.



Incident Containment

The IRT plays a significant role in reducing an incident's magnitude or complexity in preventing further damage to the organization. Containment focuses on limiting the scope and extent of an incident. The aim of the containment stage is to reduce any losses and/or damages from the attacks by mitigating vulnerabilities. If the systems, networks, or workstations are compromised by a security incident, the IRT must determine whether to shut down the system, disconnect the network, or continue with operations in order to monitor the system's activities. The response to all these situations depends on the type and magnitude of the incident.

Common techniques used in the containment phase are as follows.

- **Disabling of specific system services**
  - Disable system services temporarily in order to reduce the impact of the incident and to continue system operations.
  - When an unknown vulnerability affects a computer, it is removed from the network until the problem is rectified.
  - Change the passwords, and disable the account.
  - Change passwords on all systems that interact with the affected system, so that there are no more infections.
- **Complete backups of the infected system**
  - Back up data on the affected systems to reduce the damage during IR. Use a system backup for further investigation of the incident.

- **Temporary shutdown of the compromised system**
  - If the compromised computer systems have no alternate options to handle the situation, then shut them down temporarily. This shutdown limits the damage caused by the incident and provides extra time to analyze the problem.
- **System restoration**
  - Replace the recovered computers with a trusted and clean backup copy.
  - Identify the incident sources such as vulnerabilities, threats, and access paths, and patch everything before restoring the system.
- **Maintaining a low profile**
  - When detecting network-based attacks, be careful to not tip off the intruder. This is because the intruder might do more harm to other systems in the network and/or erase everything they can to eliminate the chances of being traced. Maintain standard procedures, including continuing to use the IDS and the latest antivirus and anti-spam software.

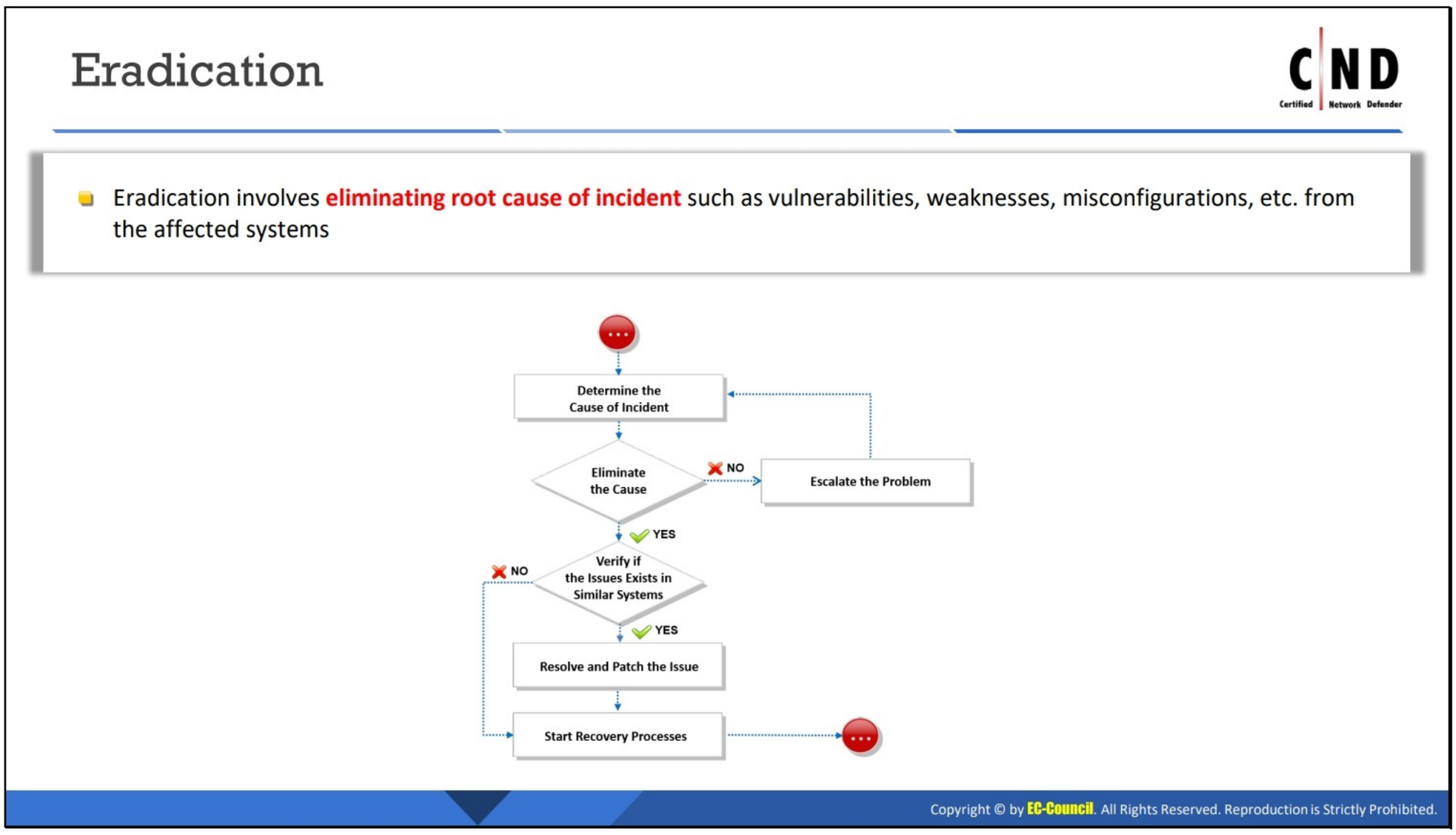
Guidelines for Incident Containment

The main purpose of the containment strategy is to control the effects of the attack and restore the information system to its normal state. This is vital to ensure the organization's business continuity. A few key considerations for an IRT in this crucial stage are as follows.

- **Compromised code:** Compromised code can lead to a data breach, increasing the chances of an intrusion. It is important for the IRT to be cautious while working with the compromised code. A minor mistake can lead to code replication and can further affect the organizations' network and functioning.
- **Safe storage:** Data should be stored in a safe location so that any intrusion or external threat does not affect or alter it.
- **Acquiring logs:** The IRT team must actively acquire and retrieve all system and router logs before, during, and after the time of occurrence of the incident. This will help the team analyze the changes the network or system underwent that caused the incident to occur.
- **Identifying risk factors:** It is important to identify the various risks if operations are to be continued.
- **Informing administrators and system owners:** The IRT should keep the administrators and system owners updated about the latest security threats that can affect the system. This helps implement preventive measures, avoiding the occurrence of a major incident.
- **Strong password policy:** After the IR is successfully completed, users must change their passwords. Administrators must implement a strong password policy in the organization.
- **Maintaining records:** It is important to maintain records of every action performed by the user or the system owners. Auditing and monitoring must be performed by administrators on a timely basis.

Organizations face a lot of problems when incident containment guidelines are not in place. For example, if an organization that is not well-prepared gets infected and then attacked by malware, it cannot handle the situation as effectively as an organization that follows incident containment guidelines. At times, this lack of preparedness allows malware to spread like wildfire. In these cases, people act haphazardly to find solutions for such incidents, and none of them have any ideas about how to deal with it. This delay in finding a solution can bring an organization's network, information systems, business, and reputation to the ground. Without proper guidelines in place, network administrators implement stopgap actions, trying everything they can to find the appropriate solution. This can cost the organization vast amounts of money and time. This situation can be avoided if an organization follows certain guidelines.

- **Dedicated team:** A team containing technical experts must be dedicated to handle any type of security issue. This team acts as the first responder during the time of an incident.
- **Securing the affected area:** In order to avoid any new changes being affected, the affected area must be secured. Review the information at the beginning of the identification phase.
- **Installation of honeypots:** Honeypots are invisible traps that play a vital role in enhancing security. Implementing honeypots in the network will help network defenders trap the attacker.
- **Following standard procedures**: Documented procedures are required, which the management, the IRT, and administrators must follow.

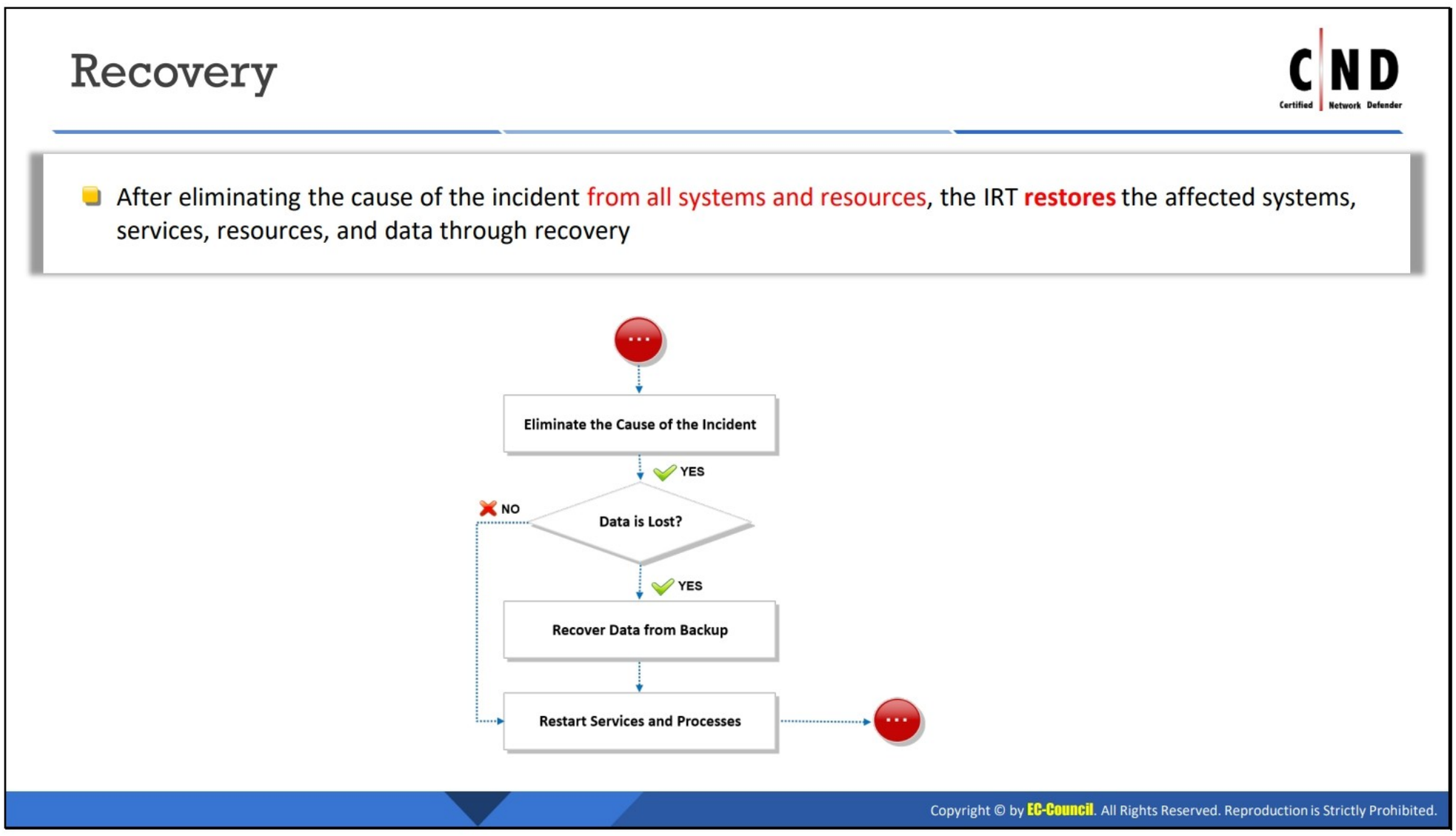


Eradication

In the eradication phase, the IRT should remove or eliminate the root cause of the incident and close all attack vectors to prevent similar incidents in the future.

The following countermeasures will help the IRT eradicate the incidents:

- Update the antivirus software with new malware signature and patterns.
- Install latest patches on systems and network devices.
- Conduct independent security audits.
- Check for policy compliance and update obsolete policies and procedures.
- Disable any unnecessary services.
- Change the passwords of all compromised systems, accounts, and network devices.
- Eliminate the access paths and exploits.
- Install updated operating systems, software, and services in compromised systems only after removing traces of attack.
- Rebuild the affected or compromised systems, servers, databases, and networks.
- Validate the effectiveness of all corrective steps or countermeasures.



Recovery

Recovery is the process of restoring the lost data from backup media. During this process, the IRT has to ensure that the backup does not have traces of malware or attack vectors before restoring. The time it takes to recover a system generally depends on the extent of the security breach. Recovery involves various techniques such as network perimeter security, tightening user ID credentials, effective patch management, renewed file and software versions, and rebuilding the systems. After recovering all lost data, the IRT must restart all withheld processes and services.

Recovering a system after an incident generally depends on the extent of the security breach. The IRT should decide whether to restore the existing system or completely rebuild it, for which they can utilize the system backup. The two steps in systems recovery are as follows.

- **Determine the course of action**

  Devise various strategies for system recovery based on the impact of the incident, and select an appropriate plan after considering the availability of resources, the criticality of the affected systems, and the results of a cost-benefit analysis.

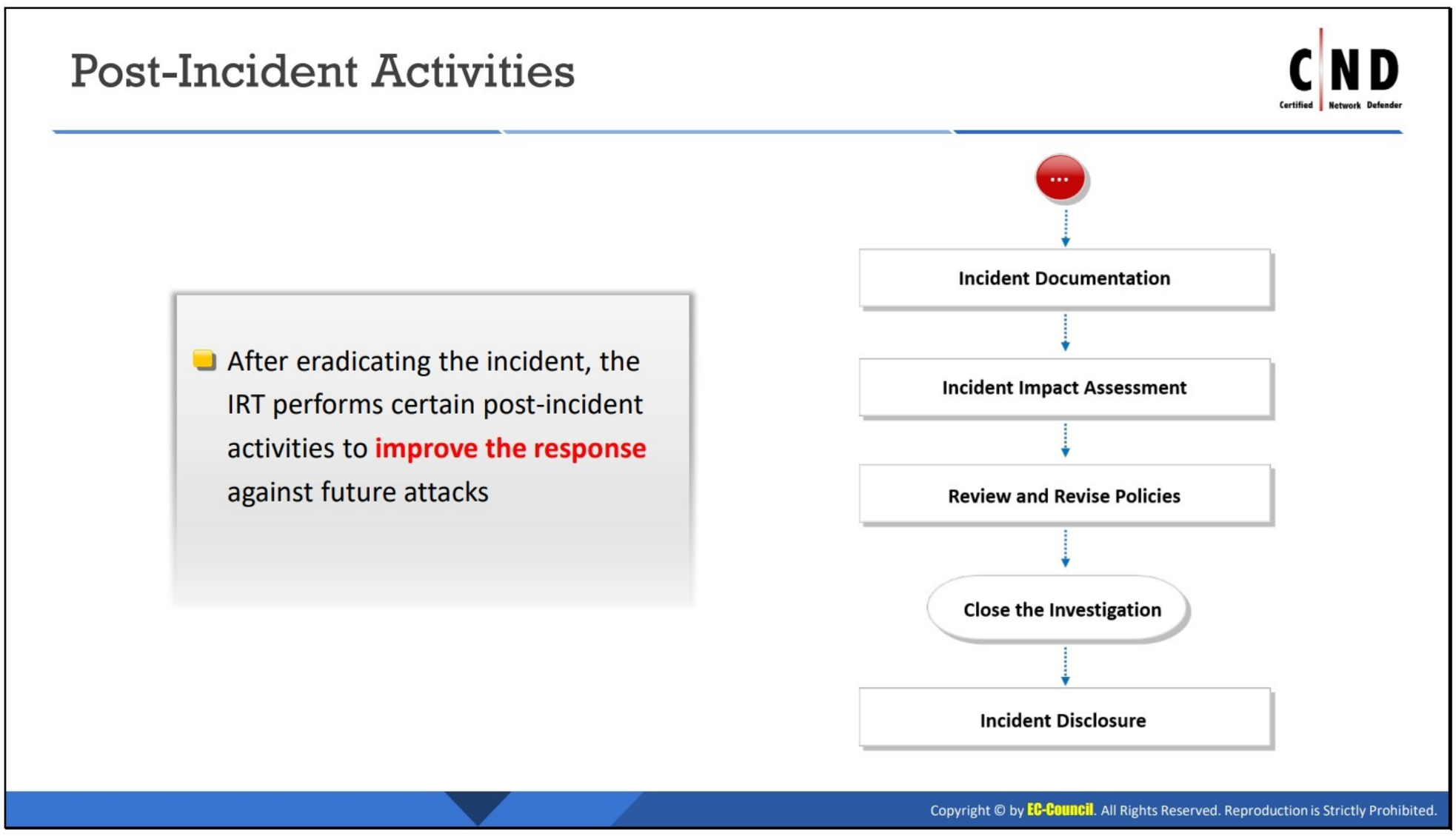
- **Monitor and validate the systems**

  Monitoring and validating systems ensures that the recovered systems do not have any traces of incident causes and are operating in normal conditions. Validation also involves checking the integrity of the restored information from a backup. Conduct regular vulnerability assessments and penetration testing to monitor the system's behavior and the possible vulnerabilities in the system or network. Monitor the system for potential back doors that can result in data loss.

Some of the actions that the response team must perform during the recovery stage include the following.

- Rebuild the system by installing a new operating system (OS).
- Restore user data from trusted backups.
- Examine the protection and detection methods.
- Examine the security patches before installation and enable system logging.

The IRT must determine the integrity of the backup file by reading its data and verifying its integrity before restoring it on the systems. Verify the success of the operation and normal condition of the system after installing the backup. Monitor the system using network loggers, system log files, and potential back doors after installation and during usage.



Post-Incident Activities

After eradicating the incident, the IRT must perform certain activities to improve the response against future attacks. Post-incident activities refer to the actions and precautions that the organization and response team perform to be better prepared to respond to future incidents. In this stage, the team discusses all limitations/problems it faced during the response functions and tries to eliminate them.

Post-incident activities help evaluate and improve the effectiveness of the IR processes. Post-incident activities enable the responders to assess lags in security posture, settings, and configurations across the organization. They also aid in suggesting measures and security products to strengthen the security and review the policies.

Organizations should conduct meetings with the staff and other relevant stakeholders to understand the lessons learned and improve the shortcomings. These activities will help evaluate and improve the effectiveness of the IR processes. It involves updating policies, procedures, security posture, settings, and configurations across the organization to build a robust network.

To learn from the experience, the IRT must create a document about the incident that could reveal details about the incident, vulnerabilities exploited, response measures implemented, results, pitfalls in the response process, drawbacks in communication and management, and so on, and try to overcome them. The IRT should document every step of the IR as well as the lessons learned. The IRT must communicate the updates and new implementations with clients, customers, management, and stakeholders.

The following figure displays the overall process flow of post-incident activities.

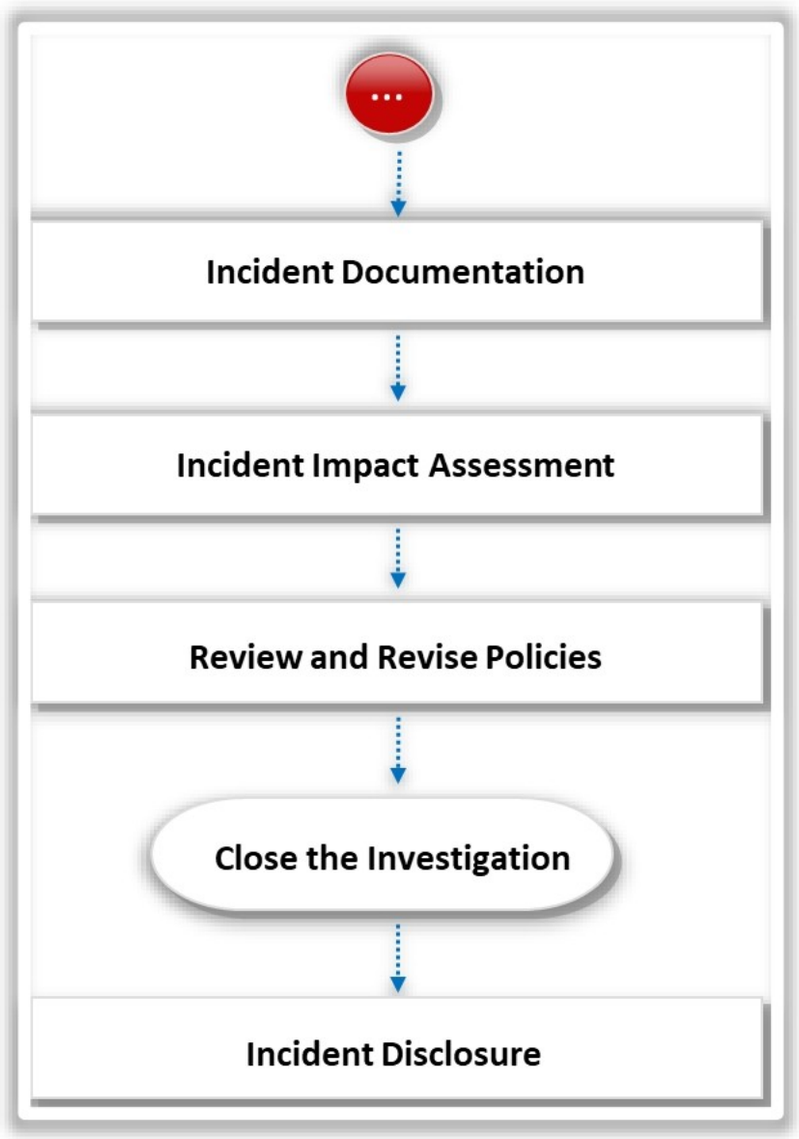
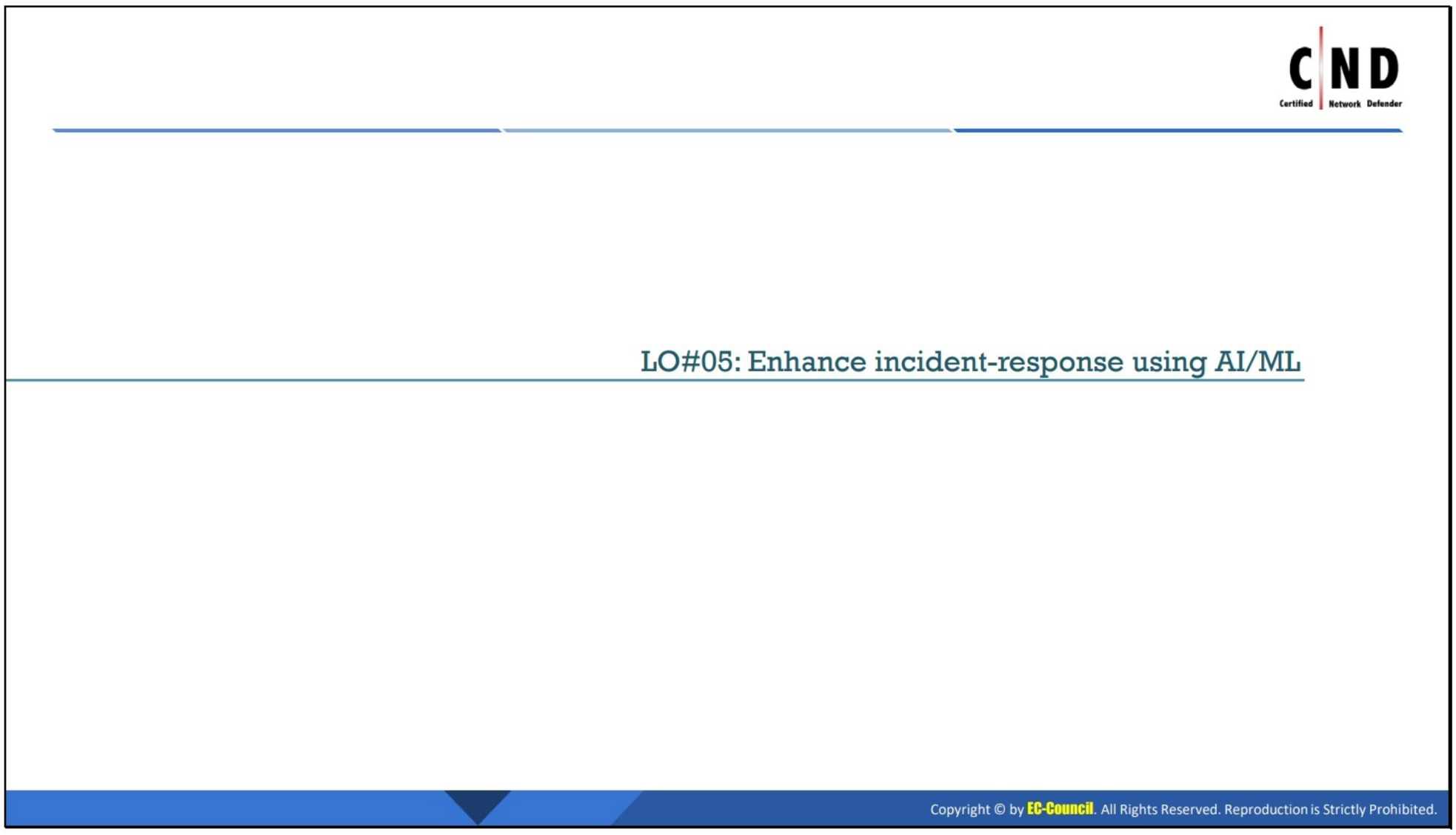
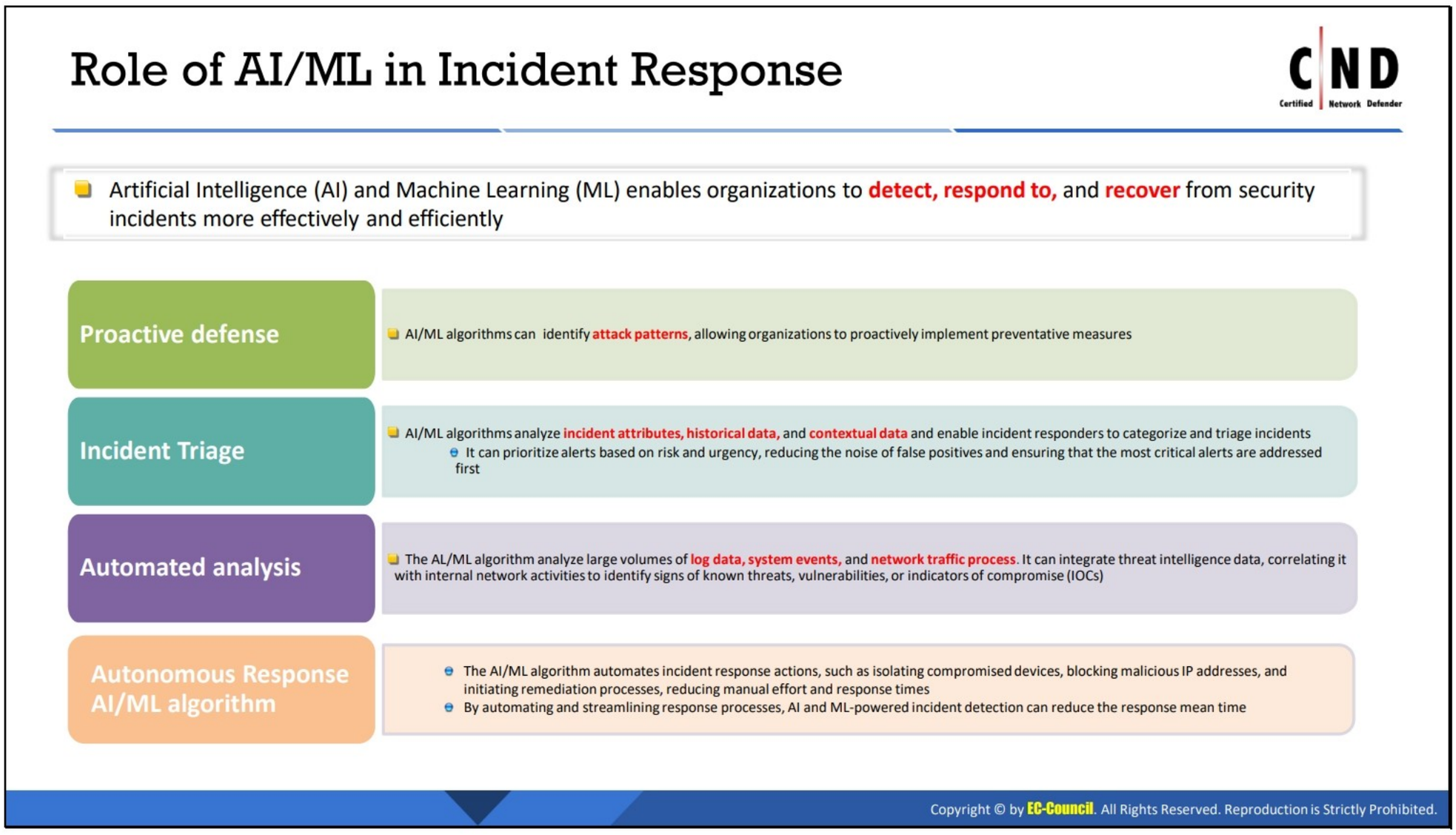


Figure 16.4: Process Flow of Post-Incident Activities



LO#05: Enhance Incident-response using AI/ML

In the ever-evolving landscape of cybersecurity, enhancing incident response has become imperative for organizations seeking to fortify their defenses against an array of threats. Artificial Intelligence (AI) and Machine Learning (ML) stand at the forefront of this evolution, offering innovative solutions to revolutionize traditional incident-response mechanisms. By harnessing the power of AI and ML, organizations can not only detect and respond to security incidents more swiftly but also bolster their resilience through automated analysis, predictive insights, and continuous learning. This section empower security teams to stay ahead of sophisticated threats and respond to the cyber incidents on their digital infrastructure.s



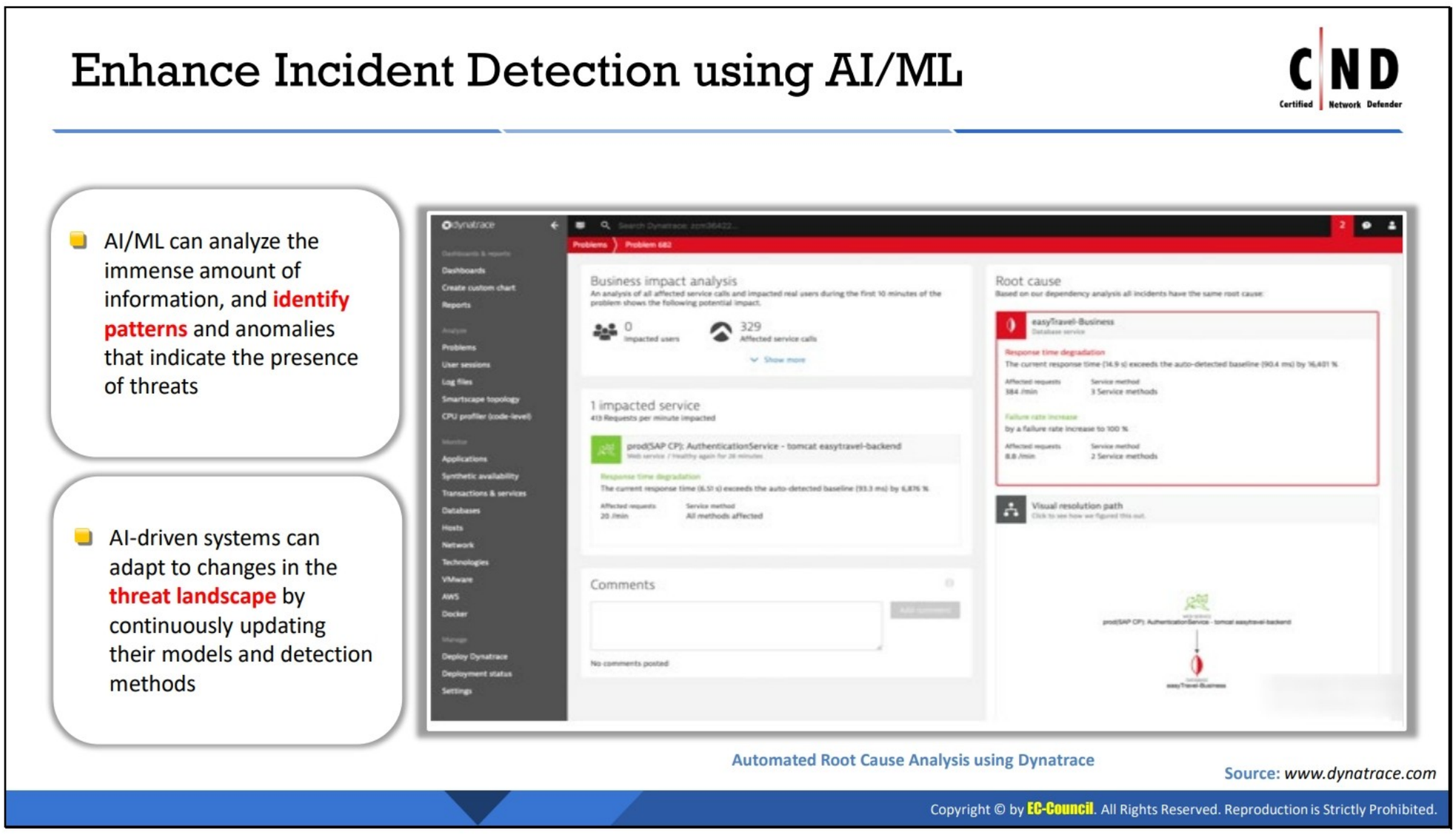
Role of AI/ML in Incident Response

Cybersecurity threats continually evolve, with organizations facing an increasing number of attacks. Technologies such as Artificial Intelligence (AI) and Machine Learning (ML) enable organizations to detect, respond to, and recover from security incidents more effectively and efficiently. Compared to manual methods, incident response systems powered by AI and ML are faster and less susceptible to human errors.

The advantages of using AI and ML in incident response include:

- **Proactive defense**: Through the analysis of historical security and threat intelligence data, AI/ML algorithms can identify attack patterns, enabling organizations to take proactive steps, such as software upgrades, vulnerability patching, and access control rule updates, to prevent potential threats. This empowers an organization to maintain a proactive stance and stay ahead of potential attackers.
- **Incident triage**: AI/ML algorithms can assist in incident triage and prioritization by considering severity, potential impact, and relevance. Autonomous response systems, through the analysis of incident attributes, historical data, and contextual information, can categorize incidents and allocate resources accordingly. It can prioritize alerts based on risk and urgency, reducing the noise of false positives, and ensuring that the most critical alerts are addressed first. This guarantees that crucial incidents are promptly addressed, all the while optimizing the distribution of security team resources.

- **Automated analysis**: AI/ML algorithms can streamline automated investigations by analyzing extensive log data, system events, and network traffic. They are also capable of processing threat intelligence data from various sources to extract insights into the latest attack methods and vulnerabilities. AI can understand attack vectors and implement preventive measures to mitigate the likelihood of similar incidents occurring in the future.
- **Autonomous response AI/ML algorithm**: The AI/ML algorithm automates incident response actions, such as isolating compromised devices, blocking malicious IP addresses, implementing security patches, disabling compromised user accounts, and initiating remediation processes, reducing manual effort and response times. By automating and streamlining response processes, AI and ML-powered incident detection can reduce the response mean time.



Enhance Incident Detection using AI/ML

AI/ML significantly enhances incident detection by utilizing advanced machine learning algorithms to analyze large volumes of data in real-time. These algorithms detect patterns and anomalies indicative of potential threats, enabling organizations to swiftly and efficiently identify and respond to cybersecurity challenges.

AI-driven systems adapt to the evolving threat landscape by continuously updating their models and detection methods. These systems are equipped to handle ever-changing threats as machine learning models consistently learn from new data, identifying new patterns and behaviors associated with emerging cyber threats. This adaptability positions organizations to stay ahead of cybercriminals and continuously improve their cybersecurity measures.

Implementing AI/ML automation technologies for incident detection, particularly those offering anomaly detection through root cause analysis, further strengthens this capability.

