EC-Council

Building A Culture Of Security

C|ND

Certified Network Defender

Certified Network Defender v3

MODULE 14

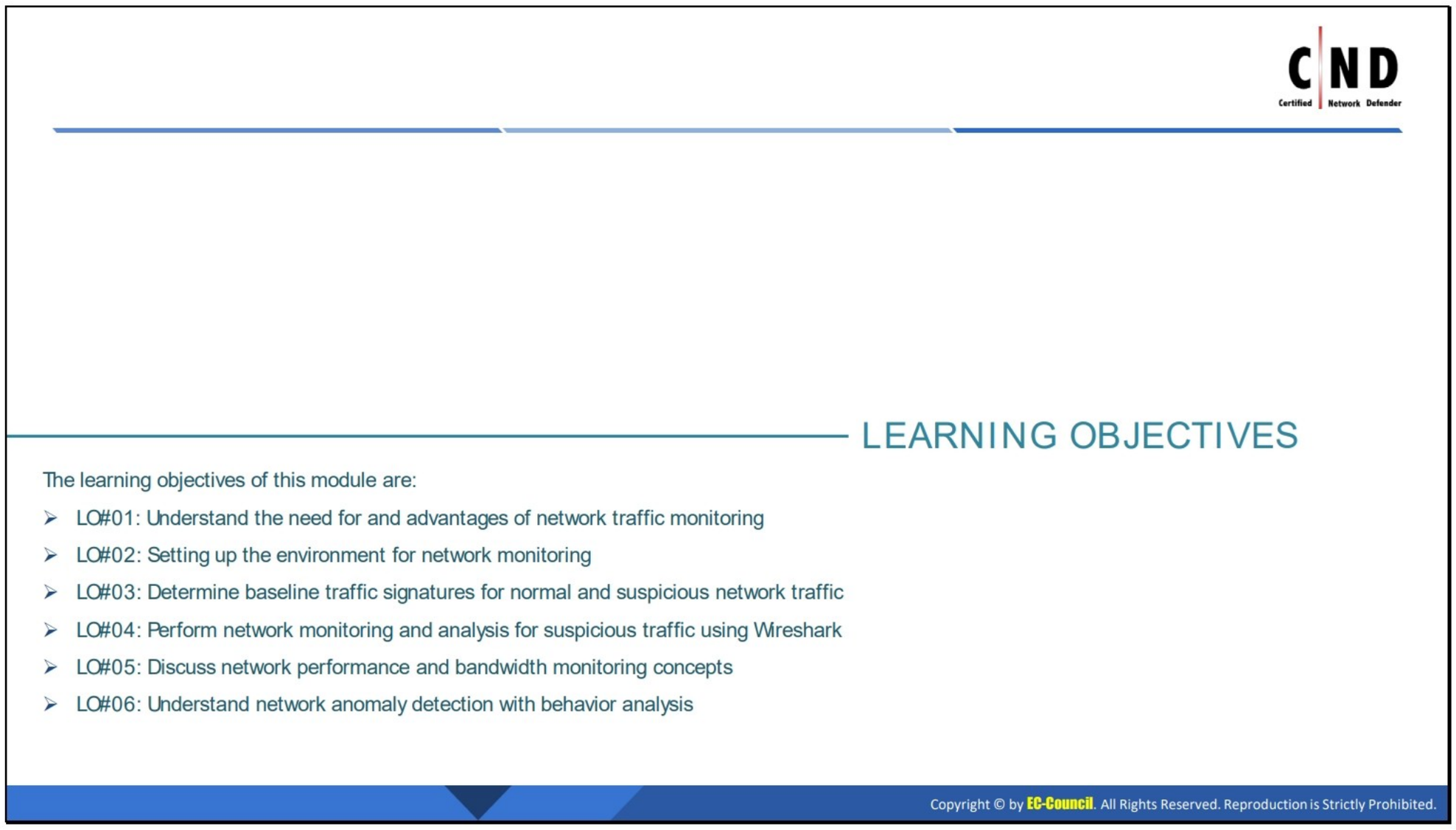
NETWORK TRAFFIC MONITORING AND ANALYSIS

EC-Council Official Curricula

https://t.me/learningnets

This page is intentionally left blank.

https://t.me/learningnets



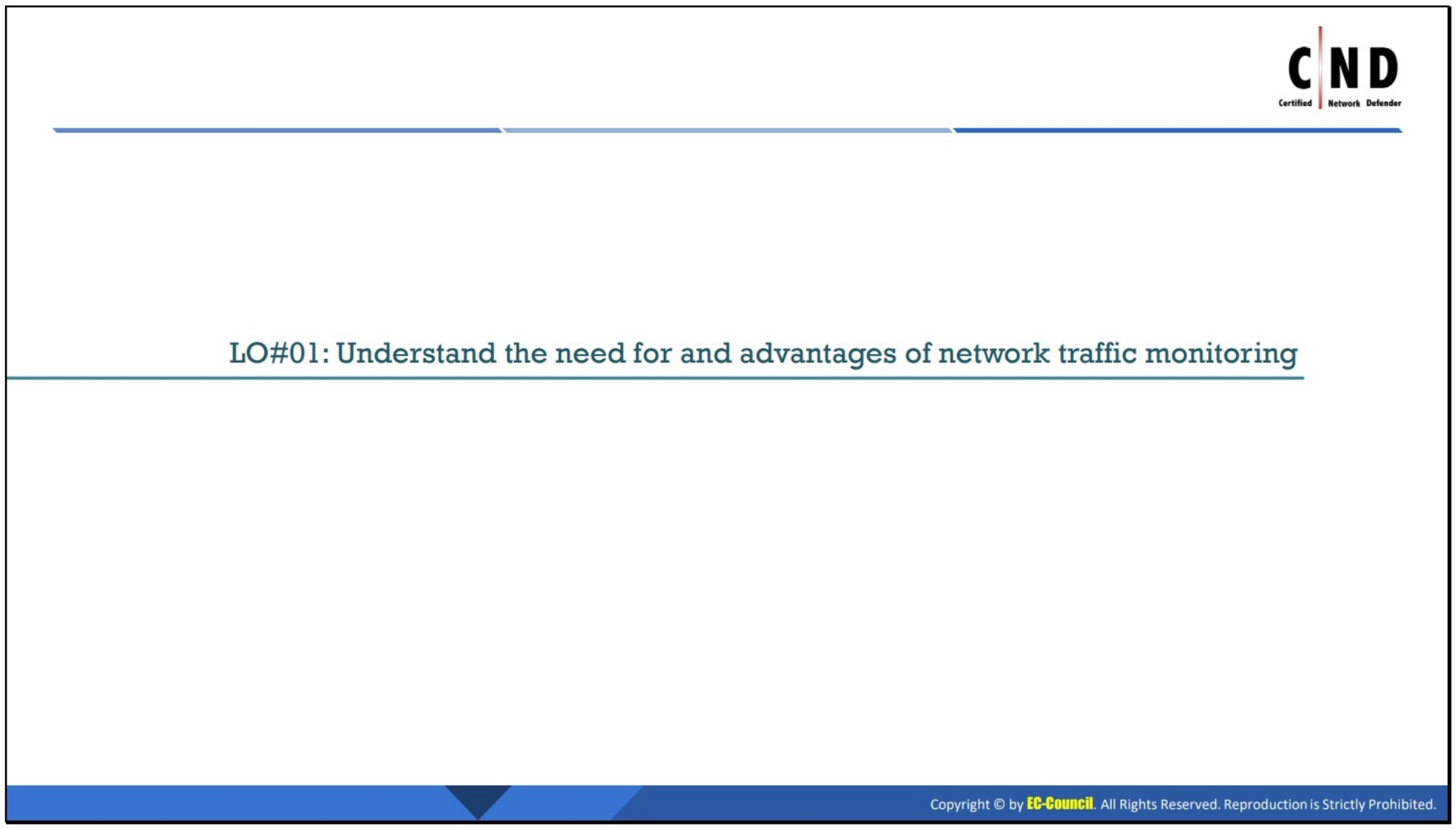
Learning Objectives

Organizations need to perform network monitoring and analyze network traffic to identify suspicious activities across their networks. This module covers the concept of network traffic monitoring. The following are the learning objectives of the module:

- Understand the need for and advantages of network traffic monitoring
- Setting up the environment for network monitoring
- Determine baseline traffic signatures for normal and suspicious network traffic
- Perform network monitoring and analysis for suspicious traffic using Wireshark
- Discuss network performance and bandwidth monitoring concepts
- Understand network anomaly detection with behavior analysis

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

https://t.me/learningnets

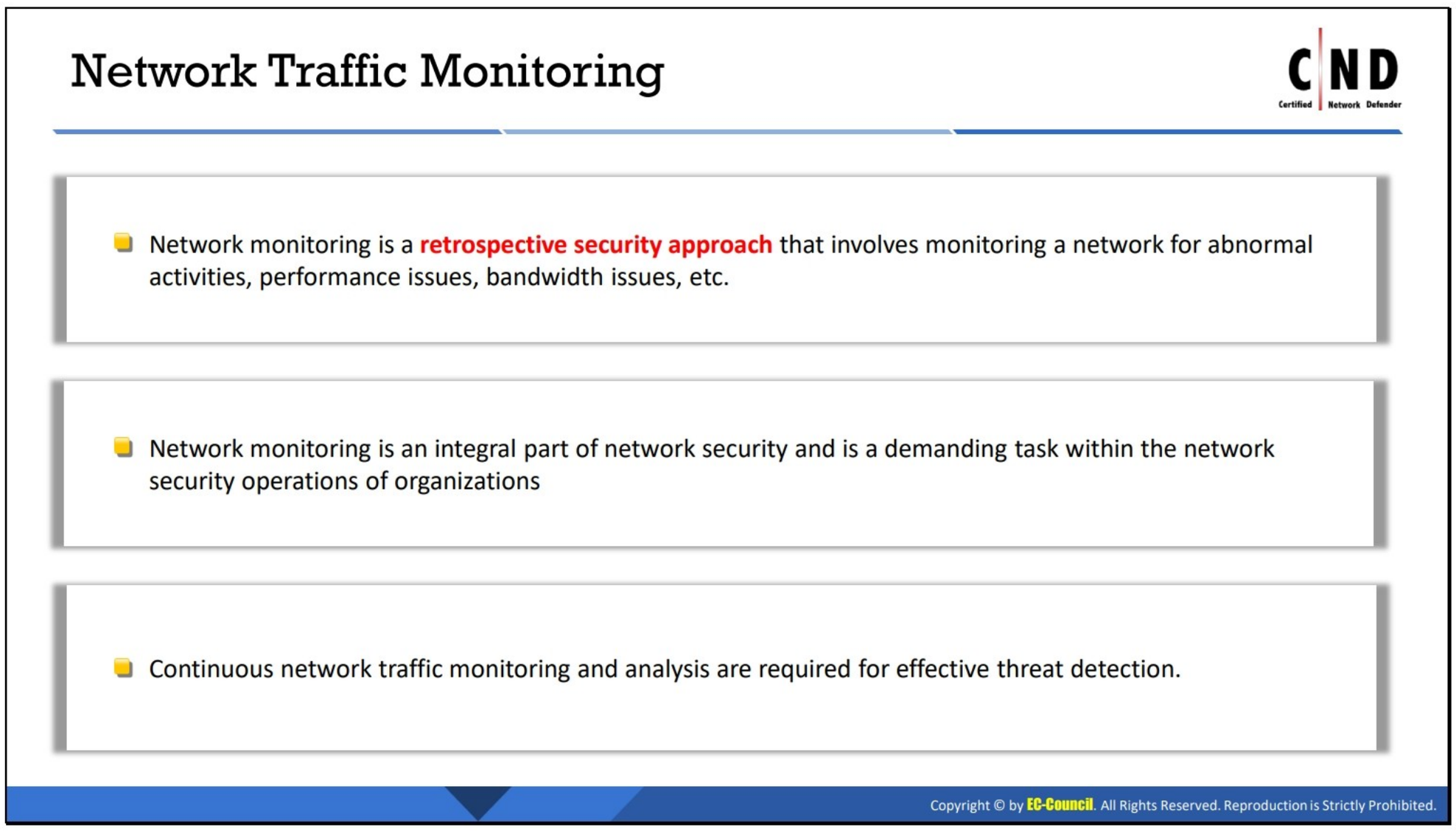


LO#01: Understand the Need for and Advantages of Network Traffic Monitoring

The objective of this section is to explain in detail the need for and advantages of network traffic monitoring.

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

https://t.me/learningnets



Network Traffic Monitoring

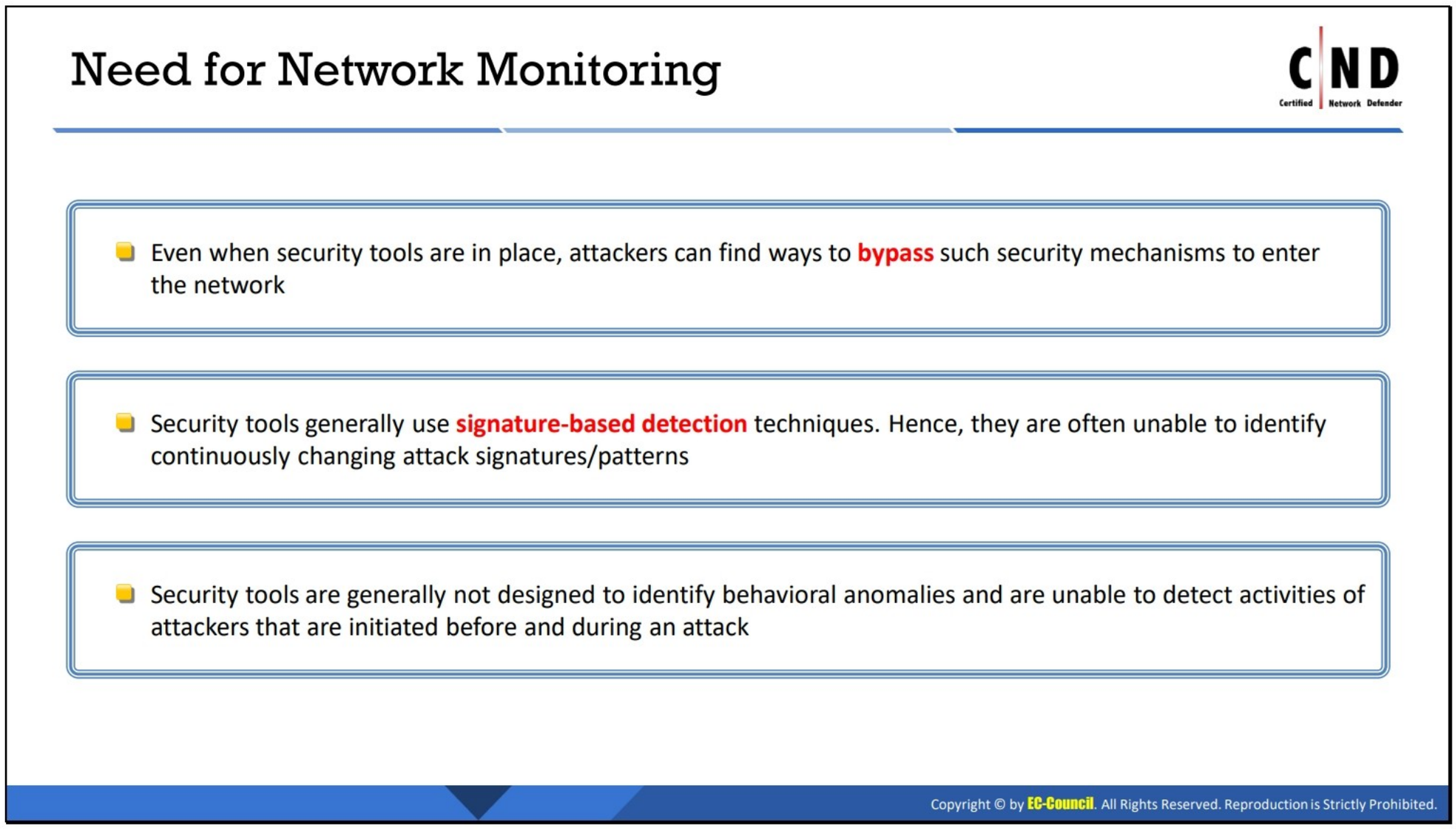
Network traffic monitoring is the process of capturing network traffic and inspecting it closely to determine what is happening on the network. Network defender should constantly strive to maintain smooth network operation. If a network goes down even for a small period, productivity within a company may decline. To be proactive rather than reactive, the traffic movement and performance must be monitored to ensure that no security breach occurs within the network.

The network monitoring process involves sniffing the traffic flowing through the network. For this purpose, network packets must be captured and a signature analysis must be conducted to identify any malicious activity.

Network operators use network traffic analysis tools to identify malicious or suspicious packets hiding within traffic. They monitor download/upload speeds, throughput, content, traffic behaviors, etc. to understand the status of the network operations.

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

https://t.me/learningnets



Need for Network Monitoring

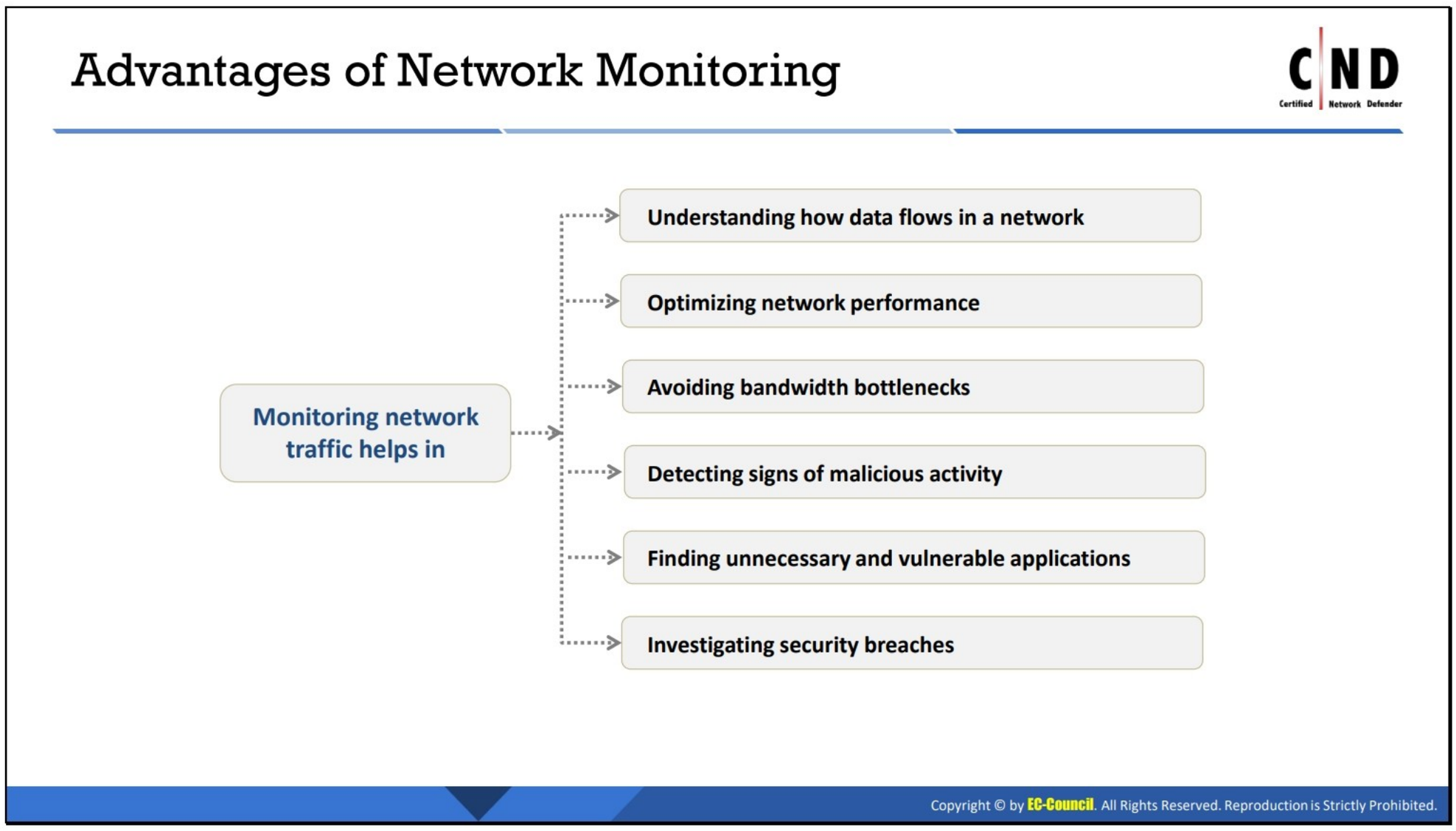
Networking monitoring helps network defenders identify possible issues before they affect business continuity. If an issue occurs in the network, the root cause can be determined easily with network monitoring, and with network automation tools, the problem can be fixed automatically. Networking monitoring not only prevents outages but also gives visibility to potential issues. Continuous network monitoring minimizes downtime and increases the performance of the network.

Even when security tools are in place, an attacker can gain access to the network and exploit it. Security tools generally use signature-based detection techniques, and it is difficult to identify continuously changing attack signatures/patterns. These tools are not designed to identify behavioral anomalies and are unable to detect attackers' activities that are initiated before and during attacks.

Network monitoring tools provide the first level of security and help identify anomalous conditions in the network, which indicate attacker activity.

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

https://t.me/learningnets



Advantages of Network Monitoring

Network traffic analysis is performed to gain in-depth insight into the types of network packets or data flowing through a network. Typically, it is performed through network monitoring or network bandwidth monitoring utilities. The traffic statistics from network traffic analysis helps in the following:

- Understanding and evaluating network utilization
- Determining download/upload speeds
- Determining the type, size, origin, destination, and content/data of packets

The typical advantages of network monitoring are as follows.

- **Proactive:** Network monitoring proactively detects applications that consume the maximum bandwidth and reduces the bandwidth. It manages server bottleneck situations and other systems connected to the network. Moreover, network monitoring delivers an efficient quality of service to users. It creates a record of all the irregularities occurring in the network that network defender can handle later.
- **Utilization:** It is important to understand the need for network utilization, especially with all the new and evolving technology. Network monitoring provides complete details on the infrastructure. It provides an idea about the amount of load a network can handle during periods of heavy traffic, enabling the efficient utilization of the space in the network.
- **Optimization:** Network monitoring techniques gather network infrastructure information in a timely manner and save it for the network defenders. Network defender can then take the required actions before the situation worsens. These techniques identify applications that prove vulnerable to the network.

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

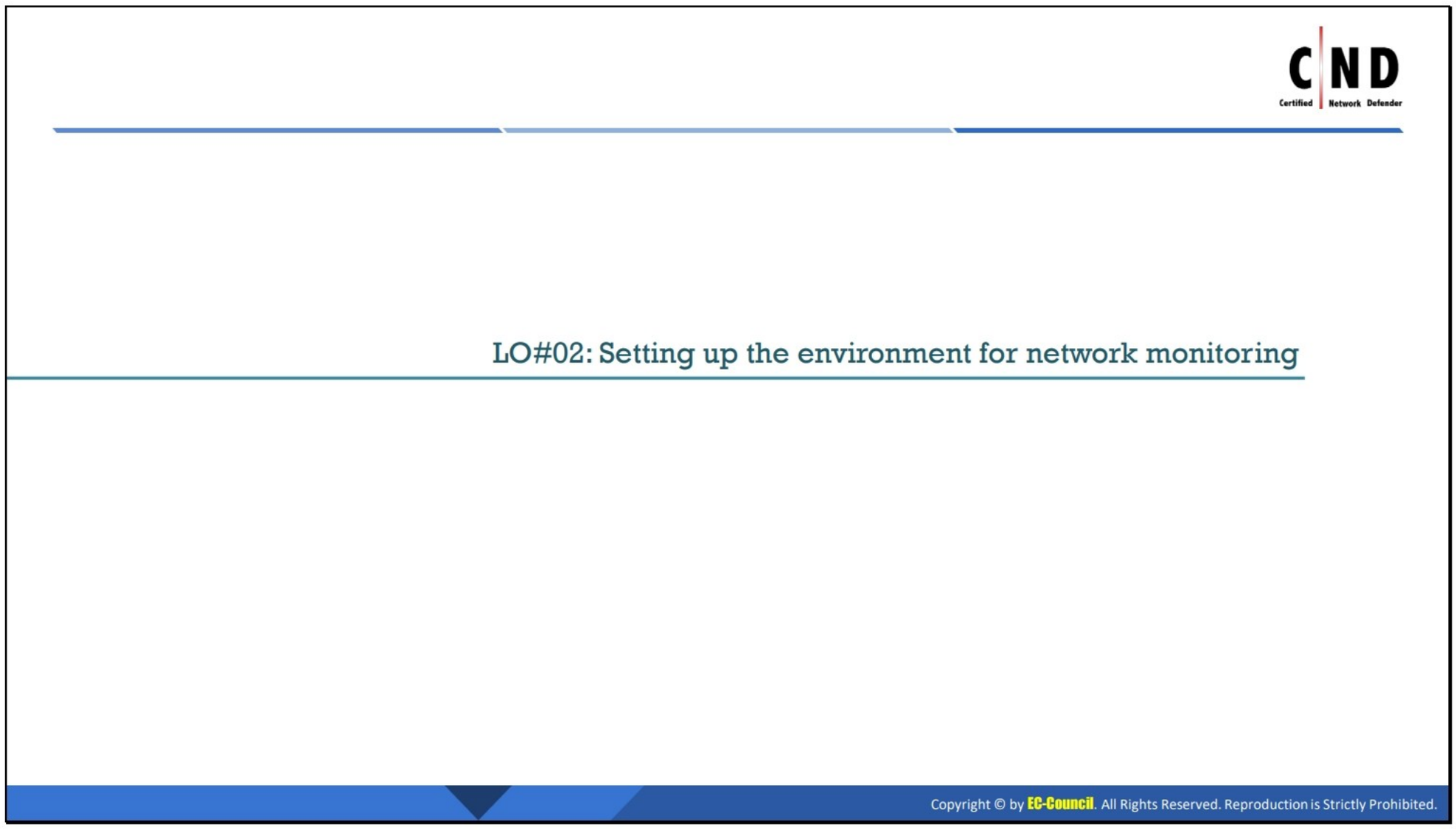
https://t.me/learningnets

- **Minimizing risk:** Network monitoring techniques are necessary for establishing service-level agreements (SLAs) and compliance applicable to users or consumers. Complete infrastructure information is required when drafting SLAs. The real-time monitoring of network topologies and channels helps in creating the SLAs.

Network monitoring techniques are beneficial for network defenders. They are very easy to setup and implement, considering the complexity of networks.

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

https://t.me/learningnets

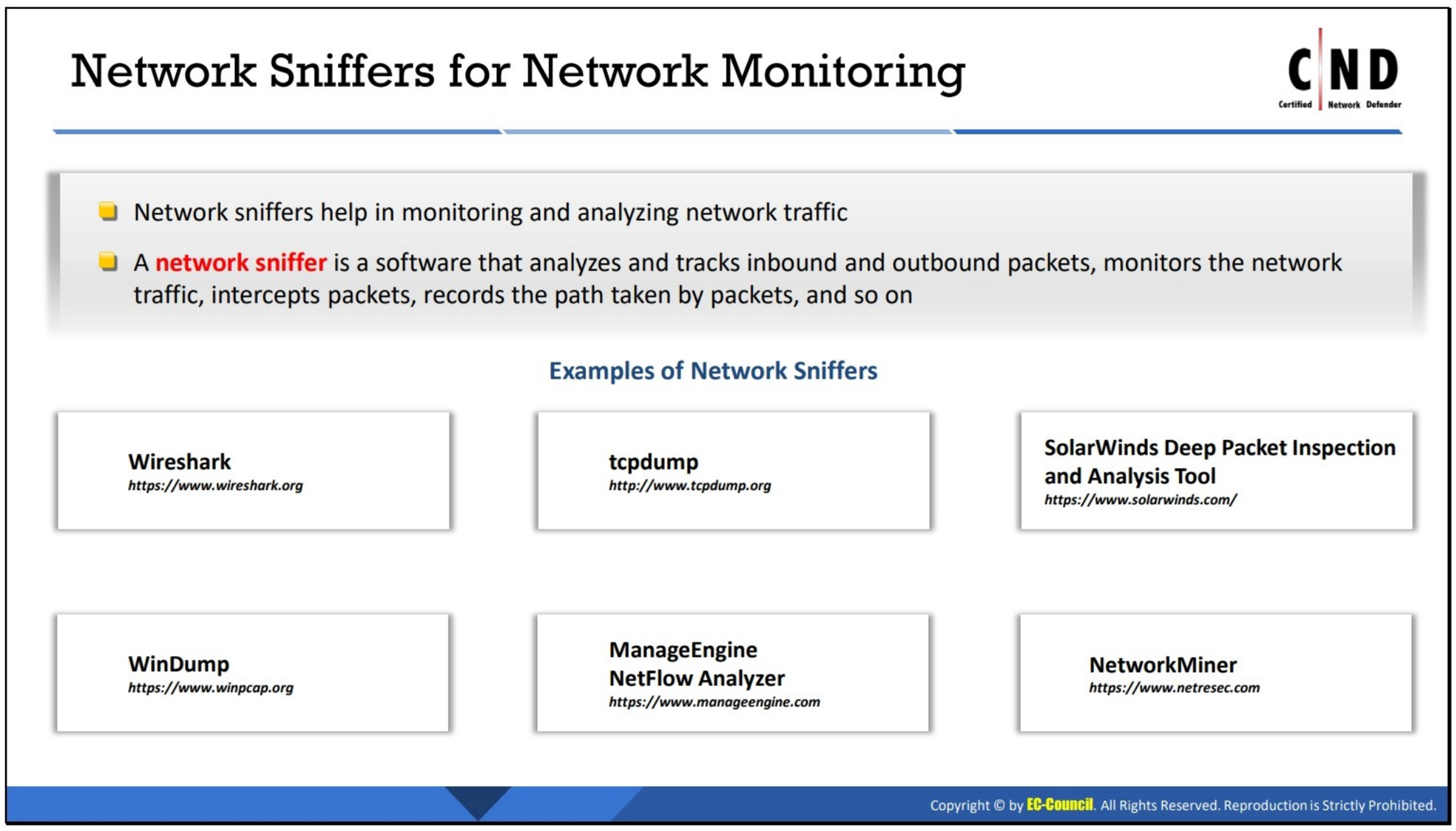


LO#02: Setting up the Environment for Network Monitoring

The objective of this section is to explain how to setup the environment for network monitoring and describe the use of various network sniffing tools for network monitoring.

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

https://t.me/learningnets



Network Sniffers for Network Monitoring

A network sniffer or packet sniffer is a tool that can intercept and log traffic passing through a network. Sniffers are used in network management because of their monitoring and analyzing features, which help detect intrusions, supervise network contents, troubleshoot network, and control traffic. They are used to analyze the behavior of an application or device causing network issues.

The information flowing through a network is a valuable source of evidence to counter intrusions or anomalous connections. The need to capture this information has led to the development of packet sniffers.

Some examples of network sniffers are discussed below.

Wireshark

Source: https://www.wireshark.org

Wireshark is an open-source cross-platform packet capture and analysis tool. It is available for Windows and Linux operating systems (OSes). Wireshark's graphical user interface (GUI) provides a detailed breakdown of the network protocol stack for each packet. Wireshark can also save packet data to a file for offline analysis as well as export and import packet captures to and from other tools. Statistics can also be generated for packet capture files.

tcpdump

Source: http://www.tcpdump.org

tcpdump is a command-line network analyzer tool or, more technically, a packet sniffer. Network defenders can use this utility for network analysis.

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

https://t.me/learningnets

SolarWinds Deep Packet Inspection and Analysis Tool

https://www.solarwinds.com/

SolarWinds track network and application traffic on a packet level. It uses response time metrics to measure the time it takes for packets to travel between clients and servers. This allows administrators to manage traffic flows and distinguish between network and application problems.

WinDump

Source: https://www.winpcap.org

WinDump is the Windows version of tcpdump and can be used to watch, diagnose, and save network traffic according to various complex rules.

ManageEngine NetFlow Analyzer

Source: https://www.manageengine.com

NetFlow Analyzer is a complete traffic analytics tool that leverages flow technologies to perform network traffic analysis by providing real-time visibility to traffic patterns.