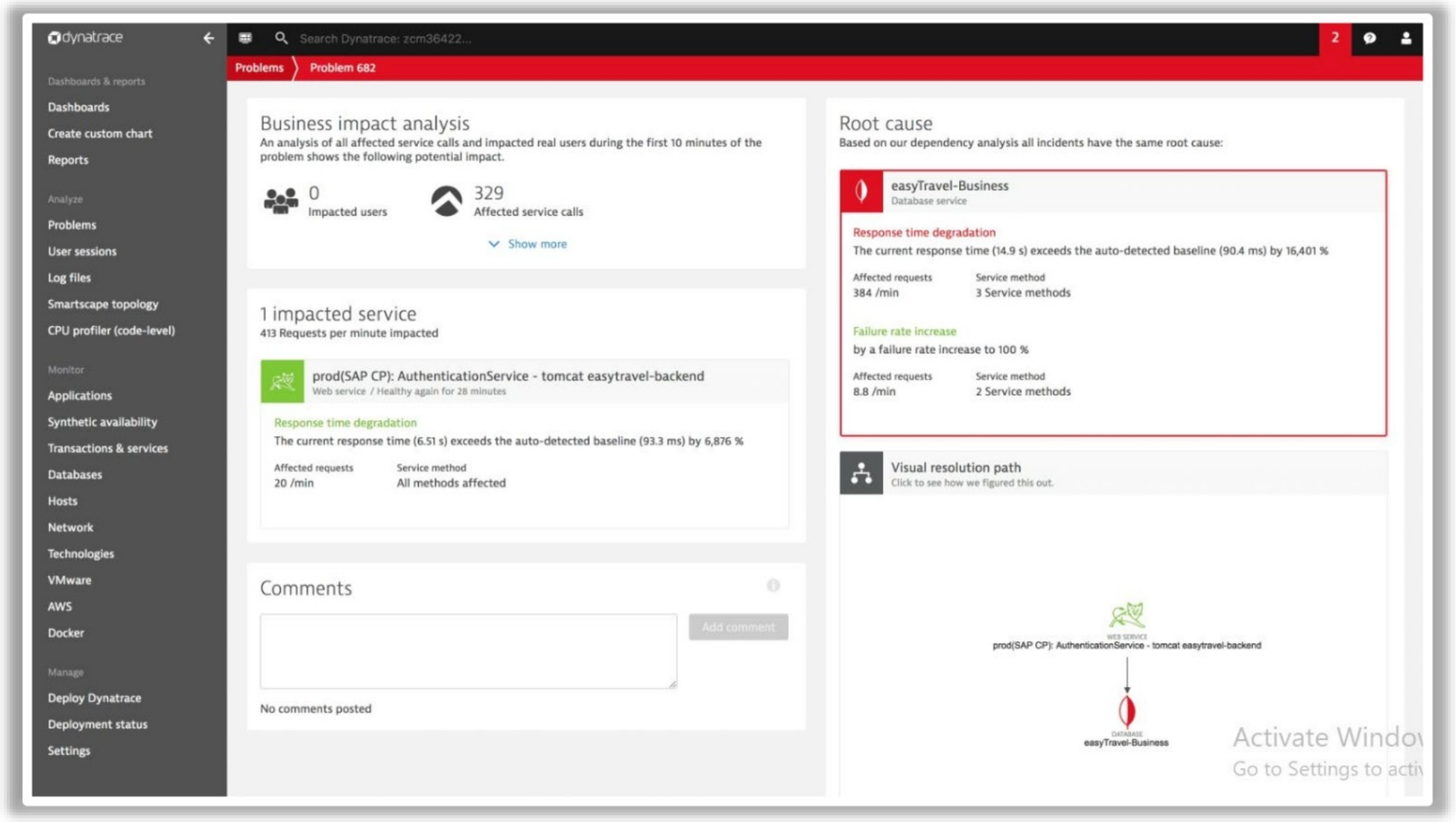
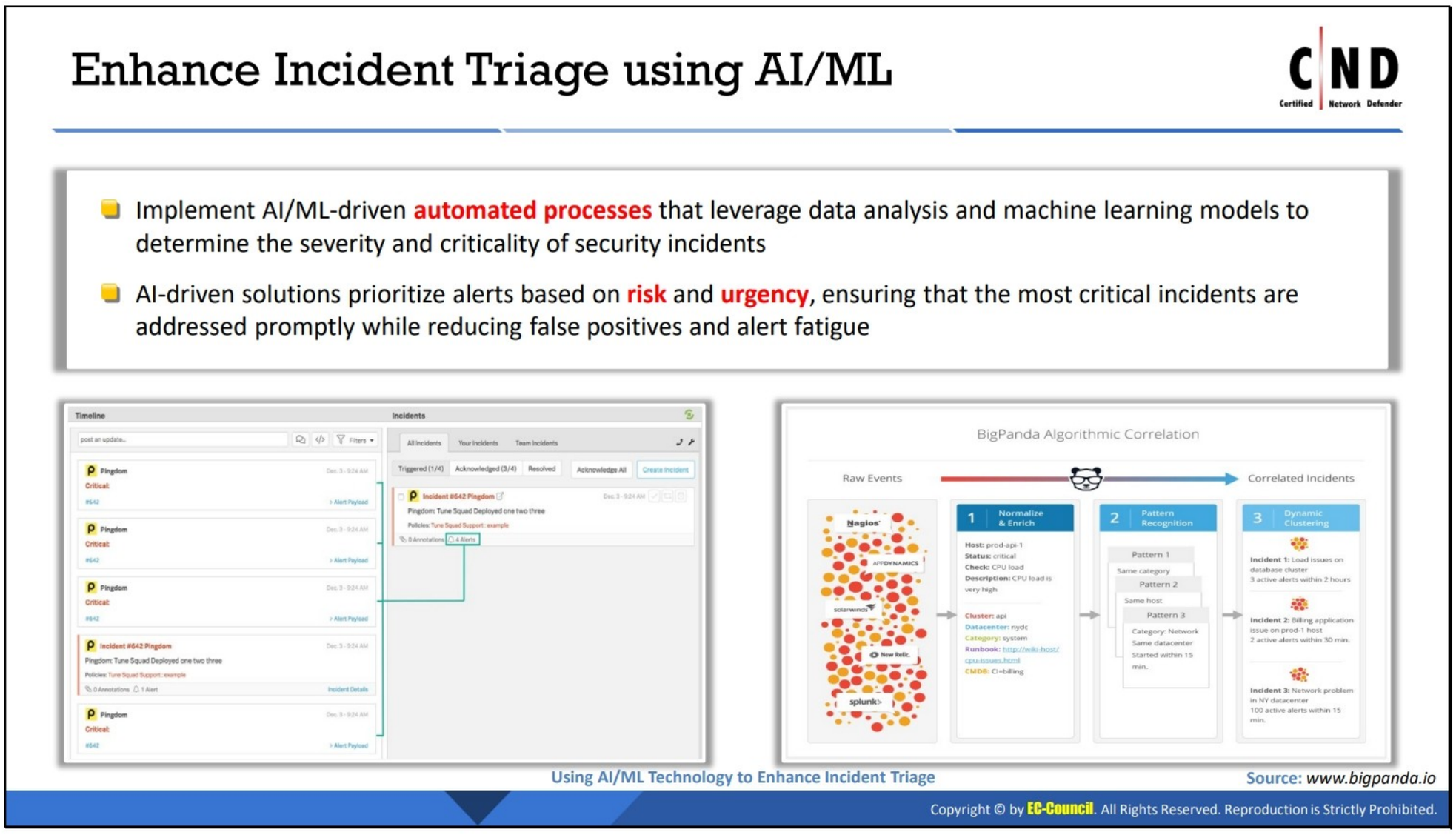


Figure 16.5: Automated Root Cause Analysis using Dynatrace



Enhance Incident Triage using AI/ML

Integrating incident response triage with various AI algorithms and ML models results in techniques focused on data analysis. These models provide a structured and standardized approach to thoroughly evaluate security systems, identifying vulnerabilities and potential threats that could harm critical security infrastructure. This strategy helps prioritize threats and responses based on their severity, adding an extra layer of security to the organization's security architecture.

These advanced systems analyze vast datasets with precision, prioritizing severe vulnerabilities to be addressed first. This method not only bolsters security postures but also minimizes false alarms and unnecessary operational disruptions. Focused on critically improving decision-making in real-world cyber threat detection, it also mitigates alert fatigue by reducing exposure to persistent alarms. Moreover, this approach promotes cost-effective measures, resorting to manual operations only when necessary.

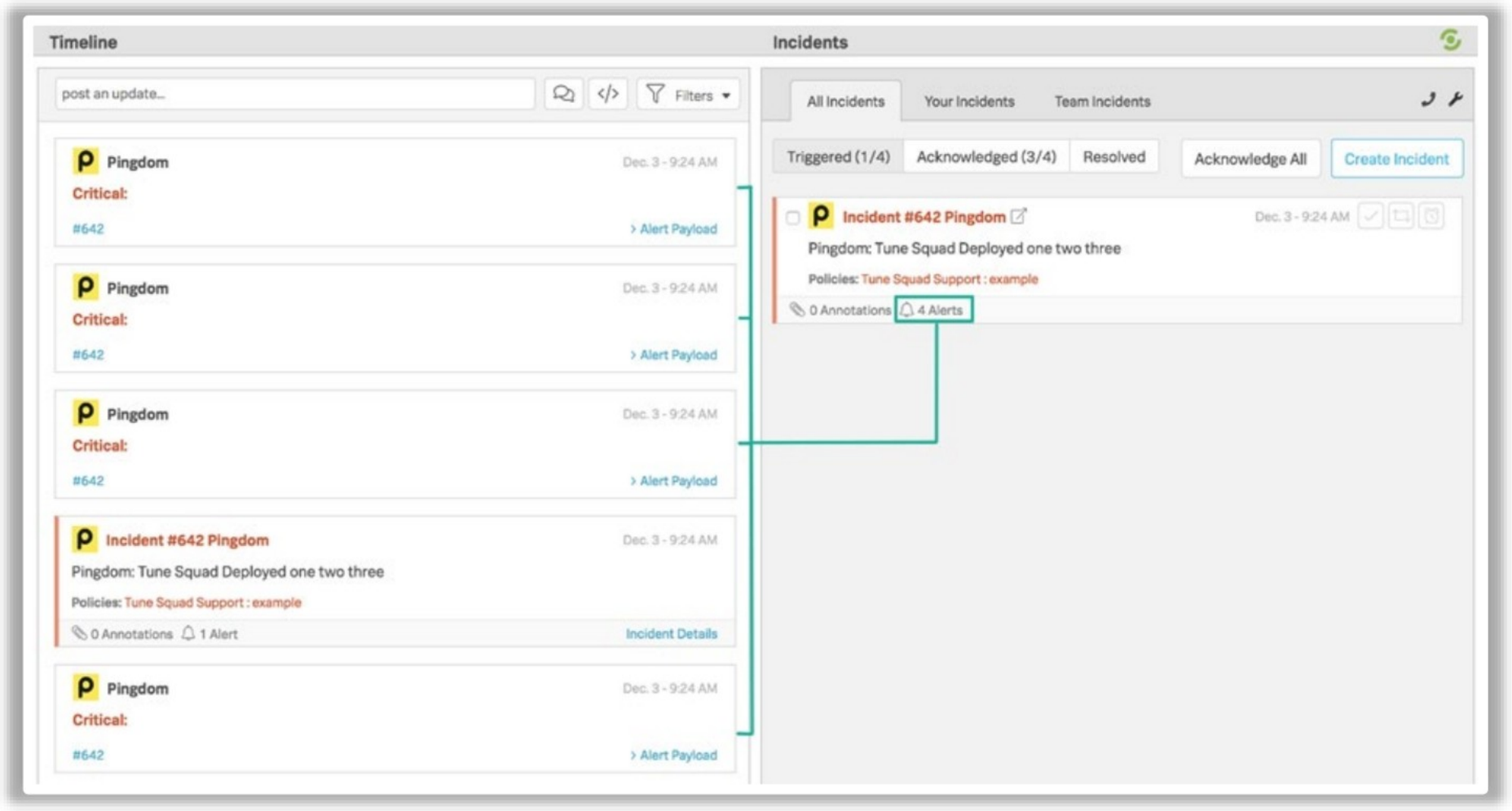


Figure 16.6: Using AI/ML Technology to Enhance Incident Triage

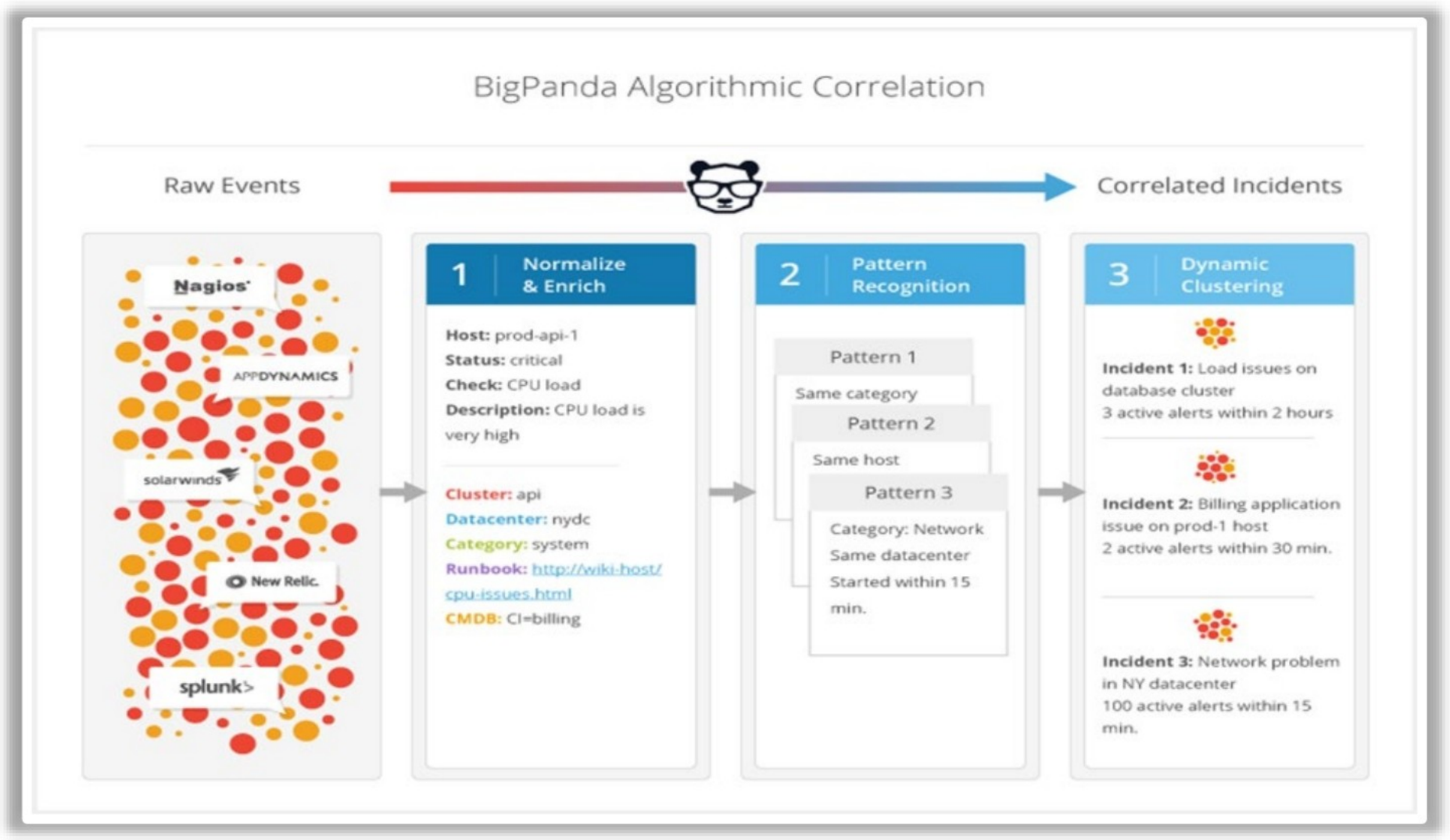
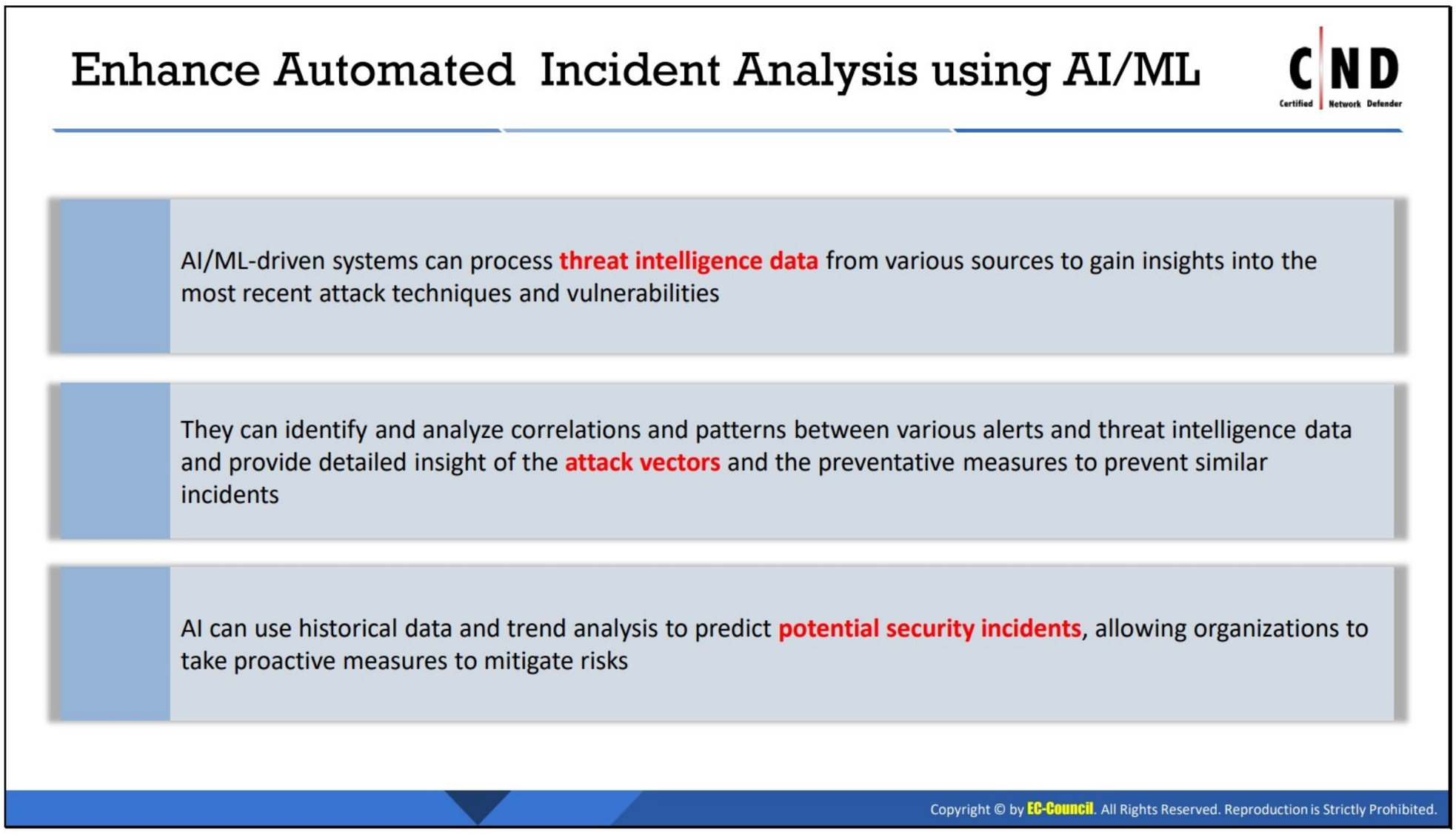


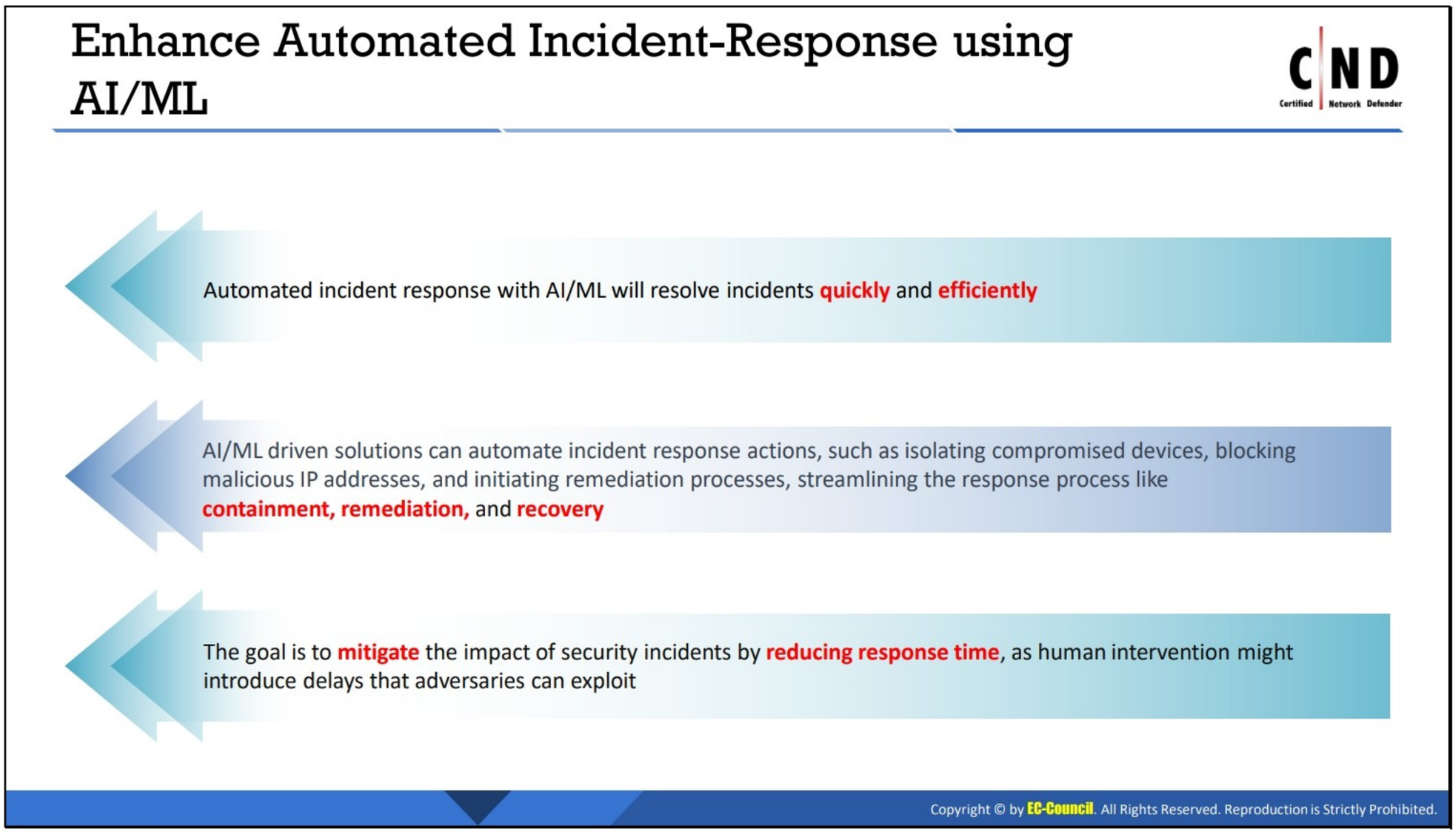
Figure 16.7: Using AI/ML Technology to Enhance Incident Triage



Enhance Automated Incident Analysis using AI/ML

Enhancing automated incident analysis through AI/ML empowers the system to continuously learn from new data. Traditional threat detection methods often rely on predefined data and constraints, which can limit their effectiveness. By incorporating AI/ML into incident response, the system can discover new patterns, analyze datasets, and propose innovative techniques to strengthen the security of the environment. AI/ML algorithms and models can process the organization's diverse datasets to identify the latest attack strategies and vulnerabilities that may pose a risk to the organization's security.

AI-driven solutions excel at identifying correlations and patterns among various alerts, warnings, and other intelligence data. This comprehensive analysis provides valuable insights into preventive measures that minimize operational disruptions and ensure business efficiency. Once an incident is detected, AI/ML models learn from it and can mitigate similar incidents in the future if the security posture is vulnerable to such threats. Additionally, historical attack trends are analyzed to predict potential cyberattacks, enabling organizations to proactively and efficiently address them with strategic approaches.

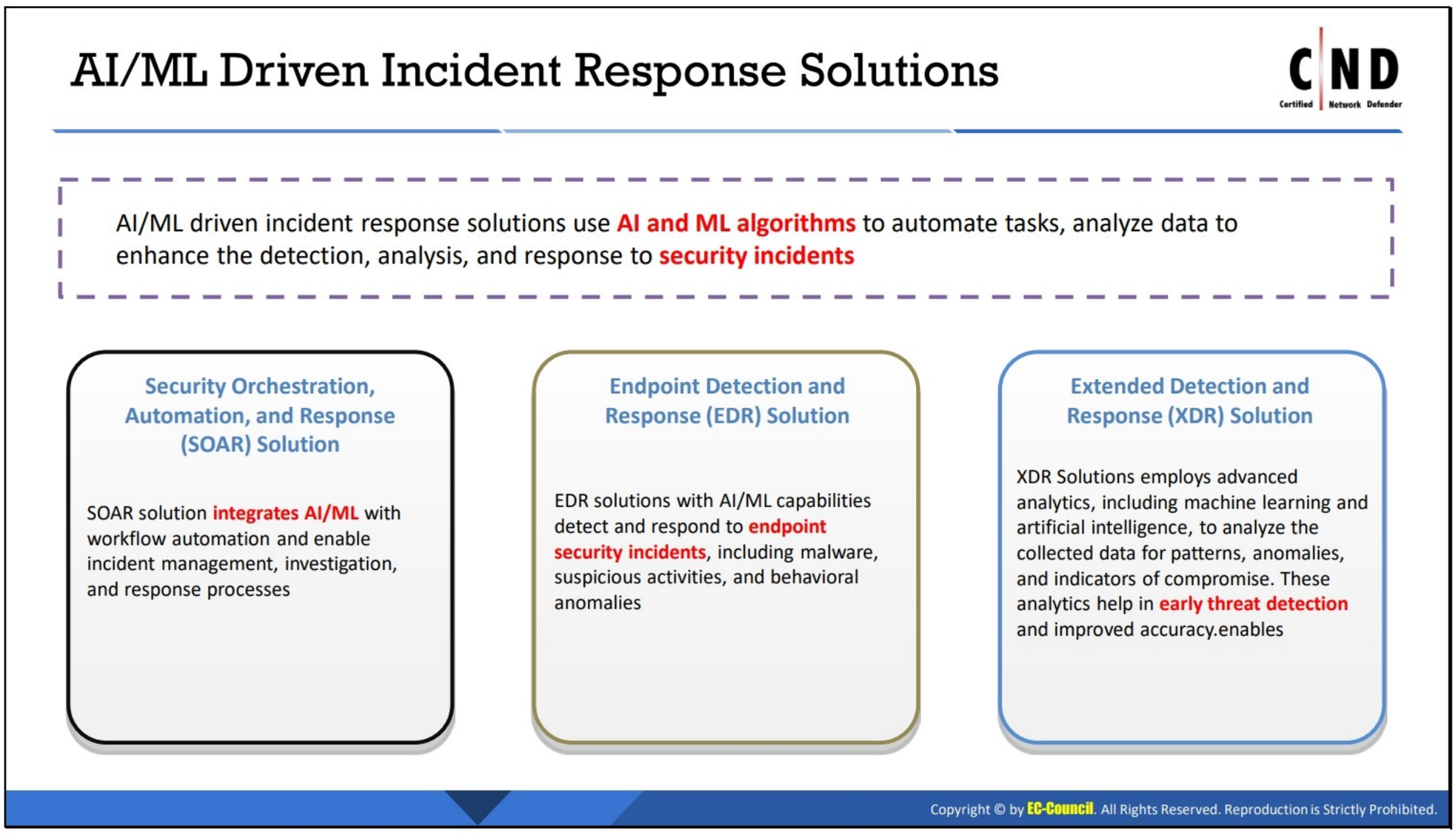


Enhance Automated Incident-Response using AI/ML

Automated incident response (IR) can track millions of security events per day, a significant contrast to traditional incident response strategies. AI automation reduces incident management time, leading to swift threat identification and rapid recovery. It is considered a primary contributor to the reliability of incident response automation.

AI and ML-powered solutions empower organizations to promptly identify and isolate compromised devices, block malicious IP addresses, and initiate remediation procedures. Streamlining incident response processes enhances efficiency and minimizes the impact of security incidents, facilitating rapid recovery.

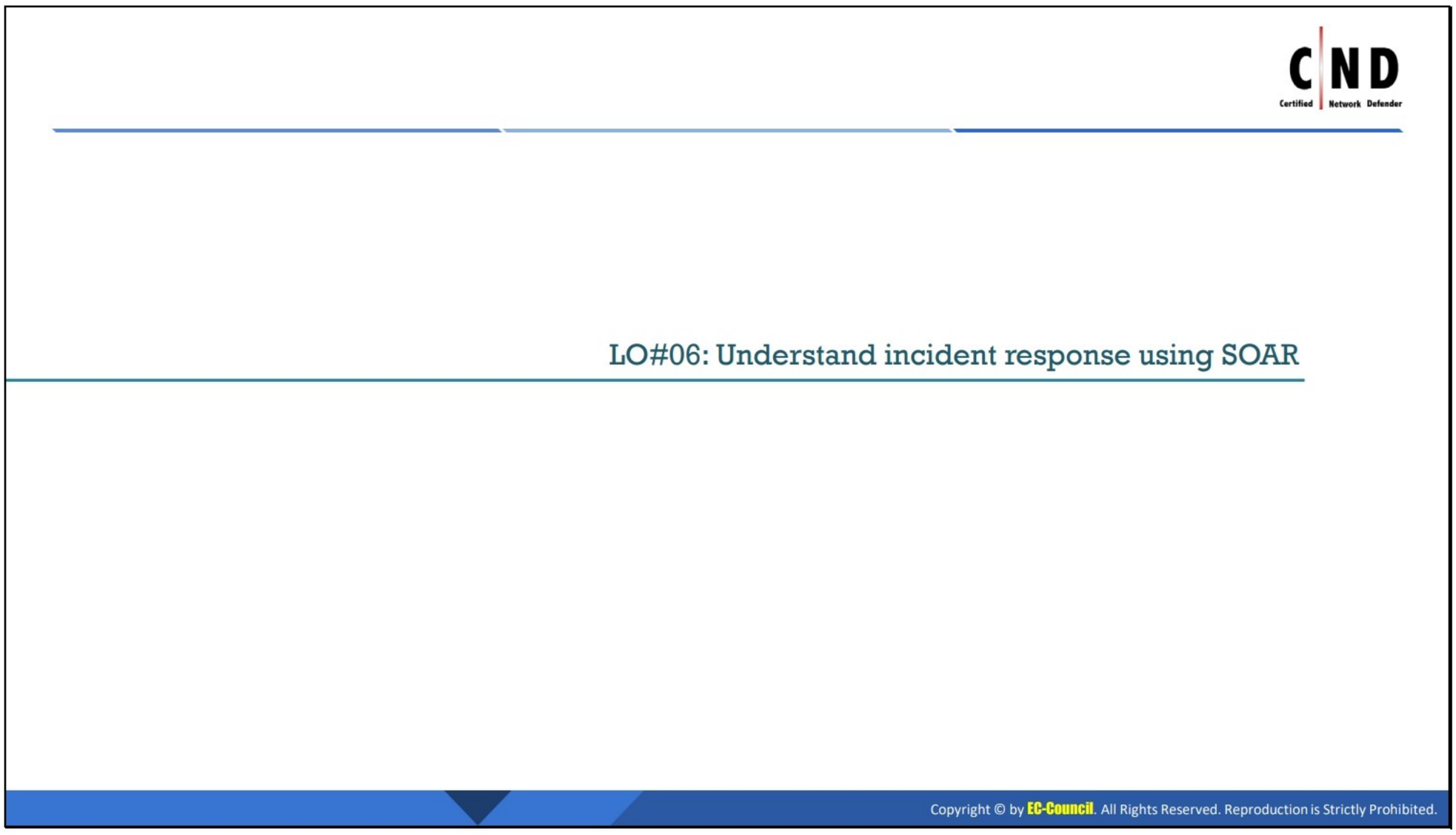
The objective of employing AI/ML in incident response is to reduce response time, thereby mitigating risks and their impact. This rapid response not only limits harm to the organization but also increases the likelihood of preventing further incidents by identifying all exploitable vulnerabilities. Choosing AI/ML over human intervention is motivated by the potential for human involvement to introduce delays, which could benefit attackers in accelerating their attacks.



AI/ML Driven Incident Response Solutions

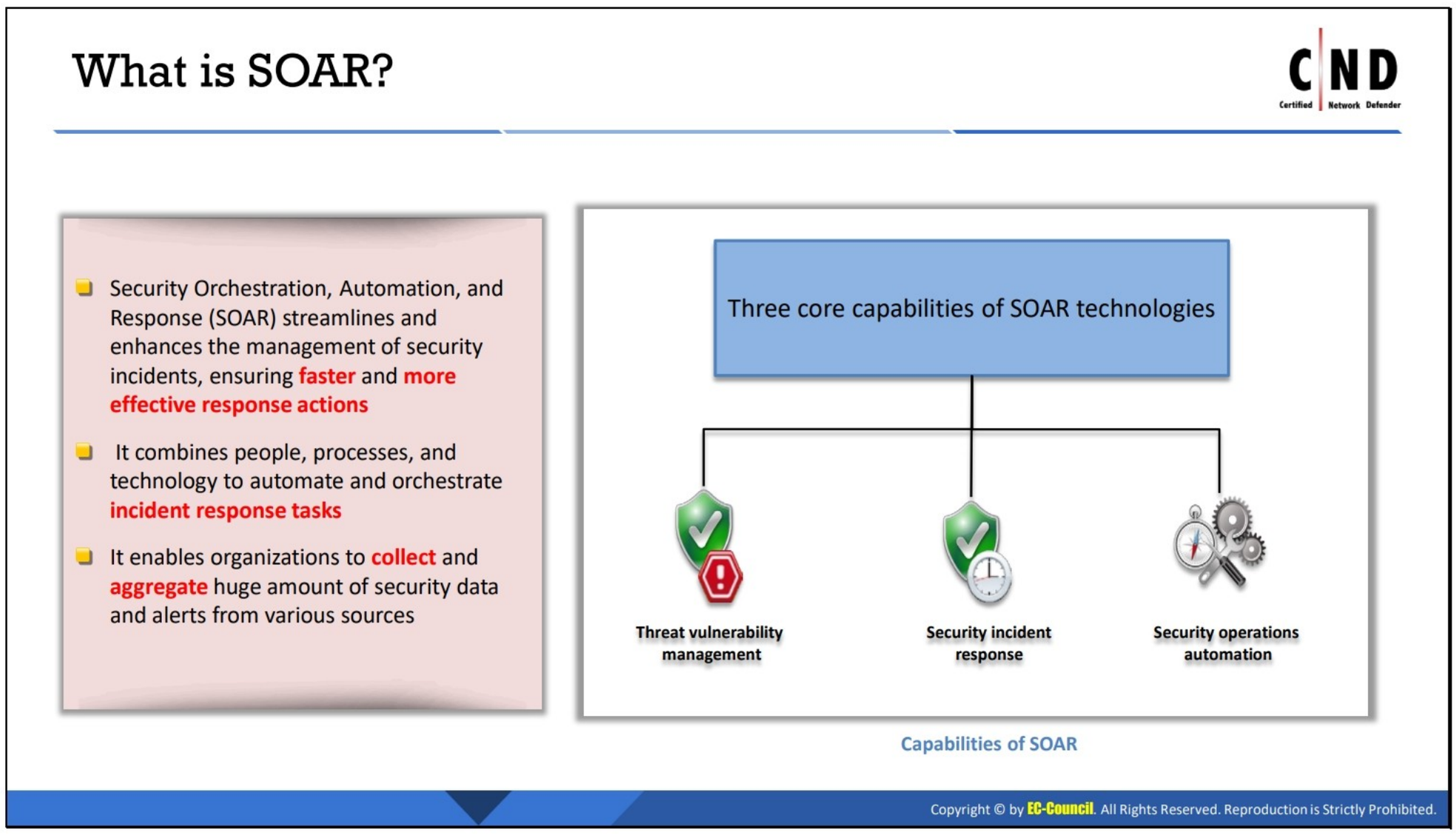
AI/ML-driven incident response solutions utilize AI and ML algorithms to automate tasks and enhance the detection, analysis, and response to security incidents across an organization's endpoints, applications, and network.

- **Security information and event management (SIEM) solution:** AI/ML-driven SIEM solutions analyze various security events, detecting patterns and anomalies to improve threat detection and alerting. AI-driven SIEM incorporates automation features to streamline and expedite the incident response process. They can automatically initiate alerts, execute predefined response measures, and even orchestrate complex response workflows.
- **User and entity behavior analytics (UEBA) solution:** UEBA leverages behavioral analytics, machine learning algorithms, and automation to identify atypical and potentially risky user and device behavior. AI/ML is used to monitor user and entity behavior, identifying unusual or risky activities that may indicate insider threats or compromised accounts.
- **Security orchestration, automation, and response (SOAR) solution**: SOAR solutions integrate AI/ML with workflow automation, enabling incident management, investigation, and response processes. They extract insights from data sources such as threat intelligence alerts and logs.
- **Endpoint detection and response (EDR) solution**: EDR solutions with AI/ML capabilities detect and respond to endpoint security incidents, including malware, suspicious activities, and behavioral anomalies. They assist organizations in proactively enhancing endpoint cybersecurity, improving threat detection, and accelerating threat response.



LO#06: Understand Incident Response using SOAR

Utilizing Security Orchestration, Automation, and Response (SOAR) is a game-changer in incident response. By seamlessly integrating automated workflows and response mechanisms, SOAR not only accelerates the identification and mitigation of security incidents but also enhances overall response efficiency. This section discusses SOAR to empower the security teams to orchestrate complex tasks, automate repetitive actions, and collaborate seamlessly, ultimately fortifying an organization's resilience against evolving cyber threats.



What is SOAR?

Security orchestration, automation, and response (SOAR) integrates three core components: orchestration, automation and response into a combined framework providing faster and more effective response actions. It combines people, processes, and technology to automate and orchestrate incident response tasks. By streamlining alert triage and making sure various security tools are working together, SOAR helps reduce the mean time to detect and the mean time to respond, thereby improving overall security posture.

Capabilities of SOAR

- **Threat and vulnerability management**: It supports the remediation of vulnerabilities, thereby providing formalized workflow, collaboration capabilities and reporting.
- **Security operations automation**: SOAR automates low-level operations like event enrichment and alert prioritization. AI-driven SOAR analyzes data from security tools and recommends security measures to handle threats in the future.
- **Security incident response**: SOAR's orchestration and automation capabilities enable it to function as a centralized console for managing security incident response. It allows us to investigate and resolve incidents without switching between multiple tools. By utilizing SOAR data, security teams can pinpoint previously undetected, ongoing threats and concentrate their threat-hunting efforts in the most pertinent areas.

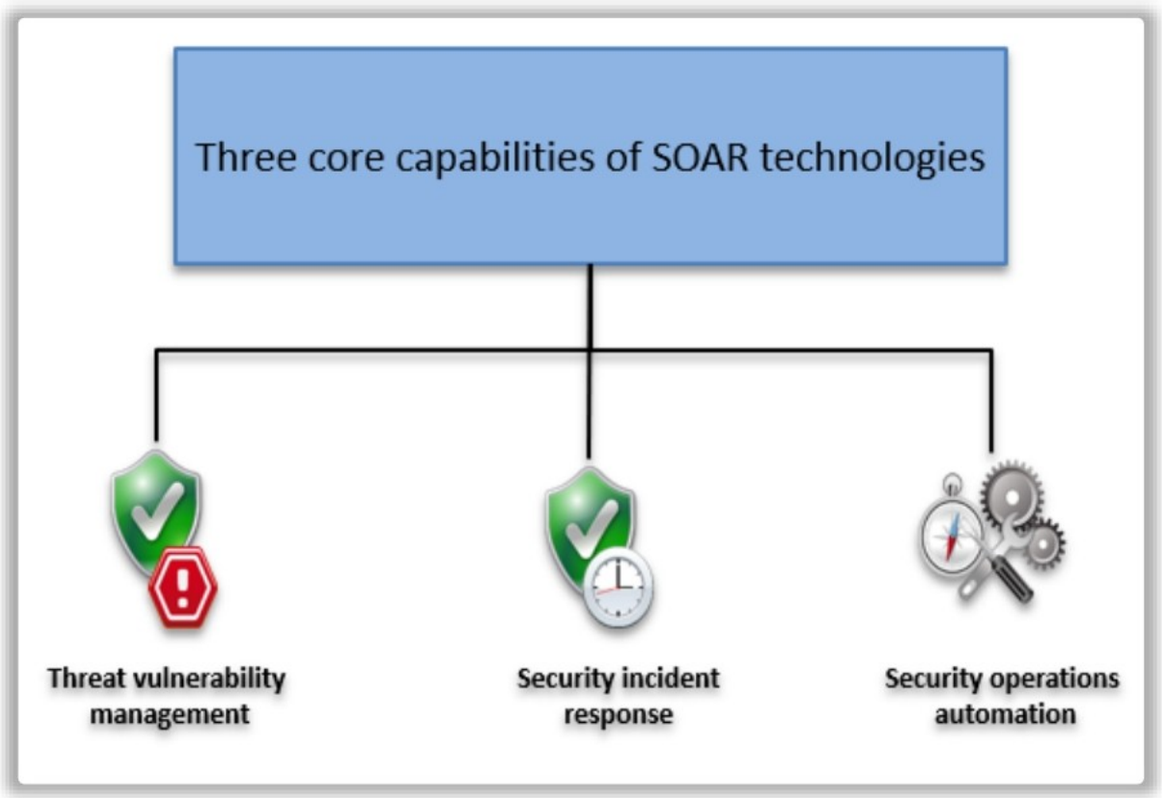
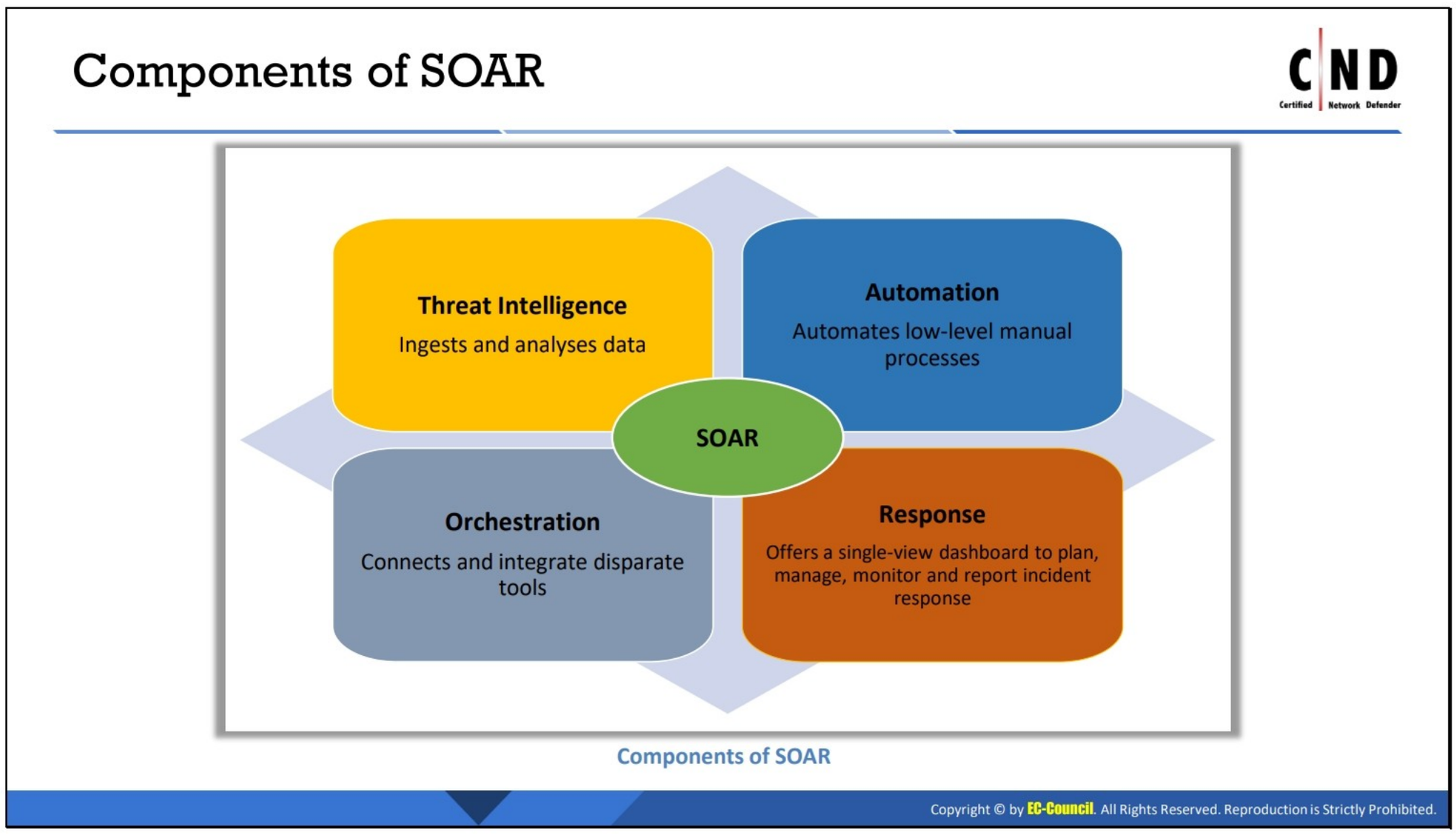


Figure 16.8: Capabilities of SOAR



Components of SOAR

SOAR offers a mix of threat intelligence, orchestration and automation capabilities allowing an effective incident response.