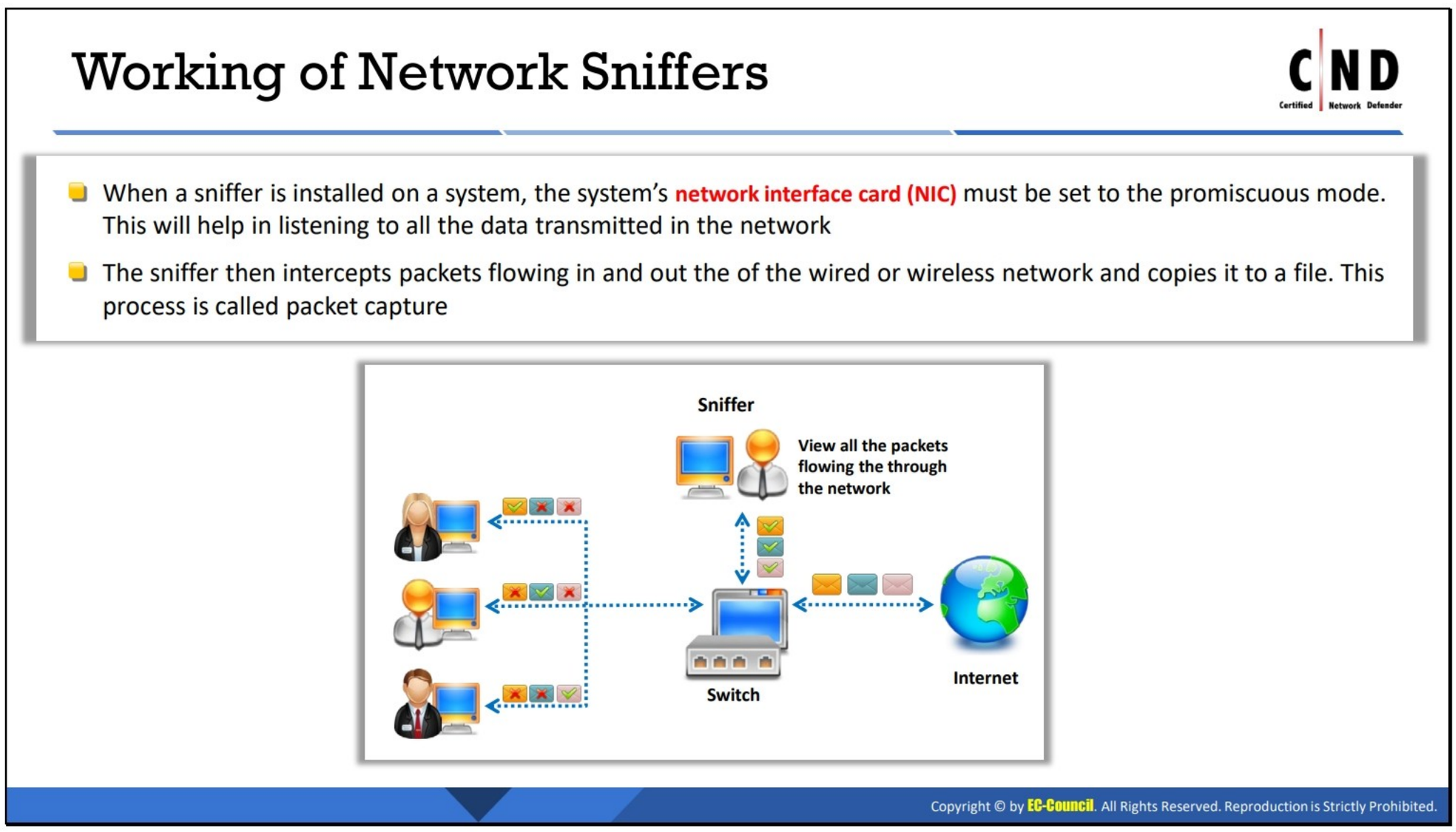
NetworkMiner

Source: https://www.netresec.com

NetworkMiner can be used as a passive network sniffer/packet capturing tool to perform advanced network traffic analysis (NTA); its displays extracted artifacts in an intuitive user interface.

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

https://t.me/learningnets

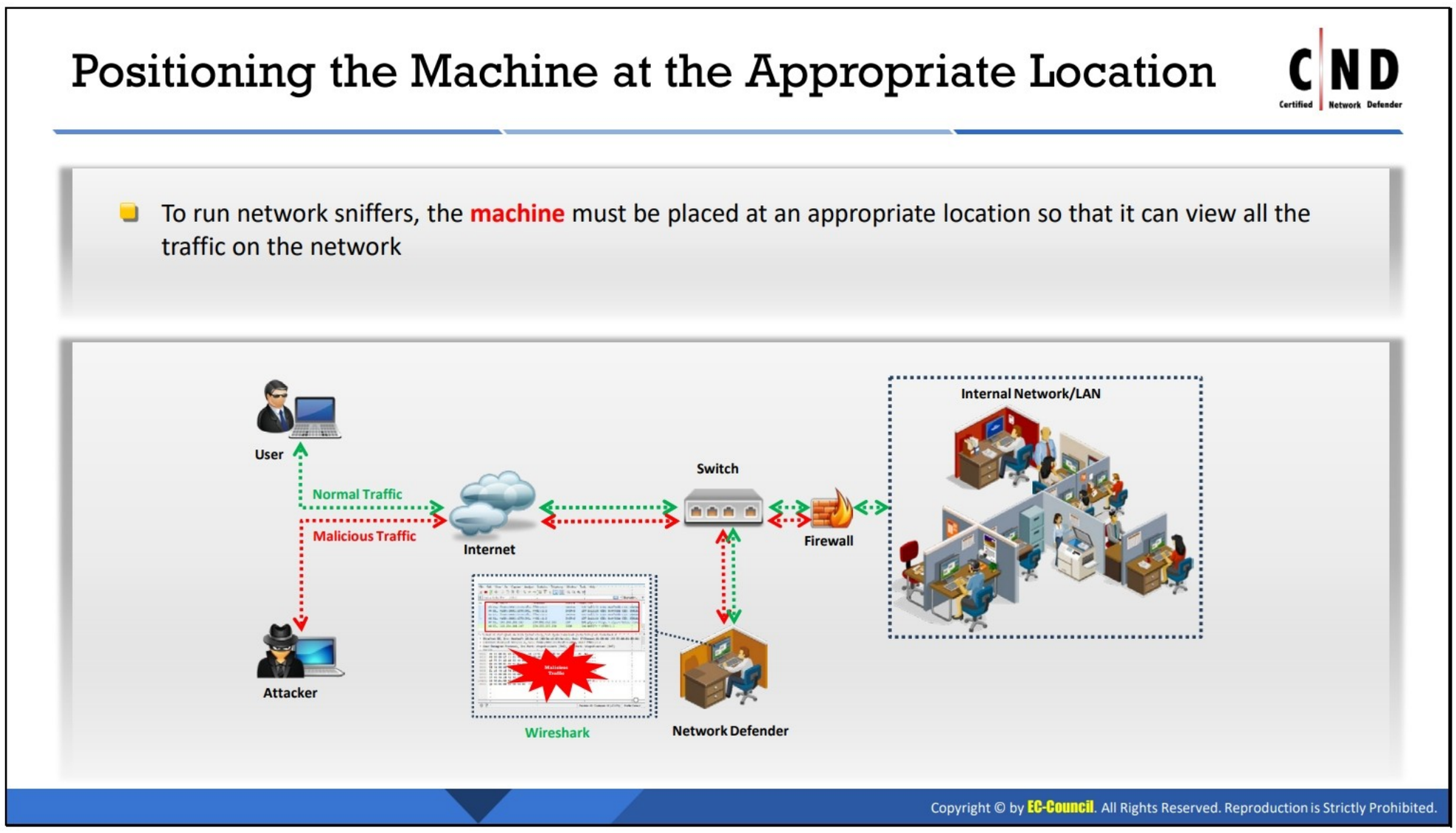


Working of Network Sniffers

The most common way of networking computers is through Ethernet. A computer connected to a local area network (LAN) has two addresses: a media access control (MAC) address and an Internet Protocol (IP) address. A MAC address uniquely identifies each node in a network and is stored on the network interface controller (NIC) of a device. The Ethernet protocol uses the MAC address to transfer data to and from a system while building data frames. The data-link Layer of the OSI model uses an Ethernet header with the MAC address of the destination machine instead of the IP address. The network layer is responsible for mapping network IP addresses to MAC addresses, as required by the data-link protocol. It initially looks for the MAC address of the destination machine in a table, usually called the Address Resolution Protocol (ARP) cache. If there is no entry for the IP address, an ARP broadcast of a request packet goes out to all machines on the local sub-network. The machine with that particular address responds to the source machine with its MAC address. The source machine's ARP cache adds this MAC address to the table. The source machine subsequently uses this MAC address in all its communications with the destination machine.

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

https://t.me/learningnets



Positioning the Machine at the Appropriate Location

Systems should be placed and connected in such a manner that all the inbound and outbound traffic flowing through the network can be viewed. Each packet must be inspected against policy violations, and a machine must be placed as shown in Figure 14.1. It should connect to a switch in front of a firewall and must be installed with the required packet sniffing and network monitoring tools.

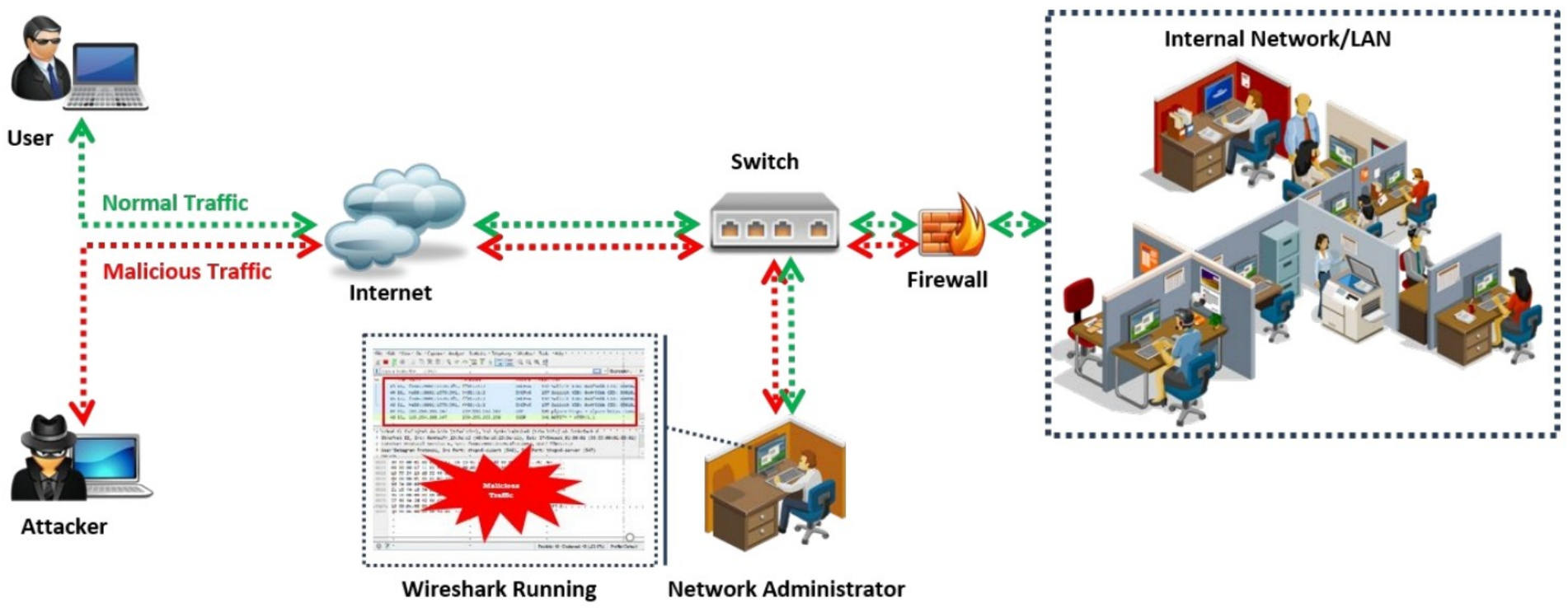
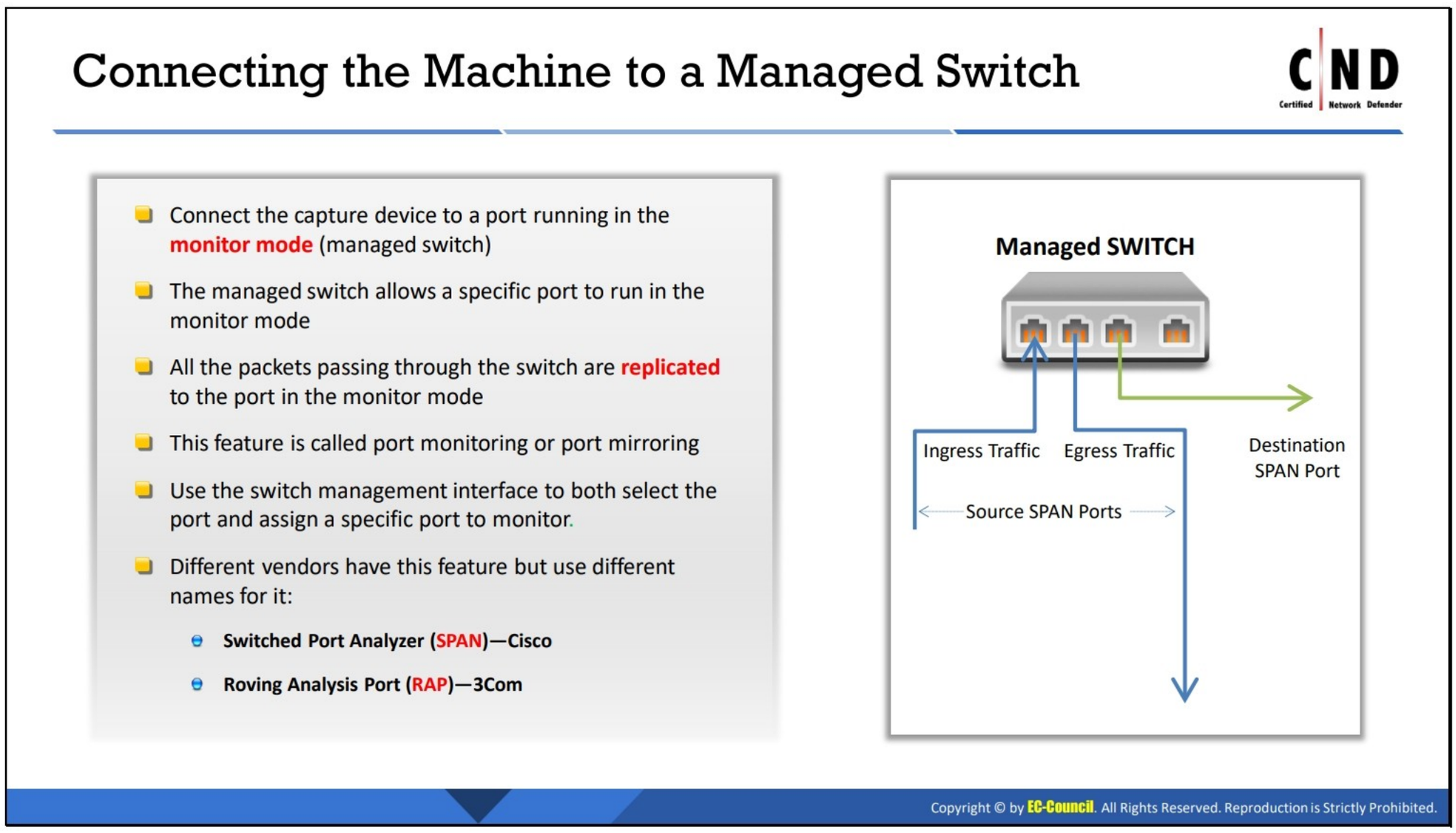


Figure 14.1: Deployment of machines at appropriate locations

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

https://t.me/learningnets



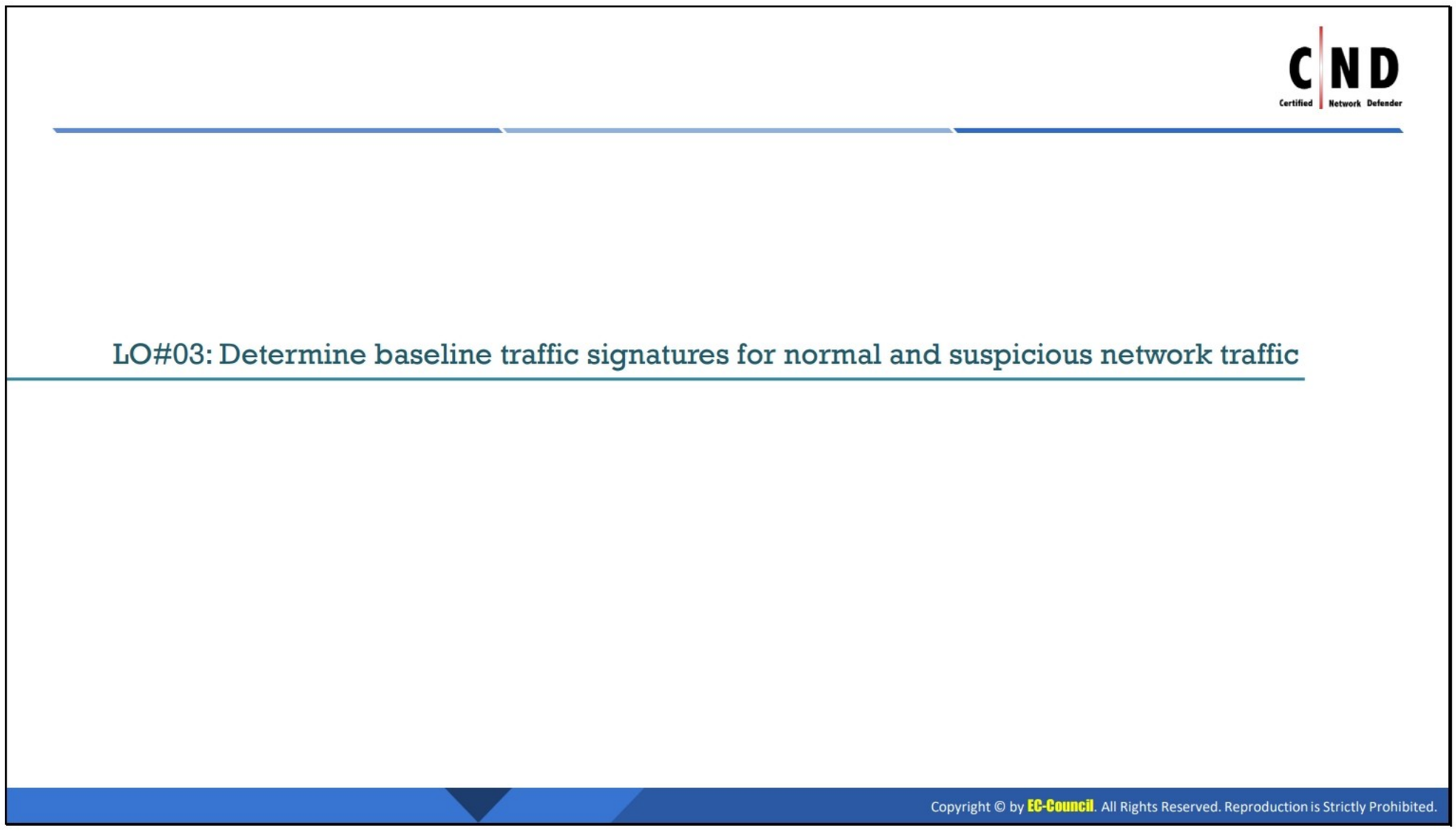
Connecting the Machine to a Managed Switch

The switch in the network should be connected and configured as a managed switch, which can only view the network traffic. A switch can be configured as a managed switch by enabling the port monitoring or port mirroring feature on a specific port in the switch. Different vendors have different names for this feature. For example, the port mirroring feature on Cisco switches is known as the Switched Port Analyzer (SPAN) port. The port mirroring process includes copying the switch network traffic and sending it to another port in the switch so that the monitoring tool can analyze it.