The components of SOAR are as follows.

Threat Intelligence

Threat intelligence gives the security teams insights about potential threats. It comprises vast amount of data and this data needs to be correlated properly to identify attack patterns, threats and incidents. The threat intelligence feeds are prioritized by the impact and severity of the threats in the organization.

Security Orchestration: Security orchestration provides a robust framework that easily integrates various internal and/or external tools using built-in/custom integrations and application programming interfaces. It eliminates inefficiency in sharing data across complex networks by centralizing information and allowing integrated responses. This coordination provides quick incident handling and improves overall security resilience. The more data gathered, the more the chances of detecting threats in the network.

Security Automation: Security automation collects the data that is gathered by orchestration. The collected data is analysed and examined by replacing the manual processes with automated tools. Tasks such as log analysis, red flags detection, anomaly detection, and centralizing data-sharing methods will be performed by the automation tools that are required to be implemented in the network. This ensures integrity and confidentiality in the environment and avoids unauthorized restrictions. Using AI algorithms and machine learning models, the complexity of performing these tasks goes down by analysing previous trends and various behavioural patterns which gives comprehensive insights into the network traffic.

Security Incident Response: Security analysts offer a single view to monitor and report actions that are performed to mitigate and eliminate threats. This single view ensures the integration of various advancements and correlation between multiple warnings to look at the issue in a detailed and bigger picture. It also suggests post-response activities (for example, case mangement, reporting, etc) that could enhance the effectiveness of security frameworks and the robustness of the network.

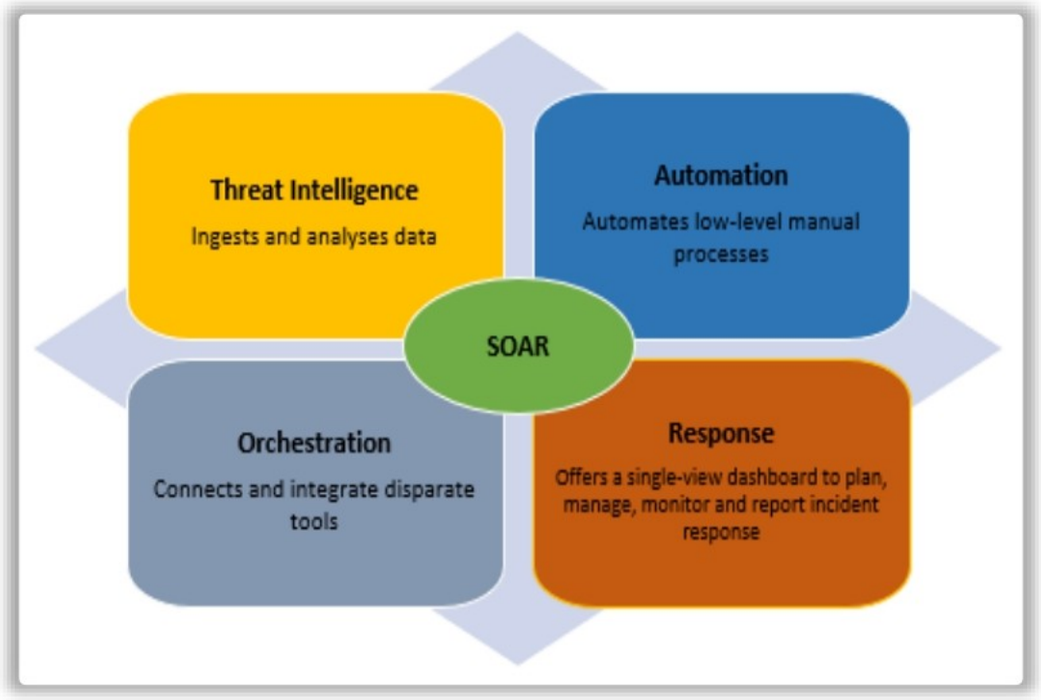
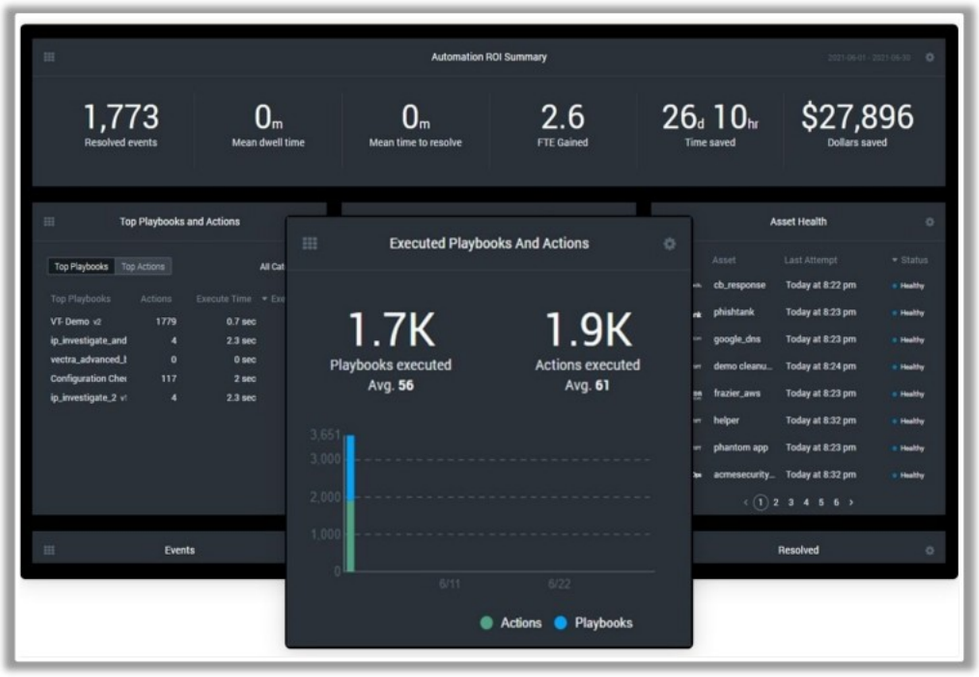


Figure 16.9: Components of SOAR

SOAR Integration with Security Tools

SOAR solutions integrate with various security tools and systems, like SIEMs, firewalls, IDS, endpoint security solutions, threat intelligence feeds, ticketing systems, and more which allows for **data sharing** and **coordination** between security solution products



Executed Playbooks and Actions Shown in Splunk SOAR

Source: *https://www.splunk.com/*

SOAR Integration with Security Tools

The integration of SOAR with advanced tools will channel the efficiency into workflows to detect, prioritize, and eliminate potential threats. This can facilitate the network with effective data sharing and secured transmission channels of communication. This offers a comprehensive approach to dealing with vulnerabilities and attacks attached to them. The tools that can be integrated are security orchestration can be vulnerability scanners, security information and event management (SIEM) solutions, user and entity behavior analytics (UEBA), intrusion detection system (IDS), intrusion prevention systems (IPS), endpoint security software, external threat intelligence feeds, firewalls, endpoint detection and response (EDR) solutions, and other third-party sources. Use any of the SOAR technology that can provide an overview of all the data, playbooks, connections with security tools, ROI, etc.

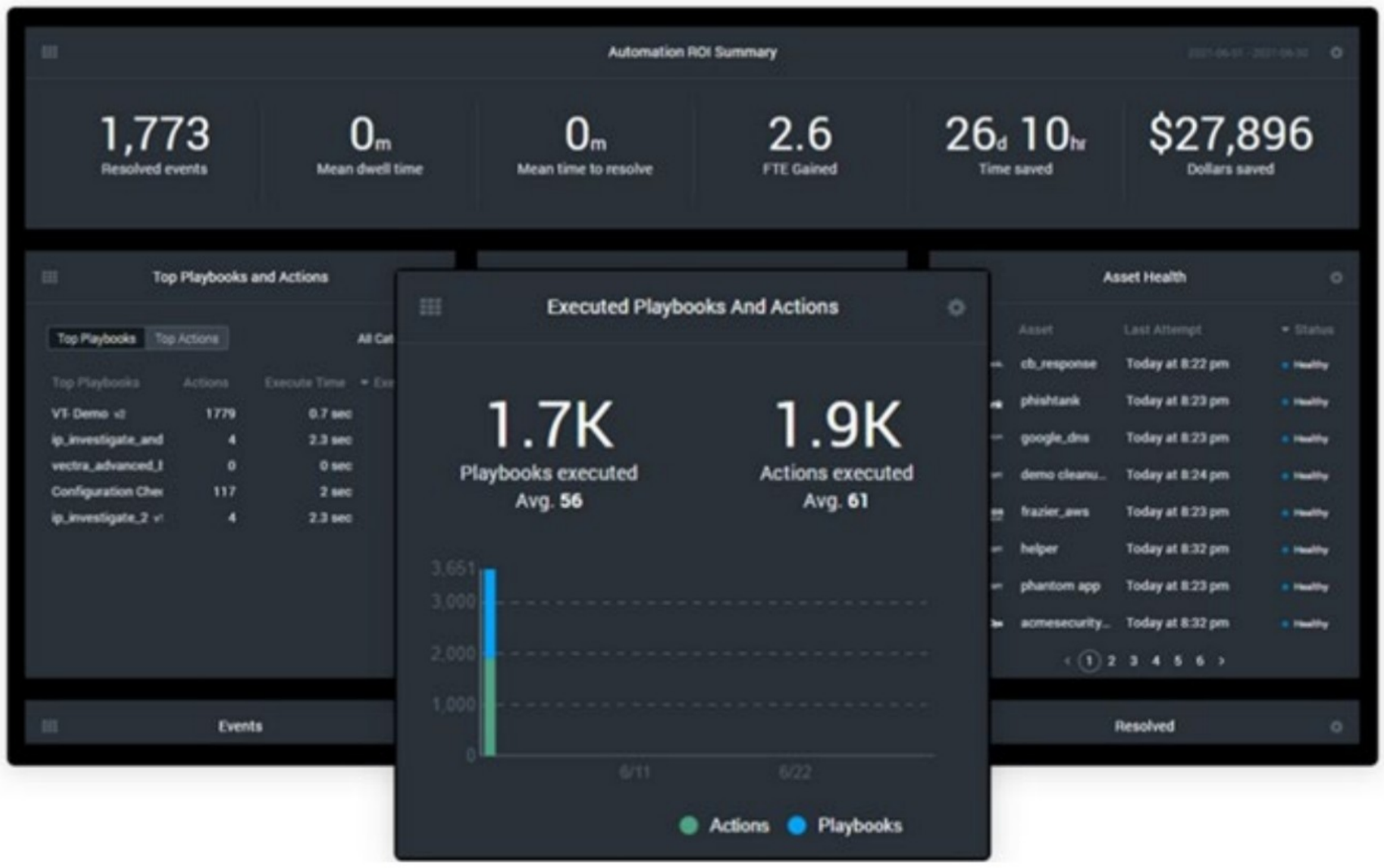
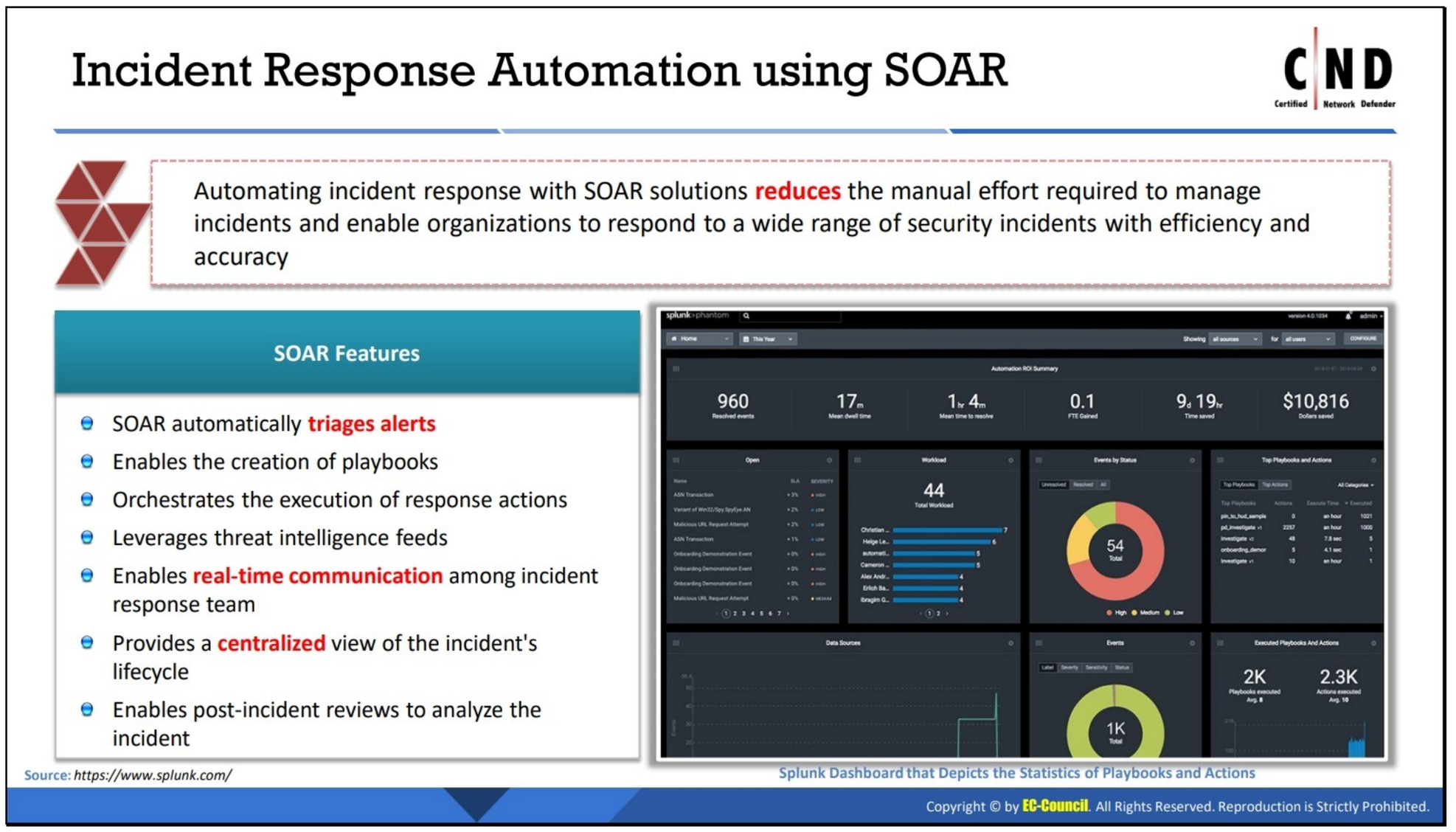


Figure 16.10: Executed Playbooks and Actions Shown in Splunk SOAR



Incident Response Automation using SOAR

SOAR enables organizations to limit risks and maintain a proactive security posture by eliminating human interference. SOAR systems provide the seamless integration of security technologies and provide real-time analytics, allowing businesses to predict and determine new threats while maximizing resource allocation. It employs SOAR technology for incident response automation is critical in protecting digital assets, increasing resilience, and building a strong cybersecurity architecture.

SOAR technologies provide the following interms of incident repsonse automation.

- SOAR is capable of autonomously strategizing and approaching dangers using active incident tactics.
- It allows for the playbooks creation.
- It allows orchestrating the executiion of response acions
- It allows leveraging threat intelligence feeds.
- It allows for real-time communication among incident response team members.
- It provides a centralized view of the incident’s lifecycle.
- It allows evaluating incidents once they occur.

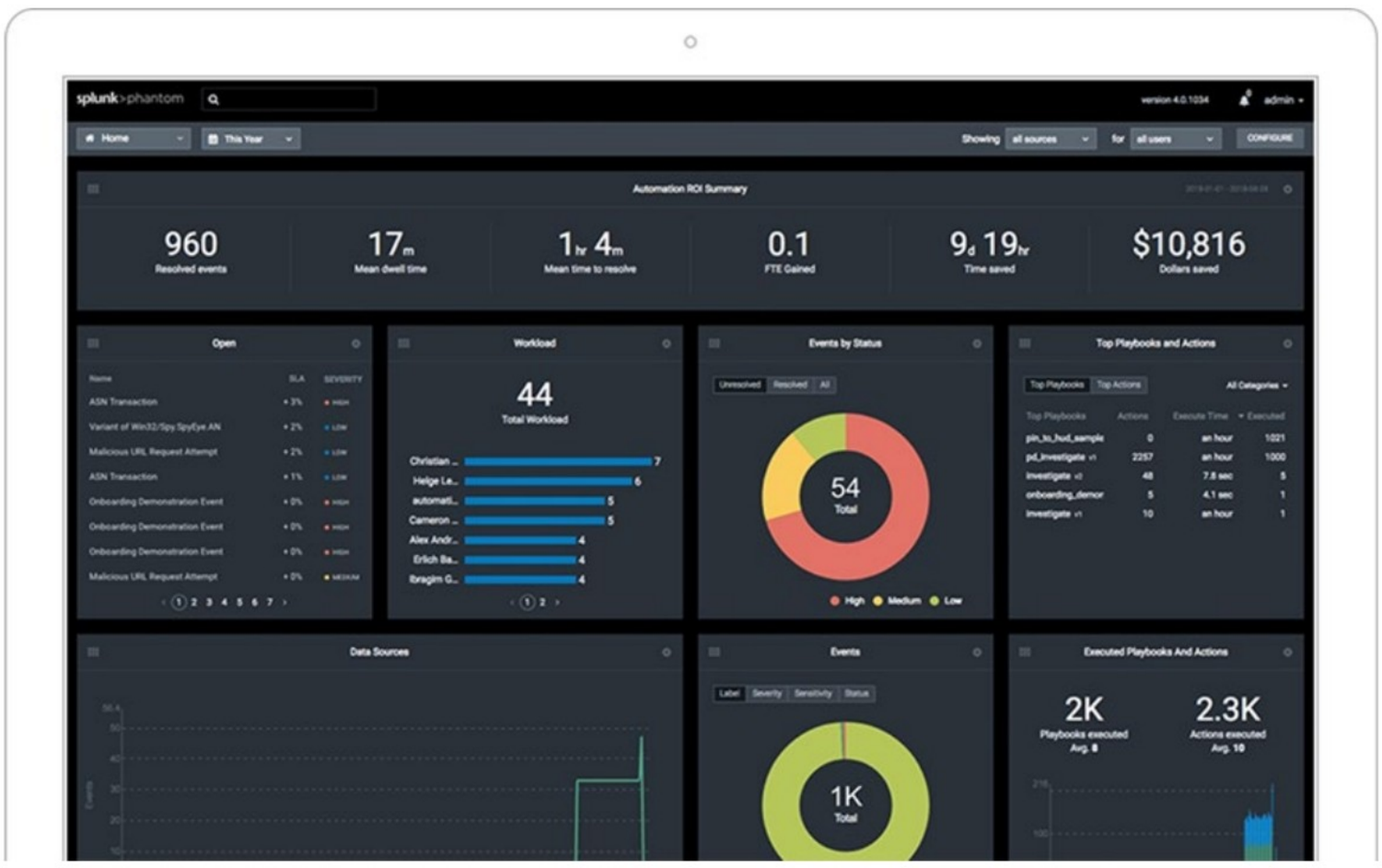
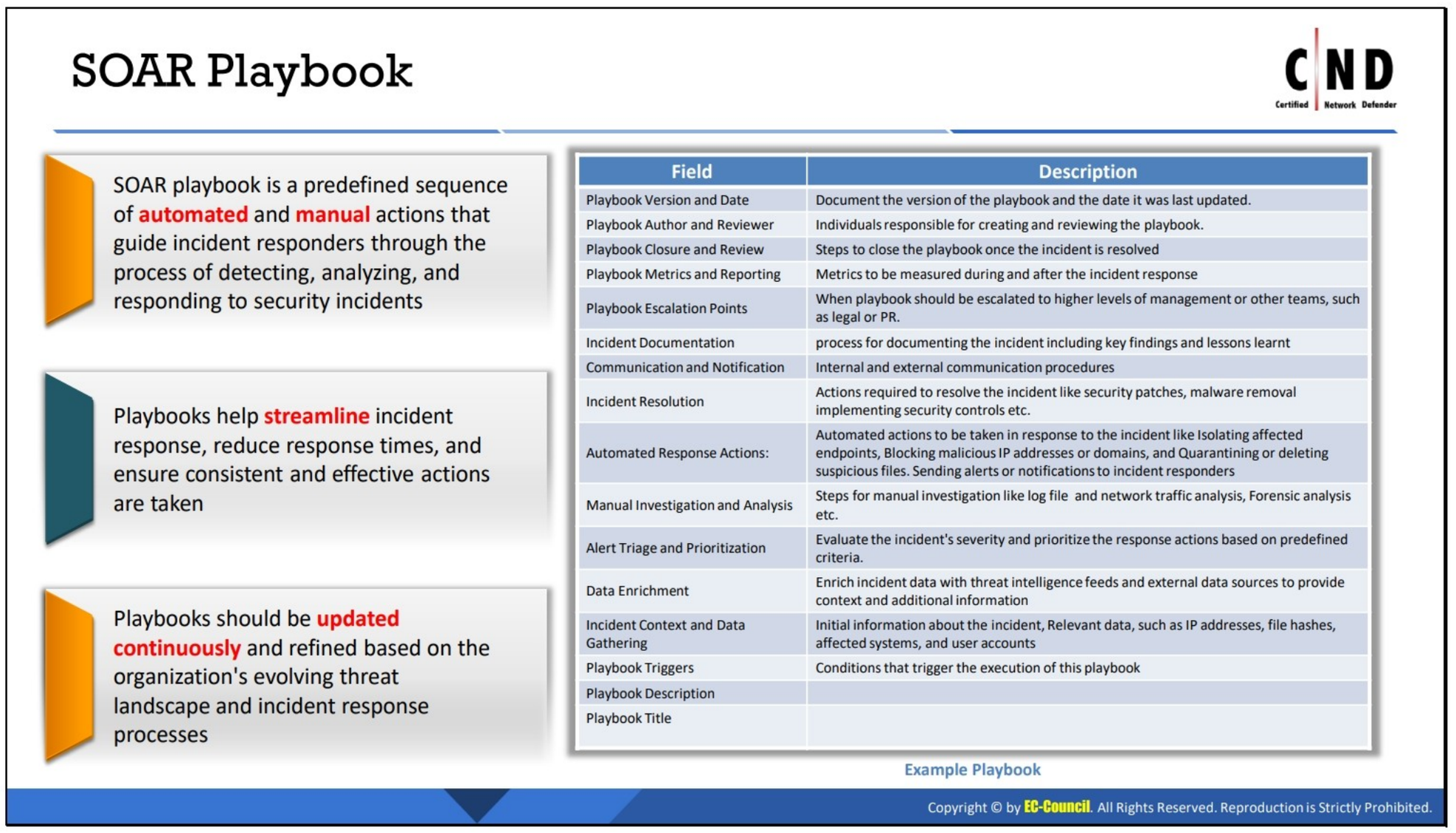


Figure 16.11: Splunk Dashboard that Depicts the Statistics of Playbooks and Actions



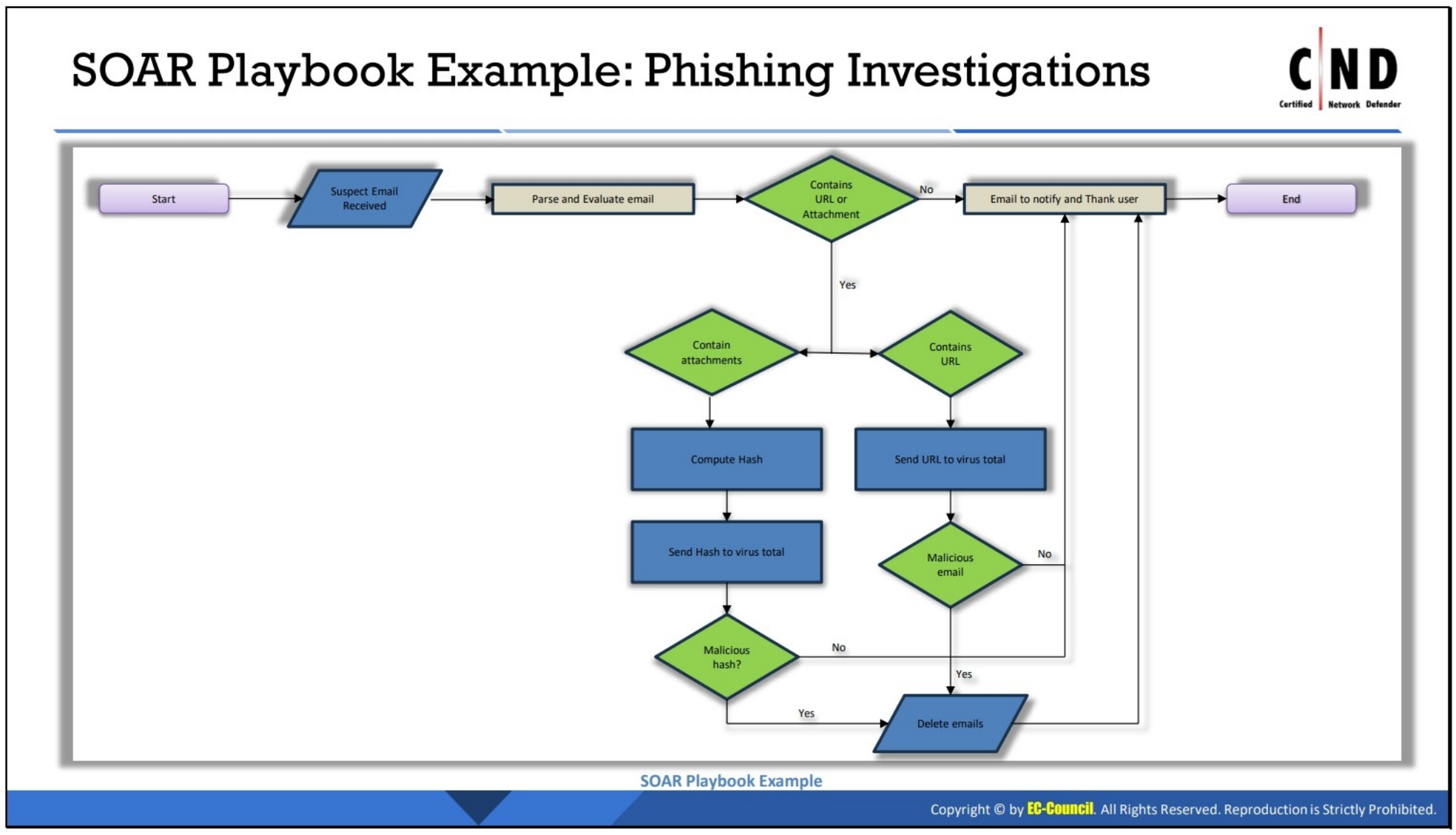
SOAR Playbook

SOAR playbooks are helpful guidelines that combine automatic and manual procedures to help security teams quickly detect, analyse, and determine security threats. They improve an organization’s ability and endurance to withstand potential threats and mitigate those quickly and effectively by using automated response processes and promoting the use of AI/ML algorithms and models.

Because cyber security is volatile, paybooks must be updated and upgraded frequently. It is essential to adapt to the organization’s dynamic nature i.e., changing threat landscape and incident response protocols. This regular procedure ensures that incident response plans are not only effective but also flexible and ensures increasing the organization’s resilience against possible security breaches and allowing proactive steps to protect the organization’s vital assets and resources.

Example Playbook:

Playbook Title
Playbook Description
Playbook Triggers: Conditions that trigger the execution of this playbook
Incident Context and Data Gathering: Initial information about the incident, Relevant data, such as IP addresses, file hashes, affected systems, and user accounts
Data Enrichment: Enrich incident data with threat intelligence feeds and external data sources to provide context and additional information
Alert Triage and Prioritization: Evaluate the incident's severity and prioritize the response actions based on predefined criteria.
Automated Response Actions: automated actions to be taken in response to the incident like Isolating affected endpoints, Blocking malicious IP addresses or domains, and Quarantining or deleting suspicious files. Sending alerts or notifications to incident responders
Manual Investigation and Analysis: Steps for manual investigation like log file and network traffic analysis, Forensic analysis etc.
Incident Resolution: Actions required to resolve the incident like security patches, malware removal implementing security controls etc.
Communication and Notification: Internal and external communication procedures
Incident Documentation: process for documenting the incident including key findings and lessons learnt
Playbook Escalation Points: when playbook should be escalated to higher levels of management or other teams, such as legal or PR.
Playbook Metrics and Reporting: metrics to be measured during and after the incident response
Playbook Closure and Review: Steps to close the playbook once the incident is resolved
Playbook Author and Reviewer: Individuals responsible for creating and reviewing the playbook.
Playbook Version and Date: Document the version of the playbook and the date it was last updated.



SOAR Playbook Example: Phishing Investigations

Orchestration and automation solutions play an important role in speeding investigative procedures by effortlessly executing work and allows the team to focus on other vital areas of the investigation. These tools ensure that critical situations are handled effectively and efficiently, greatly lowering reaction time. Further, they enable enterprises to create automated workflows that address security issues like phishing emails quickly by automating remediation actions.

A phishing playbook is a detailed and structured document or set of suggestions that defines a systematic strategy for detecting, reacting to, and mitigating phishing attempts inside an organization. It is a thorough reference for security personnel, describing exact measures to follow at different phases of a phishing attack.

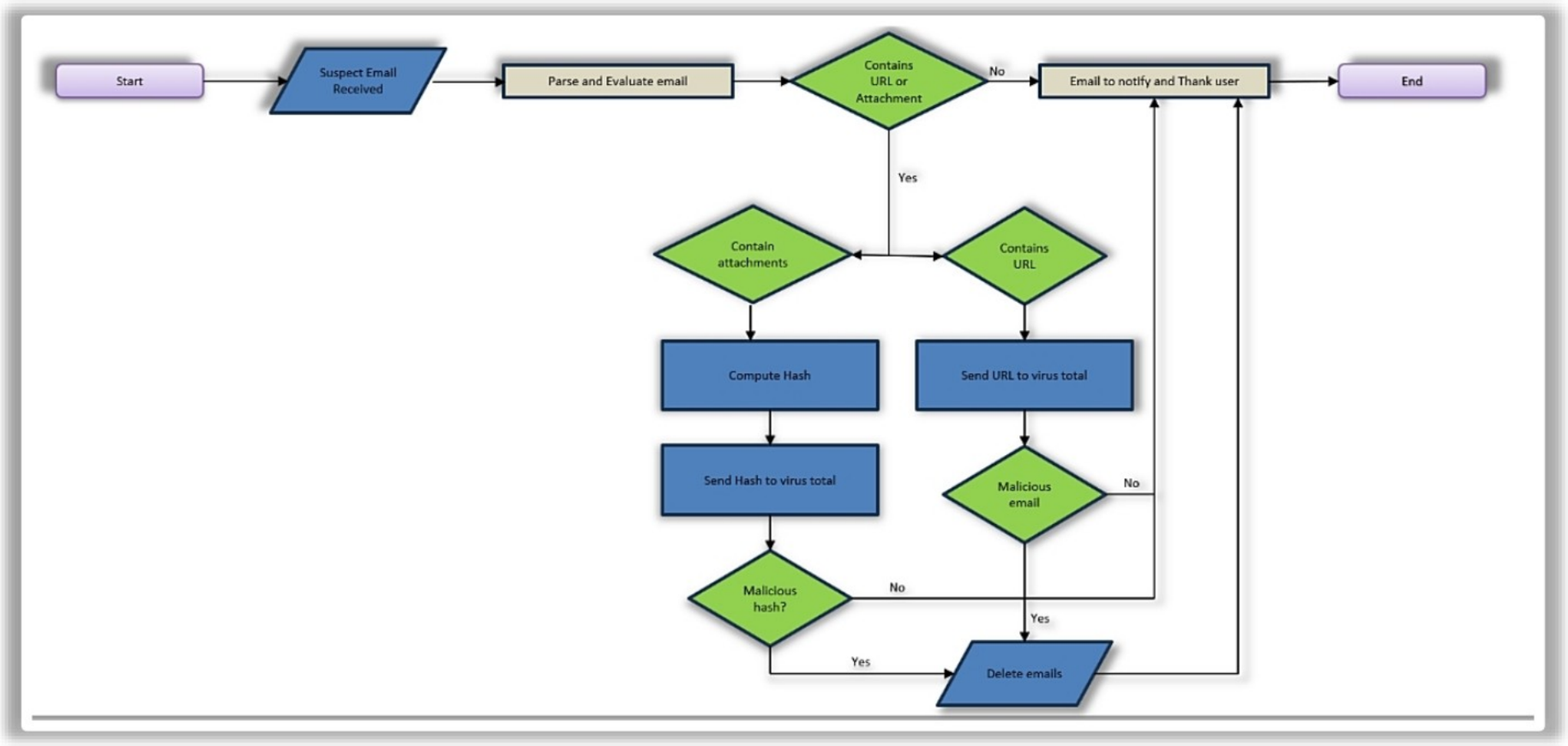
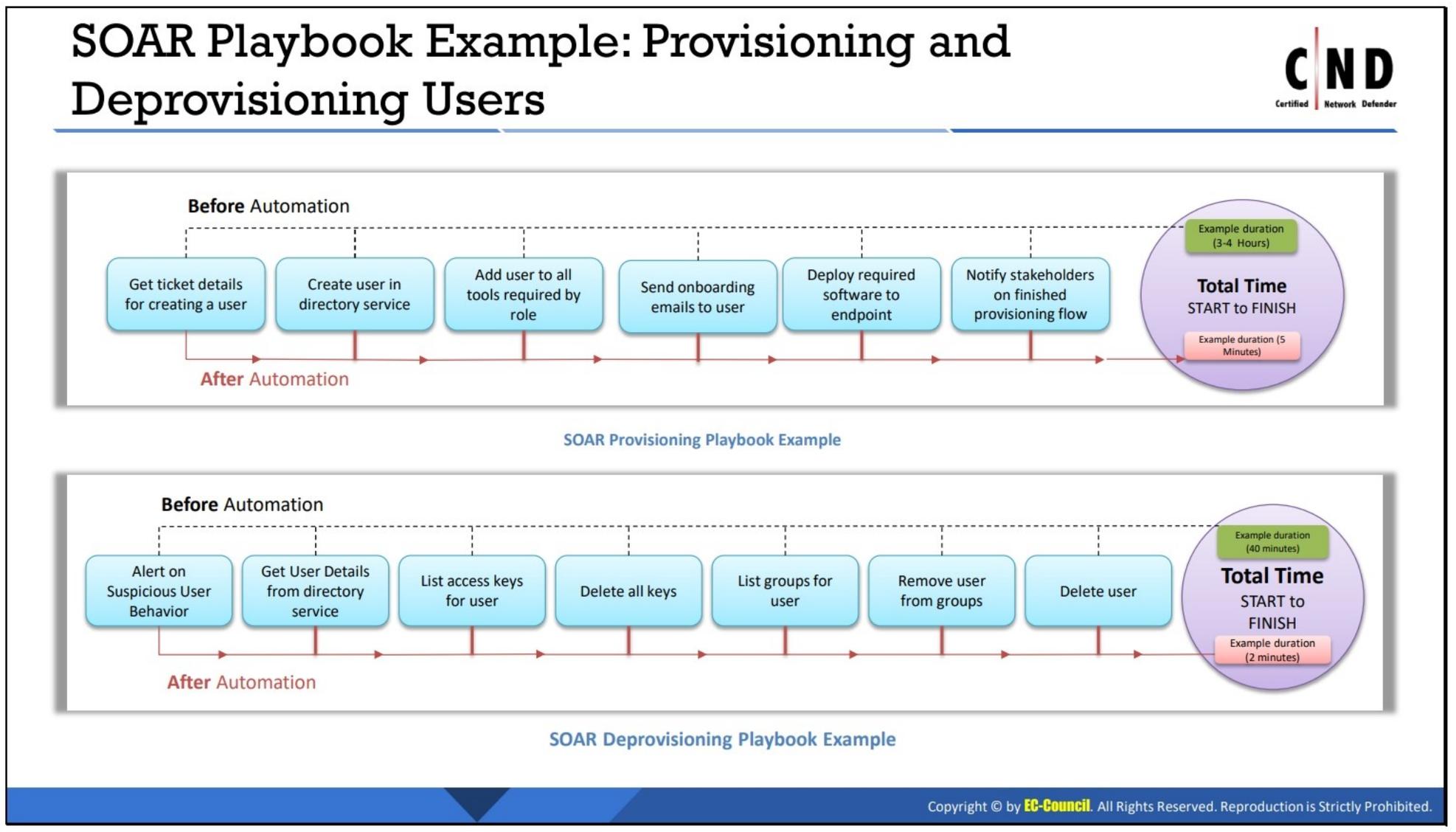


Figure 16.12: Phishing Playbook

Follow the below to investigate the phishing incidents using a SOAR Playbook.

- **Scan attachments and URLs:** Use plugins offered by a SOAR technology for safe browsing, sandboxes, and other tools to confine and evaluate suspicious attachments and URLs.
- **Leverage workflows to find threats:** Use threat intelligene from different resources to set a workflow that can analyze email URLs and file attachments. Get reports that detail the identified indicator.
- **Configure workflows:** It creates processes to trigger a decision point on how to continue once routine scans and investigations have been completed. A few Examples include labelling phishing as verified, immediately issuing a message via Slack notifying others in business of the phishing danger, and other steps.



SOAR Playbook Example: Provisioning and Deprovisioning Users

Security orchestration and automation can remove the manual efforts of managing user accounts in terms of provisioning and deprovisioning users in the event of an incident.