A managed switch can configure, manage, and monitor a LAN. It allows greater control over the flow of data in the network. Accessibility to manage the data flow significantly decreases the chances of an intrusion. Though a managed switch may cost more than an unmanaged switch, it assures better security and filtered data transmissions.

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

https://t.me/learningnets

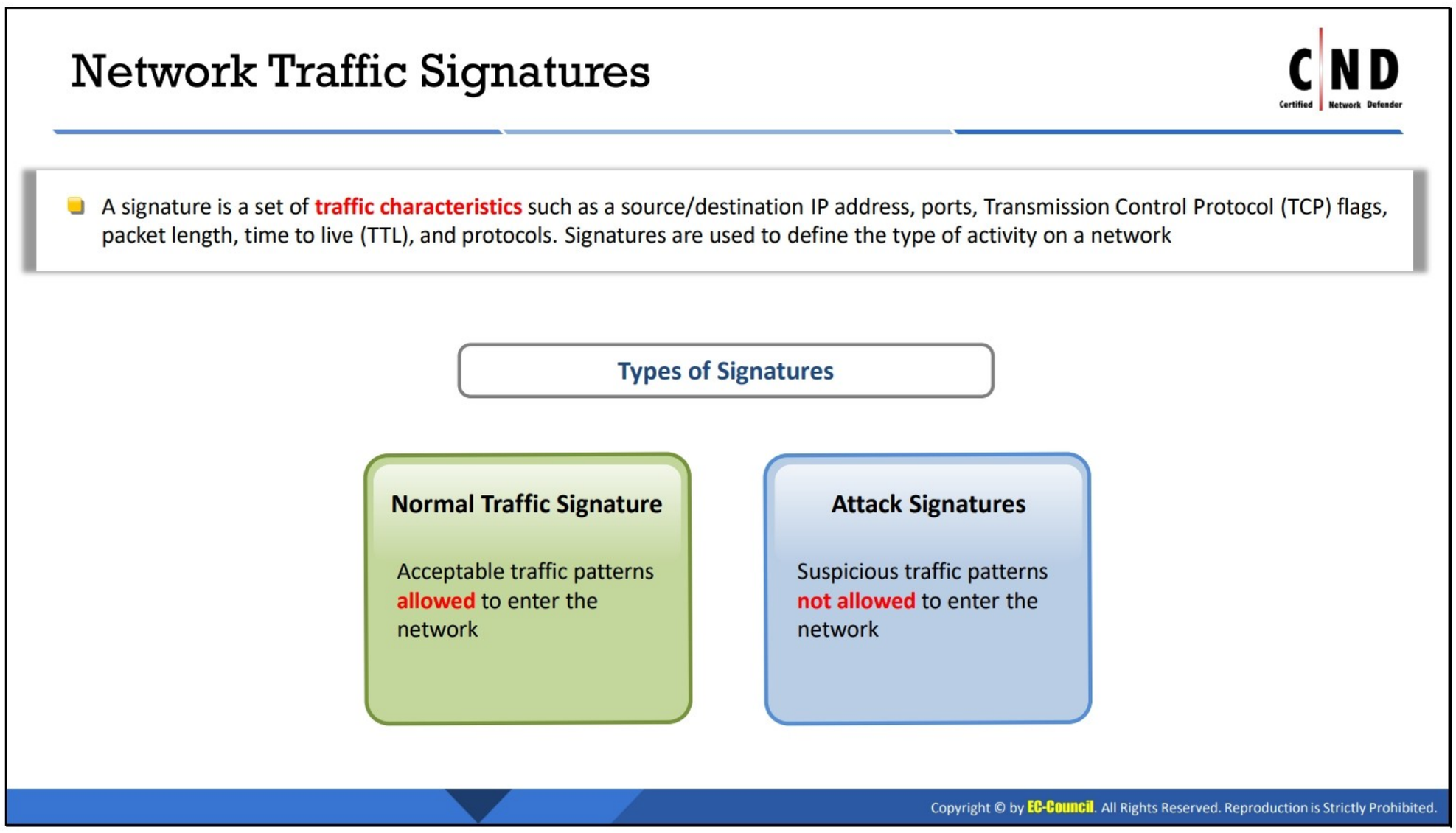


LO#03: Determine Baseline Traffic Signatures for Normal and Suspicious Network Traffic

The objective of this section is to explain the various types network traffic signatures and the concept of baselining normal traffic signatures. It describes the categories of suspicious network traffic signatures and attack signature analysis techniques.

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

https://t.me/learningnets



Network Traffic Signatures

A signature is a set of characters that define network activity, including IP addresses, Transmission Control Protocol (TCP) flags, and port numbers. It includes a set of rules used to detect malicious traffic entering a network. Signatures are used to perform the following:

- Raise alerts in the case of unusual traffic on the network.
- Identify suspicious header characteristics in a packet.
- Configure an intrusion detection system to identify attacks or probes.
- Acquire knowledge on a specific attack that occurred or a vulnerability that can be exploited.
- Match patterns in a packet analysis.

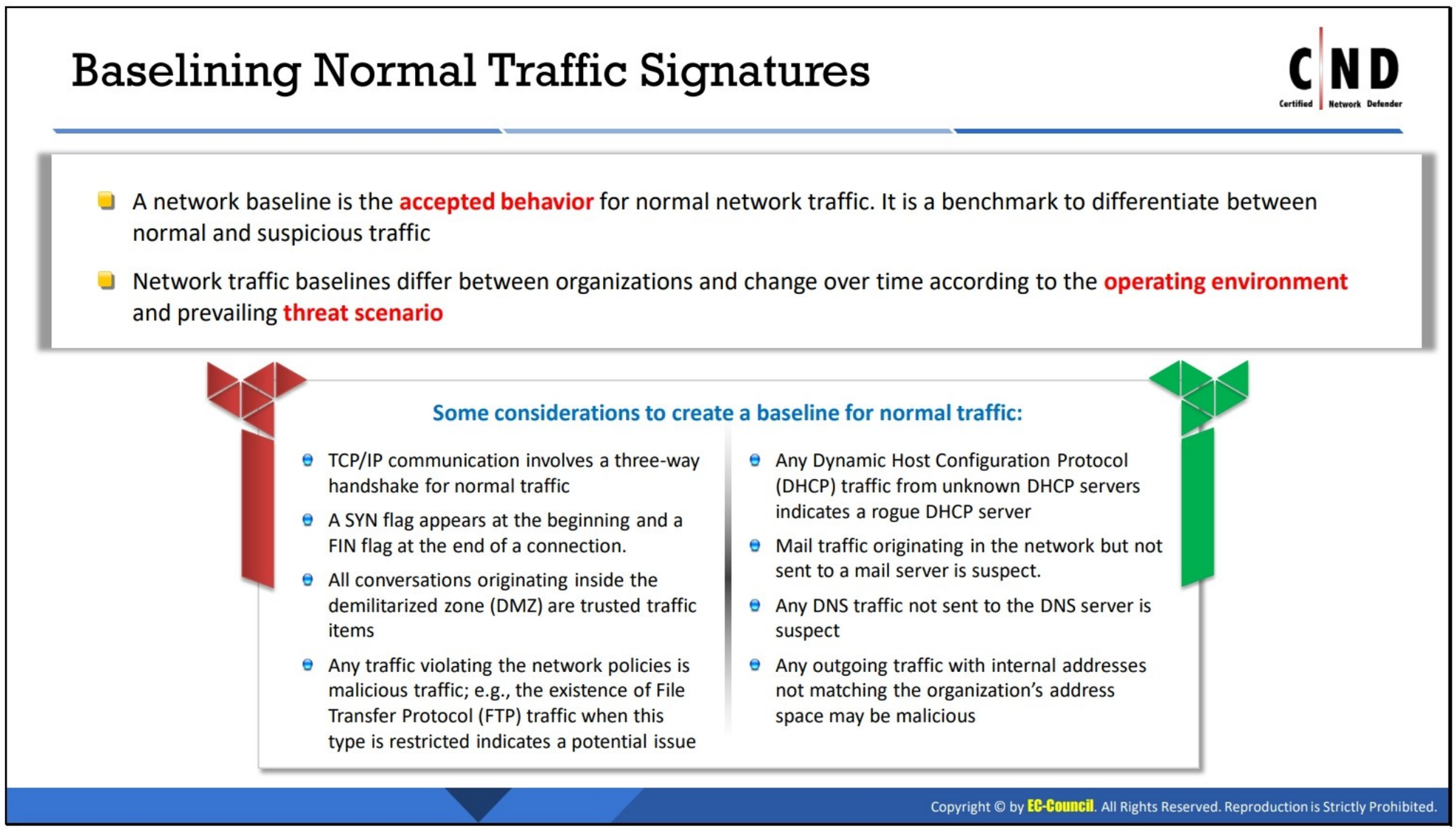
Type of Signatures

Signatures are classified into two main categories depending on their behavior, as described below.

- **Normal traffic signatures**: These include the normal network traffic in the network and are defined based on a normal traffic baseline for the organization. These signatures do not contain any malicious patterns and can be allowed to enter the network.
- **Attack Signatures**: Traffic patterns that appear suspicious are generally treated as attack signatures. These signatures should not be allowed to enter the network. If allowed, they often cause a network security breach. These signatures deviate from the normal signature behavior and should be analyzed.

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

https://t.me/learningnets



Baselining Normal Traffic Signatures

A network traffic baseline helps understand the behavioral patterns of a network. Baselining allows a set of metrics to monitor network performance. These metrics define the normal working condition of an enterprise's network traffic. The network traffic is compared with metrics to detect any changes in the traffic that could indicate a security issue in the network. A network traffic baseline establishes the accepted packets that are safe for the organization. Baselining the traffic facilitates the detection of suspicious activities on the network. Any deviation from the normal traffic baseline can be considered a suspicious traffic signature. The network defender should define a network baseline for their organization and validate the traffic against it. Baselining is more effective if it works in parallel with the organization's policy. With the help of normal traffic baselining, network defenders can judge the requirements to secure the network.

Although there is no industry standard to measure network traffic performance baselines, there are network monitoring tools that provide estimates of what type of traffic is normal. A network traffic baseline should be defined for all incoming and outgoing Internet traffic and wide area network (WAN) links. The network traffic baseline should also contain the traffic for critical business data and backup systems.

- According to a network traffic baseline, normal traffic signatures for TCP packets should have the following characteristics:
  - To establish a three-way handshake, TCP uses SYN, SYN ACK, and ACK bits in every session.
  - The ACK bit should be set in every packet, except for the initial packet, in which the SYN bit is set.

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

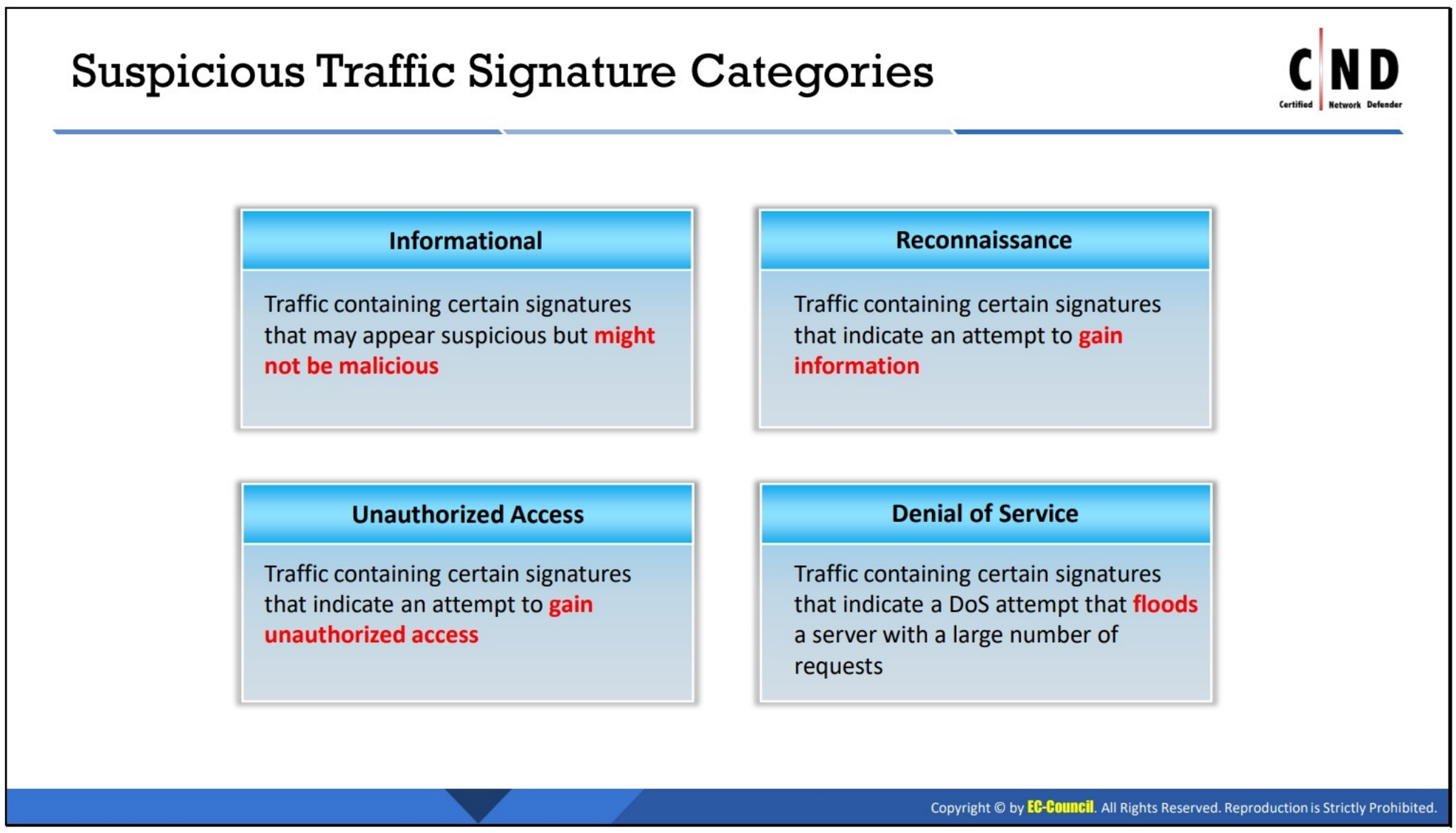
https://t.me/learningnets

- FIN ACK and ACK are used in terminating a connection. PSH FIN and ACK may also be used initially in the same process.
- RST and RST ACK are used to quickly end an on-going connection.
- During a conversation (after a handshake and before termination), packets only contain an ACK bit by default. Occasionally, they may also have a PSH or URG bit set.

- A suspicious TCP packet has one or more of the following characteristics:
  - If both SYN and FIN bits are set, the TCP packet is illegal.
  - SYN FIN PSH, SYN FIN RST, and SIN FIN PSH RST are all variants of SIN FIN. An attacker sets these additional bits to avoid detection.
  - A packet having only a FIN flag is illegal as FIN can be used in network mapping, port scanning, and other stealth activities.
  - Some packets have all six flags unset; these are known as NULL flags and are illegal.
  - The source or destination port is zero.
  - If the ACK flag is set, then the acknowledgement number should not be zero.
  - If a packet has only the SYN bit, which is set at the beginning to establish a connection, and any other data are present, then it is an illegal packet.
  - If the destination address is a broadcast address (ending with 0 or 255), it is an illegal packet.
  - Every TCP packet has two bits reserved for future use. If either or both are set, then the packet is illegal.

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

https://t.me/learningnets



Suspicious Traffic Signature Categories

Network traffic deviating from normal behavior is categorized as a suspicious traffic signature. It is classified into four categories as follows.