Provisioning users: In an organization, different users require different levels of access. This access pertains to various privileged tools, accounts, and to critical resources. In this case, the SOAR Playbook can easily connect technologies like Okta or Active Directory to initiate automation for specific user accounts.

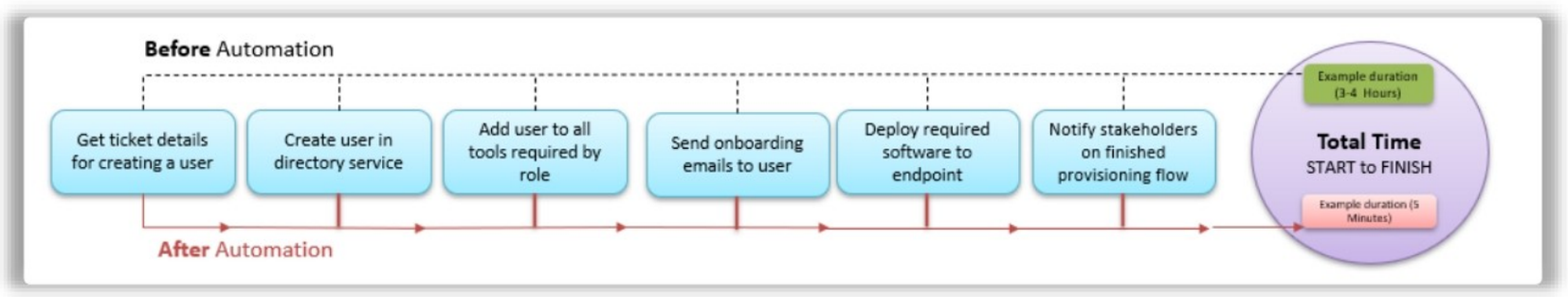


Figure 16.13: SOAR Playbook Example for Provisioning

Deprovisioning users: Use SOAR playbook to deprovision the users immediately if they quit the organization. In the case of phishing attack, remove the permissions for the affected accounts and revoke permissions once the threat is contained.

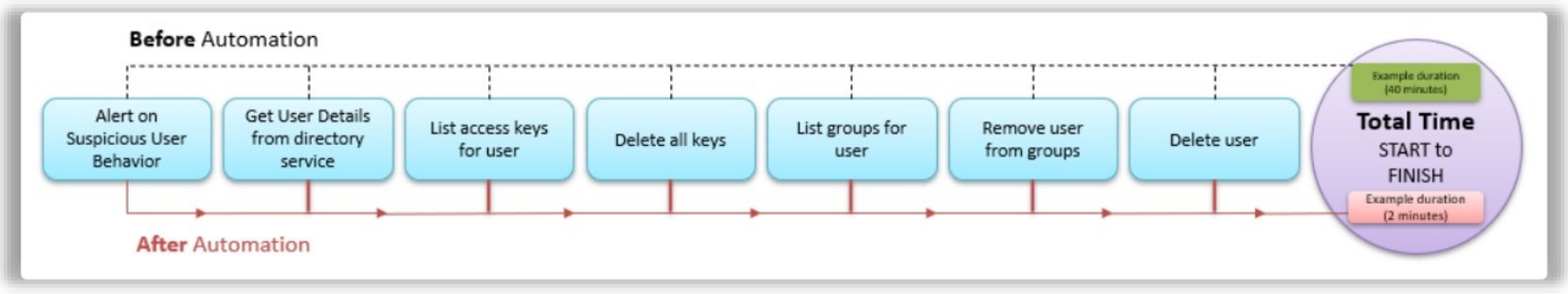
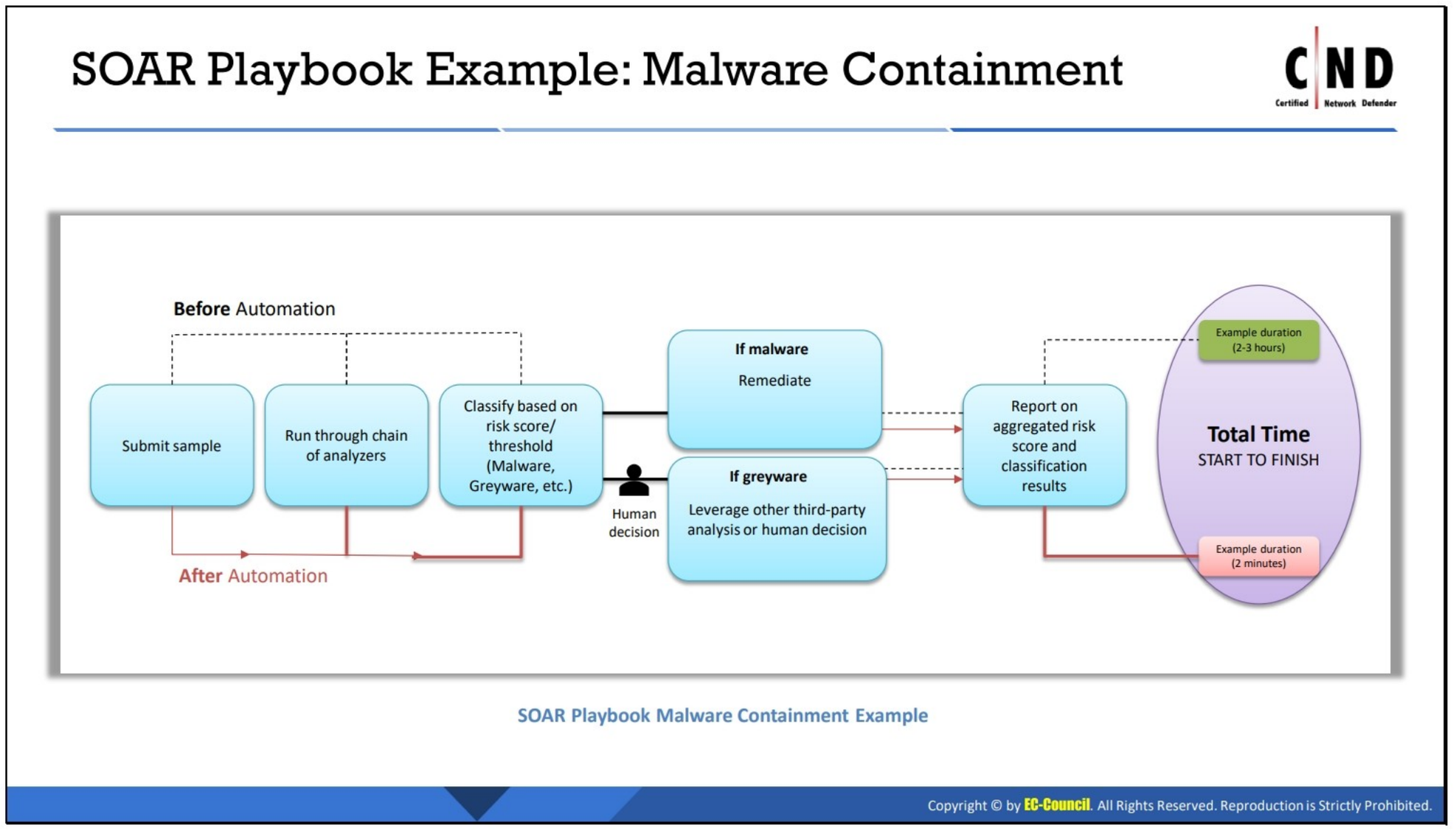


Figure 16.14: Example of Deprovisioning user



SOAR playbook Example: Malware Containment

Use SOAR to automate the investigation and containment of malware and prevent the damage they cause to the organization's network.

Follow the below to contain malware using SOAR playbook

- **Identify malicious activities:** Look for signs that have the potential to compromise the network. Use the automated processes to identify threat indicators such as mis-spelled names, and abnormal activities.
- **Investigate the threats:** Use standard workflows that can make the security teams find the root cause of the threats.
- **Prefer containment and removal:** Detect which critical sources are affected and isolate them from active networks by leveraging automation.

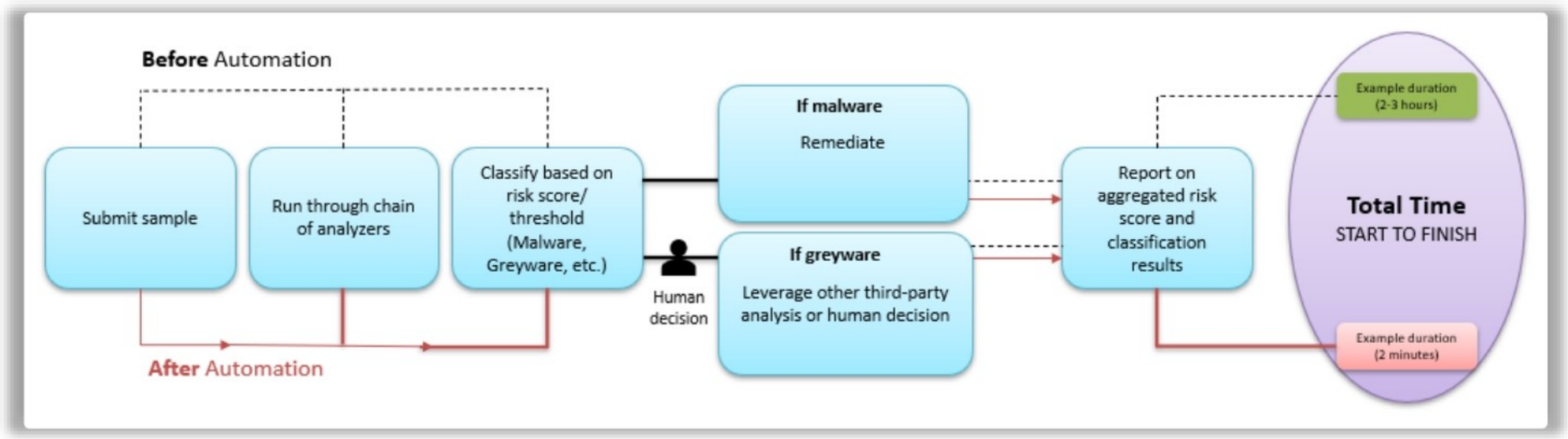
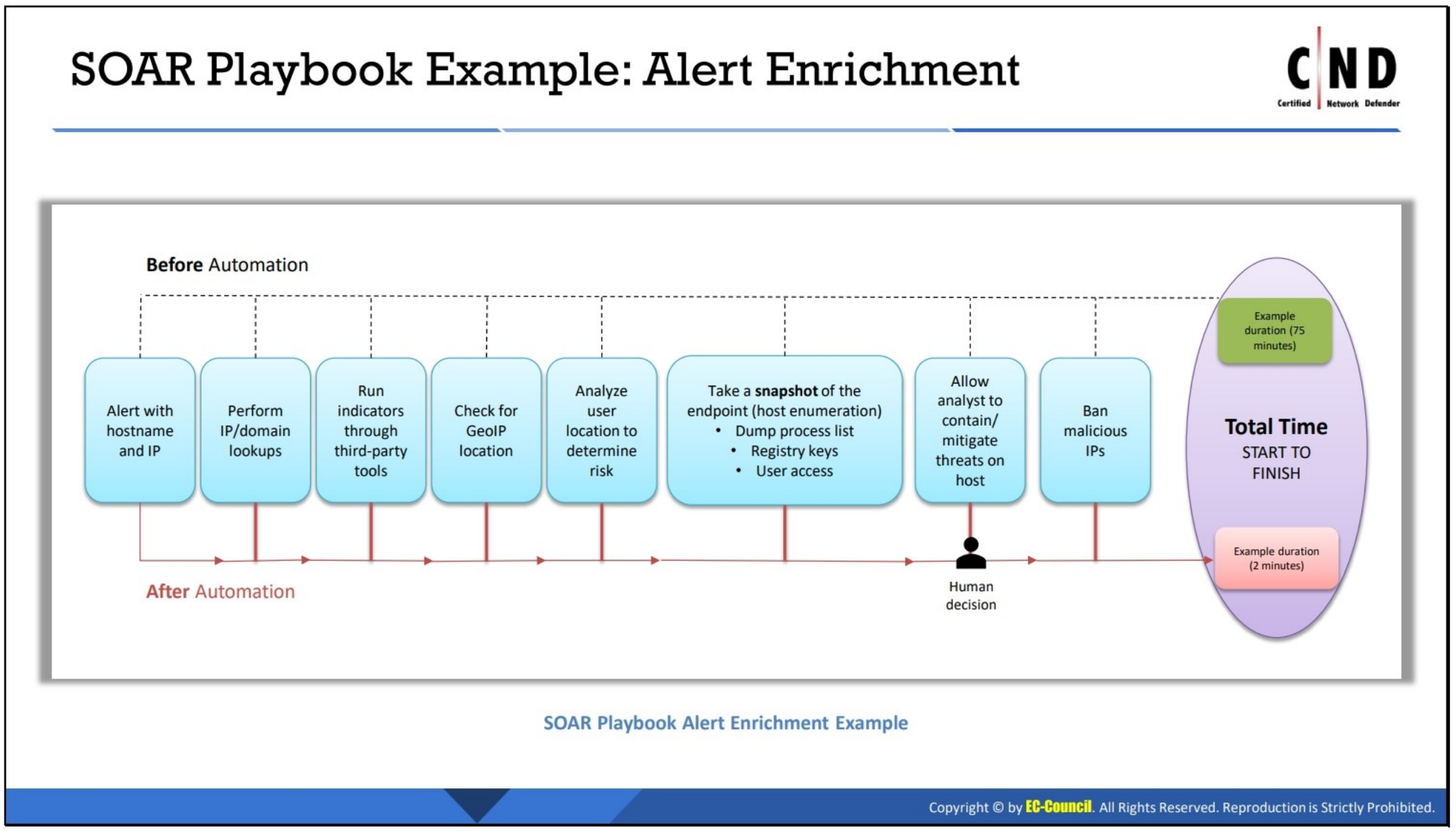


Figure 16.15: Example of malware containment



SOAR Playbook Example: Alert Enrichment

Enrich the quality of the received security alerts, accelerate detection, and weed out false positives automatically. This gives security team greater context to fight the threats.

Follow the below to enrigh alerts using SOAR Playbook

- Stop spending too much time in manually collecting data, automate gathering and compiling relevant context about a security event, switch your focus to incident analysis.
- Optimize operations by automating most repetitive tasks.
- Enrich security alerts with important information such as domain analysis, malware detonation, etc.

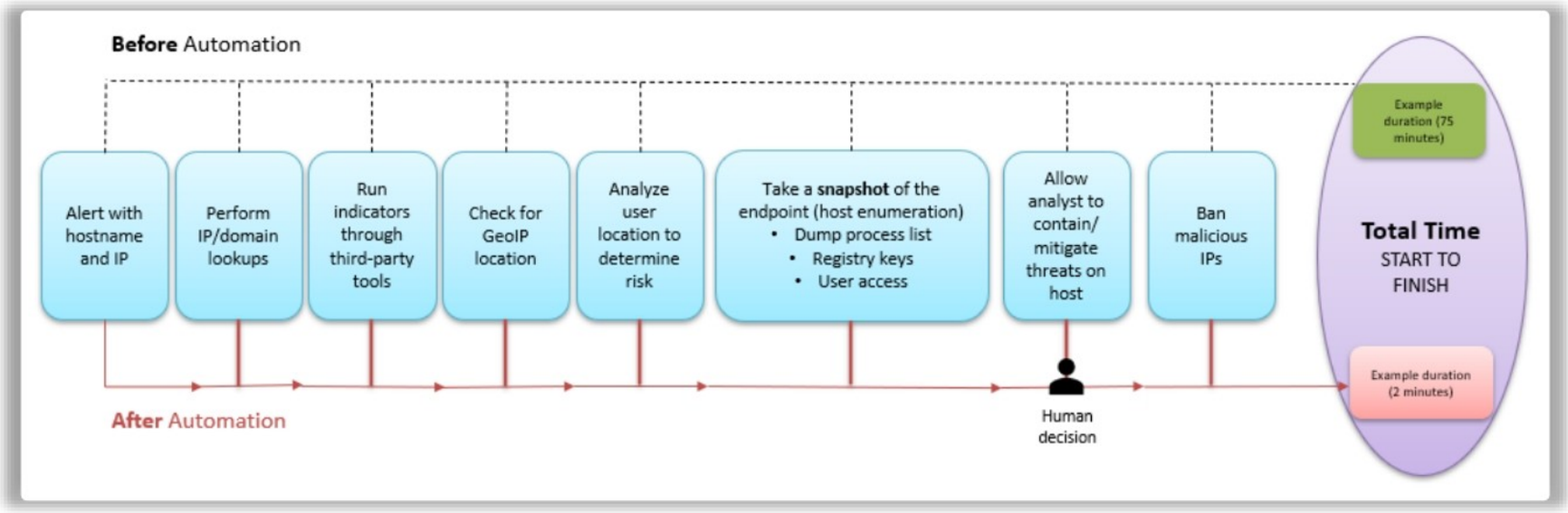
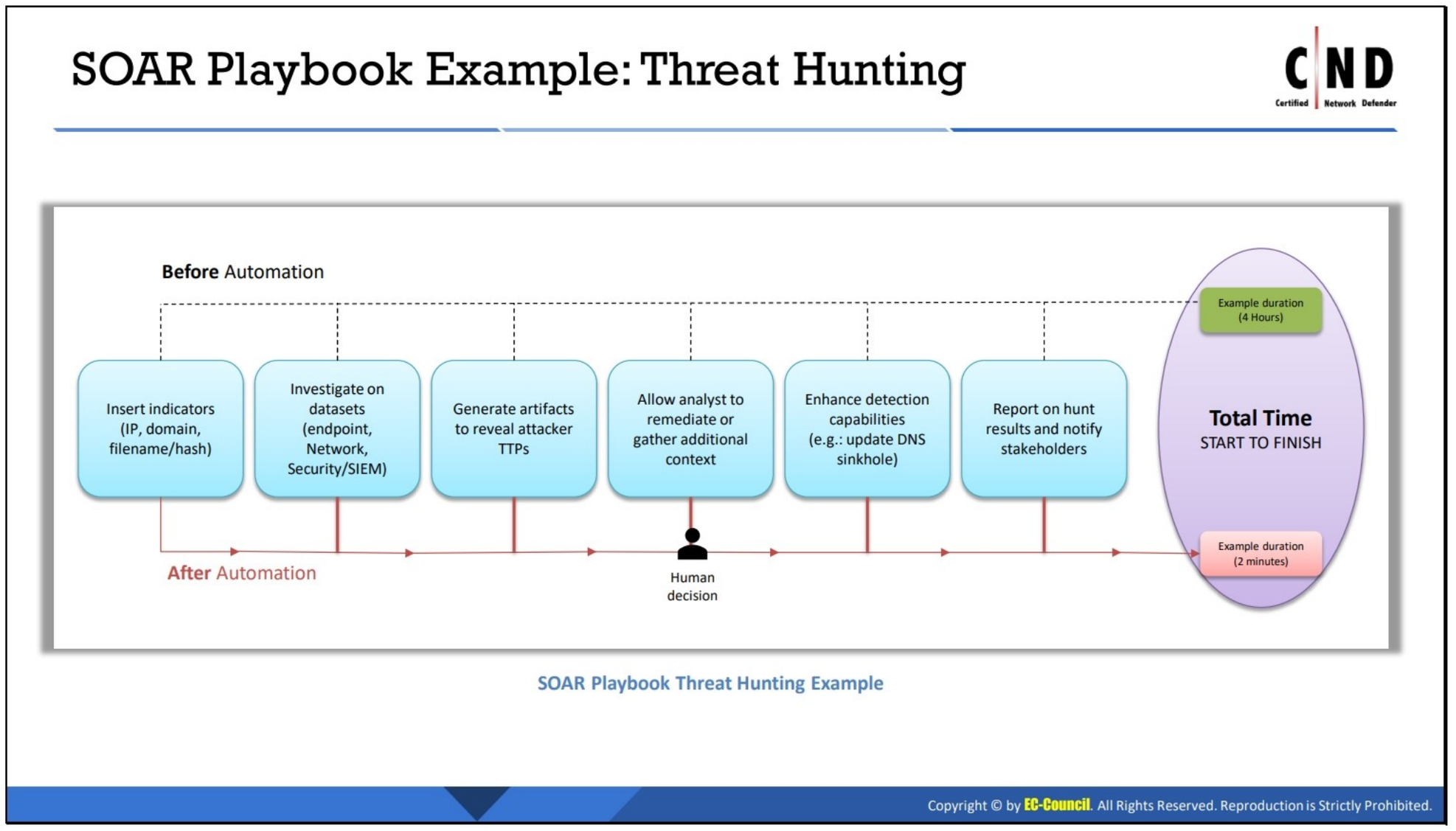


Figure 16.16: Example of alert enrichment using SOAR



SOAR Playbook Example: Threat Hunting

Use SOAR to automate processes around identifying indicators such as suspicious malware and domains.

Follow the below for threat hunting suing SOAR Playbook

- The more comprehensive and proactive will be the threat hunting approaches to mitigate compromise
- Automate repeatable tasks that gives the team to spend additional time on productive processes such as scanning, data enumeration, and to find the flags.
- Follow standard protocols and standard operating procedures in the workflows to let the stakeholders and particular designations in the business hierarchy gets notified as quicky as possible to ensure immediate response.

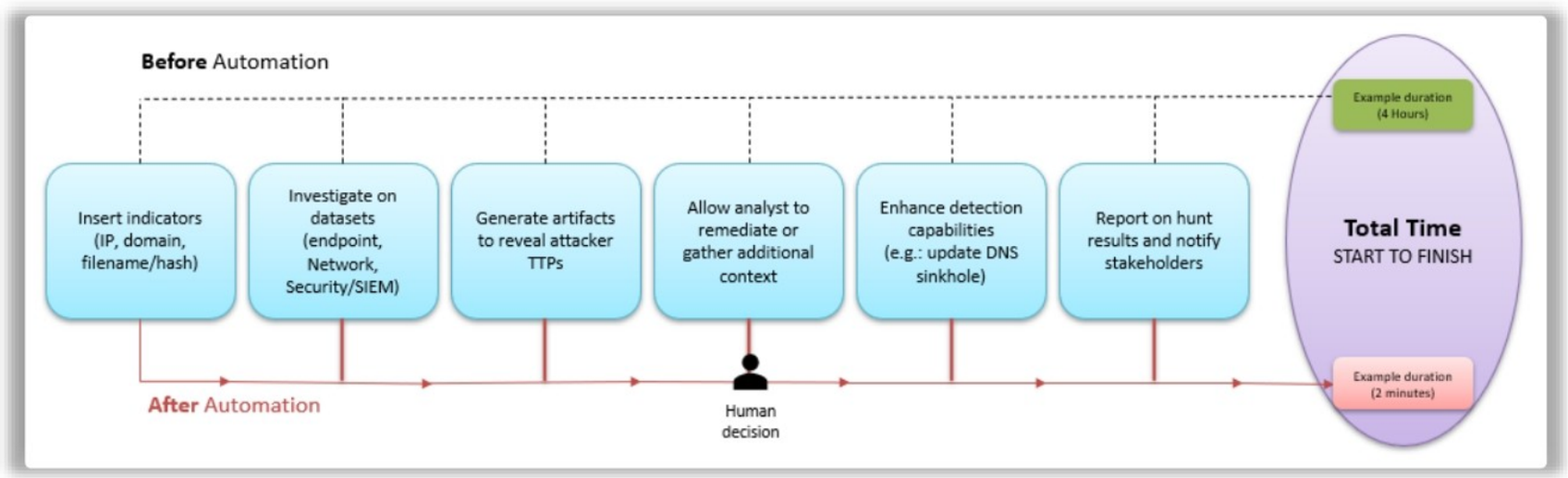
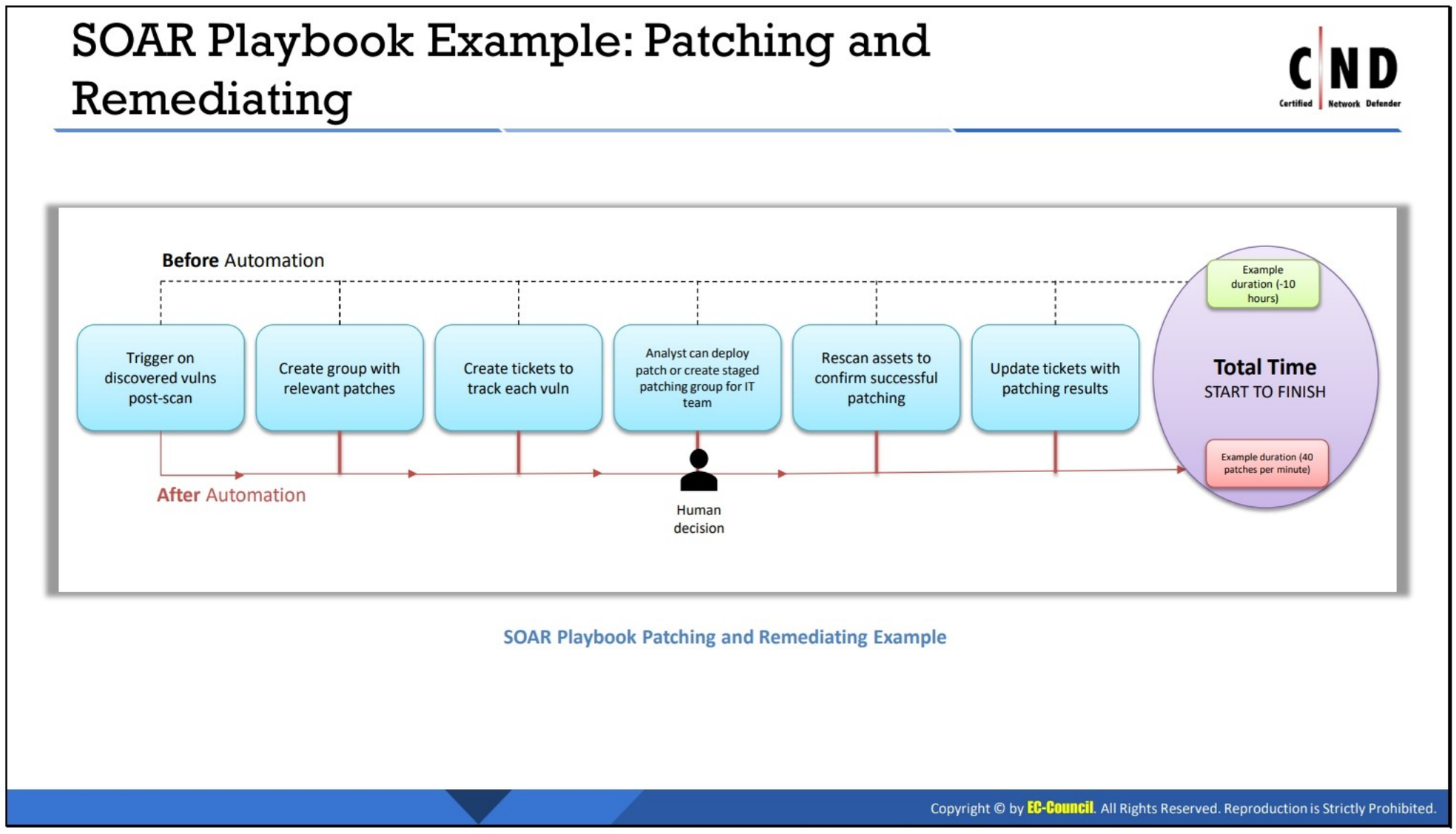


Figure 16.17: Example of Threat Hunting workflow



SOAR playbook Example: Patching and Remediating

Integrate the SOAR solution with the existing orchestration tools of organization from vulnerability detection to vulnerability elimination. This approach ensures to detect critical potential threats and effective patching and remediating.

Follow below to patch and remediate the critical issues using SOAR playbook:

- Build workflows to monitor advisories and come up with decisions as per requirements.
- Automate the creation of service tickets when a vulnerability needs to be addressed.
- Ensure the automation enables tasks to happen within organizational compliances.

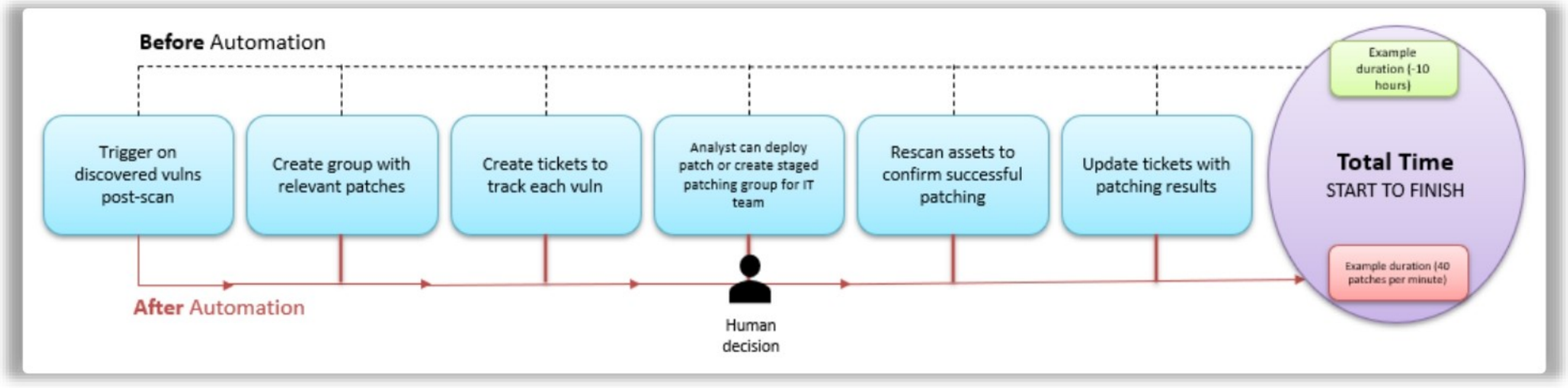
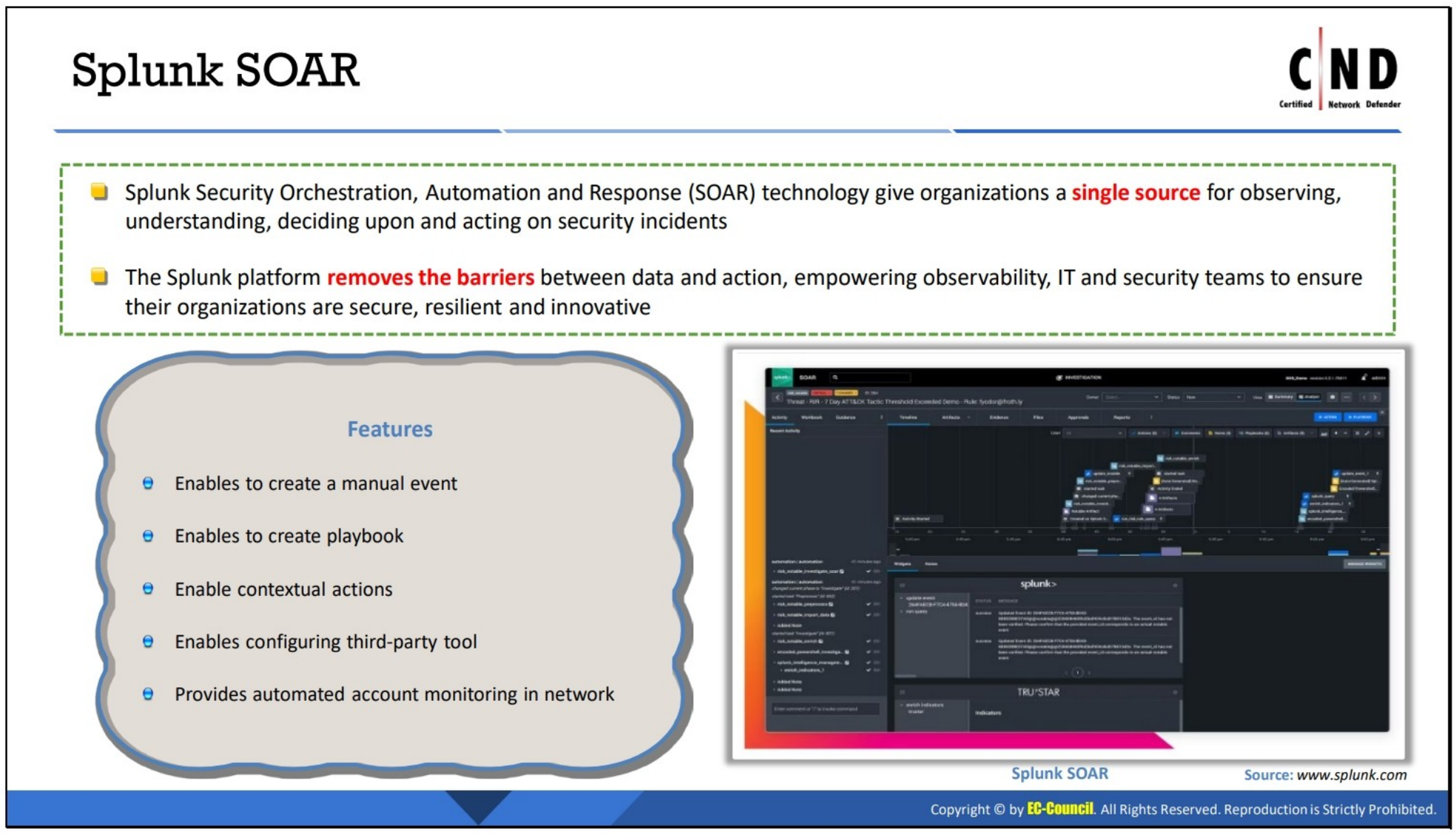


Figure 16.18: Example of patching and remediating.



Splunk SOAR

Source: www.splunk.com

Splunk Security Orchestration, Automation and Response (SOAR) technology give organizations a single source for observing, understanding, deciding upon, and acting on security incidents. The Splunk platform removes the barriers between data and action, empowering observability, IT and security teams to ensure their organizations are secure, resilient and innovative.

Features:

- Enables to create a manual event.
- Enables to create playbook.
- Enable contextual actions.
- Enables configuring third-party tool.
- Provides automated account monitoring in network.

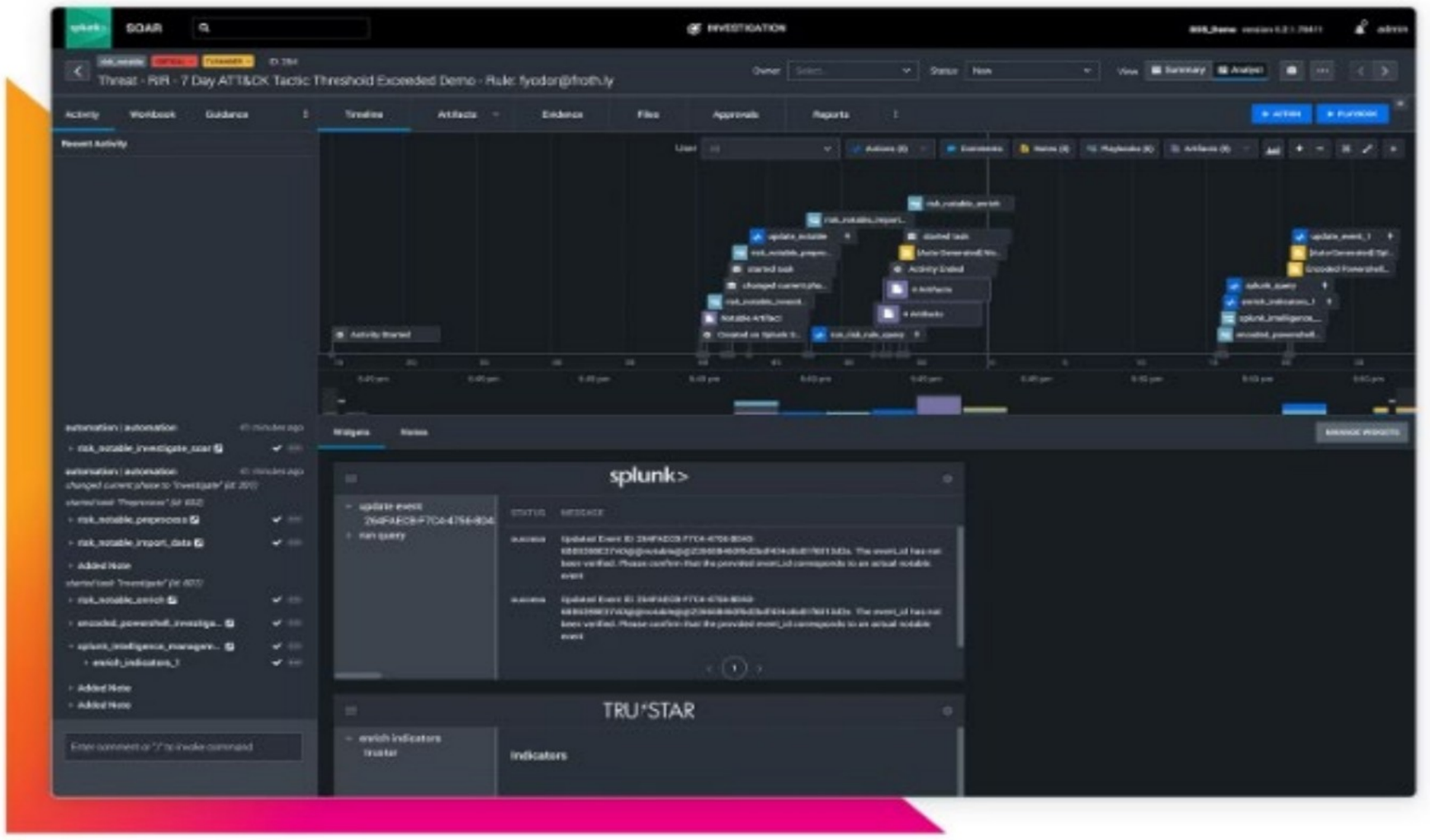
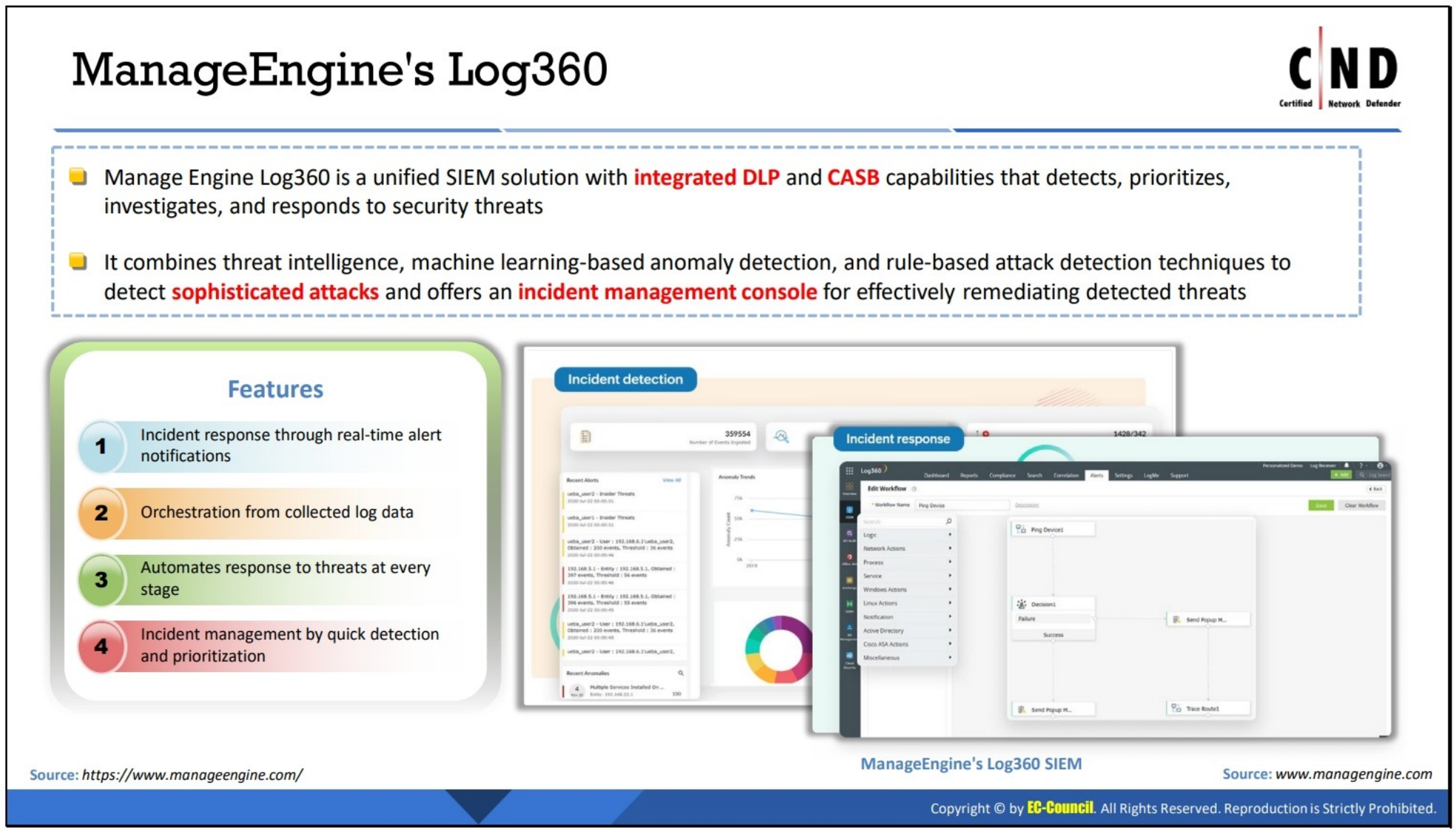


Figure 16.19: Splunk SOAR



ManageEngine's Log360

Manage Engine Log360 is a unified SIEM solution with integrated DLP and CASB capabilities that detects, prioritizes, investigates, and responds to security threats. It combines threat intelligence, machine learning-based anomaly detection, and rule-based attack detection techniques to detect sophisticated attacks and offers an incident management console for effectively remediating detected threats.