- **Informational:** The informational traffic signature detects normal network activity. Although it may not appear suspicious, the data gathered through the informational signature can be used for suspicious activities. For example, informational traffic signatures may include the following:
  - Internet Control Message Protocol (ICMP) echo requests
  - TCP connection requests
  - User Datagram Protocol (UDP) connections
- **Reconnaissance**: Reconnaissance traffic consists of signatures that indicate an attempt to scan the network for possible weaknesses. Reconnaissance is an unauthorized discovery of vulnerabilities, which maps of systems and services. Reconnaissance is also known as information gathering, and it precedes a network attack in most cases. For example, reconnaissance traffic signatures may include the following:
  - Ping sweep attempts
  - Port scan attempts
  - Domain Name System (DNS) query attempts
- **Unauthorized access:** Traffic may contain signs of someone attempting to gain unauthorized access, unauthorized data retrieval, system access or privilege escalation, etc. An attacker who does not have privileges to access an organization's network usually

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

https://t.me/learningnets

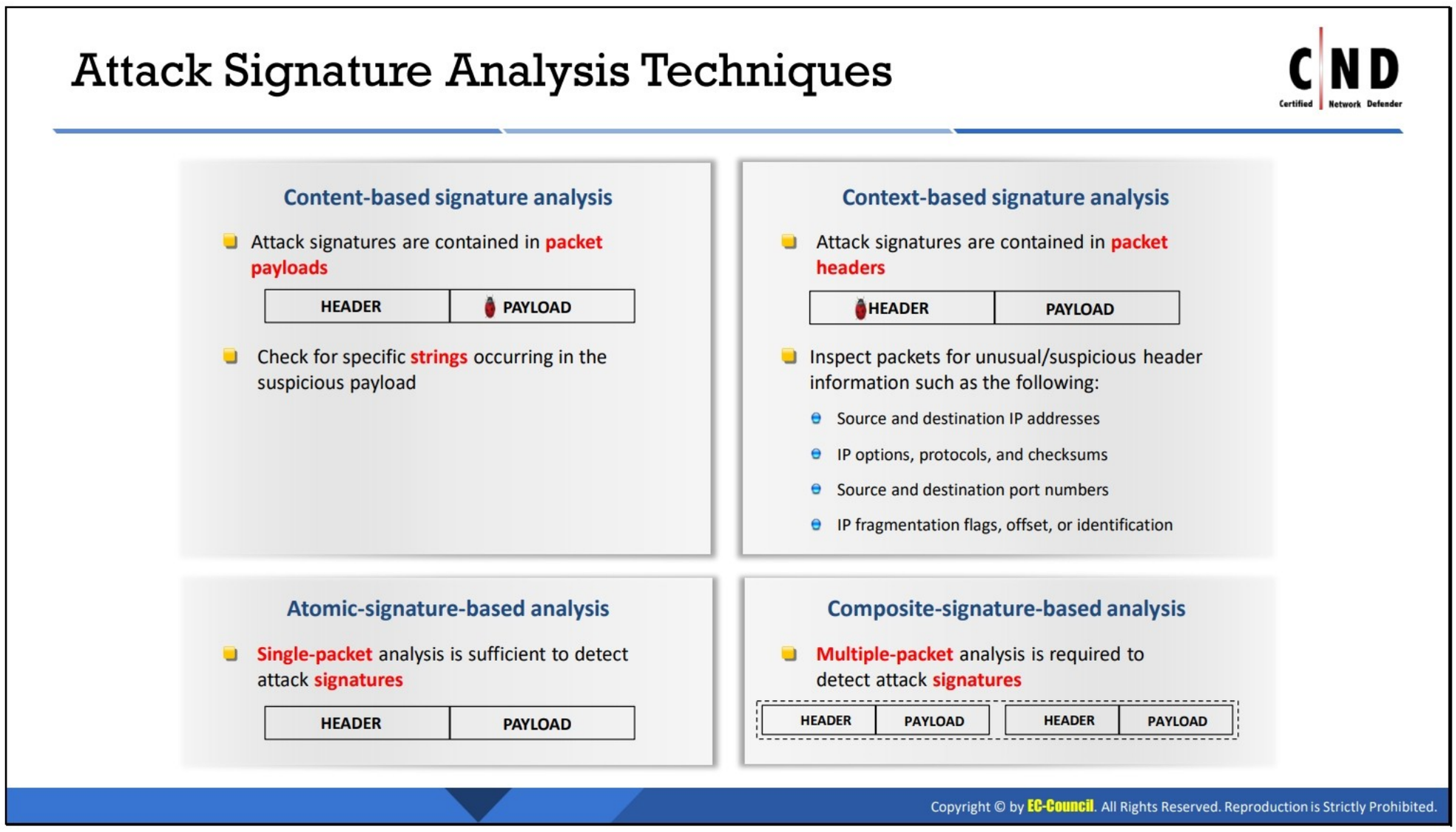
generates this type of traffic with the intention of capturing sensitive data. For example, unauthorized access traffic signatures may include the following:

- Password cracking attempts
- Sniffing attempts
- Brute-force attempts

- **Denial of service (DoS):** This type of traffic may contain a large number of requests from a single source or multiple sources, which are sent as an attempt to perform a DoS attack. This type of attack is performed to disrupt the service of the target organization. For example, DoS traffic signatures may include the following:
  - Ping of death attempts
  - SYN flood attempts

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

https://t.me/learningnets



Attack Signature Analysis Techniques

Attack signature analysis techniques are classified into four different categories as follows.

- **Content-based signature:** Content-based signatures are detected by analyzing the data in the payload and matching a text string to a specific set of characters. If undetected, these signatures can open backdoors in a system, providing administrative controls to an outsider.
- **Context-based signature:** Packets are usually altered using the header information. Suspicious signatures in the header can include malicious data that can affect the following:
  - Source and destination IP addresses
  - Source and destination port numbers
  - IP options
  - IP protocols
  - IP, TCP, and UDP checksums
- **Atomic signature:** To detect an atomic signature, network defender need to analyze a single packet to determine whether the signature includes malicious patterns. Network defenders do not require any knowledge of past or future activities to detect these signature patterns.
- **Composite signature:** In contrast to atomic signatures, network defenders need to analyze a series of packets over a long period of time to detect composite attack signatures. Detecting these attack patterns is exceedingly difficult. ICMP flooding is an example of an attack performed using composite signatures. In this attack, multiple ICMP packets are sent to a single host so that the server remains busy responding to the requests.

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

https://t.me/learningnets

Attacker signatures may be in either the header or payload of the packet.

Unusual/Suspicious Information in the Header

The attacker can alter the packet header information to bypass the filter and enter the network. To detect packets with malicious header formats, network defenders should understand the header fields they can modify. Header fields include suspicious signatures such as the following:

- Source and destination IP addresses
- Source and destination port numbers
- IP options, protocol, and checksums
- IP fragmentation flags, offset, or identification

Network defenders should also understand the various attack signatures that may exist in the header information. This helps them take remediation actions against suspicious packets.

Although an illegal header value is certainly a fundamental component of these signatures, network defenders should also understand that valid headers can have suspicious header values. For example, suspicious connections to port numbers may provide a quick method to identify possible trojan activity. Unfortunately, normal traffic may also use these odd port numbers. A detailed signature includes other traffic characteristics and is needed to determine the true nature of this traffic. Suspicious but legal values such as a port number are best used in combination with other values.

Suspicious Data in the Payload

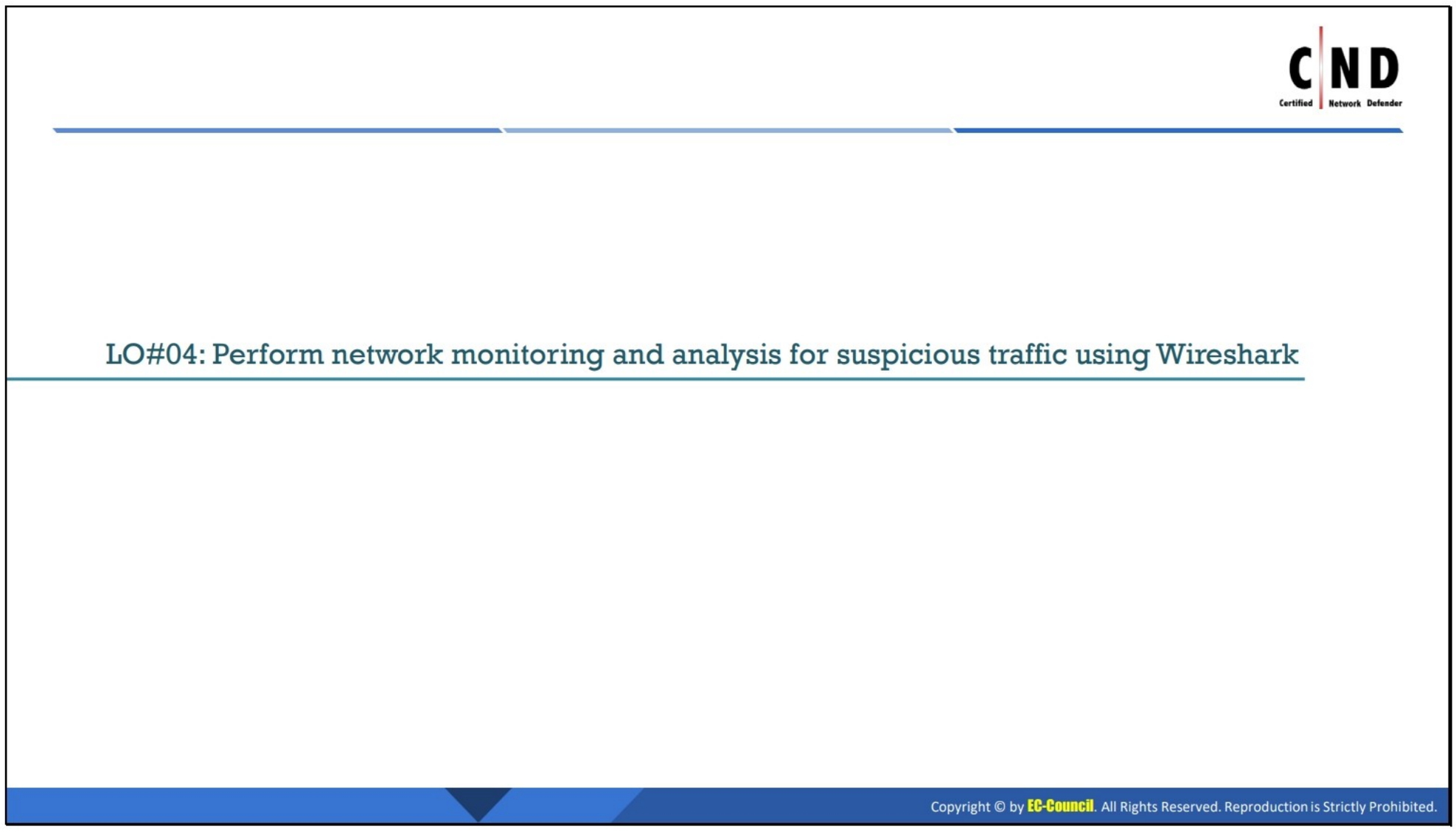
Network defenders should also understand the possible attack signatures that may exist in the payload data. They should check for specific strings occurring in the payload of each packet before allowing it through the network.

Network defenders need to examine the packet payloads within TCP and UDP to identify suspicious payload values. They should understand that protocols such as DNS are contained within TCP or UDP. Decoding a packet's IP header information gives a clear indication of whether its payload contains TCP, UDP, or another protocol. If the payload is in TCP, network defenders need to process some of the TCP header information within the IP payload before accessing the TCP payload. DNS data are contained within UDP and TCP payloads.

An example is a DNS buffer overflow attempt contained in the payload of a query. By parsing the DNS fields and checking the length of each, network defenders can identify an attempt to perform a buffer overflow using a DNS field. Another method is to look for any exploitation of shellcode sequences in the payload.

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

https://t.me/learningnets

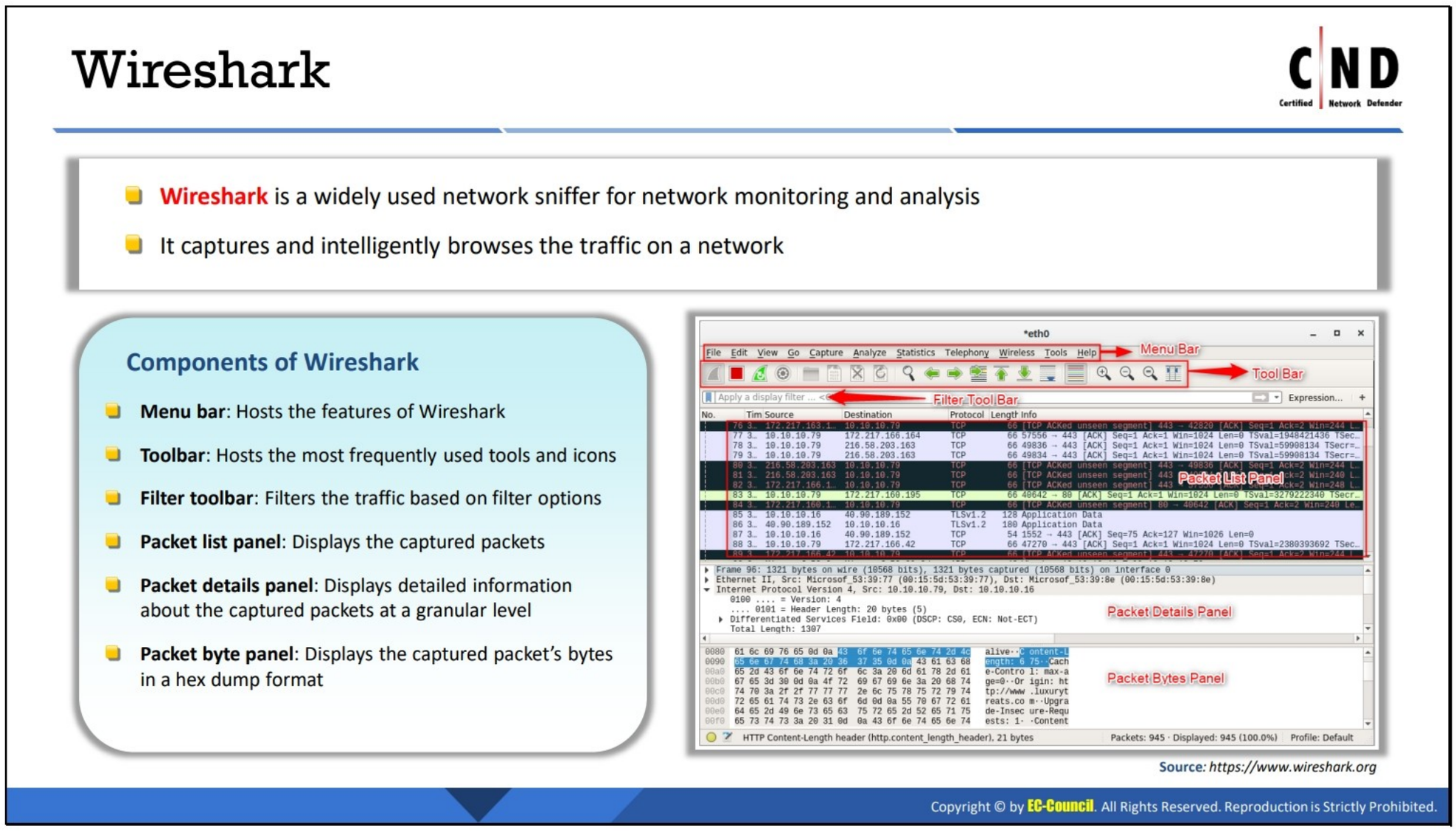


LO#04: Perform Network Monitoring and Analysis for Suspicious Traffic using Wireshark

The objective of this section is to explain how to use Wireshark to perform network monitoring and analysis. It describes how to use Wireshark for monitoring and analyzing File Transfer Protocol (FTP) traffic, Telnet traffic, Hypertext Transfer Protocol (HTTP) traffic, passive OS fingerprinting attempts, ping sweep attempts, ARP sweep/ARP scan attempts, TCP half open/stealth scan attempts, SYN/FIN Distributed DoS (DDoS) attempts, UDP scan attempts, password cracking attempts, sniffing attempts, MAC flooding attempts, ARP poisoning attempts, Structured Query Language (SQL) injection attempts, etc.

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

https://t.me/learningnets



Wireshark

Wireshark is a packet sniffer that can be used for network troubleshooting to investigate security issues and to analyze and understand network protocols. It can exploit information passed in plain text.

- **Features**

  Wireshark has a rich feature set that includes the following:

  - Identify poor network performance due to high path latency.
  - Locate internetwork devices that drop packets.
  - Validate the optimal configuration of network hosts.
  - Analyze application functionality and dependencies.
  - Optimize application behavior for best performance.
  - Analyze network capacity before application launch.
  - Verify application security during launch, login, and data transfer.
  - Identify unusual network traffic indicating potentially compromised hosts.

- **Prerequisites for network packet capture**

  Setting up Wireshark to capture packets for the first time can be tricky. The following are a few common problems that are encountered while capturing packets with Wireshark for the first time:

  - Special privileges are required to start a live capture.

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

https://t.me/learningnets

- The correct network interface must be chosen to capture packet data from.
- Network packets should be captured at the correct location in the network to view the desired traffic.