Features:

- **Incident response:** Accelerate threat mitigation through real-time alert notifications and automated incident response workflows.
- **Automation:** Automate responses to threats at every stage with prebuilt workflows and automatic ticket assignment.
- **Incident management:** Reduce the mean time to detect (MTTD) and the mean time to resolve (MTTR) an incident by quickly detecting, categorizing, analyzing, and resolving an incident accurately with a centralized console.
- **Orchestration:** Gain meaningful security context from collected log data to identify security events quickly and streamline incident management by integrating with external ticketing tools.

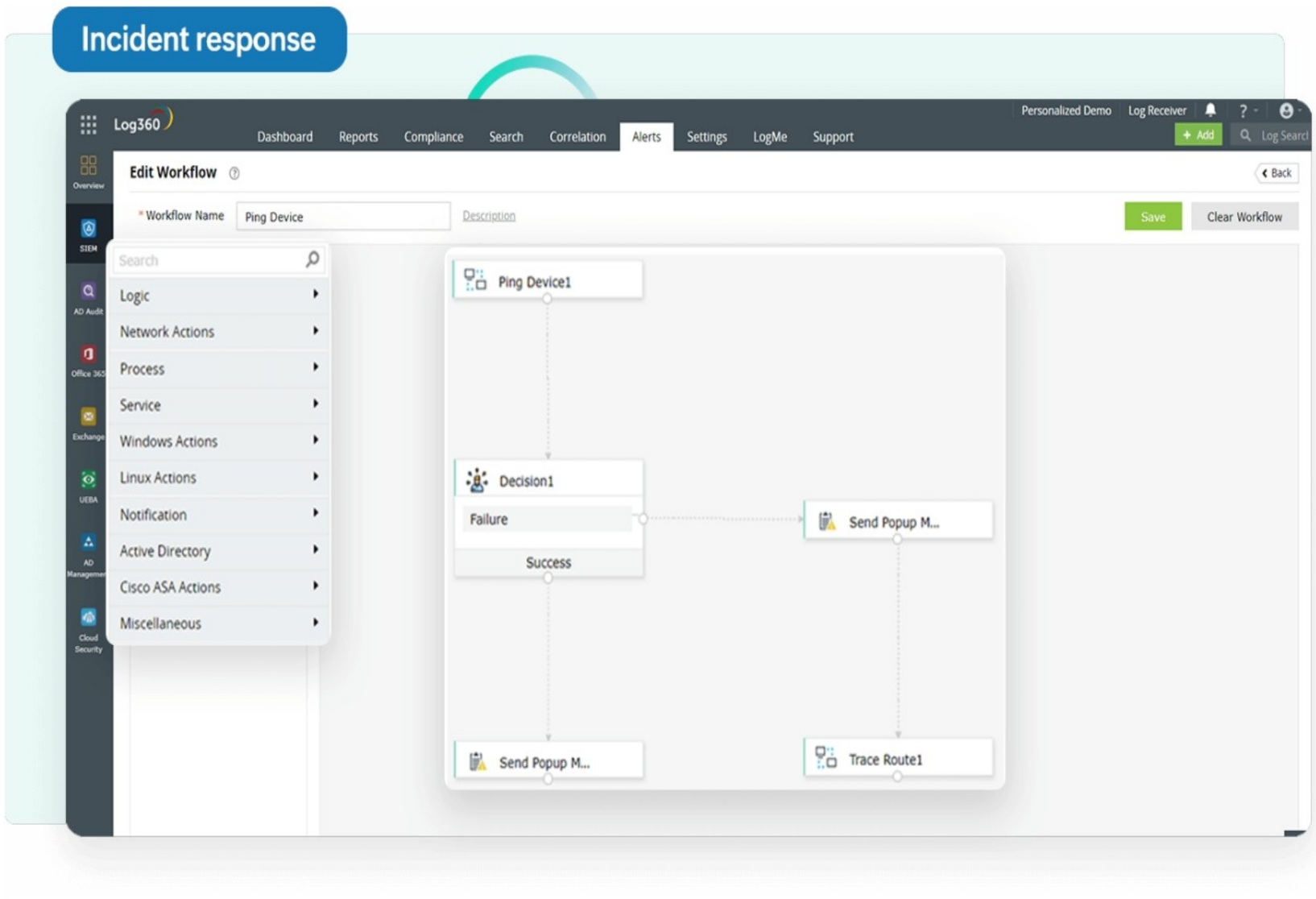


Figure 16.20: ManageEngine's Log360

SOAR Tools

The SOAR tools are as follows.

ServiceNow Security Incident Response

Source: www.servicenow.com

The ServiceNow® Security Incident Response application tracks the progress of security incidents from discovery and initial analysis, through containment, eradication, and recovery, and into the final post incident review, knowledge base article creation, and closure. This tool eliminates manual tasks with automated, intuitive experiences.

Features:

- Respond collaboratively to critical security incidents such as ransomware, data breaches, and other targeted attacks.
- Stay ahead of attackers with the MITRE ATT&CK framework integration, providing advanced context.
- Automate assignments and coordinate incident prioritization and remediation across IT and security.

Heimdal Threat Hunting and Action center

Source: https://heimdalsecurity.com

A single platform to manage alerts, data, and security responses in single window with context & assists at every level. The Heimdal Threat-hunting and Action Centre is a platform that is powered by our advanced XTP engine and fully integrated Heimdal suite. It provides security teams with

an advanced threat and risk-centric view of their entire IT landscape, offering granular telemetry across endpoints and networks for easy decision-making.

Features:

- **Visualize:** Stay vigilant and eliminate the possibility of threats slipping past undetected.
- **Hunt:** Harness the power of intelligent insights to neutralize adversaries.
- **Action:** Respond to threats effectively with the instant action center.
- **Eliminate:** Eliminate alert fatigue & manual investigations.

IBM Security QRadar SOAR

Source: https://www.ibm.com

IBM Security® QRadar® Suite is a threat detection and response solution designed to unify the security analyst experience and accelerate their speed across the full incident lifecycle. The portfolio is embedded with enterprise-grade AI and automation to dramatically increase analyst productivity, helping resource-strained security teams work more effectively across core technologies. It offers integration for endpoint security (EDR, XDR, MDR), log management, SIEM and SOAR, all with a common user interface, shared insights and connected workflows.

Features:

Threat Investigation: The investigation fetches artifacts attached to the case and starts data mining. It consists of MITRE ATT&CK tactics and techniques in a chain graph of the incident.

Automation: Use automation to bridge skill gaps. Artifact correlation, investigation and case prioritization are automated before someone even touches the case.

Breach response: Prepare for and respond to privacy breaches by integrating privacy reporting tasks into your overall incident response playbooks.

Swimlane SOAR

Source: https://swimlane.com

Swimlane's security orchestration, automation and response solution centralize security operations (SecOps) activities. It manages and automates the response to security alerts and incidents identified by existing monitoring and detection systems. Swimlane standardizes response and notification processes to mitigate risk, speed resolution and streamline communications through a purpose-built SecOps management dashboard.

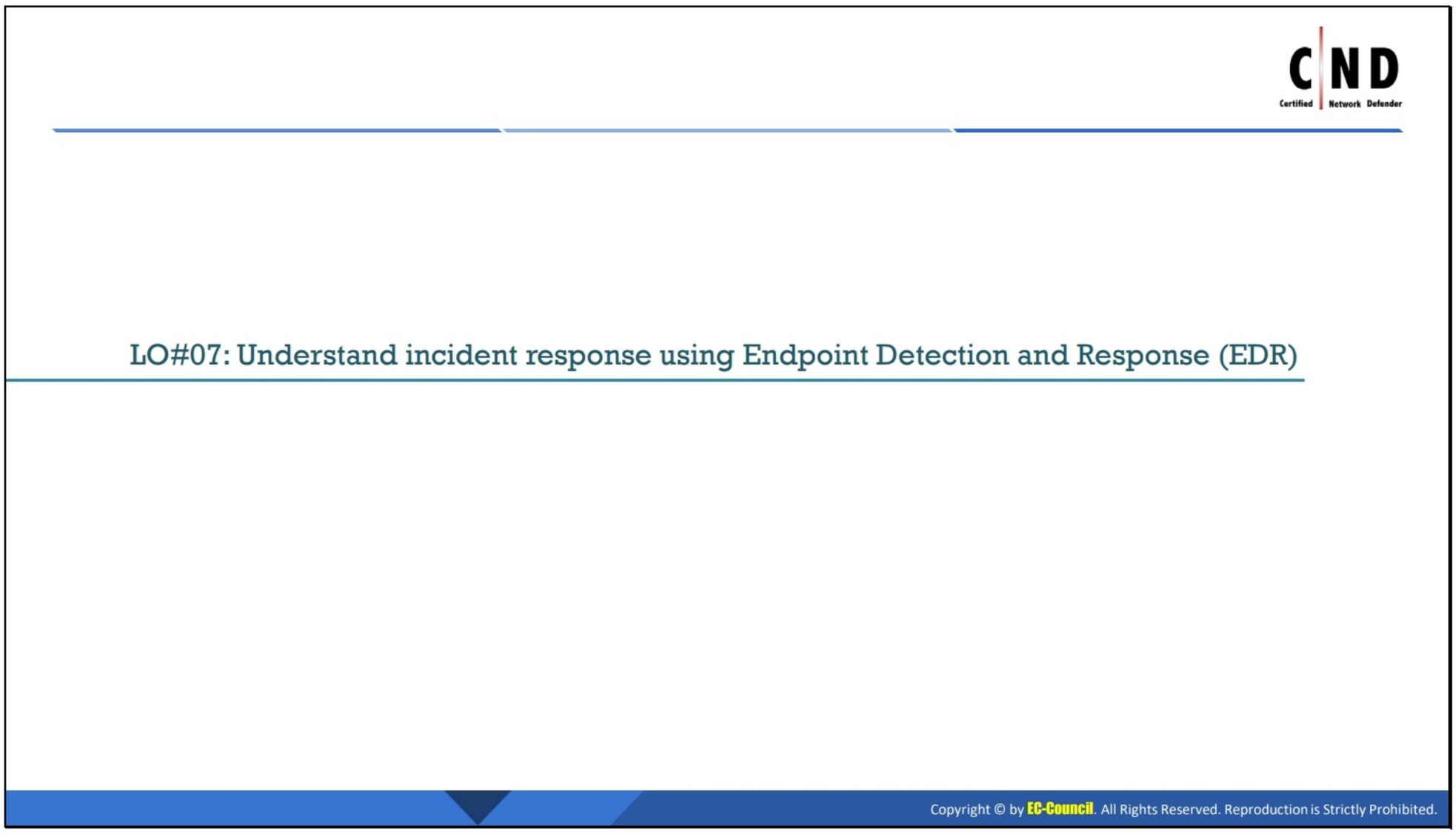
Features:

- Flexible configuration.
- Role based Access control.
- Extended visibility and accessibility.
- Unifies workflow, Elementary and Teams.

Demisto Enterprise security operation platform

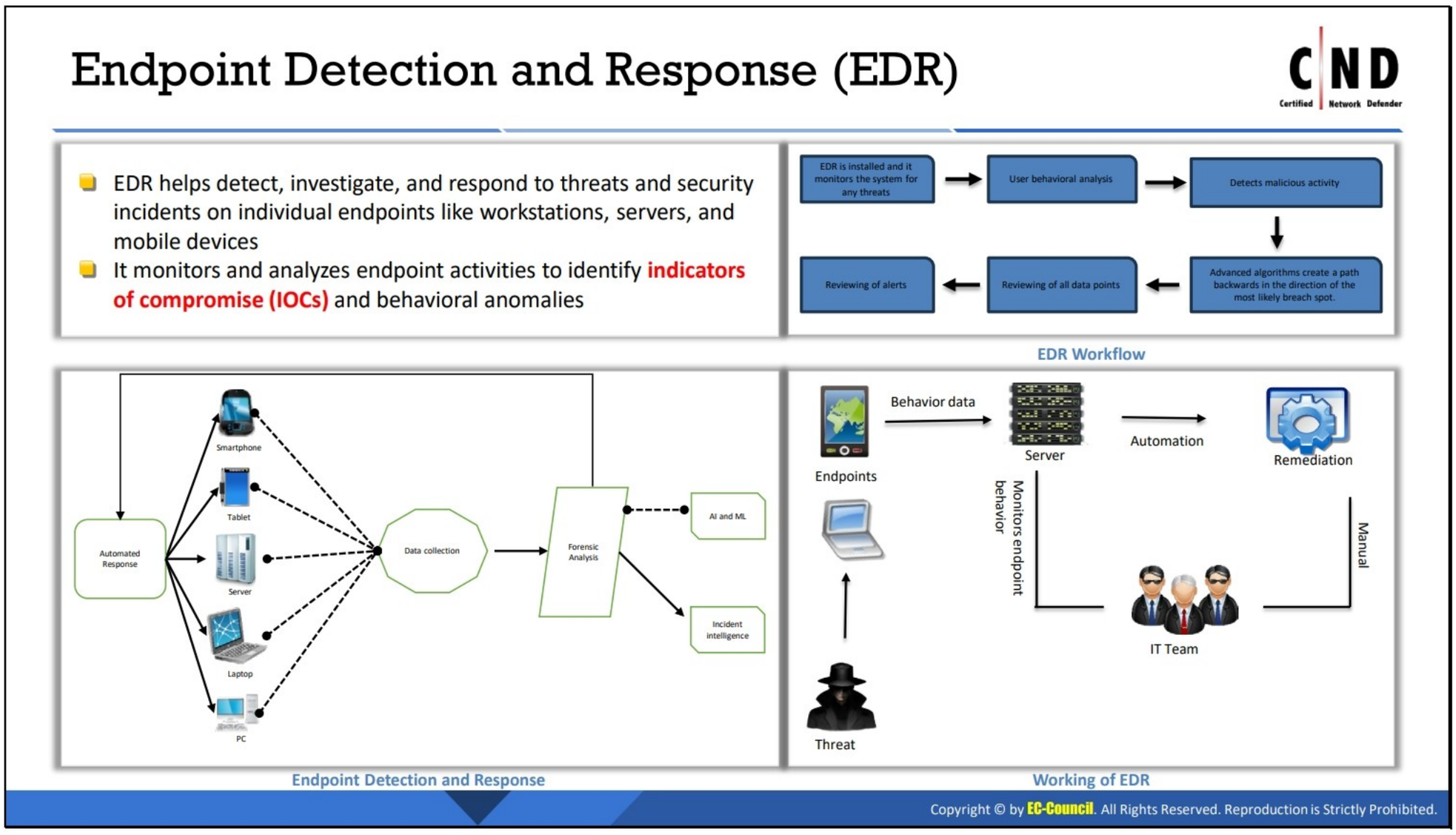
Source: https://apps.paloaltonetworks.com

Demisto is a security orchestration, automation, and response (SOAR) platform that combines full incident management, security automation and orchestration, and real-time collaboration to improve the efficiency of your security operations and incident response. The Demisto app on Cortex™ provides automated alert ingestion, real-time execution of response actions within Demisto, and unified activation of your security product stack through task-based playbooks.



LO#07 Understand Incident Response using Endpoint Detection and Response (EDR)

In the rapidly evolving landscape of cybersecurity, Endpoint Detection and Response (EDR) has emerged as a critical pillar in the realm of incident response. EDR not only provides real-time visibility into endpoint activities but also equips organizations with the capability to swiftly identify, investigate, and mitigate security incidents at the source. This section delves into the pivotal role of EDR in bolstering incident response strategies, offering granular insights into endpoint behavior, and fortifying the overall cybersecurity posture of organizations in the face of persistent and sophisticated threats.



Endpoint Detection and Response (EDR)

EDR systems establish a robust defense mechanism against evolving cyber threats by isolating compromised endpoints and blocking malicious network traffic. Their ability to initiate remediation processes ensures that potential risks are mitigated before they escalate, thereby enhancing the organization's overall security posture. This proactive approach not only safeguards sensitive data but also fosters trust among stakeholders, leading to the development of a resilient and agile cybersecurity architecture.

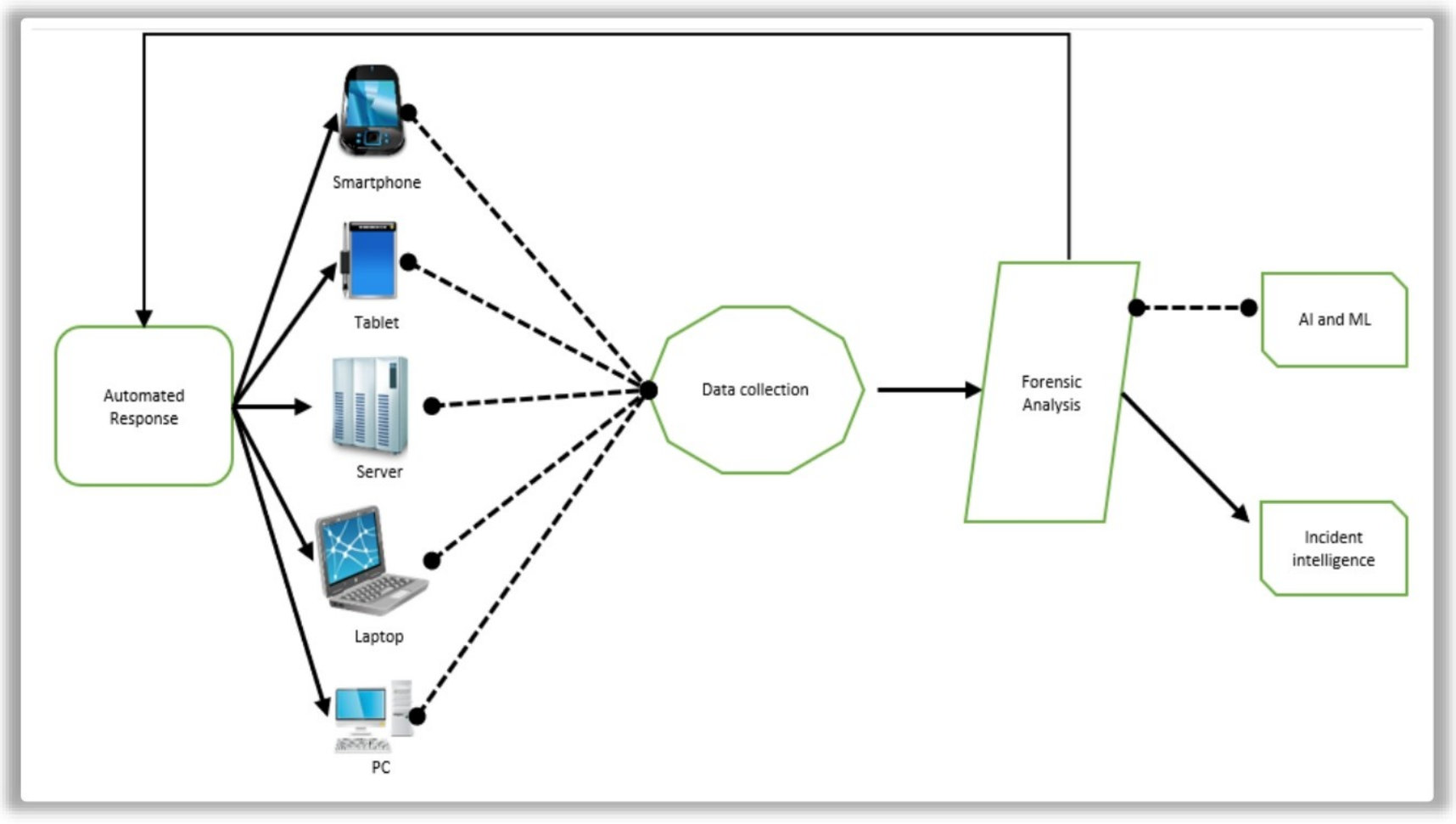


Figure 16.21: Representing Endpoint Detection and Response

How does EDR work?

An EDR solution works in the following manner:

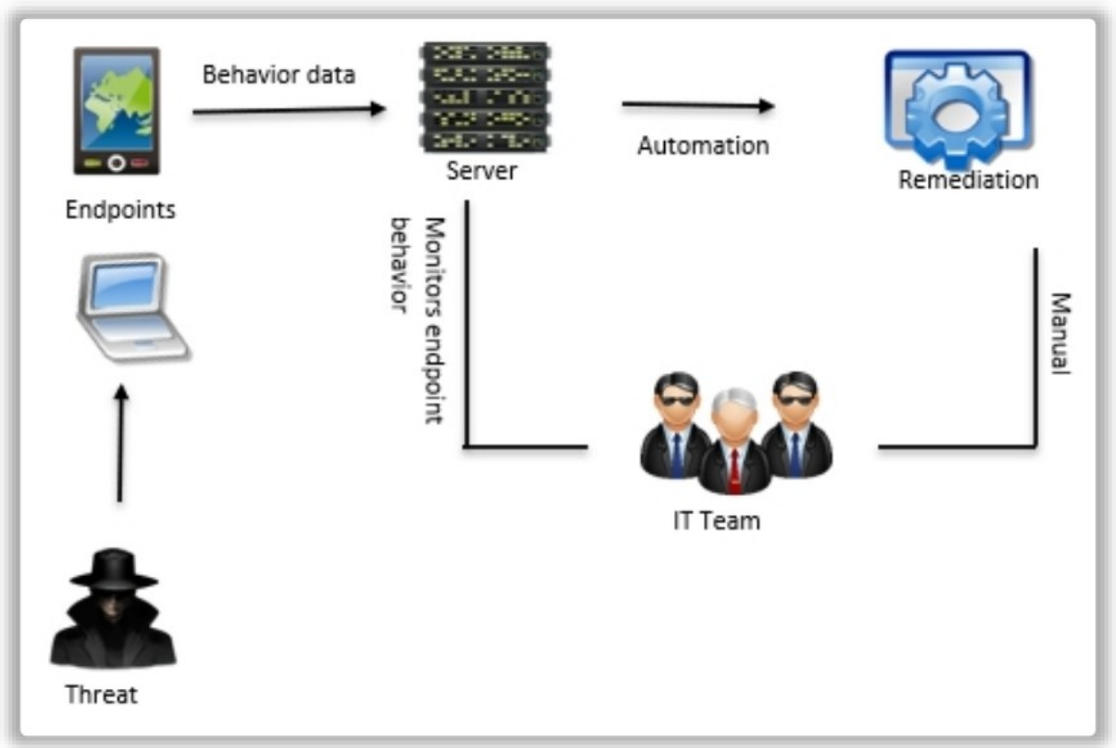


Figure 16.22: Working of EDR

- **Detect security incidents:** The core role of an EDR solution is to identify cyber threats. It continuously monitors and analyzes network traffic to precisely detect potential threats and take control measures to eliminate them. When malicious activity is detected, the EDR solution flags incoming files.
- **Threat actors:** These are individual groups or malicious actors that pose potential threats to the organization by compromising various security layers.
- **Contain the Incident at the endpoint:** In this step, an EDR solution halts the cyber threat upon identifying a dangerous file. This containment reduces the impact of an attack on processes, applications, and users, minimizing the network's exposure to the virus.
- **Investigate security incidents:** When a cyberattack occurs, an EDR solution conducts an investigation to gain insights into how it happened, whether it resulted from endpoint or network vulnerabilities. The findings of this investigation can help prevent similar future attacks.
- **Remediation:** In this step, the network can be automatically restored using the investigative findings, returning it to its pre-infestation state. Remediation is executed using automated models that incorporate investigative findings and root cause analysis to restore the network's original condition.

EDR Workflow

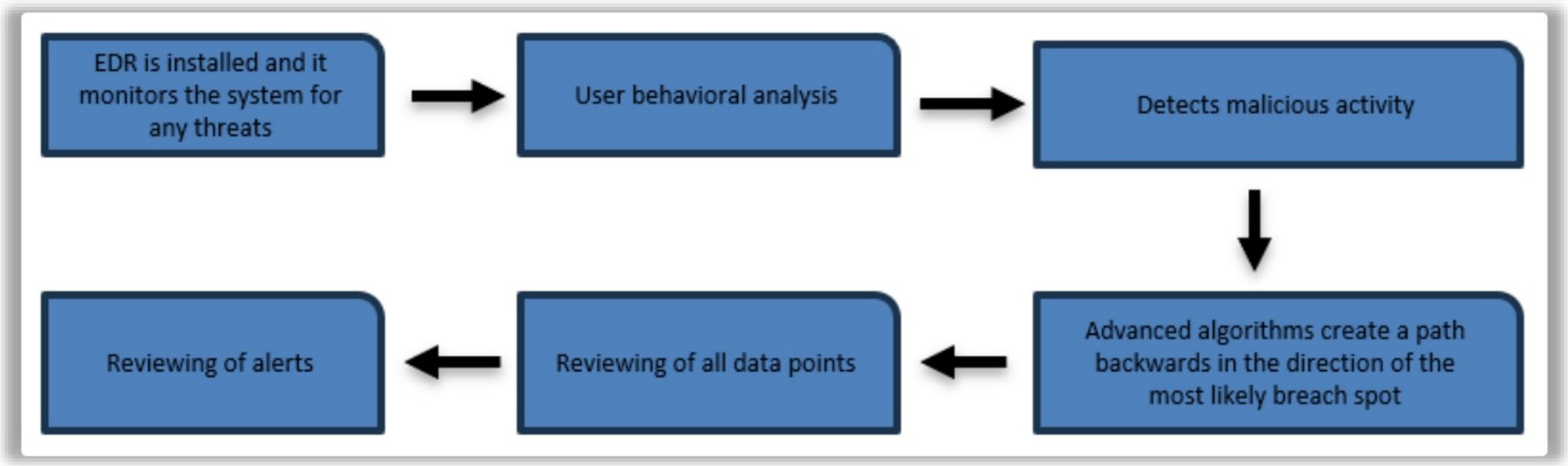
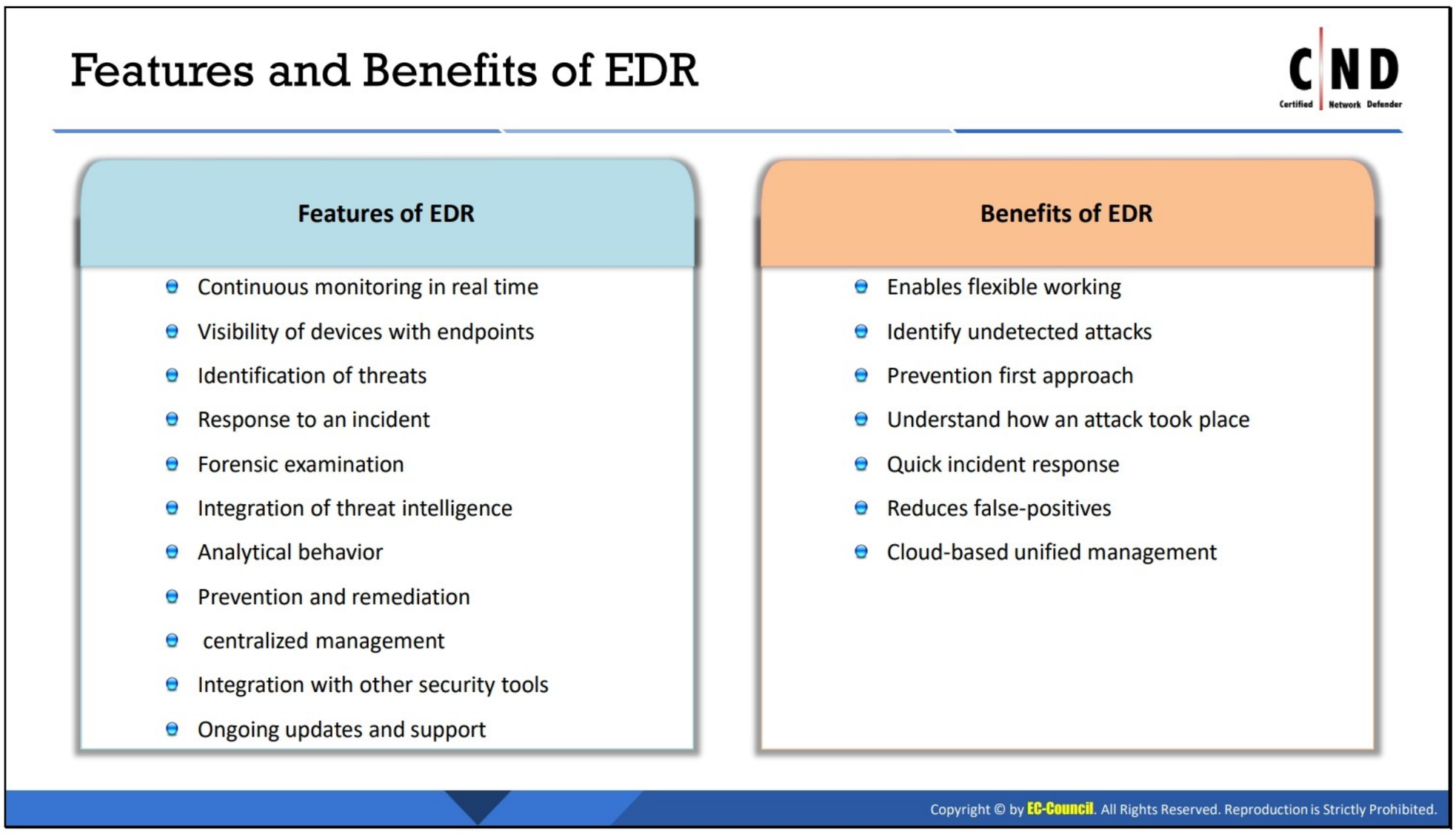


Figure 16.23: EDR Workflow

Endpoint detection and response (EDR) initiates comprehensive threat monitoring within the system upon installation. It employs advanced behavior analysis algorithms to identify patterns and connections between various actions. EDR operates diligently, ensuring real-time threat awareness by consistently detecting and reporting potentially harmful activities. It traces the routes of suspicious activities using sophisticated algorithms to pinpoint the most probable compromise location, thereby enhancing its effectiveness in threat assessment. Additionally, the system categorizes extensive datasets, enabling more efficient evaluations. Dedicated analysts and engineers rigorously assess this processed information, delivering essential insights to customers and thereby enhancing the system's security posture and enabling proactive threat mitigation.



Features and Benefits of EDR

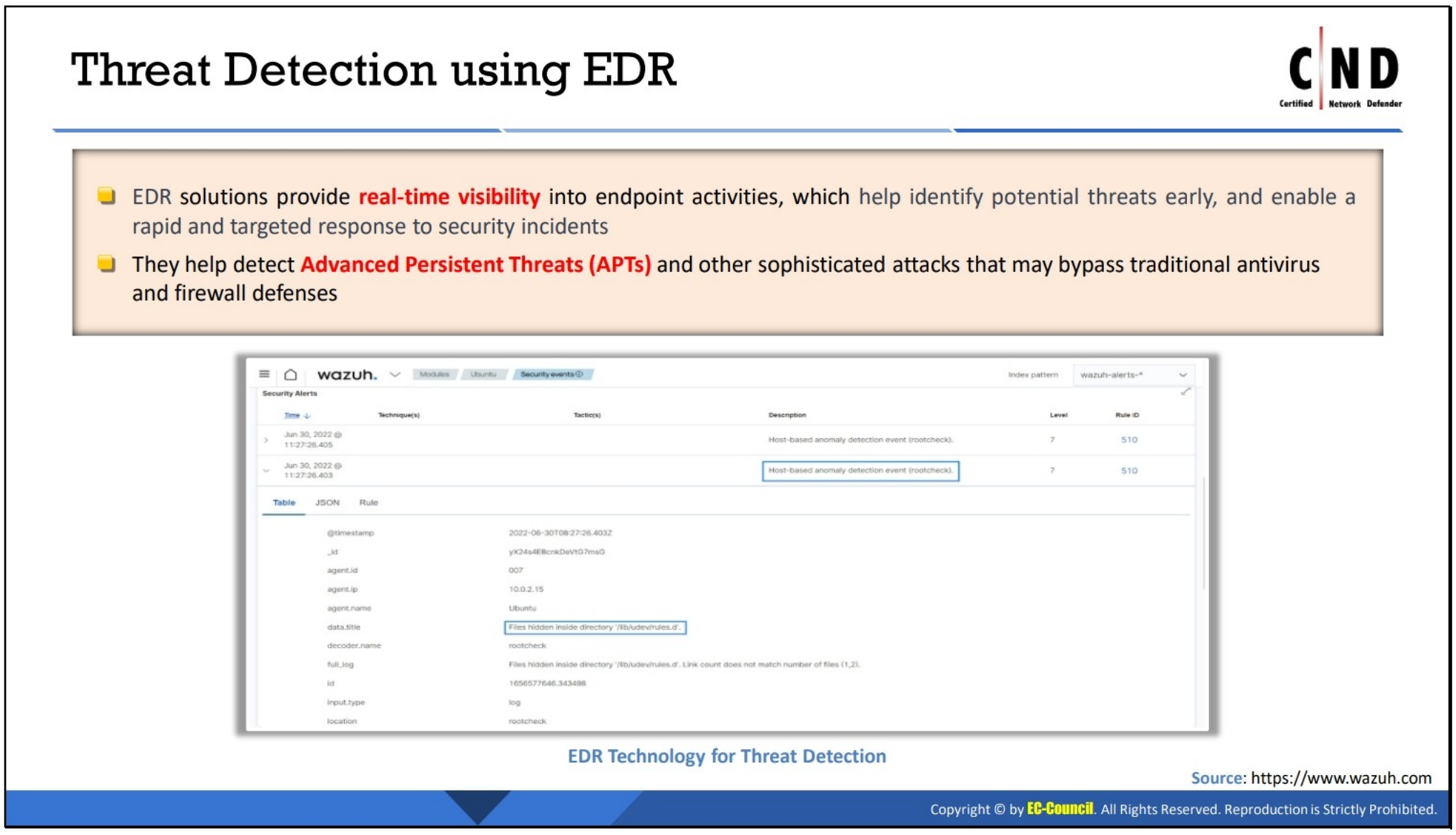
The features of EDR are as follows:

- **Continuous monitoring in real-time:** Endpoints within the network are continuously monitored to detect abnormal operations and potential threats.
- **Visibility of devices with endpoints:** Security teams should have full visibility into details about devices and their functions on each endpoint, including processes, applications, network connections, and user behaviors.
- **Identification of threats:** The EDR system employs sophisticated threat detection techniques, including behavior analysis, machine learning, signature-based detection, and automated incident response, to identify potential threats or signs of compromise.
- **Response to an incident:** When a vulnerability is detected, the EDR solution enables prompt responses, such as isolating affected endpoints or quarantining suspicious data.
- **Forensic examination:** EDR systems have comprehensive forensic investigation capabilities that allow security teams to conduct in-depth analysis of incidents, identify root causes, and gather evidence for remediation and legal proceedings.
- **Integration of threat intelligence:** The EDR system enhances its detection capabilities by integrating with external threat intelligence sources, utilizing the latest information on known threats, indicators of compromise, and malicious IP addresses or domains.
- **Analytical behavior:** The EDR solution utilizes behavioral analytics to establish a baseline of typical endpoint behavior, effectively identifying abnormalities. These signs may indicate a security breach or behavioral anomaly.

- **Prevention and remediation:** The automated approach aids security teams in precisely mitigating potential risks and threats to the organization by identifying malicious data and implementing stringent compliance measures proactively.
- **Centralized management:** Both SIEM and CSIR teams can access the entire endpoint security architecture through a single interface. The EDR solution offers centralized administration and reporting procedures.
- **Integration with other security tools:** Integration with security systems like firewalls, threat intelligence platforms, and SIEM (Security Information and Event Management) enhances overall security posture and enables more comprehensive threat detection and response.
- **Ongoing updates and support:** To stay abreast of newly discovered threats and vulnerabilities, the EDR system undergoes regular updates, incorporating new threat signatures, detection algorithms, and software patches.

The benefits of implementing EDR in an organization are as follows:

- **Enables flexible working:** Advanced technology, such as automated incident handling strategies, defends network endpoints against cyberattacks. EDR reduces the need for significant human intervention, allowing IT and security teams to manage operations efficiently. This flexibility enables organizations to work from various geographic locations and adapt priorities accordingly.
- **Identify undetected attacks:** EDR adds an additional layer of security to the organization's security posture by detecting potentially hidden security events. EDR solutions provide analysts with a list of suspicious events, prioritizing threats based on their threat score.
- **Prevention first approach:** EDR solutions employ proactive threat detection techniques to identify and eliminate potential attacks before attackers have the opportunity to execute malicious code and compromise target systems.
- **Understand how an attack took place:** EDR offers a comprehensive investigative approach and root cause analysis, allowing organizations to understand the reasons behind cyberattacks.
- **Quick Incident response:** EDR tools empower security teams with automated strategies to efficiently mitigate and respond to threats.
- **Reduce false positives:** The use of high-quality and accurate features provided by the EDR tool is essential for reducing false positives. This capability allows the security posture to employ a trial-and-error approach, enabling the early identification of red flags.



Threat Detection using EDR

Threat detection refers to the process of examining and assessing a network or computer system for malicious applications and data. EDR not only facilitates the timely identification and mitigation of various threats but also continuously analyzes user behavior and the activities of other devices on the network. This allows it to detect threats like ransomware and the presence of malware by identifying abnormal activities, ensuring accurate anomaly detection in the software. The Wazuh file integrity monitoring (FIM) module can be used to locate malicious files on inspected endpoints.