- **Wireshark network analysis activities**

  Capturing live network data is one of the major features of Wireshark. The Wireshark capture engine enables network defenders to perform the following:

  - Capture from different types of network hardware such as Ethernet and 802.11.
  - Stop the capture based on different triggers such as the amount of captured data, elapsed time, or number of packets.
  - Simultaneously show decoded packets while capturing is in progress.
  - Filter packets to reduce the amount of data to be captured.
  - Save packets in multiple files during a long capture.
  - Simultaneously capture from multiple network interfaces.

- **First network packet capture using Wireshark**

  To capture packets using Wireshark, first install and launch the tool on the target network. Select the appropriate network interface to capture traffic from. The following are the steps to start capturing packets with Wireshark:

  1. Double-click on an interface in the main window.
  2. An overview of the available interfaces can be obtained using the Capture Interface dialog box.
  3. Start a capture from this dialog box using the Start button.
  4. A capture can be immediately started using the current settings by selecting **Capture → Start** or by clicking the first toolbar button.
  5. If the name of the capture interface is known, Wireshark can be launched from the command line through the following command: $ wireshark -i eth0 –k

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

https://t.me/learningnets

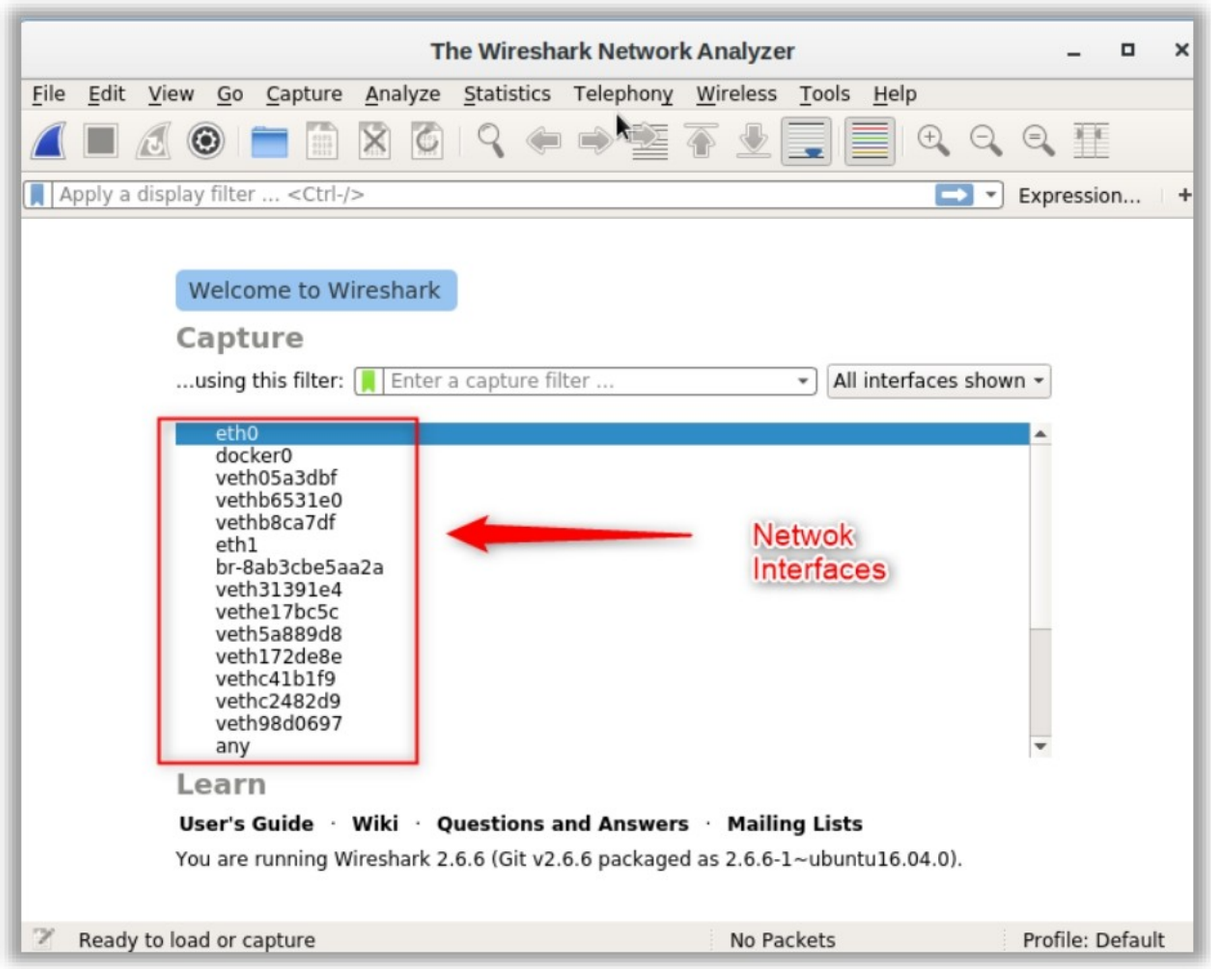


Figure 14.2: Wireshark Network Interfaces

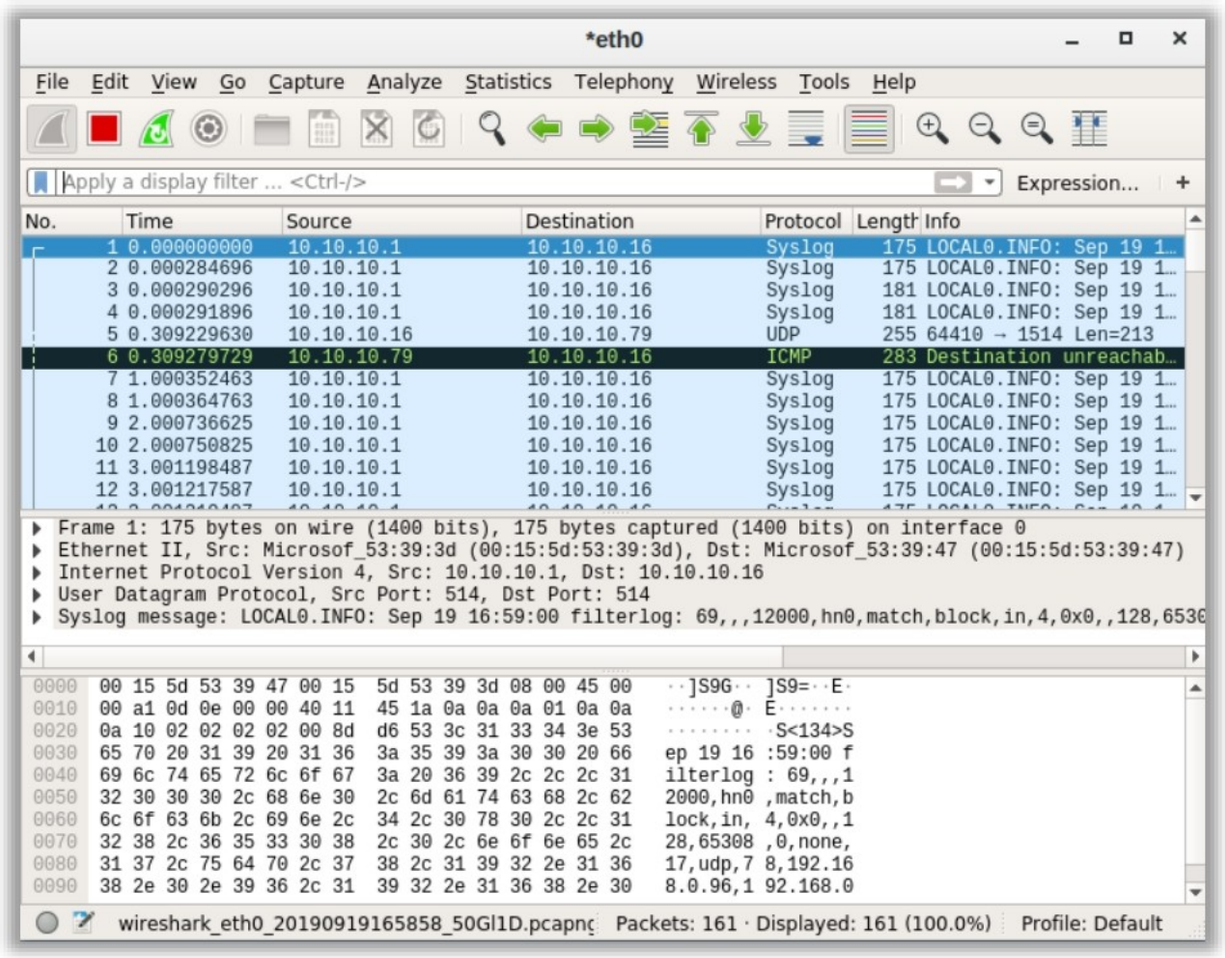


Figure 14.3: Capturing Traffic

- **Wireshark components**

The main menu of Wireshark contains the following items:

- **File:** This menu contains items to open and merge, capture files, save, print, import and export capture files in whole or in part, and quit the Wireshark application.
- **Edit:** This menu contains items to find a packet, time reference, and mark one or more packets. It handles configuration profiles and sets preferences.

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

https://t.me/learningnets

- **View:** This menu controls the display of the captured data, including the colorization of packets, font zoom, display of a packet in a separate window, and expanding and collapsing of the packet tree details.
  - **Colorize packet list:** This option allows network defenders to control whether Wireshark should colorize the packet list. Enabling colorization slows down the display of new packets while capturing and loading capture files.
  - **Coloring rules:** This option allows network defenders to color packets in the packet list pane according to the filter expressions of their choice. It can be very useful for spotting certain types of packets.
  - **Colorize conversation:** This menu item brings up a submenu that allows the color of the packets to be changed in the packet list pane based on the addresses of the currently selected packet. This makes it easy to distinguish packets belonging to different conversations.
- **Go:** This menu contains options to navigate to a specific packet including a previous packet, the next packet, the corresponding packet, the first packet, and the last packet.
- **Capture:** This menu allows the network defenders to start, stop, and restart capture and to edit capture filters.
  - **Capture filters:** This option allows network defenders to create and edit capture filters. Filters can be named and saved for future use.
- **Analyze:** This menu contains items to manipulate, display and apply filters, enable or disable the dissection of protocols, configure user-specified decodes, and follow a different stream including TCP, UDP, and Secure Sockets Layer (SSL).
  - **Follow TCP stream:** This option displays all the captured TCP segments that are on the same TCP connection as a selected packet.
  - **Follow UDP stream:** This option displays all the captured UDP segments that are on the same UDP connection as a selected packet.
  - **Follow SSL stream:** This option displays all the captured SSL segments that are on the same SSL connection as a selected packet.
- **Statistics:** This menu contains options to display various statistic windows, including a summary of the packets that have been captured, display protocol hierarchy statistics, IO graphs, and flow graphs.
- **Telephony:** This menu contains options to display various telephony-related statistic windows including a media analysis, flow diagrams, and display protocol hierarchy statistics.
- **Wireless:** This menu shows Bluetooth and IEEE 802.11 wireless statistics.
- **Tools:** This menu contains various tools available in Wireshark including the creation of firewall access control list (ACL) rules and use of the Lua interpreter.

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

https://t.me/learningnets

- **Firewall ACL rules:** This tool can be used create command-line ACL rules for many different firewall products, including Cisco IOS, Linux Netfilter, OpenBSD and Windows Firewall. Rules for MAC addresses, IPv4 addresses, TCP and UDP ports, and IPv4+port combinations are supported. It is assumed that the rules will be applied to an outside interface.
- **Lua:** This tool includes options that allow network defenders to work with the built-in Lua interpreter of Wireshark. Wireshark uses Lua to write protocol dissectors.

- **Help:** This menu contains items to help the user, including access to basic help manual pages for the various command-line tools, online access to some webpages, and the About Wireshark dialog.
- **Main toolbar:** The main toolbar provides quick access to frequently used items from the menu. This toolbar cannot be customized by the user. If the space on the screen is needed to show more packet data, then the toolbar can be hidden using the View menu. As in the menu, only the items that can be used in the current program state will be available. The others will be greyed out.
- **Filter toolbar:** The filter toolbar allows network defenders to quickly edit and apply display filters.
- **Packet list panel:** This panel displays a list of packets in the current capture file. It colors the packets based on the protocol. Each line in the packet list corresponds to one packet in the capture file. If a line in this pane is selected, more details will be displayed in the Packet Details and Packet Bytes panes.

  The default columns show the following:

  - **No:** This column shows the number of the packets in the capture file. This number does not change, even if a display filter is used.
  - **Time**: This column shows the timestamp of the packet. The presentation format of this timestamp can be changed.
  - **Source:** This column shows the source address of the packet.
  - **Destination**: This column shows the destination address of the packet.
  - **Protocol**: This column shows the protocol name in the abbreviated form.
  - **Info**: This column shows additional information about the packet content.
- **Packet details panel:** This panel displays the details of the selected packet. It includes the different protocols making up the layers of data in this packet. The protocols and fields of the packet are displayed using a tree, which can be expanded and collapsed. Layers include the frame, Ethernet, IP, TCP, UDP, ICMP, and application protocols such as HTTP.
- **Packet bytes panel:** This panel displays the packet bytes in a hex dump and American Standard Code for Information Interchange (ASCII) encodings. For a hex dump, the left side shows the offset in the packet data, and the middle of the packet data is shown in a

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

https://t.me/learningnets

hexadecimal representation. On the right, the corresponding ASCII characters are displayed.

- **Status bar:** The status bar displays informational messages. In general, the left side shows context-related information, the middle part shows the current number of packets, and the right side shows the selected configuration profile. The user can drag the handles between the text areas to change the size.

- **Wireshark capture and display filters**

  Wireshark provides the opportunity to use different types of filters to sort network traffic. The tool helps confine the search and shows only the desired traffic. By default, Wireshark provides capture filters and display filters to filter the traffic.

  network defenders can define filters and give them labels for later use. This saves time in recreating and retyping complex filters that are used often.

  Display filters

  Display filters are used on captured packets. These are useful when filters need not be applied before starting packet capture. The user can capture all the packets traversing the network and then sort the captured items using display filters.

  Display filters are used while displaying packets. They allow network defenders to concentrate on the packets they are most interested in while hiding uninteresting ones. They allow network defenders to select packets based on the following options:

  - Protocol
  - Presence of a field
  - Value of a field
  - Comparison between fields

  To define a new filter or edit an existing one, select **Capture → Capture Filters or Analyze → Display Filters**. A dialog box will open with options to define new and edit existing filters.

  The mechanisms for defining and saving capture filters and display filters are almost identical. Network defenders can use the “+” (plus) button to add new filters and the “-” (minus) button to remove any unwanted filters. The copy button is used to copy a selected filter. network defenders can edit existing filters by double-clicking on the filter. After creating a new filter or editing an existing filter, click OK to save the changes.

  Capture filters

  Capture filters are applied before starting a capture of traffic on the selected network interface. Capture filters cannot be applied directly on captured traffic. A capture filter should only be applied when the network defenders knows what they are looking for. network defenders should be aware of all the capture filters available to quickly find network anomalies.