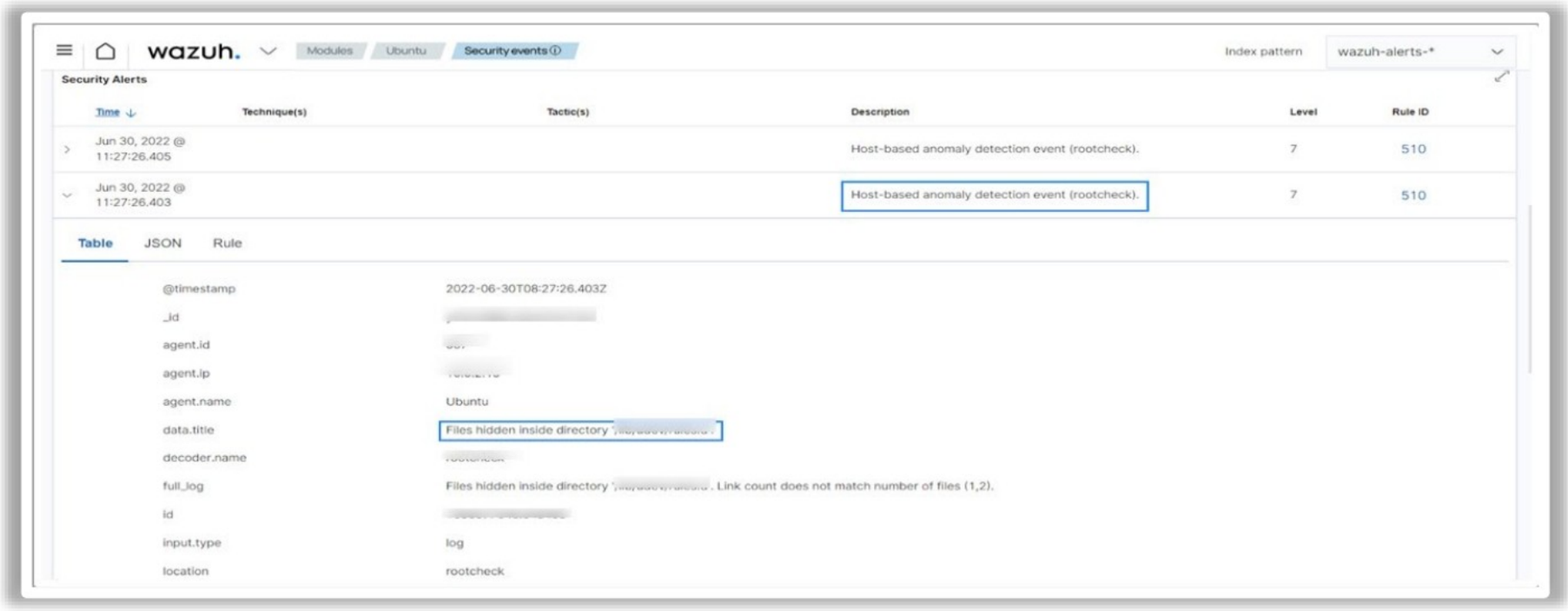
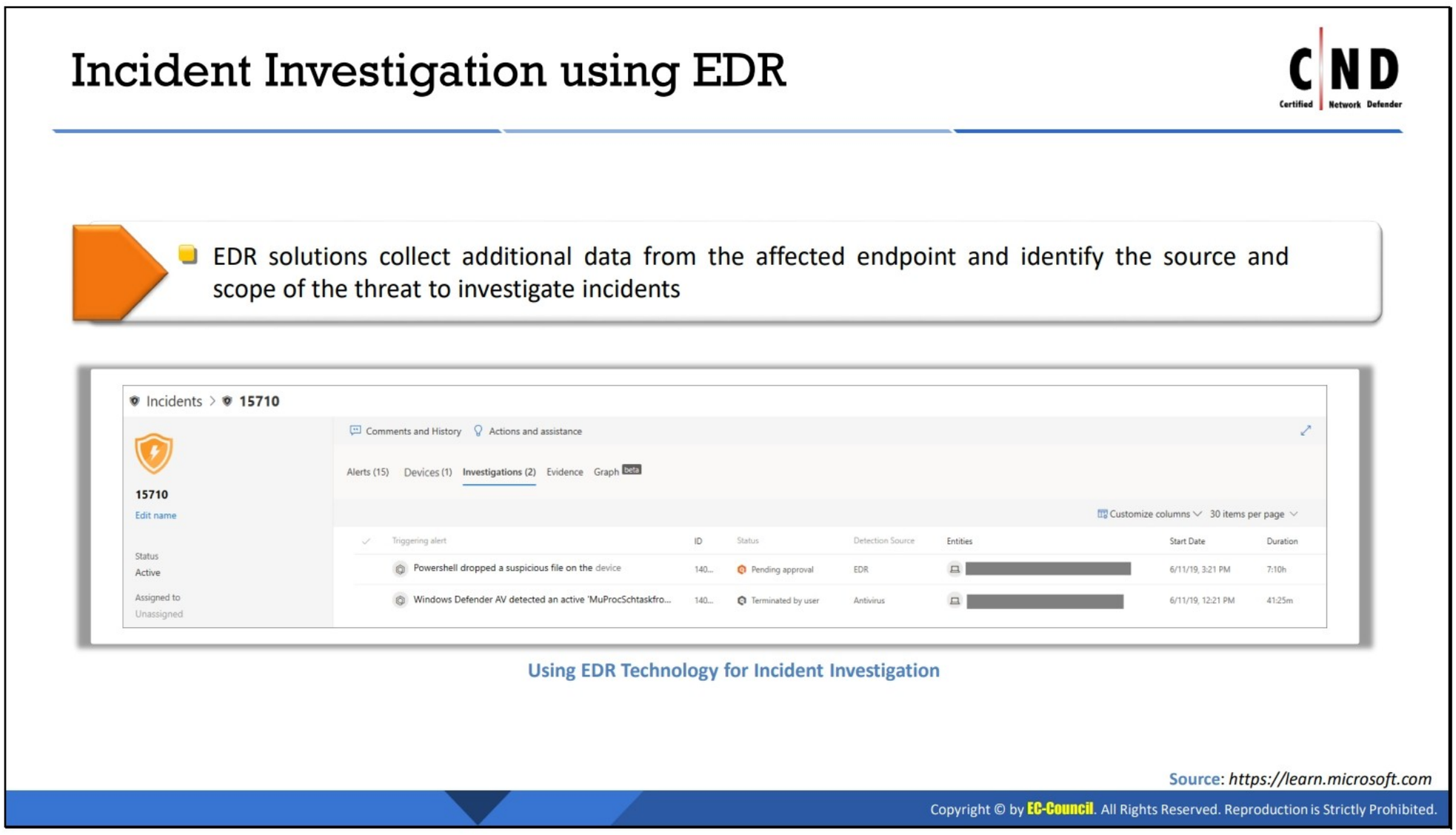


Figure 16.24: Use of EDR for Threat Detection using Wazuh

Through EDR technologies' log gathering, organizations can effortlessly collect logs from various external malware detection programs. Leveraging Wazuh's robust log-gathering capabilities provides a comprehensive view of their security infrastructure. Wazuh systematically collects and verifies logs from multiple malware detection technologies, enabling thorough analysis and examination to enhance the organization's cybersecurity protocols.



Incident Investigation using EDR

The term "incident investigation" refers to the meticulous technique and process of investigating and evaluating an incident that occurred within the organization to determine its cause, effects, and other relevant variables. An EDR tool possesses proficient threat detection, investigation, and response capabilities, including incident data analysis, investigation alert triage, verification of suspicious activities, threat hunting, and detection and containment of malicious activities.

Investigation Process

- **Data collection:** In the initial step, data is gathered from logs of endpoint devices, containing information about network connections and user activities within the network.
- **Threat detection:** In this step, data is analyzed to uncover anomalies and potential threat indicators.
- **Alert generation:** This process involves notifying the organization's hierarchy about unexpected attacks resulting from unchecked vulnerabilities. EDR performs this process for enterprises.
- **Incident prioritization:** EDR solutions prioritize threats based on their severity and impact on the organization. Higher-risk threats receive higher priority and are addressed first.
- **Incident investigation:** In this step, security analysts, using an EDR console, identify and examine compromised endpoints.
- **Threat hunting:** This proactive step involves conducting threat hunting to detect hidden threats.
- **Threat containment and eradication:** EDR solutions isolate identified threats and prevent their further movement within the network.

- **Remediation:** Preventive measures are applied before potential threats are identified and discovered. This allows security teams to remediate them early to prevent the high impact caused by specific cyber threats.

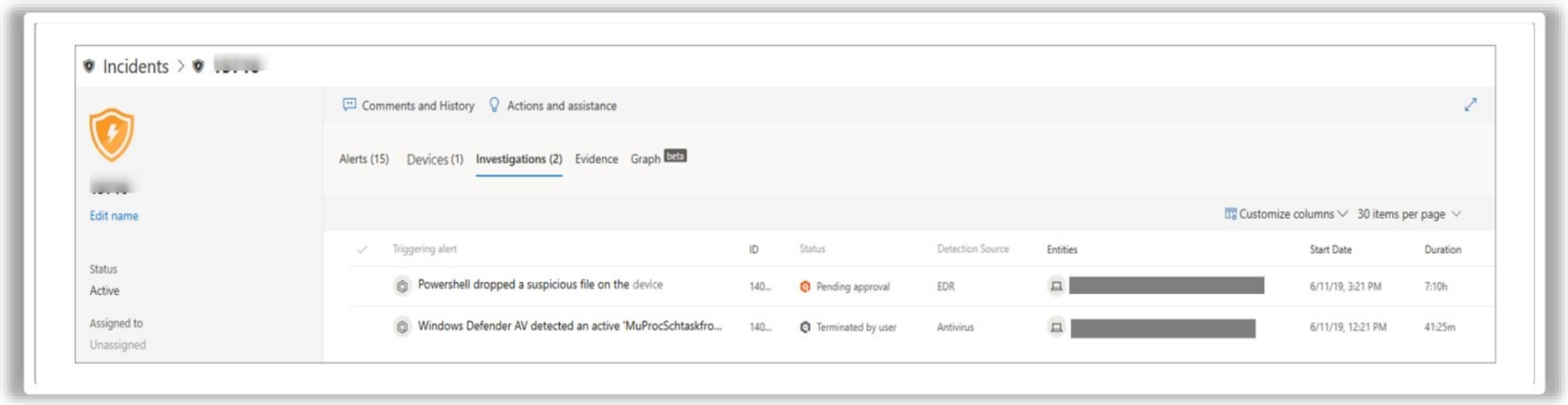
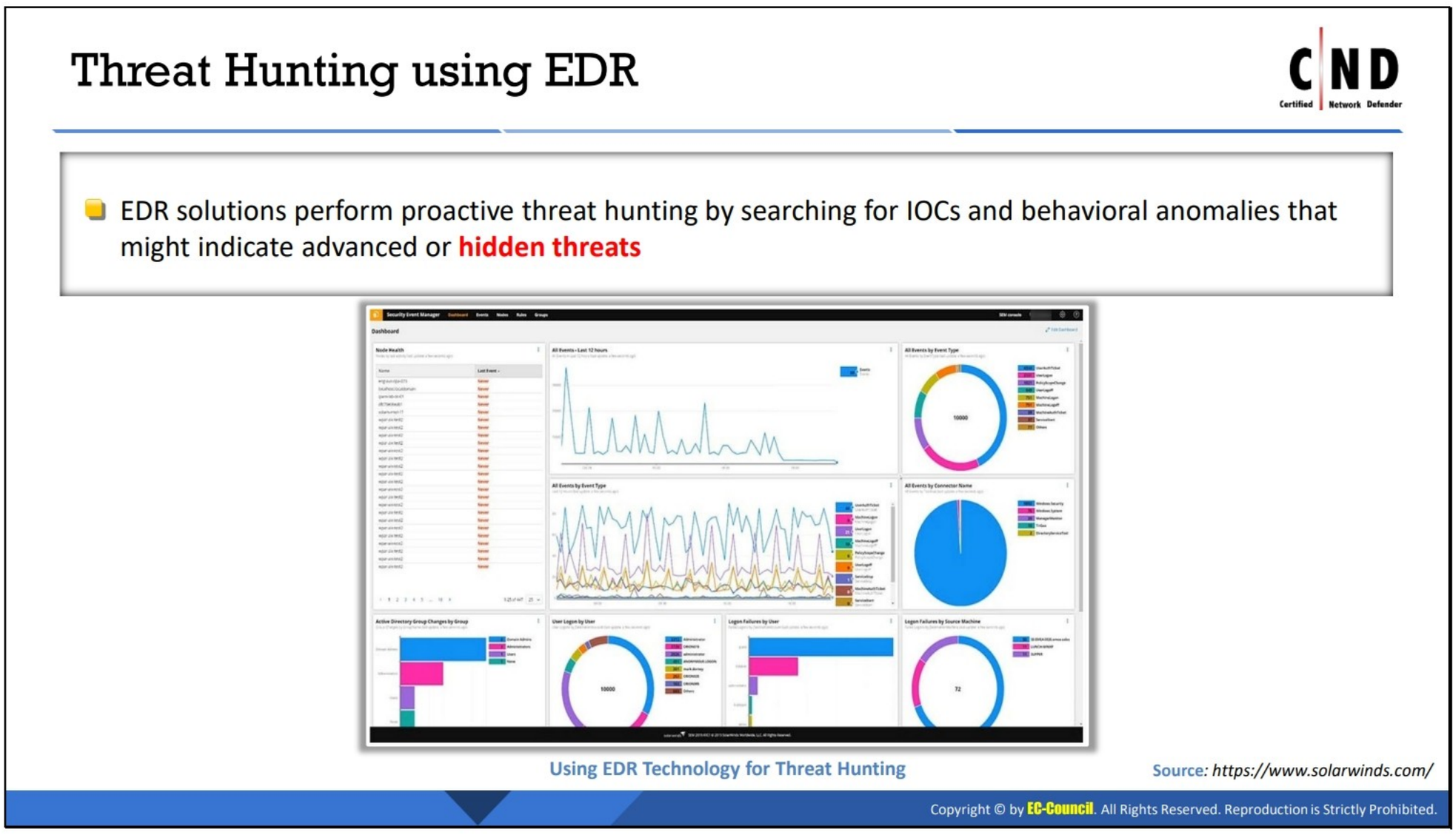


Figure 16.25: Using EDR Technology for Incident Investigation

The image portrays various abnormal incidents and displays the suspicious files detected by the EDR tool. Additionally, it showcases Windows Defender identifying active malicious content. This visual representation aids in identifying the sources of detection.

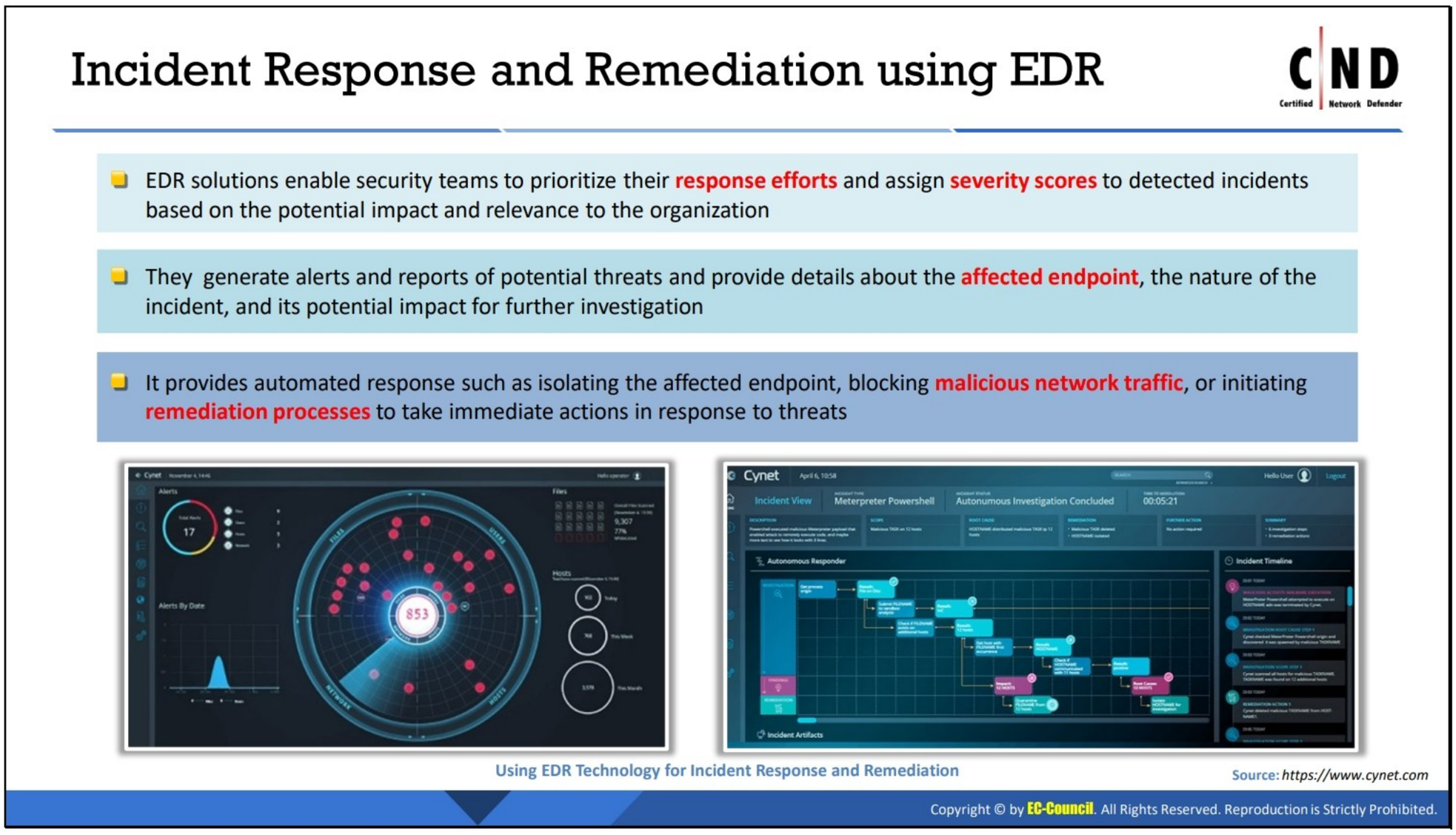


Threat Hunting using EDR

Using EDR, a Threat Hunter thoroughly examines and assesses network activities to gain comprehensive insights into minute details. This activity persists until the incident is confirmed to be harmless, providing critical validation of the system's integrity. This ensures a comprehensive analysis through EDR capabilities and features, enabling enterprises to effectively identify and respond to high-priority threats, thereby enhancing the overall security posture of the network. Real-time monitoring and the utilization of advanced algorithms contribute to the effectiveness of this process.

Figure 16.26: Using EDR Technology for Threat Hunting

In this context, the ECR tool provides graphical representations of spikes in network behavior and categorizes various events by type. It also presents information about the connectivity of devices within the network and the health status of nodes. This detailed visualization not only improves network monitoring but also enables enterprises to make quick decisions, facilitating the resolution of connection issues and ensuring the overall stability of their network infrastructure.



Incident Response and Remediation using EDR

Utilizing EDR in incident response plays a critical role in the analysis of endpoints. It identifies and prevents attacks in their early stages, thus mitigating the potential risks of their propagation. These technologies leverage powerful behavior engines, enabling security teams to monitor every phase of an attack in real-time. Modern EDR systems can automatically detect and flag abnormalities within the network and provide recommendations to mitigate the impact of cyberattacks through continuous endpoint evaluation. In cases where rogue processes are identified, EDR systems promptly shut down the affected devices to prevent pivot attacks. EDR also assists the network in limiting the impact of a successful attack, underscoring the development of robust defensive mechanisms.

EDR solutions assist security teams by enabling them to more effectively direct their response efforts. Security teams can prioritize the resolution of the most critical risks by assigning severity rankings to observed incidents based on variables such as potential effects and their impact on the enterprise. This proactive approach enhances the organization's overall security posture by facilitating a timely and targeted response to high-impact security concerns.

These systems offer warnings and detailed reports that furnish essential information about potential risks. Security teams gain comprehensive insights into the issue by providing information about the compromised endpoint, the nature of the event, and its potential consequences. This approach equips them with the necessary data for effective investigation and rapid response, enhancing the organization's resilience in addressing unforeseen cybersecurity threats.

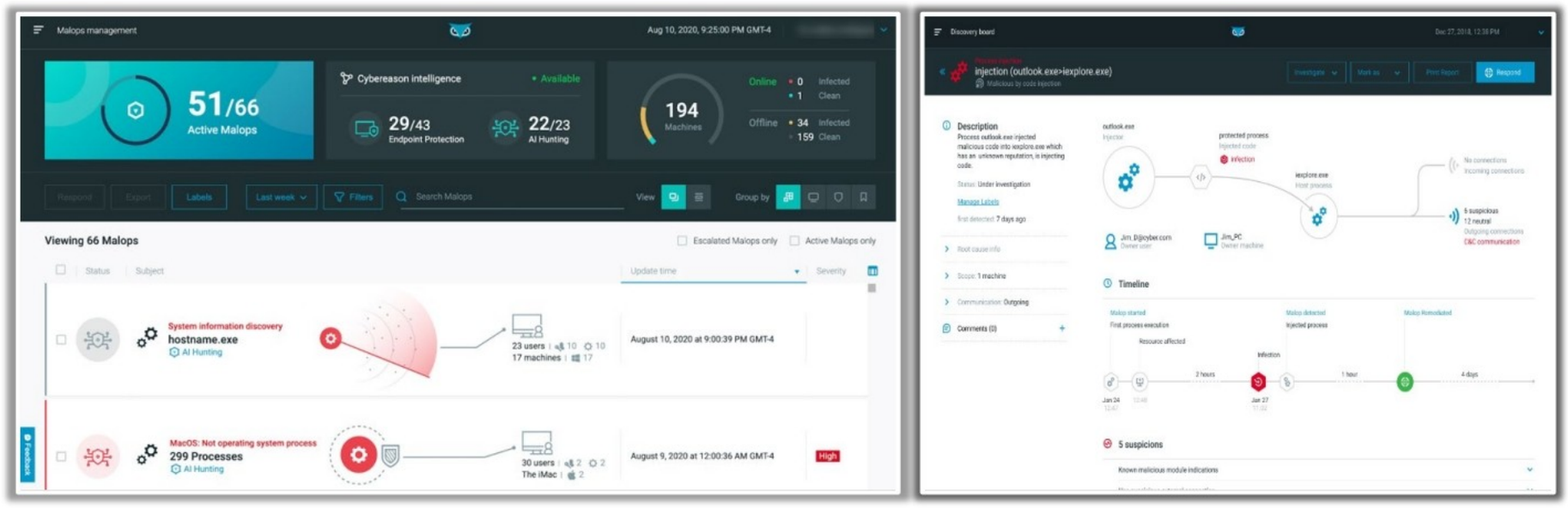
Figure 16.27: Using EDR Technology for Incident Response

Figure 16.28: Using EDR Technology for Incident Response

Businesses can establish an automated end-to-end detection system using the Cynet tool, which serves as an automated cybersecurity platform. This tool assists users by presenting alerts categorized by date, description, and the scope of the attack. It also aids in conducting in-depth investigations to determine the root cause of the incident. Additionally, it offers recommendations for implementing further security measures to safeguard the business and ensure uninterrupted operations.

Endpoint Detection and Response Tool: Cybereason

- Cybereason EDR eliminates ransomware and other malware threats, prevents file-less and in-memory attacks, and shortens investigations with correlated **threat intelligence** via an intuitive UI and automated or single-click remediation across all devices with a single lightweight agent



Endpoint Detection and Response using Cybereason

Source: *https://www.cybereason.com*

Endpoint Detection and Response Tool: Cybereason

Source: https://www.cybereason.com

Cybereason is an integrated endpoint security tool designed to detect, contain, investigate, and eliminate hostile cybersecurity threats that occur higher in the cyber kill chain. EDR (Endpoint Detection and Response) plays a crucial role in endpoint security and is essential for enhancing the overall cybersecurity posture of the organization. Continuous monitoring of the organization's endpoints and swift responses to suspicious abnormalities are imperative. The EDR platform operates as a proactive cyber investigator and resolver, consistently auditing incidents on endpoints across all operating systems within the organization. Its key features include providing threat intelligence, instant remediation, rapid detection with high accuracy, and ML-powered correlation of malicious behaviors, among others.

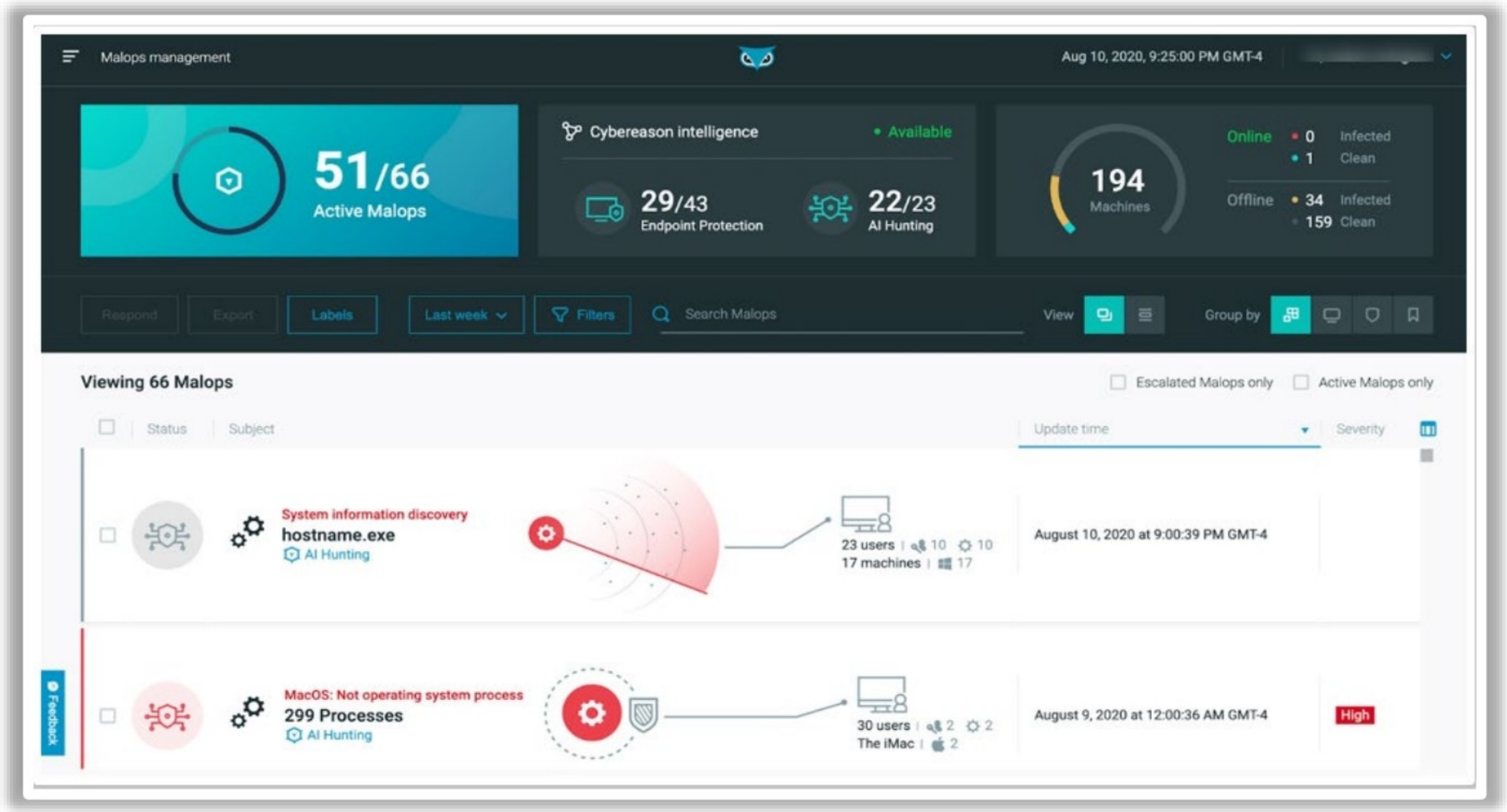


Figure 16.29: Endpoint Detection and Response using Cybereason

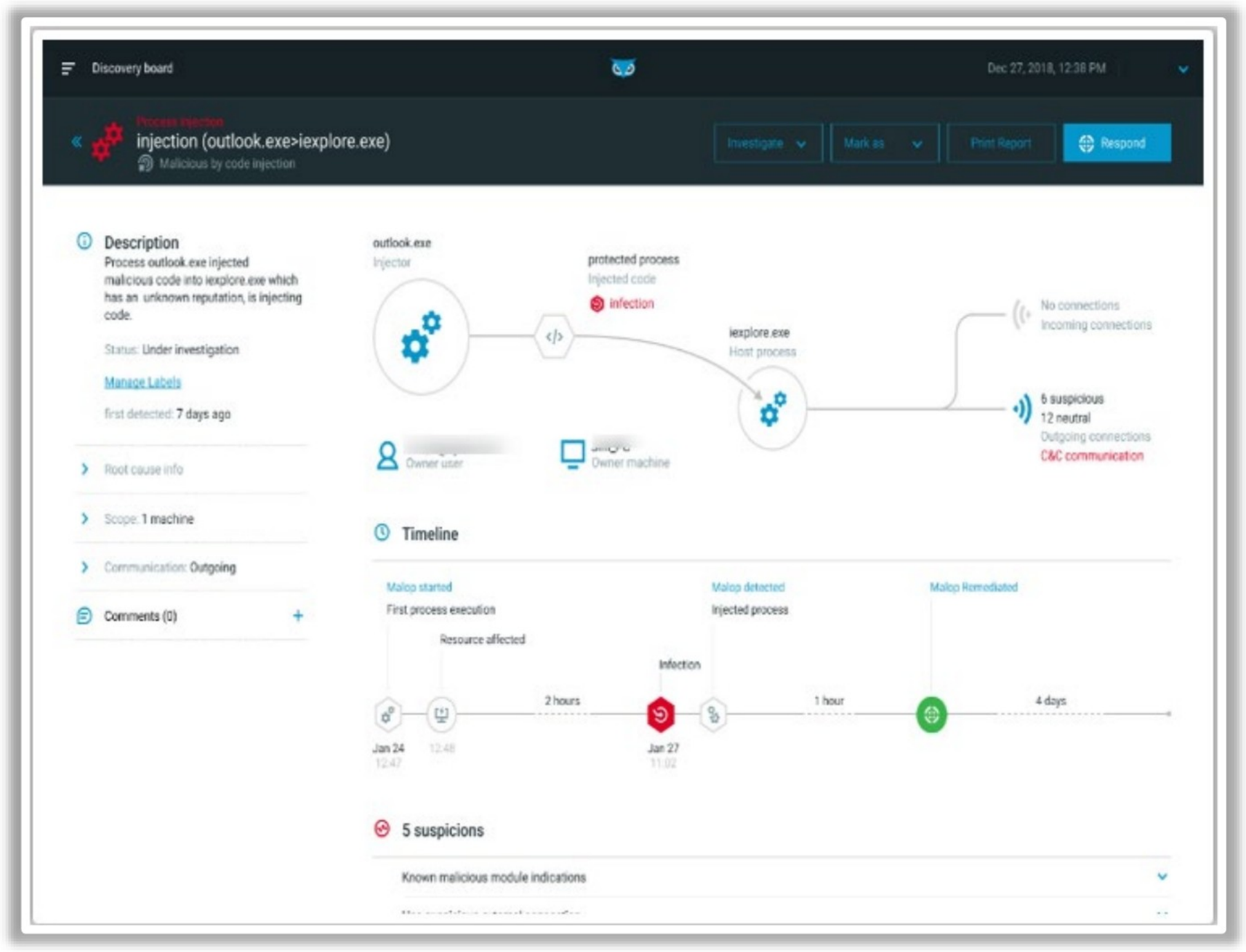
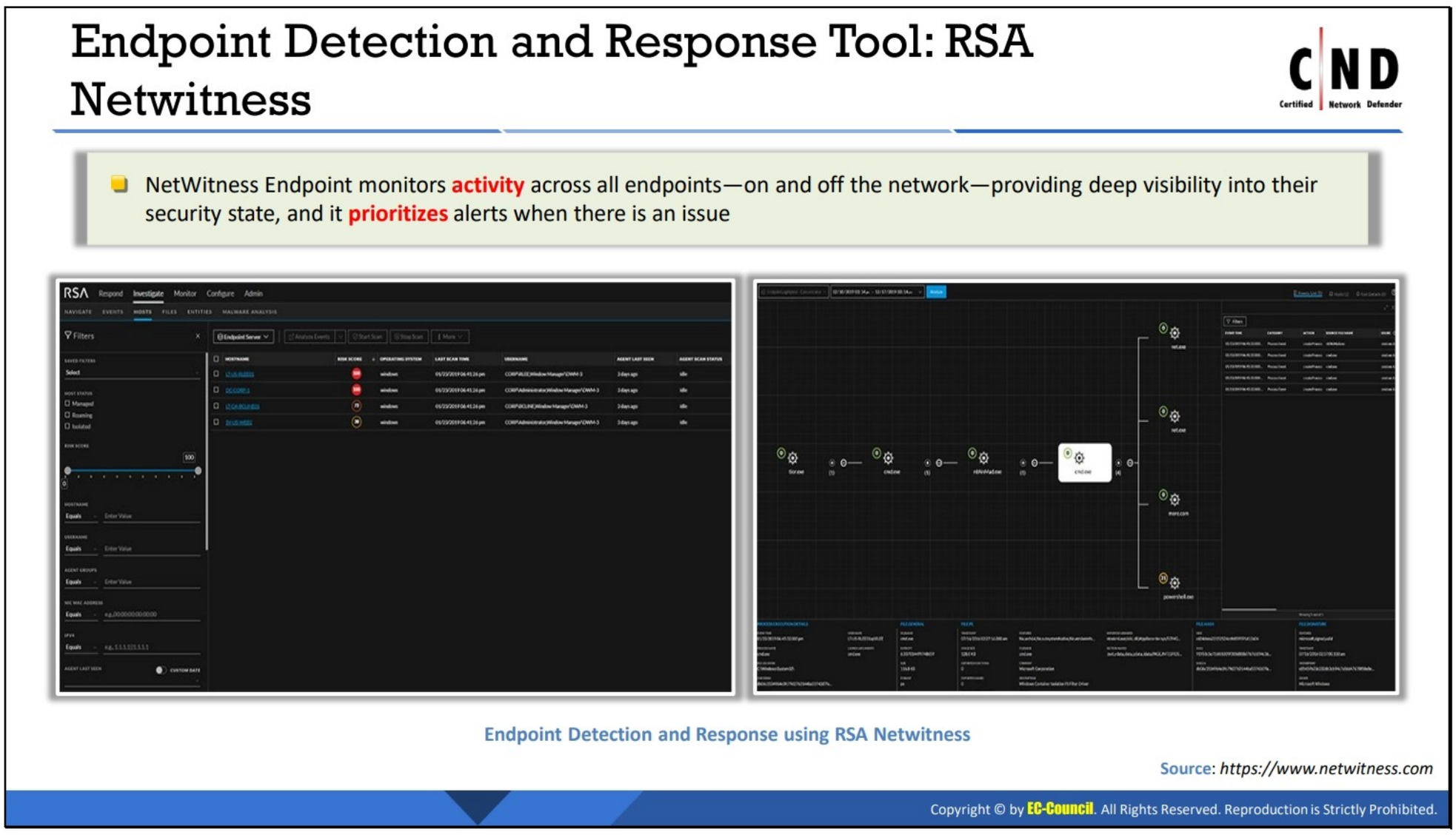


Figure 16.30: Endpoint Detection and Response using Cybereason



Endpoint Detection and Response Tool: RSA Netwitness

Source: https://www.netwitness.com

RSA NetWitness Endpoint is an EDR solution that offers continuous monitoring of endpoints, delivering comprehensive visibility and robust analysis of all activities and processes occurring on an organization's endpoints. It extends its monitoring capabilities to cover activity on both network-connected and disconnected endpoints, ensuring deep insight into their security status and promptly prioritizing alerts when issues arise.