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

https://t.me/learningnets

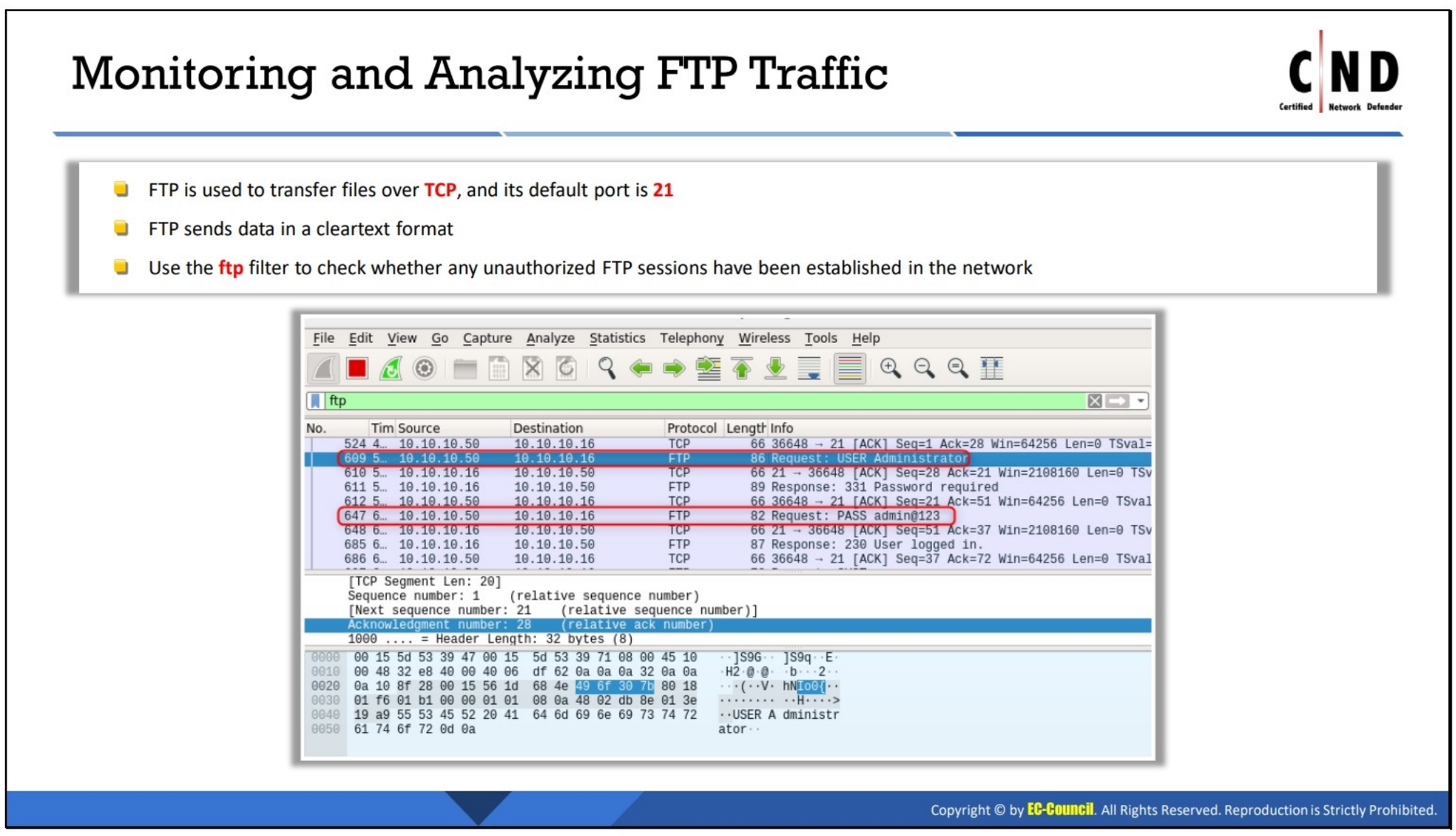
Wireshark uses the libpcap filter language for capture filters. A capture filter takes the form of a series of primitive expressions connected by conjunctions (and/or) and is optionally preceded by "not." The syntax of a capture filter is as follows: **[not] primitive [and|or [not] primitive ...]**

For example, the following expression applies a capture filter for Telnet that captures traffic to and from a particular host: **tcp port 23 and host 10.0.0.5**

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

https://t.me/learningnets

Technet24



Monitoring and Analyzing FTP Traffic

FTP offers neither a secure network environment nor secure user authentication. Individuals do not need authentication to access an FTP server in a network. This provides an easy method for attackers to enter the network and access resources. FTP does not provide encryption in the data transfer process, and the data transfer between the sender and receiver is in plain text. Consequently, critical information such as usernames and passwords is exposed to attackers. The implementation of FTP in an organization's network leaves the data accessible to external sources. Deploying FTP in a network can lead to types of attacks such as FTP bounce, FTP brute force, and packet sniffing attacks.

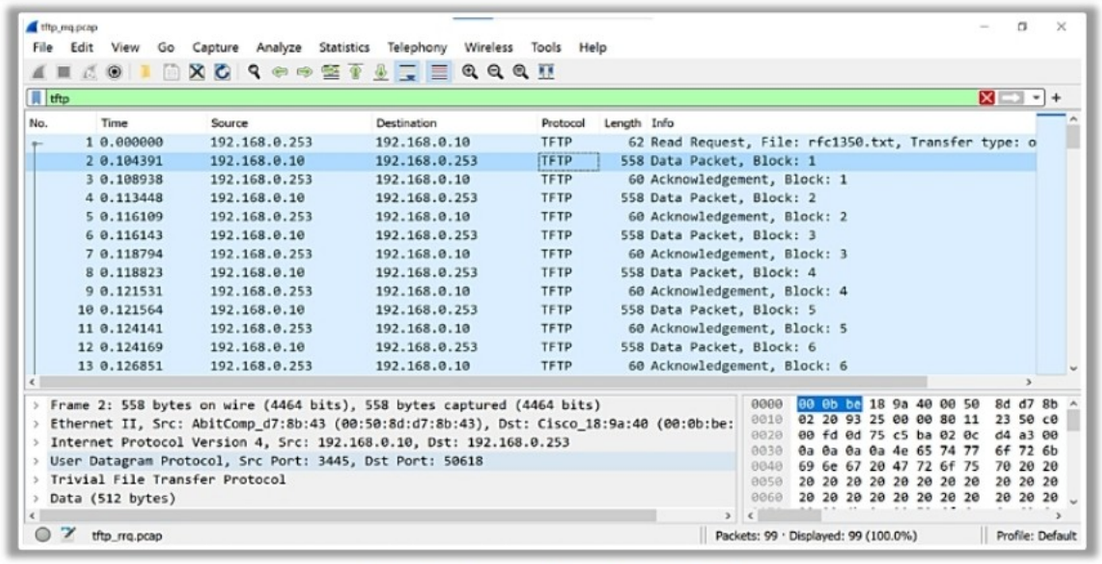
Wireshark provides complete information about the FTP traffic on a network for monitoring. Applying an FTP filter helps detect unauthorized sessions running on the server. Apart from monitoring the traffic on the FTP server, the existing file contents and file sizes in the server should be monitored.

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

https://t.me/learningnets

Monitoring and Analyzing TFTP (Trivial File Transfer Protocol) Traffic

- Monitor TFTP traffic using Wireshark to detect any unauthorized or **rogue TFTP** servers or clients within your network
- Unauthorized TFTP activity may indicate a **security breach** or misconfigured devices
- The default port for TFTP is **69**



Monitoring and Analyzing TFTP

Source: *https://www.wireshark.org*

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

Monitoring and Analyzing TFTP Traffic

Trivial File Transfer Protocol (TFTP) is a plaintext file transfer protocol used to send and receive data without authentication. Its primary applications include firmware upgrades and related tasks, especially when the client requesting the data has limited processing capabilities. Although efficient and easy to use, TFTP is quite unsafe due to its lack of encryption and absence of authentication.

To monitor TFTP traffic, use Wireshark for detecting any unauthorized or rogue TFTP servers or clients within the network. Such unauthorized TFTP activity might indicate a security breach or misconfigured devices. TFTP protocols cannot be captured directly. However, you can filter on TFTP if you know the UDP port used, since TFTP uses UDP as its transport protocol. The default UDP port for TFTP traffic is 69.

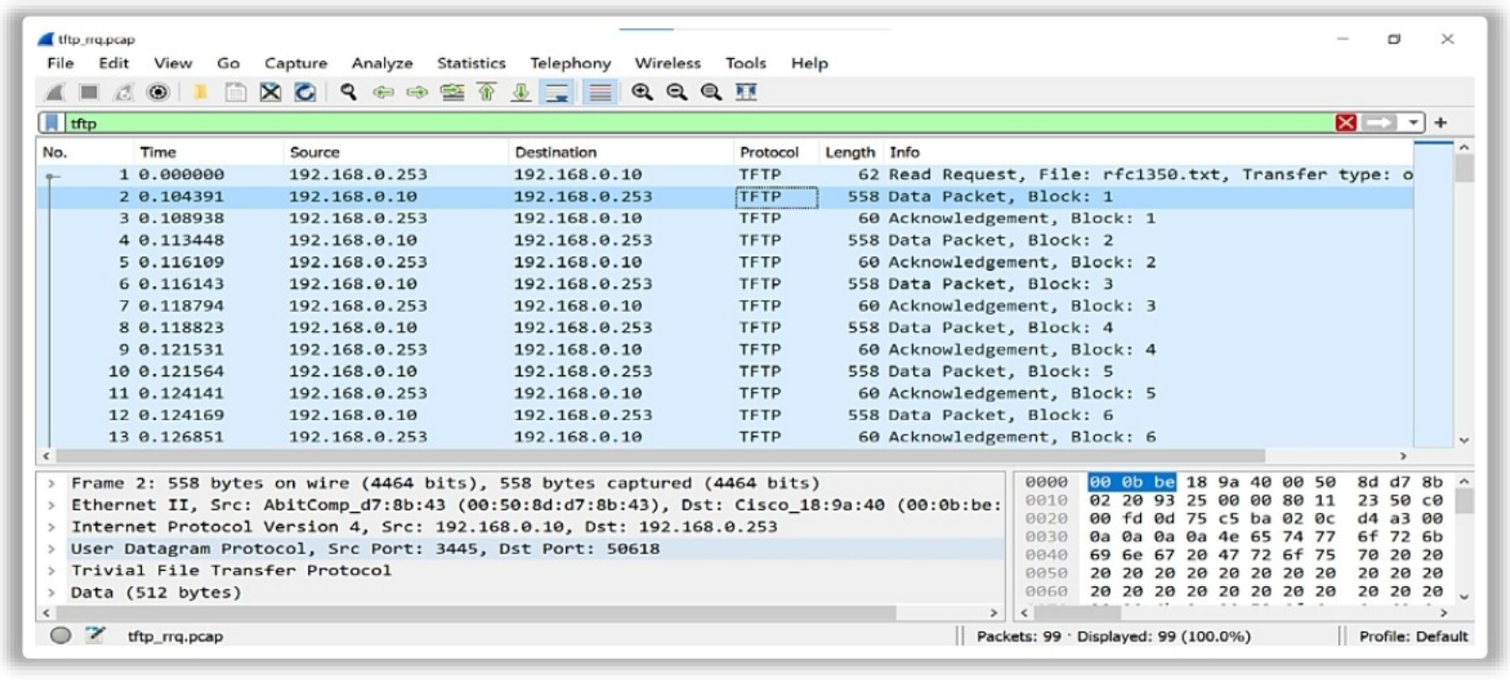


Figure 14.4: Identifying TFTP Traffic

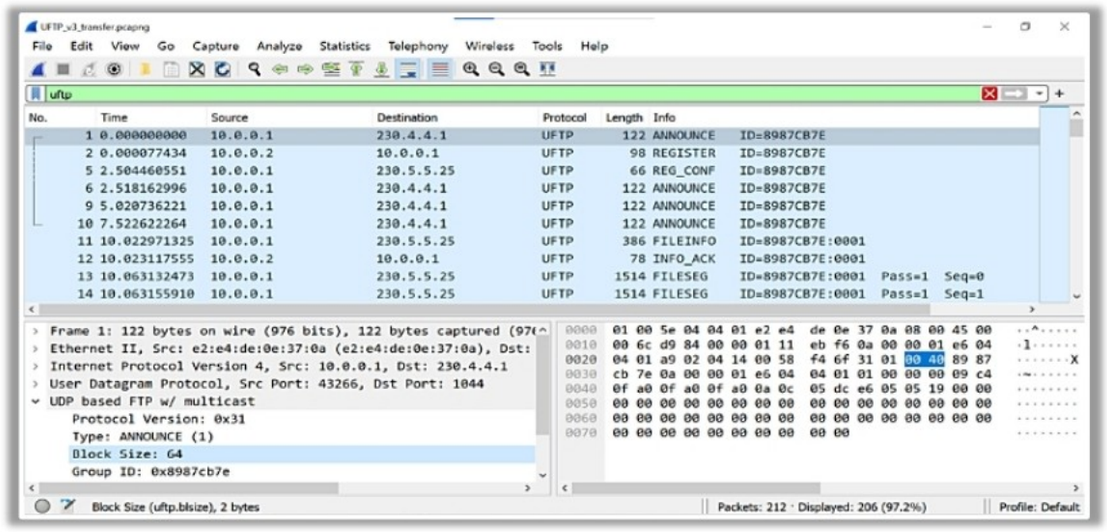
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

Technet24

Monitoring and Analyzing UFTP (Unicast Fast Transfer Protocol) Traffic

- Unicast fast transfer protocol (UFTP) is a **high-performance** file transfer protocol commonly used for fast file transfers for distributing large files across a network
- Monitoring and analyzing UFTP traffic ensures the reliability and security of your network. Default port for UFTP traffic is **1044**
- Use the uftp , uftp4 or uftp5 filter to check whether any **unauthorized UFTP sessions** have been established in the network



Monitoring and Analyzing UFTP

Source: *https://www.wireshark.org*

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

Monitoring and Analyzing UFTP Traffic

Unicast Fast Transfer Protocol (UFTP), an encrypted multicast file transfer program, securely transfers files to multiple receivers simultaneously. It is particularly useful for distributing large files over a satellite link (with two-way communication) to a large number of receivers.

Monitoring and analyzing UFTP traffic is essential for identifying potential security vulnerabilities or suspicious activities in the network. This includes detecting unauthorized access attempts, unusual transfer volumes, or atypical file types being transferred. By examining the content and behavior of UFTP transfers, you can use this information to identify security events and policy violations, enabling you to take appropriate action.

In Wireshark, you cannot directly filter UFTP protocols while capturing. You can capture only the UFTP traffic over the default port 1044, since UFTP uses UDP as its transport protocol. To find a complete list of UFTP display filter fields, use filters such as uftp, uftp4, or uftp5. These fields are detailed in the display filter reference: uftp, uftp4, uftp5.

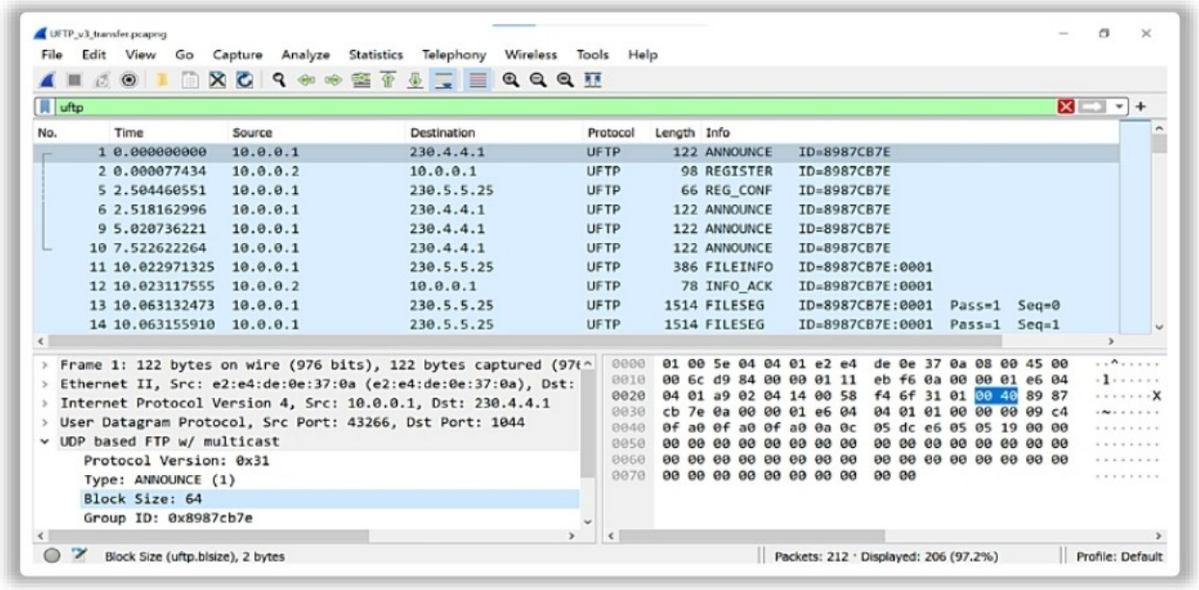
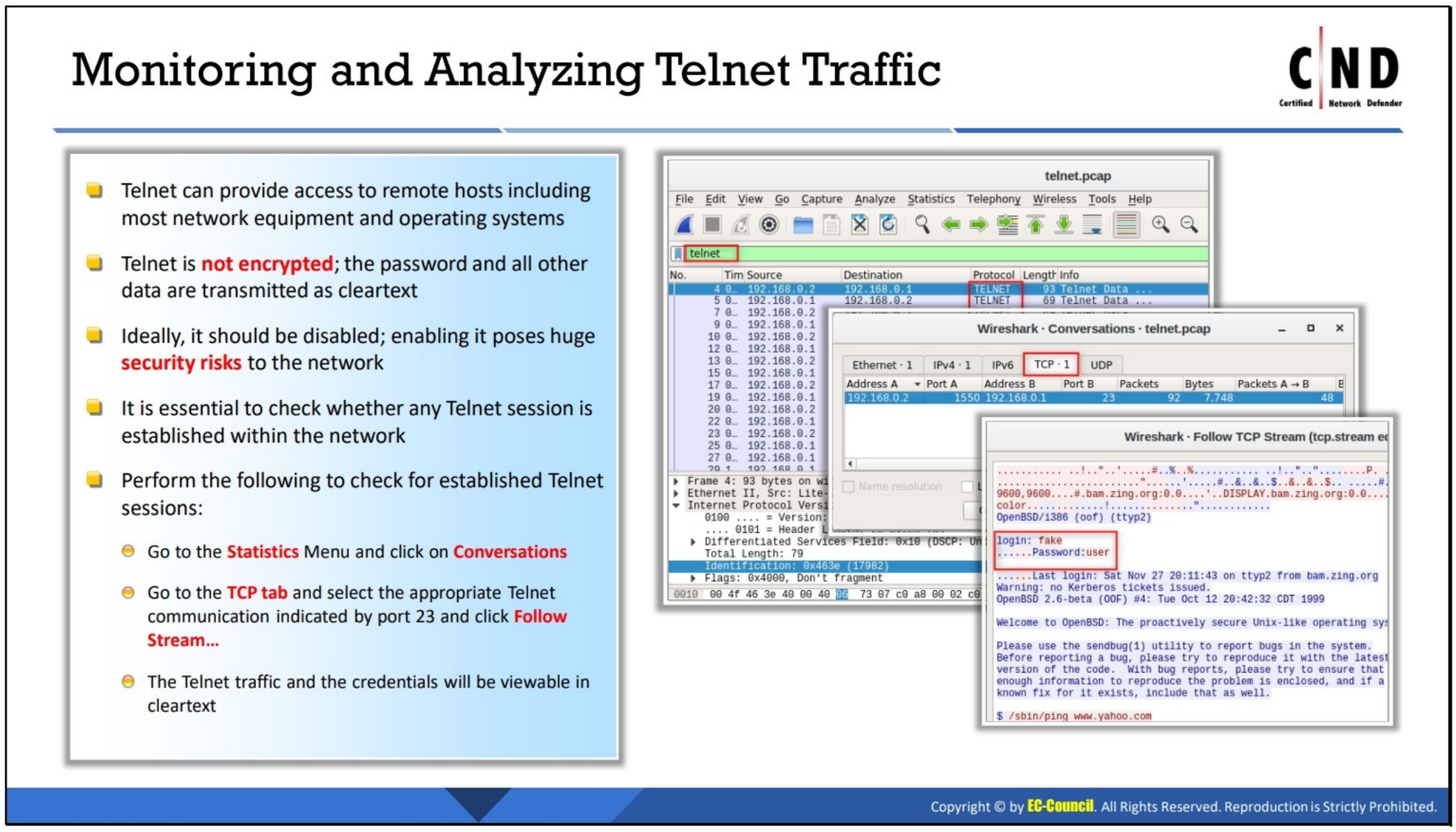