Key Features

- RSA NetWitness Endpoint equips security teams with critical data to gain a comprehensive understanding of the scope of an attack and conduct effective forensic investigations.
- It minimizes attack dwell time by swiftly performing root cause analysis and prioritizing threats, thus enhancing the efficiency of security analysts and accelerating response times.
- This solution excels in detecting all endpoint threats, even those that may be missed by other solutions, thanks to its unmatched real-time visibility across all of an organization's endpoints, whether they are connected to the network or not.
- RSA NetWitness Endpoint simplifies the process of collecting endpoint data by offering endpoint inventory scans in conjunction with Microsoft Windows log forwarding and filtering capabilities

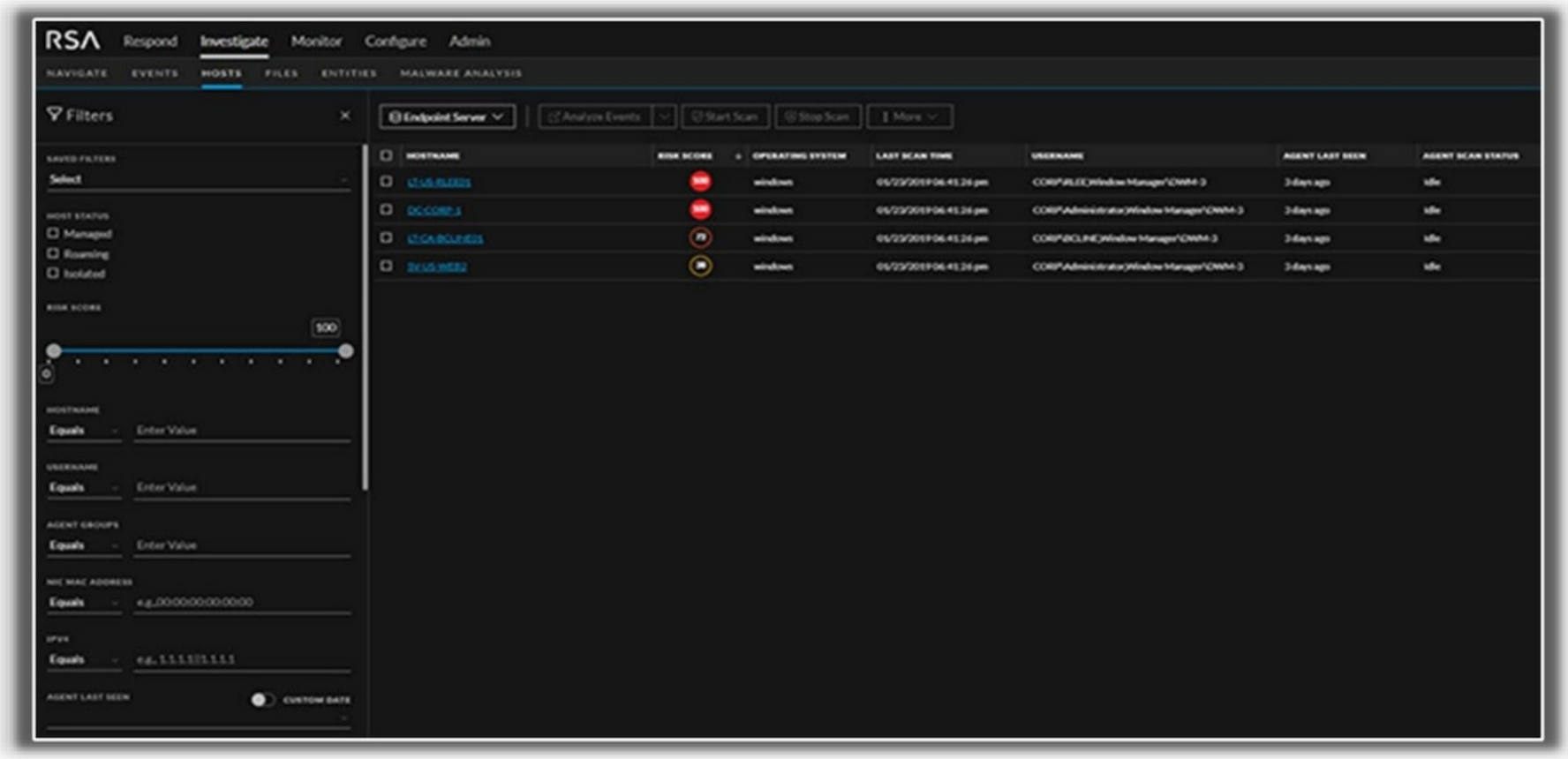


Figure 16.31: Dashboard of RSA Netwitness tool

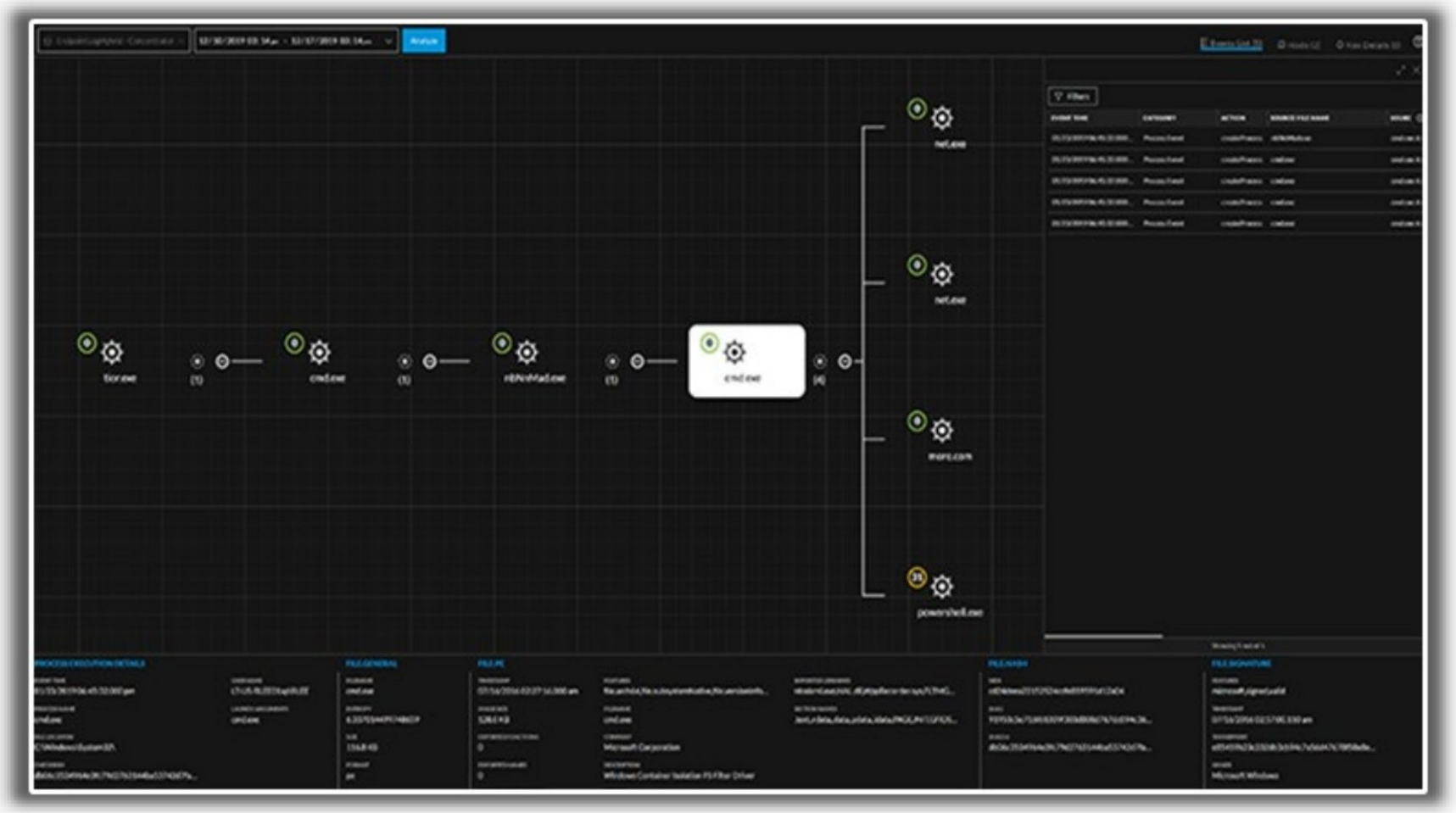
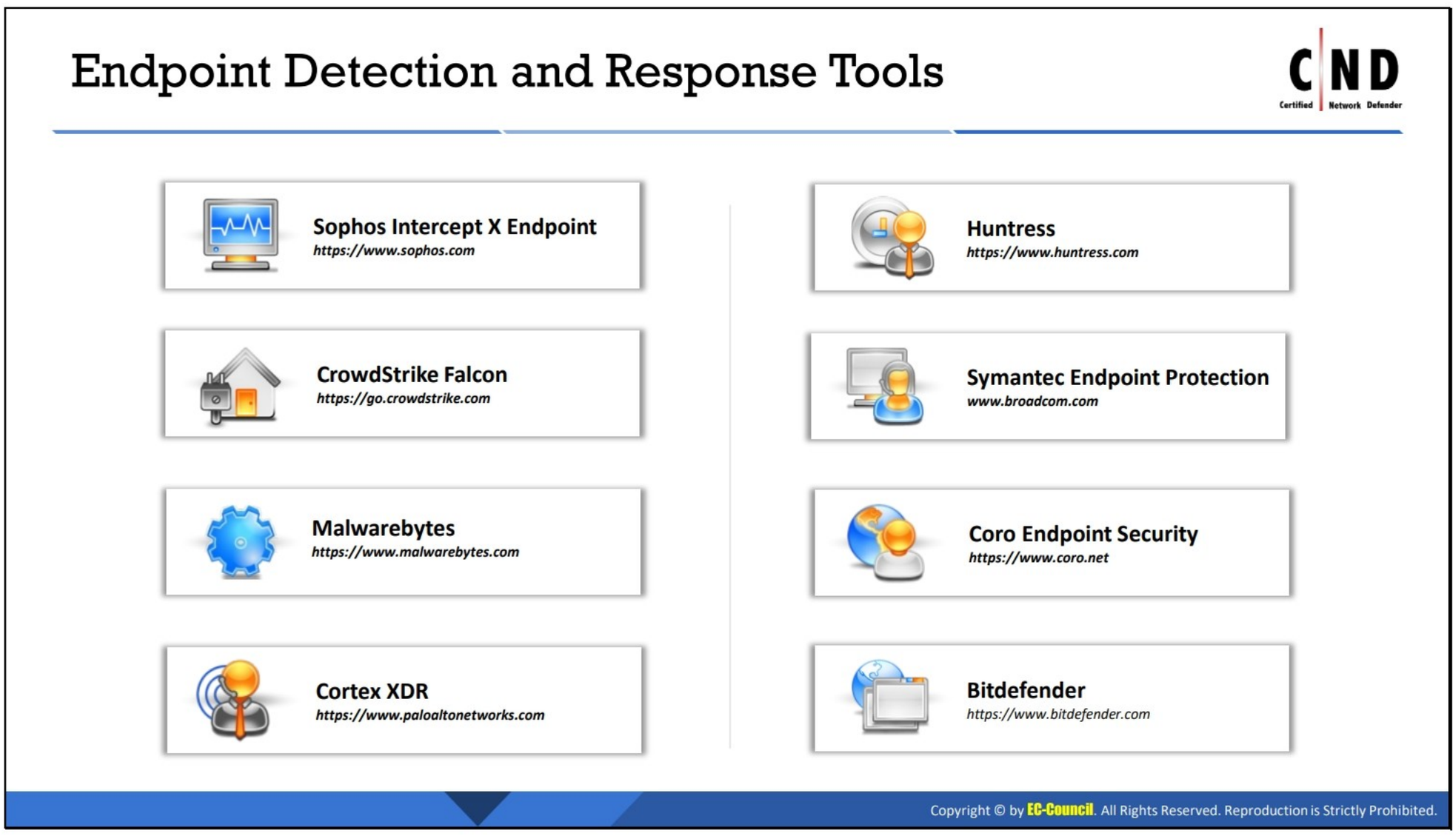


Figure 16.32: Continuous Endpoint Monitoring in RSA Netwitness Tool



Endpoint Detection and Response Tools

The endpoint detection and response tools are as follows.

Sophos Intercept X Endpoint

Source: https://www.sophos.com

Sophos Intercept X Endpoint offers exceptional *protection against advanced attacks* by employing a wide range of *sophisticated technologies to* thwart *threats before they* can *impact the organization.* It also provides robust *EDR* (Endpoint Detection and Response) *and XDR* (Extended Detection and Response) *tools* to *enable* organizations to proactively search *for, investigate, and respond to suspicious activity and indicators* of attacks.

Key Features

- Provides web protection by blocking access to phishing and malicious websites
- Anti-exploitation
- Threat exposure reduction
- Account health check
- Adaptive attack protection enables heightened defenses on an endpoint when it is attacked
- A critical attack warning alerts if adversary activity is detected across multiple endpoints or servers.

CrowdStrike Falcon Insight

Source: https://www.crowdstrike.com/

CrowdStrike Falcon Insight is a comprehensive endpoint detection and response (EDR) solution designed to provide continuous monitoring of all endpoint activities within an organization. It leverages real-time analysis of endpoint data to automatically identify and respond to threat activities, thus enhancing the organization's cybersecurity posture.

Key Features

- Real-time monitoring
- Forensic capabilities
- Risk-based vulnerability management
- Endpoint security & XDR
- Threat intelligence
- Managed selection and response

Malwarebytes

Source: https://www.malwarebytes.com

This all-in-one endpoint security portfolio provides comprehensive protection against a wide range of threats, including ransomware, malware, viruses, and other attacks. It combines multiple layers of protection, threat intelligence, and human expertise in a user-friendly solution designed to secure organizations without necessitating extensive IT staff involvement.

Key Features

- Attack isolation
- Automated remediation
- Ransomware rollback

Cortex XDR

Source: https://www.paloaltonetworks.com

Protect your organization with a trusted endpoint security solution that offers detection, response, automation, and attack surface management.

Key Features

- Proven endpoint protection
- Laser-accurate detection using ML
- Lighting fast investigation and response
- Automated analysis of the root cause of a threat

Huntress

Source: https://www.huntress.com/

Huntress offers a robust suite of managed endpoint detection and response (EDR) capabilities supported by a 24/7 team of threat hunters to defend organizations against today's persistent cybercriminals.

Key Features

- Managed EDR and Antiviruses
- Adds threat operations to the organization
- It reviews all the suspicious activity
- Quick and accurate response to cyber events

Symantec Endpoint Protection

Source: www.broadcom.com

Symantec's innovative endpoint security solutions protect the organization's laptops, desktops, mobile devices, servers, applications, cloud workloads, containers, and storage storage devices—wherever the data resides.

Key Features

- It delivers the strongest protection against stealthy malware and ransomware.
- It offers threat detection and remediation with sophisticated attack analytics and automated response.
- Intelligent automation, AI-guided policy management

Coro Endpoint Security

Source: https://www.coro.net

Modern endpoint protection with advanced threat detection and remediation is crucial for safeguarding businesses against malware and ransomware. Harness the power of AI automation and machine learning to secure devices across the threat landscape.

Key Features

- AI-driven automation, advanced threat detection, and remediation
- Real-time protection from malware, ransomware, zero-day exploits, phishing, attacks
- Behavioral-based machine learning of devices and users
- Tiered, layered defenses behind the email security tool

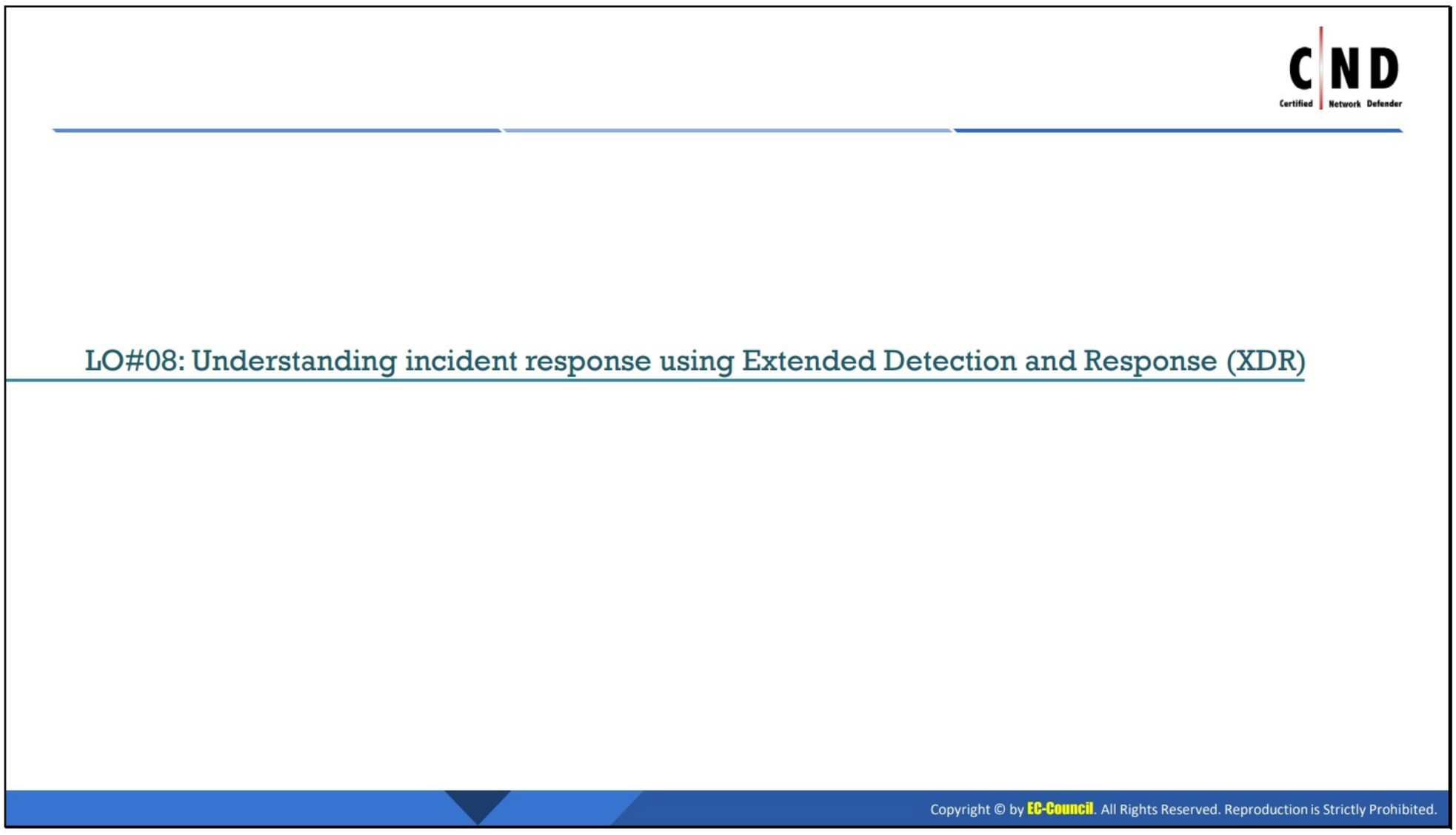
Bitdefender

Source: https://www.bitdefender.com/

Bitdefender endpoint detection and response (EDR) is a cloud-based solution that operates on the Bitdefender Gravity Zone XDR platform. Each EDR agent installed on the organization's endpoints includes an event recorder that maintains continuous monitoring of the endpoint's activities. It securely transmits insights and details of suspicious events to the centralized Gravity Zone Control Center.

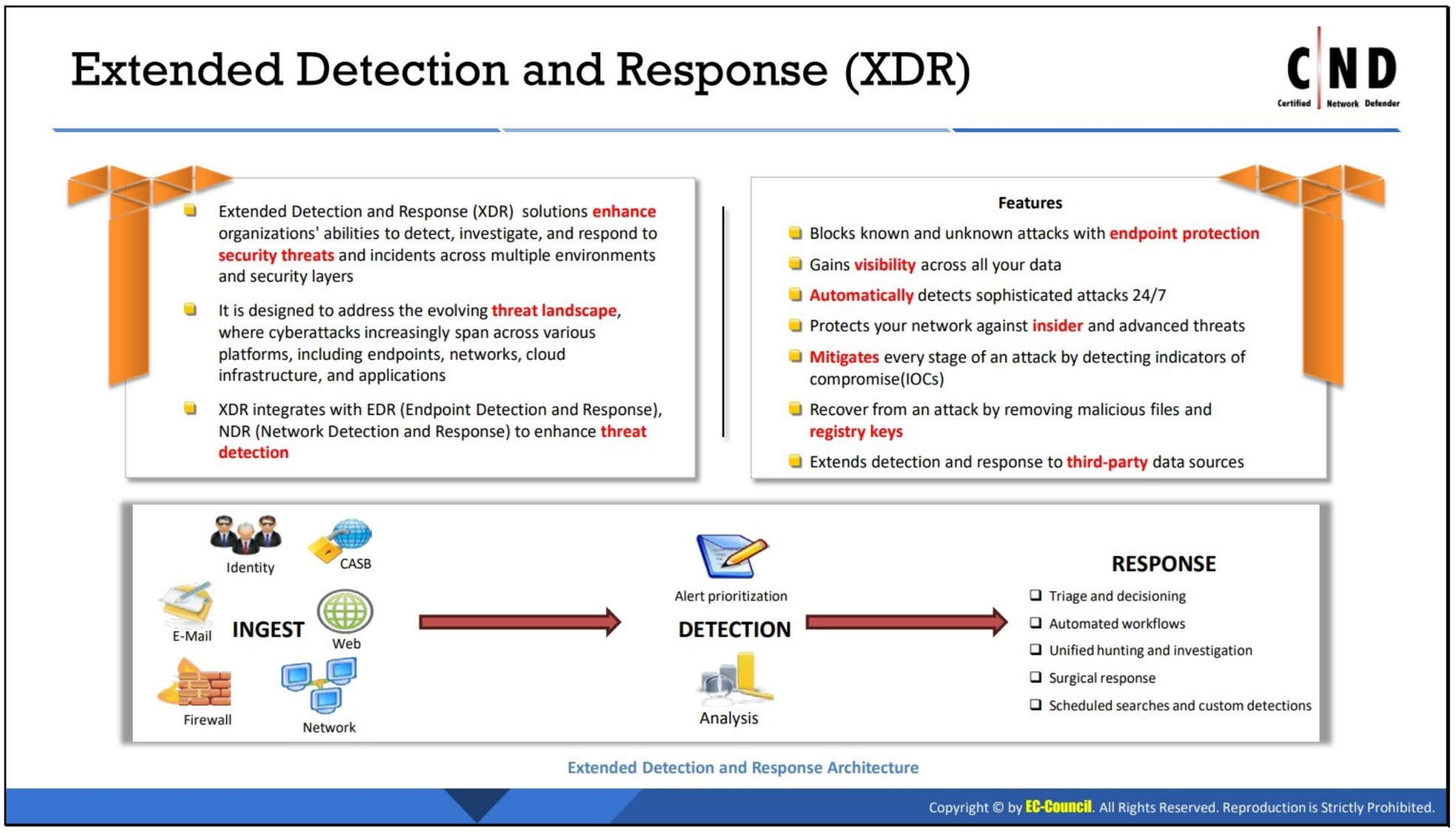
Key Feature

- Endpoint data collection
- Threat detection and analysis
- Automated response through sandboxing of suspicious files
- Threat investigation
- Integration with security infrastructure



LO#08: Understanding Incident Response using Extended Detection and Response (XDR)

As the cybersecurity landscape continues to evolve, organizations are increasingly turning to advanced solutions for robust incident response strategies. Extended Detection and Response (XDR) has emerged as a pivotal technology in this paradigm, offering a comprehensive approach to incident response. This sectioin explores the transformative role of XDR in incident response, shedding light on its capacity to enhance visibility, automate responses, and fortify organizations against the ever-changing cybersecurity threat landscape.



Extended Detection and Response (XDR)

Extended Detection and Response (XDR) offers a holistic view of an organization's security posture, empowering security teams to make informed decisions regarding detection and response strategies. XDR seamlessly integrates data from various security products, including EDR (Endpoint Detection and Response), network security, cloud security, and email security, to provide a unified perspective on security threats across the entire organization. The EDR solution within XDR leverages AI (Artificial Intelligence) and ML (Machine Learning) technologies to automate response actions, taking into account the severity of the threat and its potential impact on the organization. XDR extends its threat detection and response capabilities across multiple security layers, covering endpoints, networks, and cloud environments. Additionally, XDR integrates with EDR (Endpoint Detection and Response) and NDR (Network Detection and Response) to further enhance threat detection. XDR utilizes NDR's capabilities, including network telemetry and detection capabilities, to correlate and identify network-based threats effectively.

XDR provides advanced forensic investigation and threat hunting capabilities across multiple domains, all accessible from a single console.

How XDR Works

Working of XDR involves the following.

- **Ingest**: XDR ingests and normalizes large volumes of data from various sources, including endpoints, cloud workloads, identity systems, email, network traffic, and virtual containers.
- **Detect:** Utilizing advanced AI and ML technologies, XDR parses and correlates the ingested data to automatically identify stealthy threats.

- **Respond:** XDR prioritizes threat data based on severity, enabling threat hunters to efficiently assess and categorize new events. It also facilitates the automation of investigation and response actions to address security threats effectively.

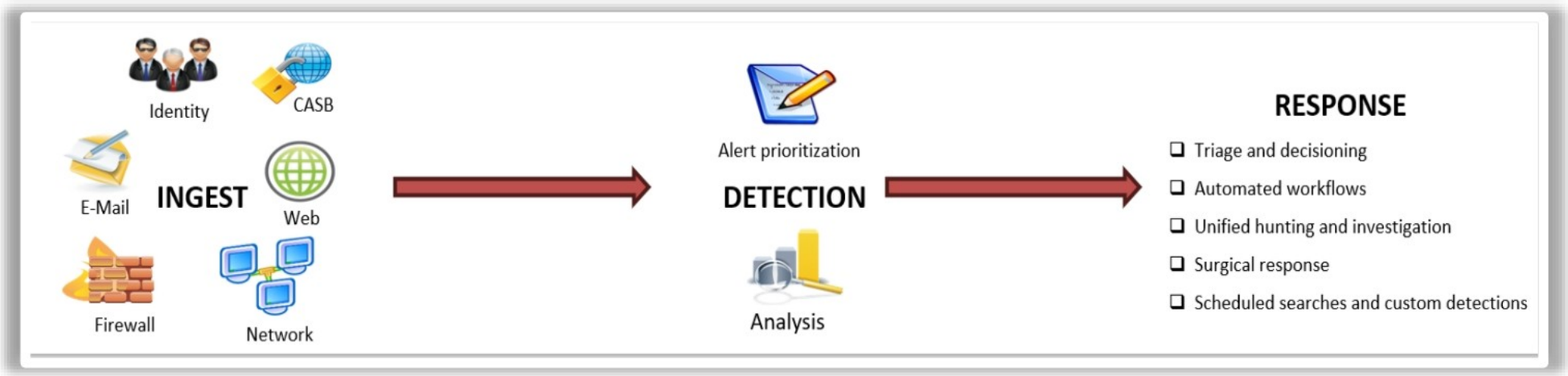


Figure 16.33: Extended Detection and Response Architecture

Benefits of XDR

The benefits of XDR as follows:

- **Blocks known and unknown attacks with endpoint protection**: XDR can effectively block exploits, malware, and fileless attacks using integrated AI-driven threat intelligence and antivirus capabilities.
- **Gains visibility across all data sources:** XDR gathers and correlates data from any source, providing comprehensive visibility to detect, triage, investigate, hunt, and respond to threats effectively.
- **Automatically detects complicated attacks 24/7:** XDR utilizes analytics and custom rules to automatically detect advanced persistent threats and other covert attacks, ensuring round-the-clock protection.
- **Protects the network against insider and advanced threats**: XDR safeguards the network against insider abuse, fileless and memory-only attacks, ransomware, external attacks, and advanced zero-day malware.
- **Mitigates every stage of an attack by detecting indicators of compromise (IOCs)**: XDR detects IOCs and anomalous behavior, prioritizing analysis with incident scoring at each stage of an attack.
- **Recovers from an attack by removing malicious files and registry keys:** In the event of a compromise, XDR facilitates quick recovery by restoring damaged files and registry keys based on remediation suggestions.
- **Extends detection and response to third-party data sources:** XDR implements behavioral analytics on logs obtained from third-party firewalls and integrates third-party alerts into a unified incident view, expediting investigations and root cause analysis.

Key Features of XDR

The key features of XDR are given below,

- **Data Collection and integration**

  XDR scrutinizes traffic from various layers of an organization's technology infrastructure, including both internal and external sources. This enables the detection of threats. XDR systems also integrate threat intelligence to recognize established attack techniques and harness machine learning-based detection to identify previously unknown and zero-day threats.

- **Advanced analytics and threat detection**

  Teams can focus on the most critical threat events and use automation to manage known or recurring incidents, as XDR prioritizes risks and reduces alert volumes through analytics and correlations.

- **Contextual visibility and investigation**

  Human-machine teaming combines all relevant threat information, applies situational security context, and uses signal-to-noise reduction techniques to quickly distinguish evidence from noise and assist in root-cause evaluation.

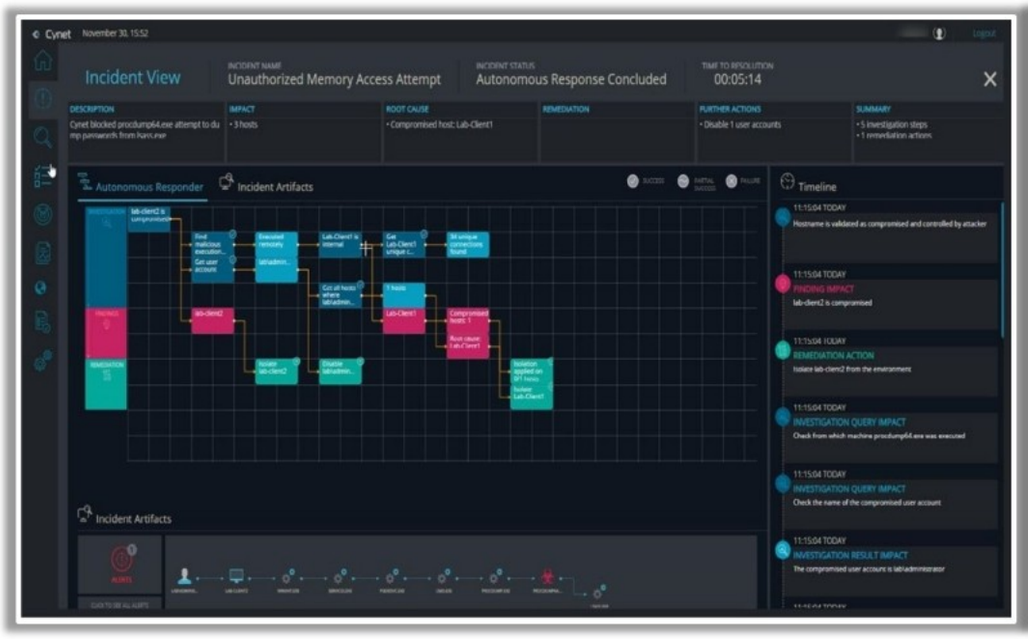
- **Automated response and orchestration**

  The entire investigation and remediation process is guided by complete, cross-domain threat context and telemetry, covering impacted hosts, root causes, evidence, and timelines. Automated alerts can trigger complex, multi-tool methods, leading to significant SOC efficiency improvements and precise threat neutralization.

  Cross-domain threat hunting

  XDR hunts for abnormal activity across cross-domain data and investigates detections. Cross-domain threat context and telemetry, including information about affected hosts, root causes, indicators, and timelines, serve as essential guides throughout the entirety of the investigation and remediation process.

Extended Detection and Response Tool: Cynet auto XDR



Cynet auto XDR Dashboard

Threat Detection

Source: *https://www.cynet.com*

Extended Detection and Response Tool: Cynet auto XDR

Cynet auto XDR is an autonomous breach protection platform that unifies and automates monitoring and control, attack prevention and detection, and response orchestration throughout the entire environment. Cynet 360 leverages artificial intelligence (AI) and machine learning (ML) technologies to automatically detect and respond to cyber threats. Its goal is to identify and mitigate security incidents in real-time without requiring constant human intervention.

Its key features included are autonomous threat detection and response, unparalleled accuracy and complete attack-surface coverage, 24/7 expert responders, and endpoint protection.

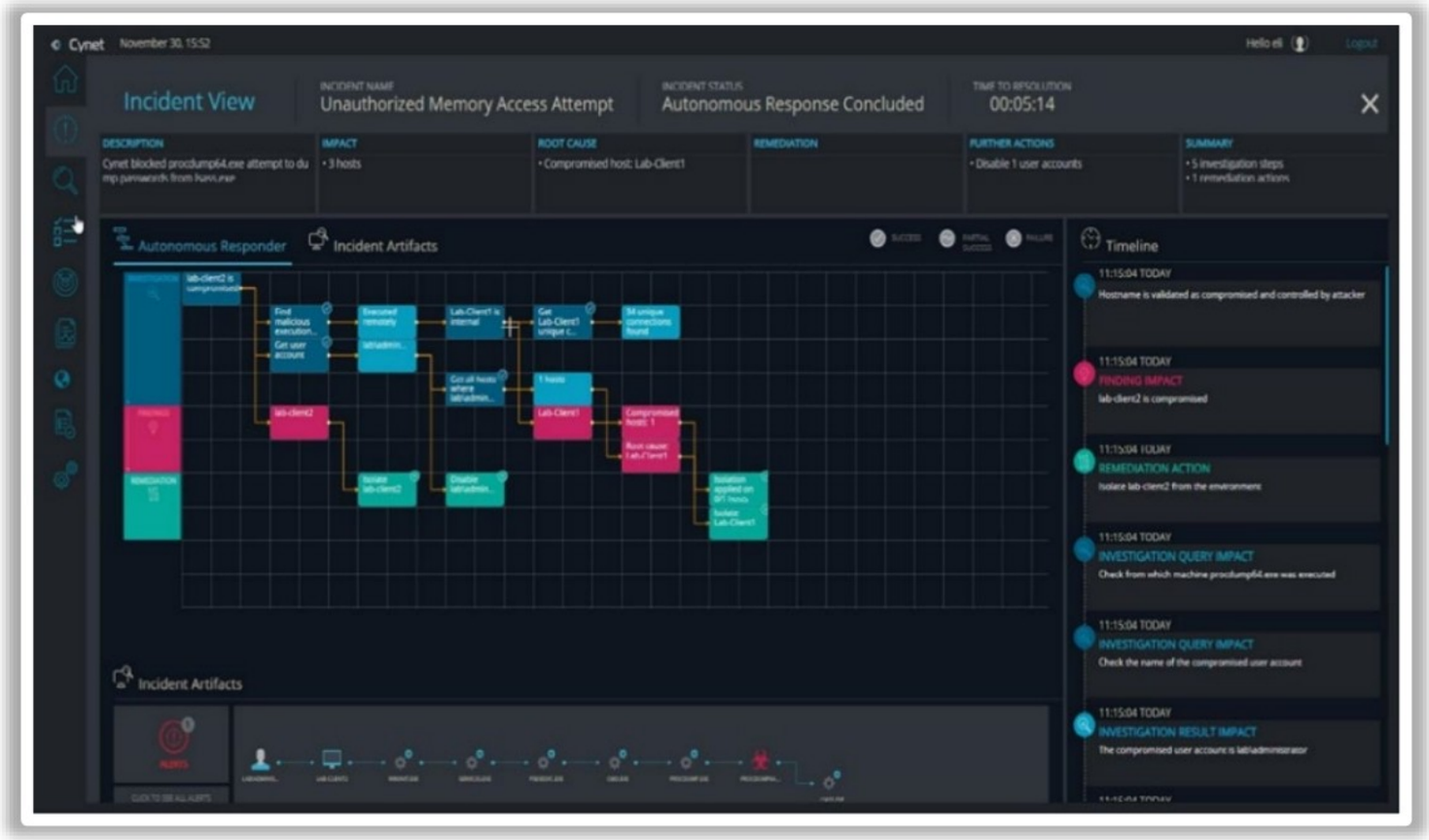
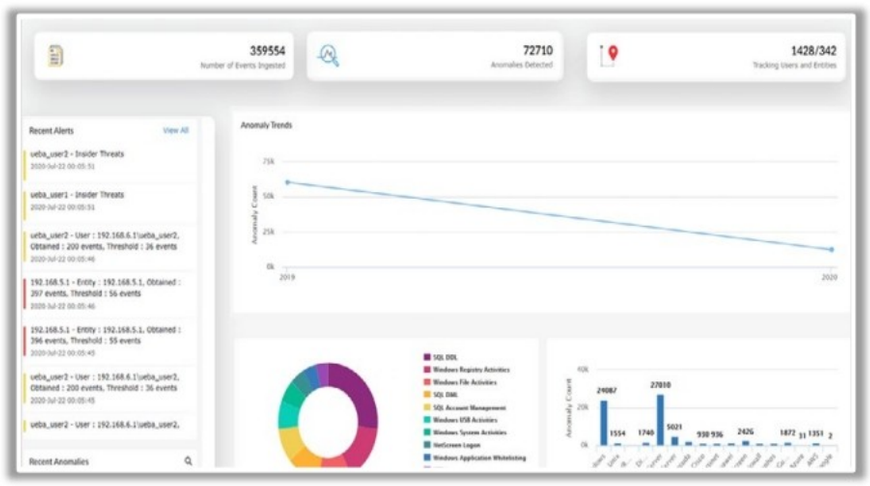


Figure 16.34: Representing Cynet Auto Xdr Dashboard

Figure 16.35: Representing Threat Detection in Cynet Auto XDR

Extended Detection and Response Tool: ManageEngine Log 360

ManageEngine Log 360 Dashboard



Incident Detection using ManageEngine Log 360

Source: *https://www.manageengine.com*

Extended Detection and Response Tool: ManageEngine Log 360

Log360 is a unified SIEM solution with integrated DLP and CASB capabilities that detects, prioritizes, investigates, and responds to security threats. It combines threat intelligence, machine learning-based anomaly detection, and rule-based attack detection techniques to detect sophisticated attacks. Additionally, it offers an incident management console for effectively remediating detected threats. Log360 provides holistic security visibility across on-premises, cloud, and hybrid networks with its intuitive and advanced security analytics and monitoring capabilities.

Key Features

- Collect and analyse log from various sources including end-user devices
- Monitor and audit critical Active Directory changes in real time
- Detect security incidents or data breaches
- Incident response

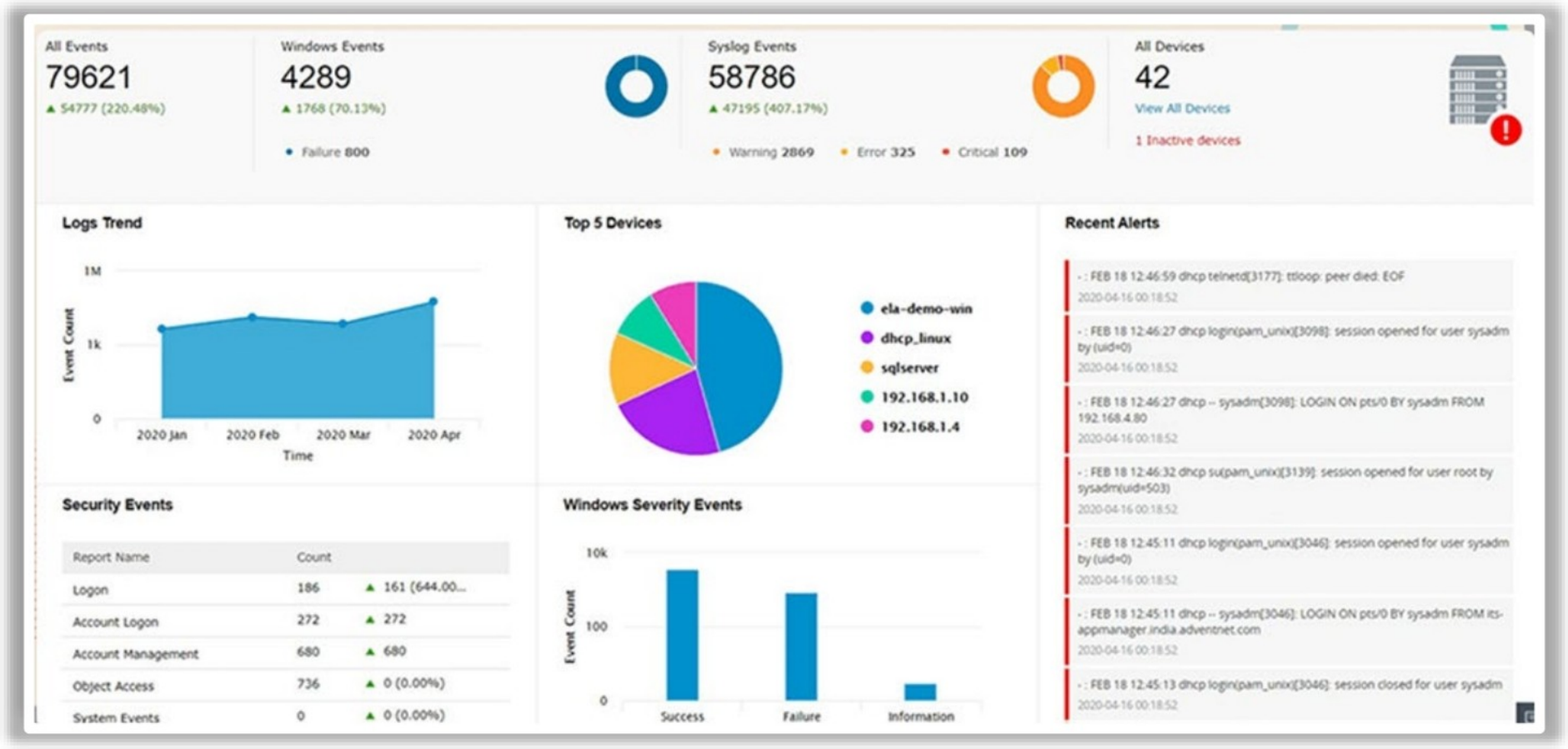


Figure 16.36: Representing ManageEngine Log 360 Tool Dashboard

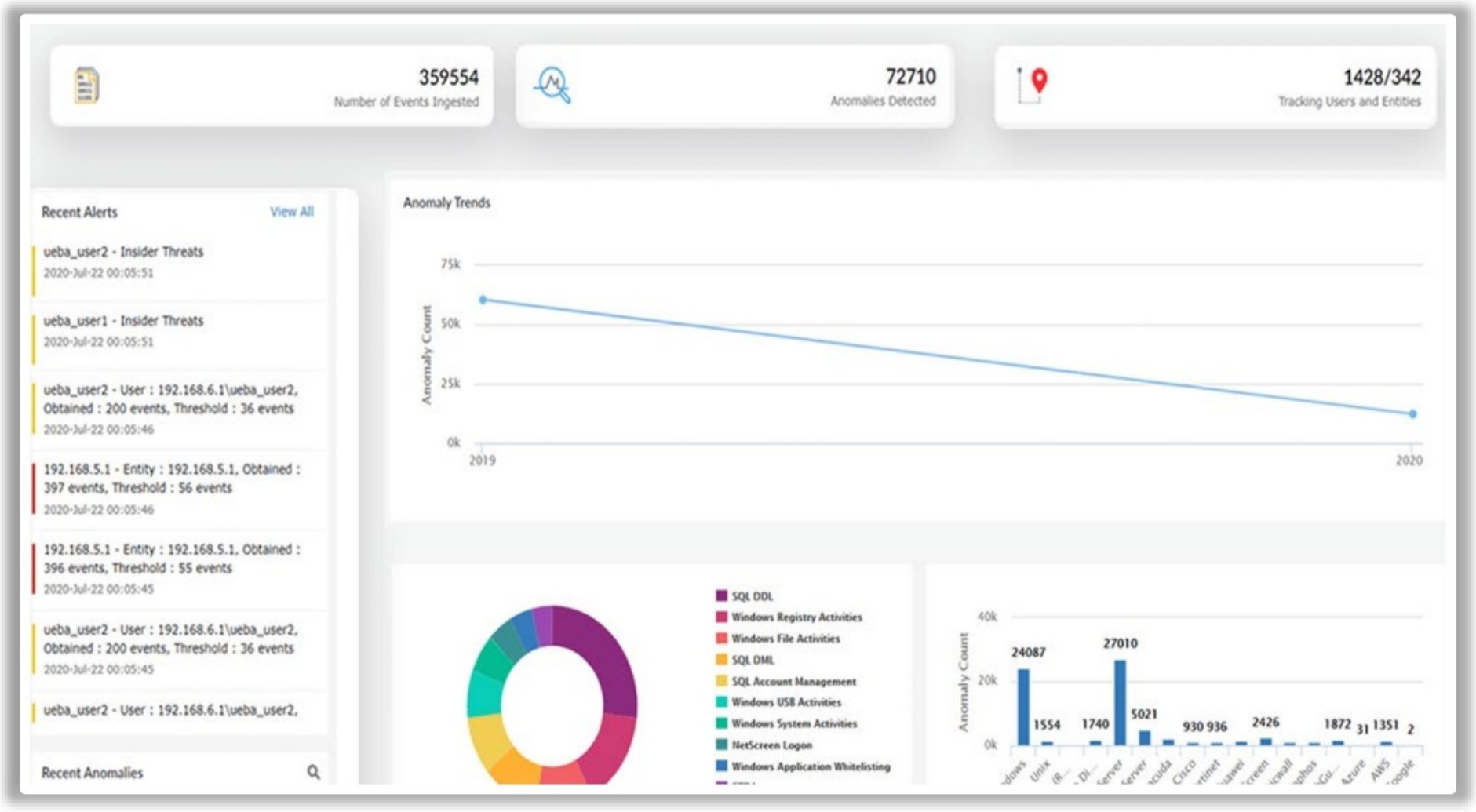
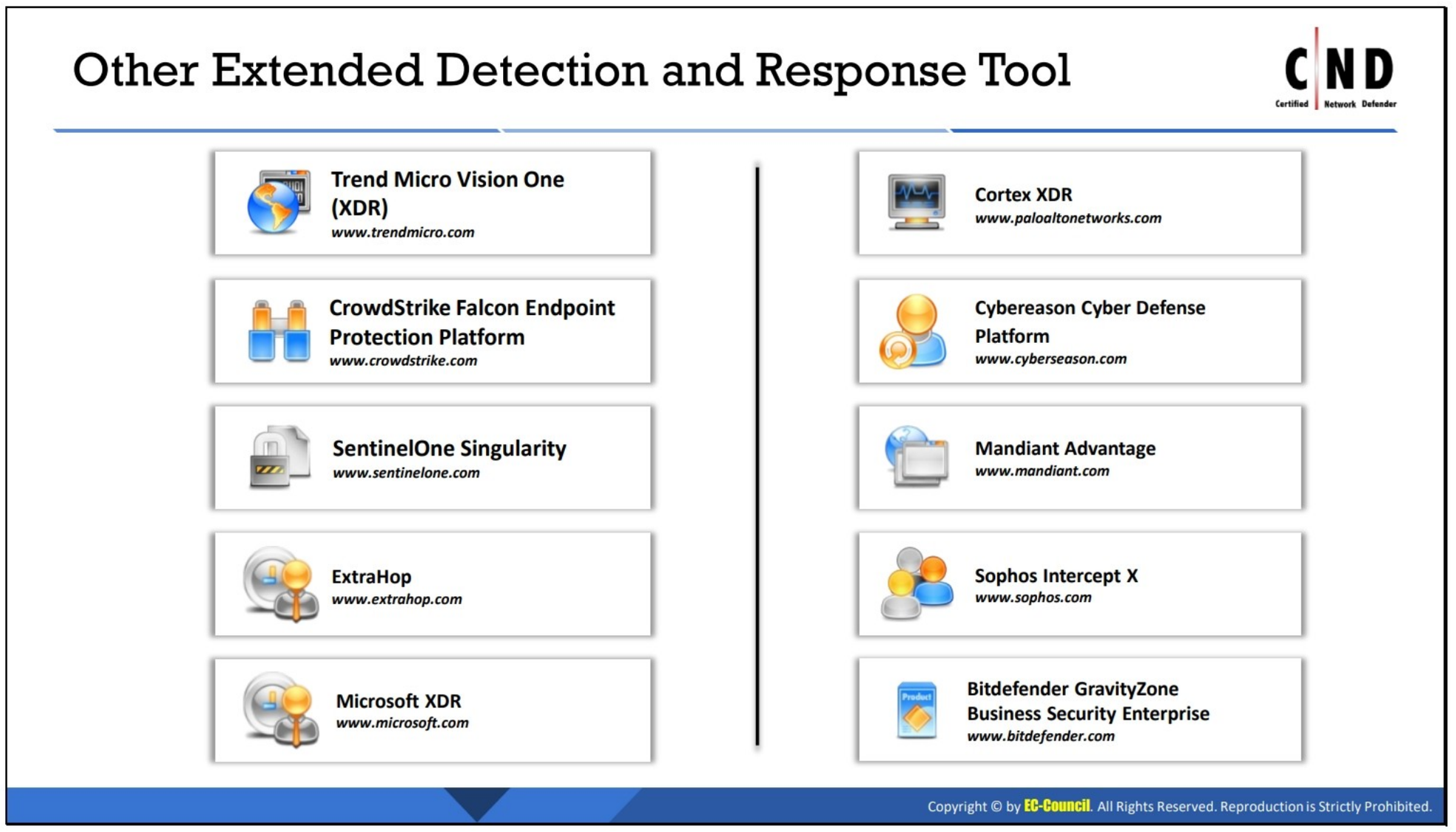


Figure 16.37: Representing Incident detection ManageEngine Log 360 Tool



Other Extended Detection and Response Tool

The other XDR tools are as follows.

Trend Micro Vision One (XDR)

The Trend Micro Vision One platform includes advanced XDR capabilities that collect and correlate deep activity data across multiple vectors, including email, endpoints, servers, cloud workloads, and networks. This enables a level of detection and investigation that is difficult or impossible to achieve with SIEM, EDR, or other individual point solutions.

Key Features

- Automated searching for indicators of compromise
- Dynamic risk assessments of threats and automated remediation tools
- Attack surface discovery that includes internet domains, containers, and private business networks
- Threat correlation from multiple security sources

CrowdStrike Falcon Endpoint Protection Platform

Falcon Insight XDR unifies third-party data sources across all key attack surfaces, providing comprehensive detection and response across third-party tools from one unified XDR command console.

Key Features:

- Third-party integrations with crowdStrike's technology alliance partners
- Graph explorer that shows cross-domain attack patterns

- Behavioral analytics
- Integrations with CI/CD pipelines

SentinelOne Singularity

Singularity XDR is the only XDR platform that brings together native endpoint, cloud, and identity telemetry with the flexibility to ingest and combine third party data within a large data lake. Singularity XDR easily and cost-effectively ingests security data from any source, empowering analysts with visibility across their entire enterprise.

Key Features

- Customizable role-based access control options
- Integration with MFA solutions
- Skylight data analytics integration for increased visibility of XDR data

ExtraHop

An integrated, best-in-class XDR strategy allows security teams to choose the best products for their environment without the fear of vendor lock-in. By integrating the leading endpoint, network, and log-based security solutions, your team can benefit from a streamlined incident response approach and achieve complete end-to-end visibility. ExtraHop works with other leading security solutions to build integrated workflows natively in ExtraHop Reveal(x) 360.

Key Features

- Faster mean time to respond
- Stronger security across the entire attack surface
- Reduce manual data gathering so analysts can focus on urgent priorities

Cortex XDR

For extended infrastructure protection, Palo Alto offers the industry-first extended solution Cortex XDR. Cortex XDR combines insights across endpoint, network, and cloud data to reduce administrators' manual work. Other key features include threat hunting and intelligence through PAN's Unit 42, ML-based behavioral analysis, and streamlined deployment.

Key Features

- Detection for issues such as insider threats and credential attacks
- Incident scoring and alert categorization to help teams choose which issues to address first
- Automated root cause analysis capabilities
- Identity threat detection and response module for uncovering malicious user issues

Cybereason Cyber Defense Platform

Offering EDR managed security services like managed detection and response (MDR) and network assessments, Cybereason has a range of security solutions that form the Cybereason

Defense Platform. Uniting all endpoints and extending visibility across the network infrastructure, Cybereason offers automated controls, remediation, and actionable threat intelligence.

Key Features

- Integrations with many security solutions, including Okta, Fortinet, Palo Alto, and Check Point
- Charts that rank malicious operations (MalOps) by severity and current status
- Full attack story for each MalOp

Mandiant Advantage

Mandiant, now part of Google, offers the Advantage platform for the XDR space. The company is known for its incident management and contributions to indicators of compromise (IOC) research. Advantage is a platform for automating security response teams. Using data science and ML, the Automated Defense software triages alerts, scales SOC capabilities, and conducts accurate investigations 24/7.

Key Features

- Dark web monitoring
- Dynamic host and malware views
- Data on threat actors
- OSINT indicators for identifying potential publicized threats

Sophos Intercept X

Sophos has gradually built a diverse portfolio that includes EDR, firewalls, cloud security, and managed services. Sophos Intercept X combines Intercept X Endpoint with a selection of other products in its XDR solution. Solution bundling options include server, firewall, cloud security posture management, and email data security solutions.

Key Features

- Highly-reviewed ransomware protection features
- 24/7 threat hunting performed by Sophos analysts
- Command line option for running scripts and editing configuration files
- Easy-to-understand user interface

Microsoft XDR

Microsoft Defender Advanced Threat Protection is a complete endpoint security solution. It has functionalities of preventive protection, post-breach detection, automated investigation, and response. It is an agentless and cloud-powered solution and hence it doesn't require any additional deployment or infrastructure.

Key Features

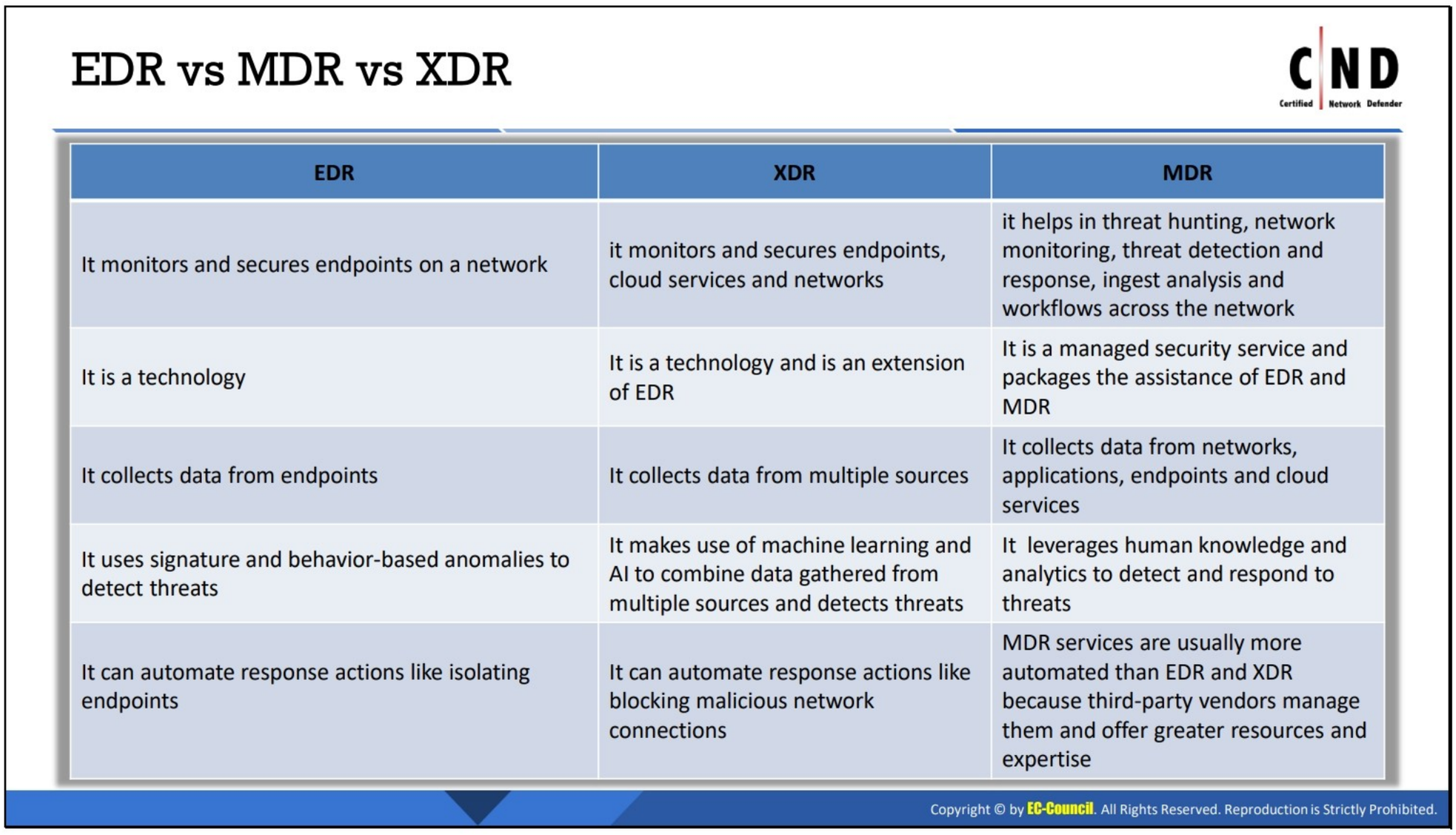
- Email security insights
- Single dashboard for incident management and alert categories
- Automatic self-healing capabilities
- Threat-hunting features with customizable queries

Bitdefender GravityZone Business Security Enterprise

The new EDR from Bitdefender extends EDR analytics and event correlation capabilities beyond the boundaries of a single endpoint, to help you deal more effectively with complex cyber-attacks involving multiple endpoints.

Key Features

- Visibility beyond managed endpoints for broad and deep observability of security incidents and events
- Root cause analysis
- Single-Click response for fast incident response across endpoints

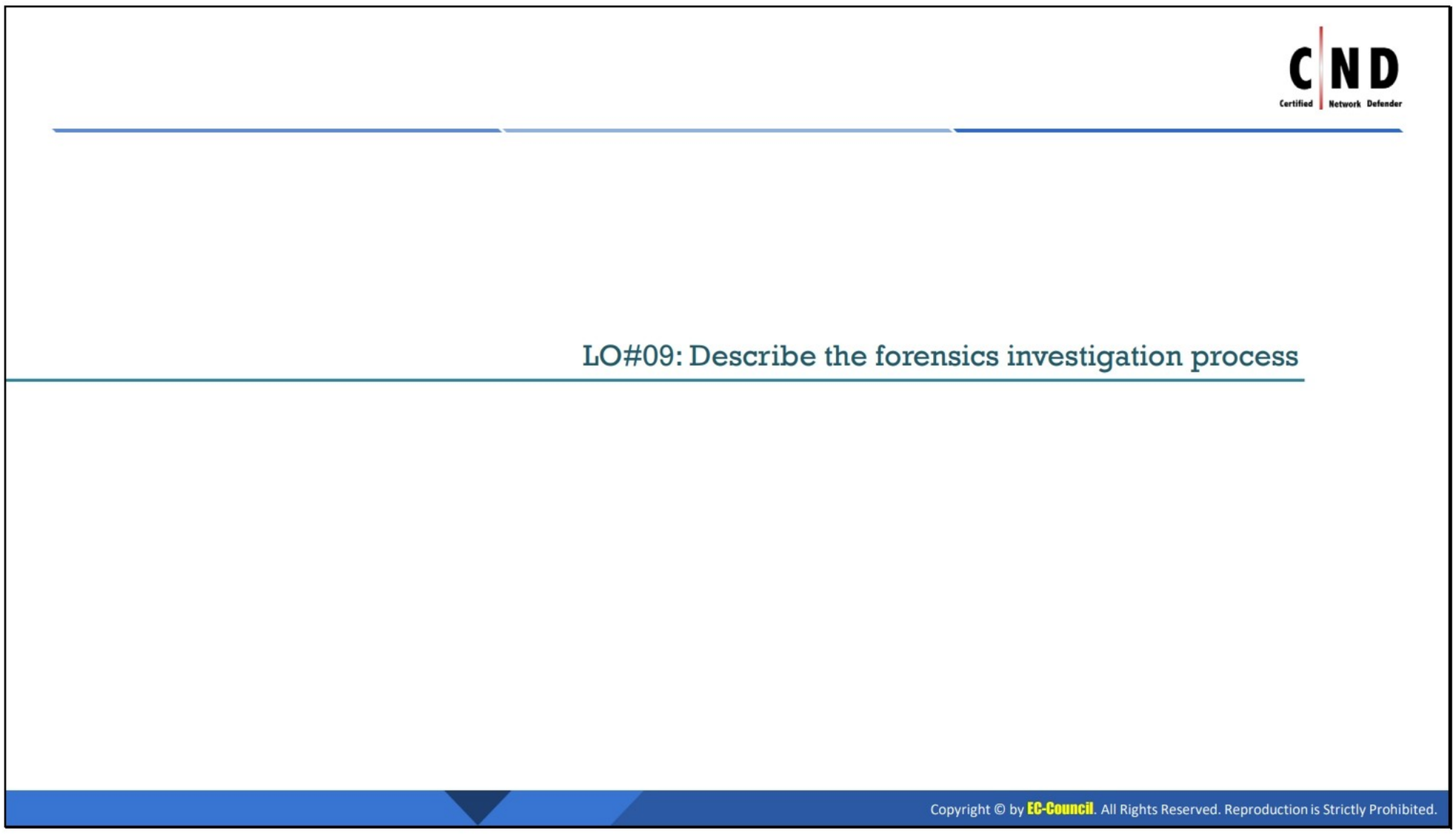


EDR vs MDR vs XDR

EDR, managed detection response (MDR), and XDR are the three main detection and response approaches that enhance an organization's cybersecurity posture. Though they share some similarities, the way they approach security is different.

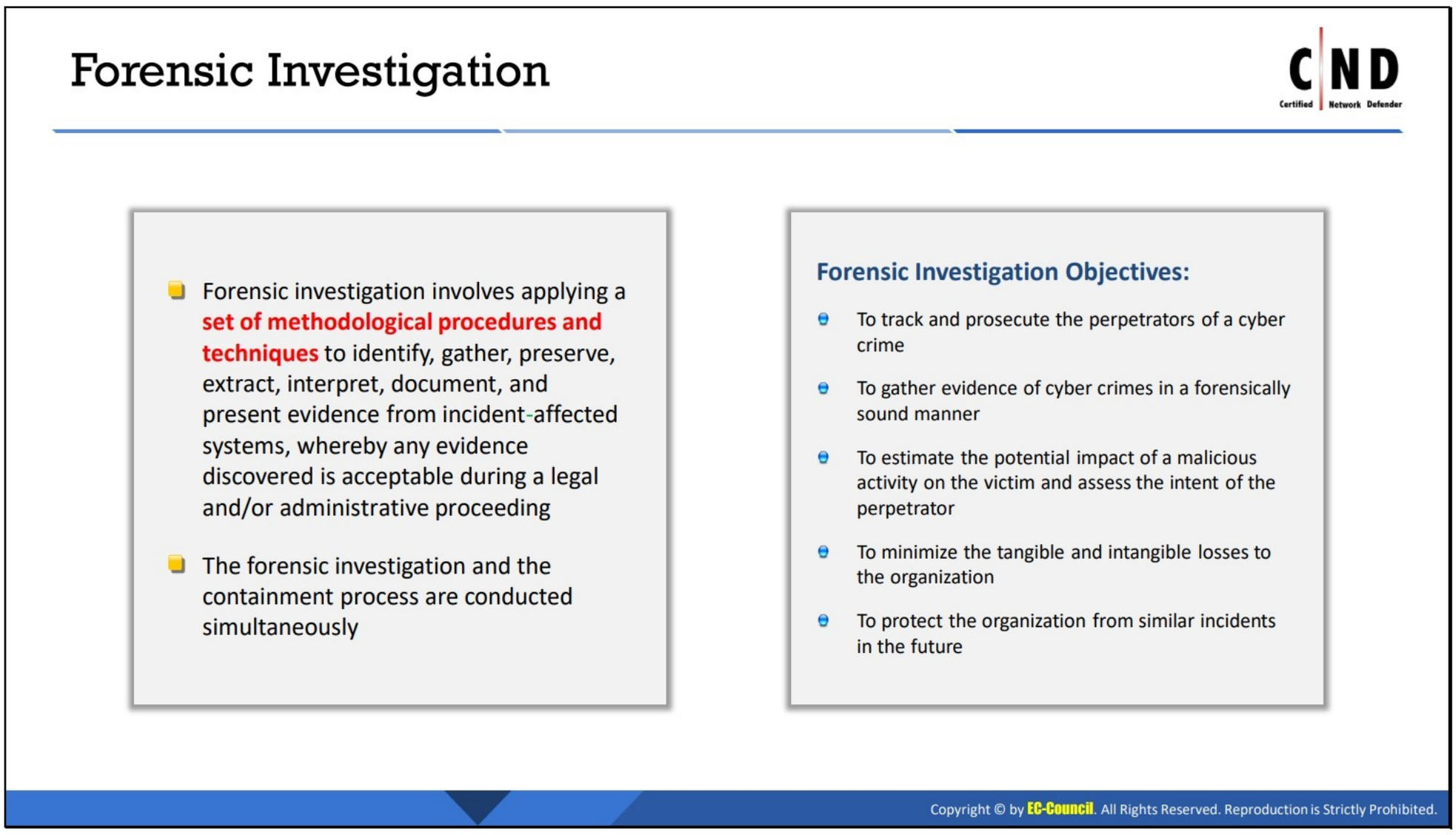
EDR	XDR	MDR
It monitors and secures endpoints on a network	It monitors and secures endpoints, cloud services and networks	It helps in threat hunting, network monitoring, threat detection and response, ingest analysis and workflows across the network
It is a technology	It is a technology and is an extension of EDR	It is a managed security service and packages the assistance of EDR and MDR
It collects data from endpoints	It collects data from multiple sources	It collects data from networks, applications, endpoints and cloud services
It uses signature and behavior-based analytics to detect threats	It uses machine learning and AI to associate data from various sources and identity threats	It uses analytics and human expertise to detect and respond to threats
It can automate response actions like isolating endpoints	It can automate response actions like blocking network connections	MDR services are usually more automated than EDR and XDR because third-party vendors manage them and offer greater resources and expertise.

Table 16.1: EDR vs MDR vs XDR



LO#09: Describe the Forensics Investigation Process

This section provides a brief overview of the forensics investigation process carried out during the incident response (IR).



Forensic Investigation

Forensic investigation is the process of gathering evidence related to an incident from the systems and networks. IR helps organizations contain security events, but a computer forensic investigation enables investigators to find the root cause of the security issue. The main goal of any computer security forensic investigation is to identify the incident, the time of the incident, the perpetrator of the incident, and steps to mitigate future occurrences. Forensic investigation and the containment process are conducted simultaneously.

Role of Forensic Analysis in an IR

Forensic analysis includes an evaluation and in-depth investigation of data from before and after the cyber-attack period.

- Forensic analysis helps in determining the exact cause of the incident.
- It helps generate a timeline for the incident that correlates different incidents.
- It helps balance operations and security based on the organization's budgetary constraints.
- Forensic analysis of the affected system helps determine the nature and impact of the incident.
- It helps to mitigate the loss caused by a breach and to begin the recovery process.
- It helps in tracking the attackers of the crime or incident.
- It extracts, processes, and interprets factual evidence that proves the attacker's actions in court.
- It saves the organization money and time by conducting a damage assessment of the victimized network.
- It also saves organizations from legal liabilities and lawsuits.

People Involved in Forensics Investigation

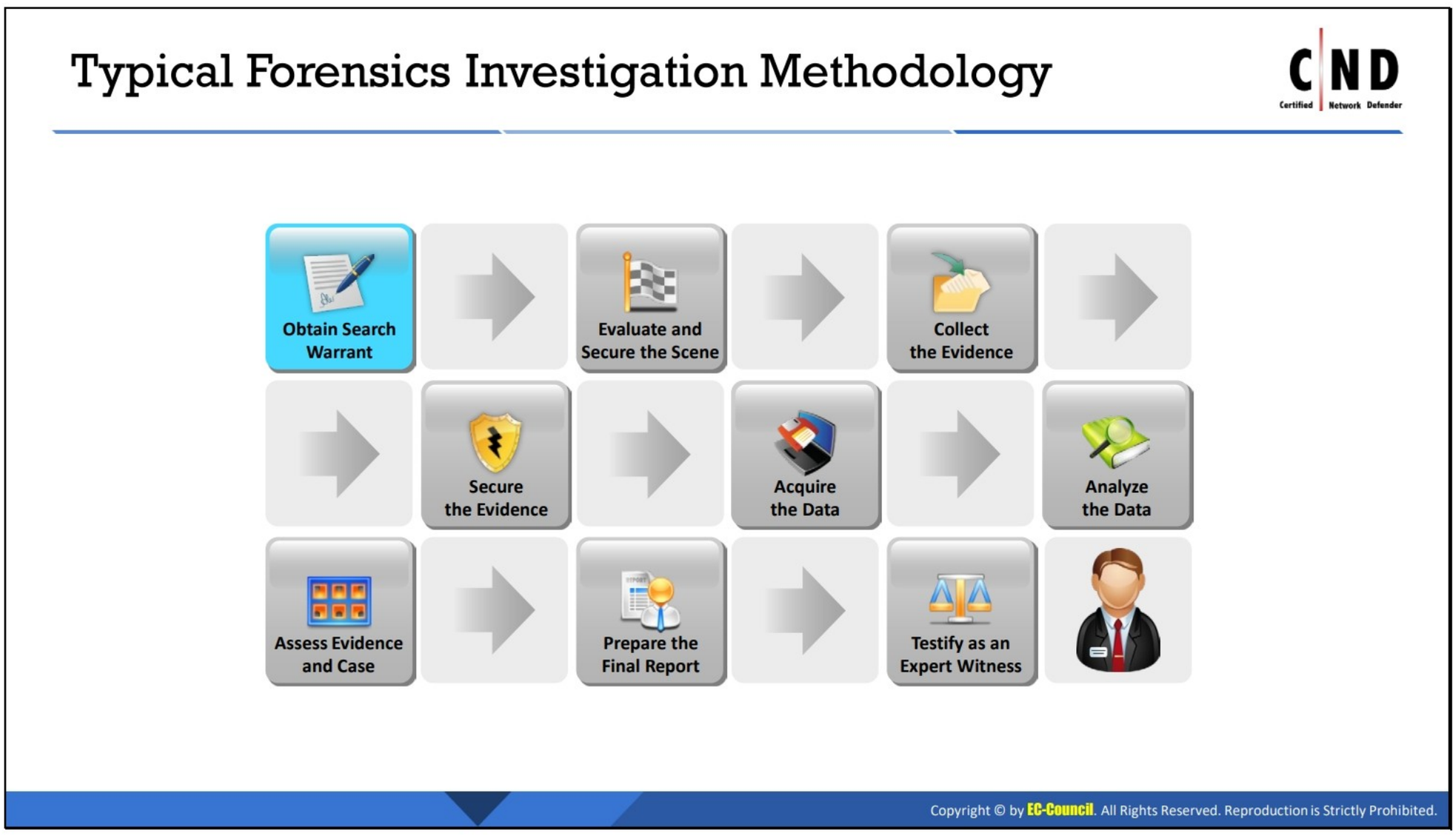
Based on the requirement of the organization, the primary users of forensic tools and techniques fall under three groups.

- **Investigators**: Responsible for investigating incidents
- **IT Professionals**: Includes technical staff and administrators
- **Incident handlers**: Respond to different computer security incidents

A detailed discussion of the people involved in a computer forensics team is provided below.

- **Attorney:** Offers legal advice about how the investigation should be carried out and the legal aspects to be complied with in the computer forensics investigation process.
- **Photographer:** Photographs the crime scene and the evidence gathered. They must be certified for evidence photography. By photographing all evidence found at the crime scene, the photographer records key evidence in the forensics process.
- **Incident Responder:** Responsible for the measures taken when an incident occurs. The incident responder is responsible for securing the incident area and collecting the evidence present at the crime scene.
- **Decision Maker:** Authority responsible for the policy or procedure followed during the investigation process. Based on the incident type, a decision maker decides the policies and procedures and adapts them to the requirements of the incident.
- **Incident Analyzer:** Analyzes the incidents based on their occurrence. They examine the incident with regard to its type, how it affects the system, different threats and vulnerabilities associated with it, among others.

- **Evidence Examiner/Investigator:** Examines the evidence acquired and sorts useful evidence. Examines and sorts the evidence according to its relevance for the case. By maintaining an evidence hierarchy, the evidence examiner appropriately prioritizes the evidence.
- **Evidence Documenter:** Documents all evidence and the phases present in the investigation process. The evidence documenter gathers information from all people involved in the forensics process and documents it in an orderly manner, from the occurrence of the incident to the end of the investigation. The documents contain complete information about the forensics process.
- **Evidence Manager:** Manages the evidence so that it is admissible in a court of law. They have all information about the evidence such as evidence name, evidence type, time, and source of evidence. They manage and maintain a record of the evidence that it is admissible in a court of law.
- **Expert Witness:** Offers a formal opinion as testimony in a court of law. Expert witnesses authenticate the facts and witnesses of a complex case. Expert witnesses are often called to cross-examine other witnesses and evidence, as a normal witness may be influenced by various factors.

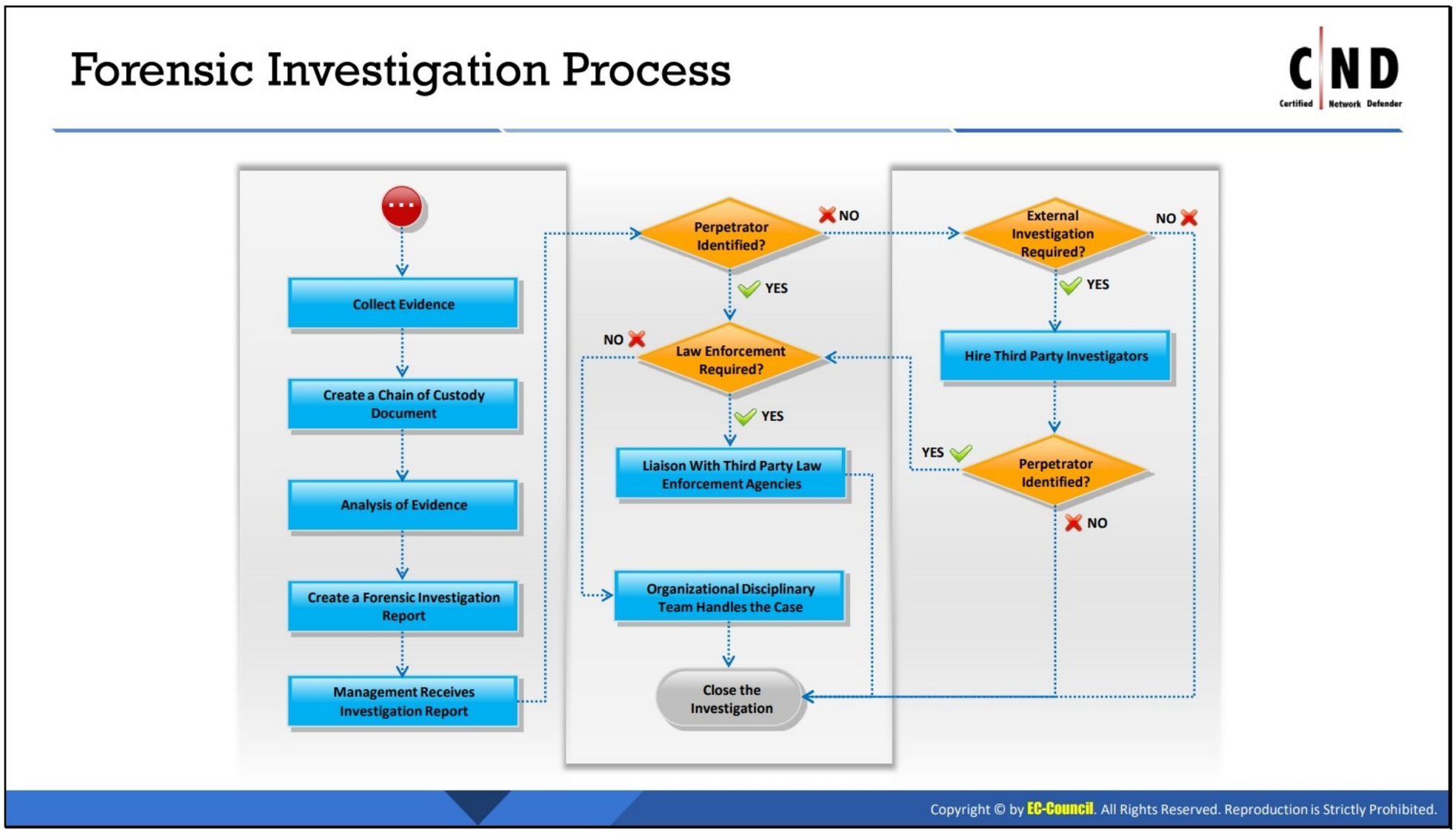


Typical Forensics Investigation Methodology

The forensic investigation methodology includes a series of steps that must be followed to carry out a successful forensic investigation. It guides the investigator in the collection of potential evidence concerning the security incident and ascertains that it is admissible in a court of law. A typical forensics investigation methodology includes the following steps.

1. **Obtain a search warrant:** Investigators obtain a search warrant before investigating any suspects. The warrant proves beneficial for the investigator.
2. **Evaluate and secure the scene:** Investigators evaluate and secure the scene before collecting the evidence. Tampering or damaging the devices can affect the evidential proof against the suspect.
3. **Collect the evidence:** Investigators collect all evidence discovered from the scene. They must not neglect any of the supporting items related to the incident that can act as evidence and be helpful in a court of law.
4. **Secure the evidence:** The investigator securely stores the collected evidence. Loss of evidence will weaken the case against the suspect.
5. **Acquire the data:** It is important to acquire the affected data. This will help the investigator identify the reason for the intrusion.
6. **Analyze the data:** Analyzing the data also includes monitoring the target's activity before, during, and after the incident. The Analysis phase is the most important phase, as the investigator gathers more evidence by monitoring logs.
7. **Assess the evidence and the case:** Once the investigator has completed the analysis, it is important to gather the evidence and assess it.

8. **Prepare the final report:** The final report includes detailed information about the actions taken by the investigator and the suspect/attacker.
9. **Testify as an expert witness:** The investigator testifies as an expert witness who confirms the facts of the case.



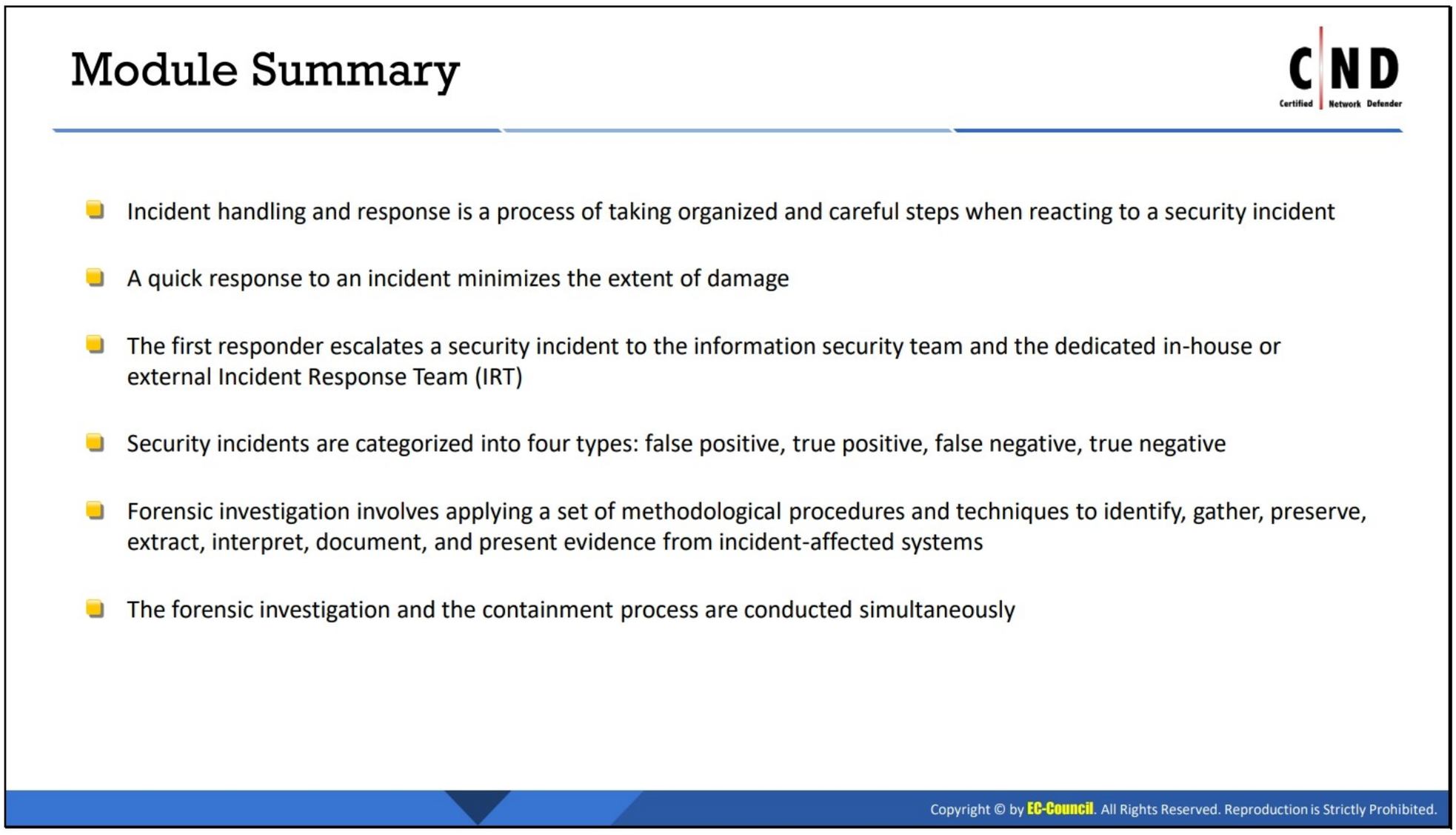
Forensic Investigation Process

A forensic investigation involves using various processes, tools, and techniques to gather valuable information. The forensics investigation team analyzes the evidence to identify the real cause and nature of the incident and trace the perpetrators after collecting and protecting the evidence. The team documents and submits the results of the forensic analysis to the management.

If the investigation report identifies the perpetrator, the management then decides whether law enforcement is required to prosecute the perpetrator or whether the organizational disciplinary team should handle the case. If there is a need for law enforcement, then the management or a designated authority contacts a third-party law enforcement agency. If the attacker is not identified, then the management decides whether to close the investigation or to pass it to an external investigation agency for further investigation. If the third-party investigators are able to investigate the incident and identify the attacker, it will be reported to the management.

The management makes further decisions regarding the prosecution of the attacker. If the third-party investigators also fail to identify the perpetrator, the IRT or management will recommend an update in the IR processes in order to carry out successful investigations in the future.

Organizations must notify external law enforcement and investigation agencies if the incident is severe and affects the employees, customers, and the general public. If the incident has caused severe damages and financial losses, the organization should report the incident to law enforcement agencies and file a case against the attackers. These agencies can include local or national law enforcement agencies, security agencies, or cyber experts, among others.



Module Summary

In this module, you have learned about the importance of providing timely responses to incidents. Timely responses prevent major losses to the organization. The first responder plays vital role in providing a timely response for incidents. The Incident Response Team (IRT) works with the initial information provided by the first responder concerning the incident. The module also provided an overview of the entire process of the incident response that the IRT follows and implements for the successful handling, eradication, containment, and investigation of, and recovery from, all types of security incidents.

This page is intentionally left blank.