Figure 14.5: Identifying UFTP traffic

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

https://t.me/learningnets



Monitoring and Analyzing Telnet Traffic

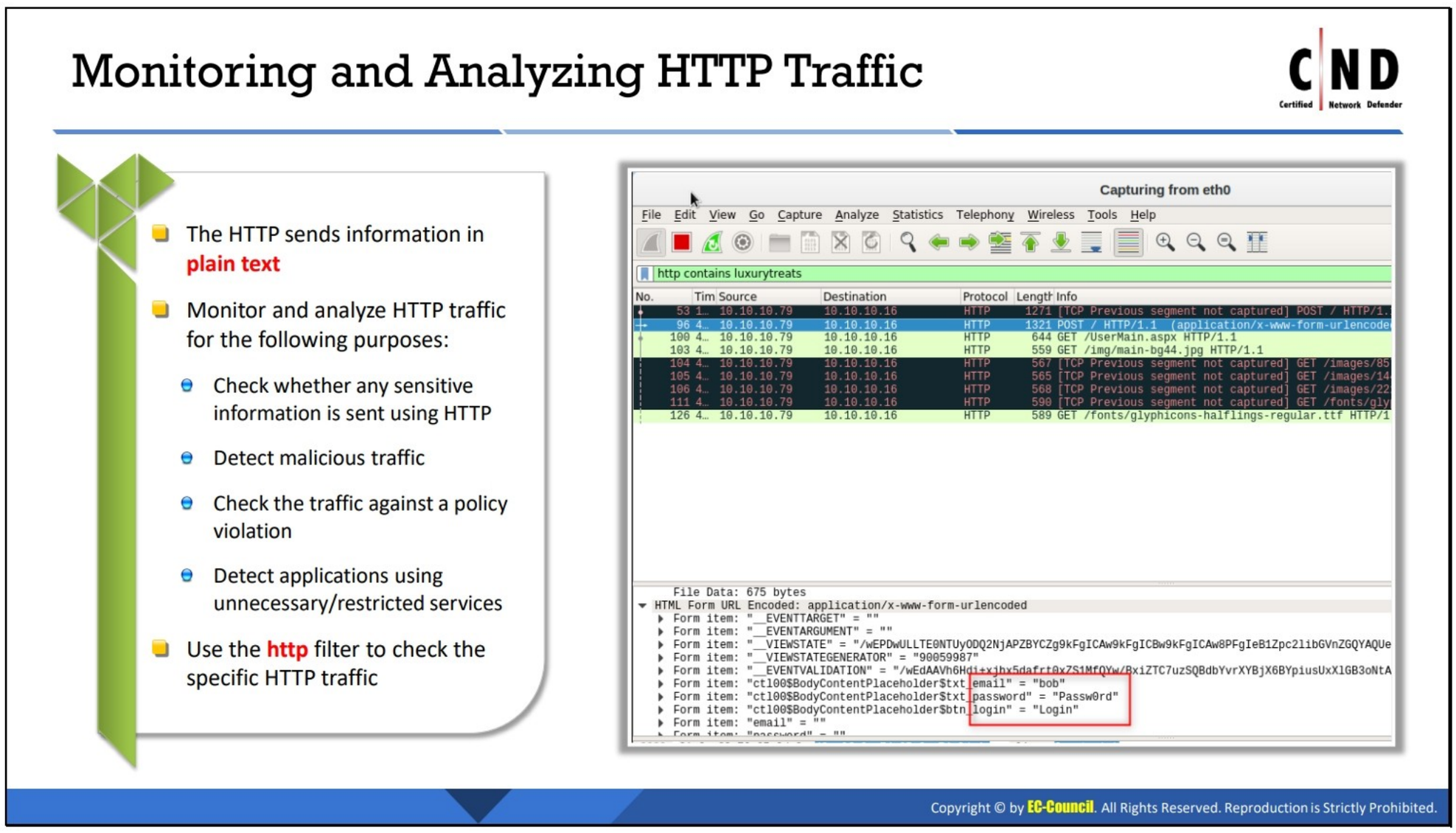
The Telnet protocol works on a client–server model. It provides access to remote network equipment and OSes. The data transferred through Telnet is not encrypted, making it easy for intruders to eavesdrop. If a person has access to a network device with Telnet configured, they can gain access to the network and user account information. Generally, Telnet should be disabled in an organization.

Telnet is a session-oriented protocol, which implies that the connection must be open for the entire session. Attackers can use Telnet open sessions to perform a network security breach. Therefore, network defenders should monitor Telnet sessions (if any) running on their network. Timely monitoring of Telnet sessions through Wireshark can greatly minimize the risk for network intrusion.

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

https://t.me/learningnets

Technet24

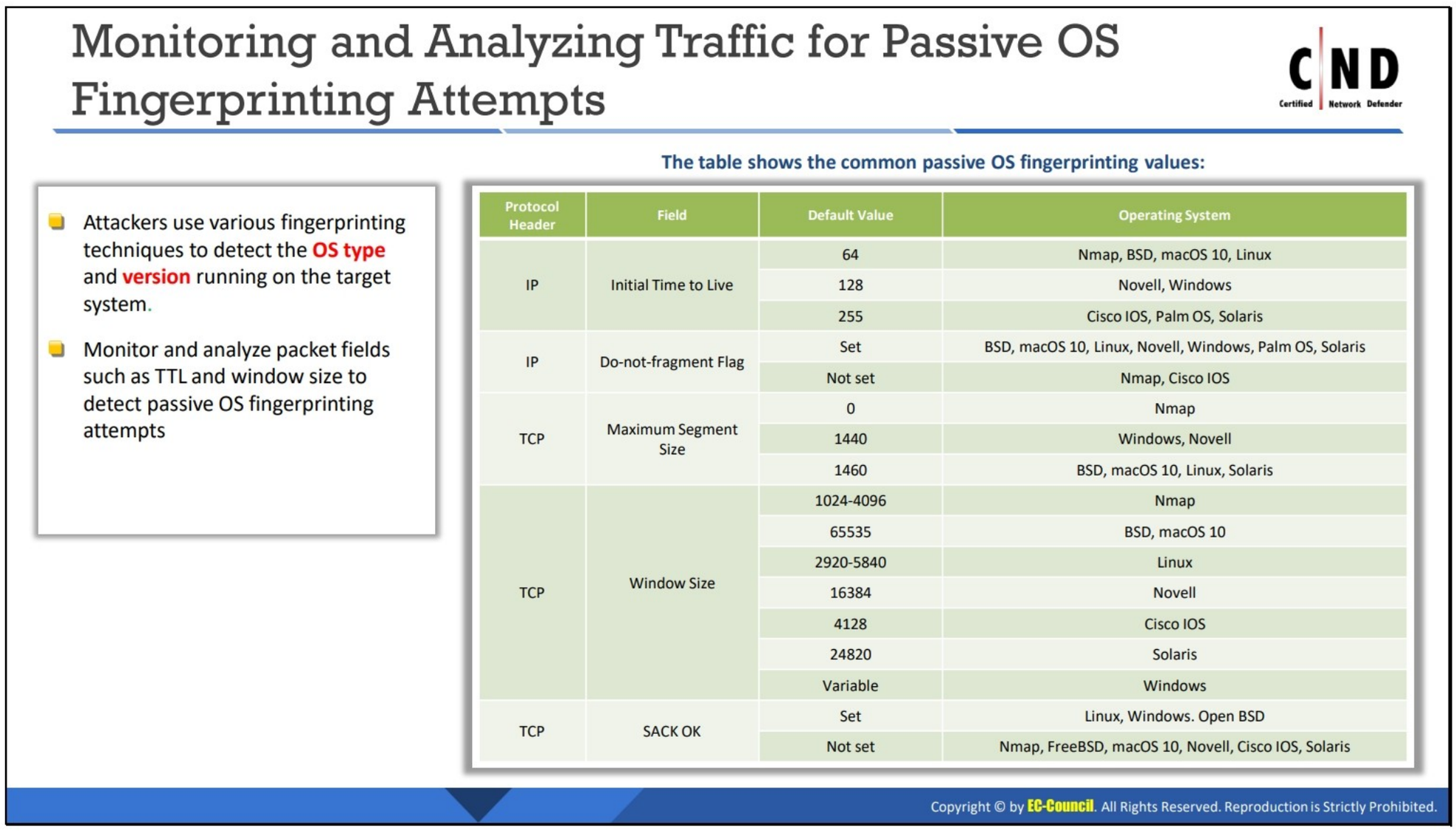


Monitoring and Analyzing HTTP Traffic

Applications implementing HTTP send data in cleartext. Implementing HTTP can pose security risks to the organization as sensitive information such as usernames and passwords are sent over as HTTP requests. The attacker can easily sniff the traffic and steal sensitive information for malicious use. Therefore, network defenders must ensure that their HTTP traffic is sent over an encrypted protocol such as HTTP Secure (HTTPS). Simultaneously, they should monitor applications and ensure that they do not send data over HTTP. Monitoring the HTTP traffic also helps detect the volume of HTTP traffic in the network.

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

https://t.me/learningnets



Protocol Header	Field	Default Value	Operating System
IP	Initial Time to Live	64	Nmap, BSD, macOS 10, Linux
		128	Novell, Windows
		255	Cisco IOS, Palm OS, Solaris
IP	Do-not-fragment Flag	Set	BSD, macOS 10, Linux, Novell, Windows, Palm OS, Solaris
		Not set	Nmap, Cisco IOS
TCP	Maximum Segment Size	0	Nmap
		1440	Windows, Novell
		1460	BSD, macOS 10, Linux, Solaris
TCP	Window Size	1024-4096	Nmap
		65535	BSD, macOS 10
		2920-5840	Linux
		16384	Novell
		4128	Cisco IOS
		24820	Solaris
		Variable	Windows
TCP	SACK OK	Set	Linux, Windows. Open BSD
		Not set	Nmap, FreeBSD, macOS 10, Novell, Cisco IOS, Solaris

Monitoring and Analyzing Traffic for Passive OS Fingerprinting Attempts

In passive OS fingerprinting, the attacker does not send any packets in the traffic; rather, they sniff TCP/IP ports. The target OS is detected based on the verification of various IP header fields. The IP header consists of fields such as the initial time to live (TTL), do-not-fragment flag, maximum segment size, window size, and selective ACK (SACK) OK. The default values of these fields can help network defenders detect fingerprinting attempts. These fields must be inspected to detect any OS fingerprinting attempts in the network. However, the default values for these fields may vary when the packet traverses two routers. Furthermore, it is very difficult to detect a passive fingerprinting attempt. Firewalls or other security devices cannot detect passive OS fingerprinting either. Therefore, it has become essential to detect these attempts manually with the help of packet sniffing tools.

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

https://t.me/learningnets

Technet24

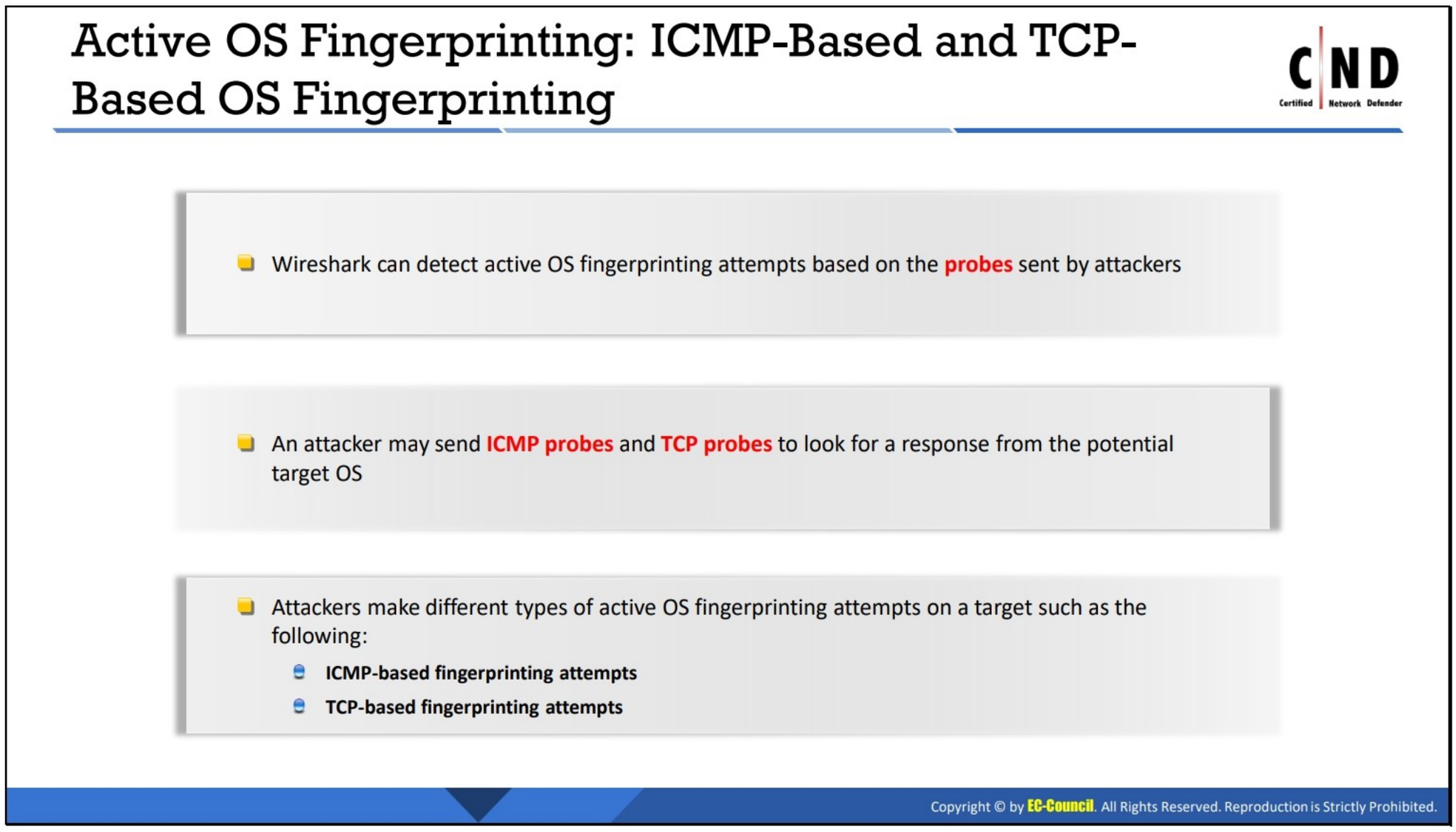
Table 14.1 lists the possible default values of IP header fields for different OSes. This table can help compare and identify OS fingerprinting attempts.

Protocol Header	Field	Default Value	Operating System
IP	Initial Time to Live	64	Nmap, BSD, macOS 10, Linux
		128	Novell, Windows
		255	Cisco IOS, Palm OS, Solaris
IP	Do-not-fragment Flag	Set	BSD, macOS 10, Linux, Novell, Windows, Palm OS, Solaris
		Not set	Nmap, Cisco IOS
TCP	Maximum Segment Size	0	Nmap
		1440	Windows, Novell
		1460	BSD, macOS 10, Linux, Solaris
TCP	Window Size	1024-4096	Nmap
		65535	BSD, macOS 10
		2920-5840	Linux
		16384	Novell
		4128	Cisco IOS
		24820	Solaris
		Variable	Windows
TCP	SACK OK	Set	Linux, Windows. Open BSD
		Not set	Nmap, FreeBSD, macOS 10, Novell, Cisco IOS, Solaris

Table 14.1: Default Values of IP Header for Different OSes

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

https://t.me/learningnets



Active OS Fingerprinting: ICMP-Based and TCP-Based OS Fingerprinting

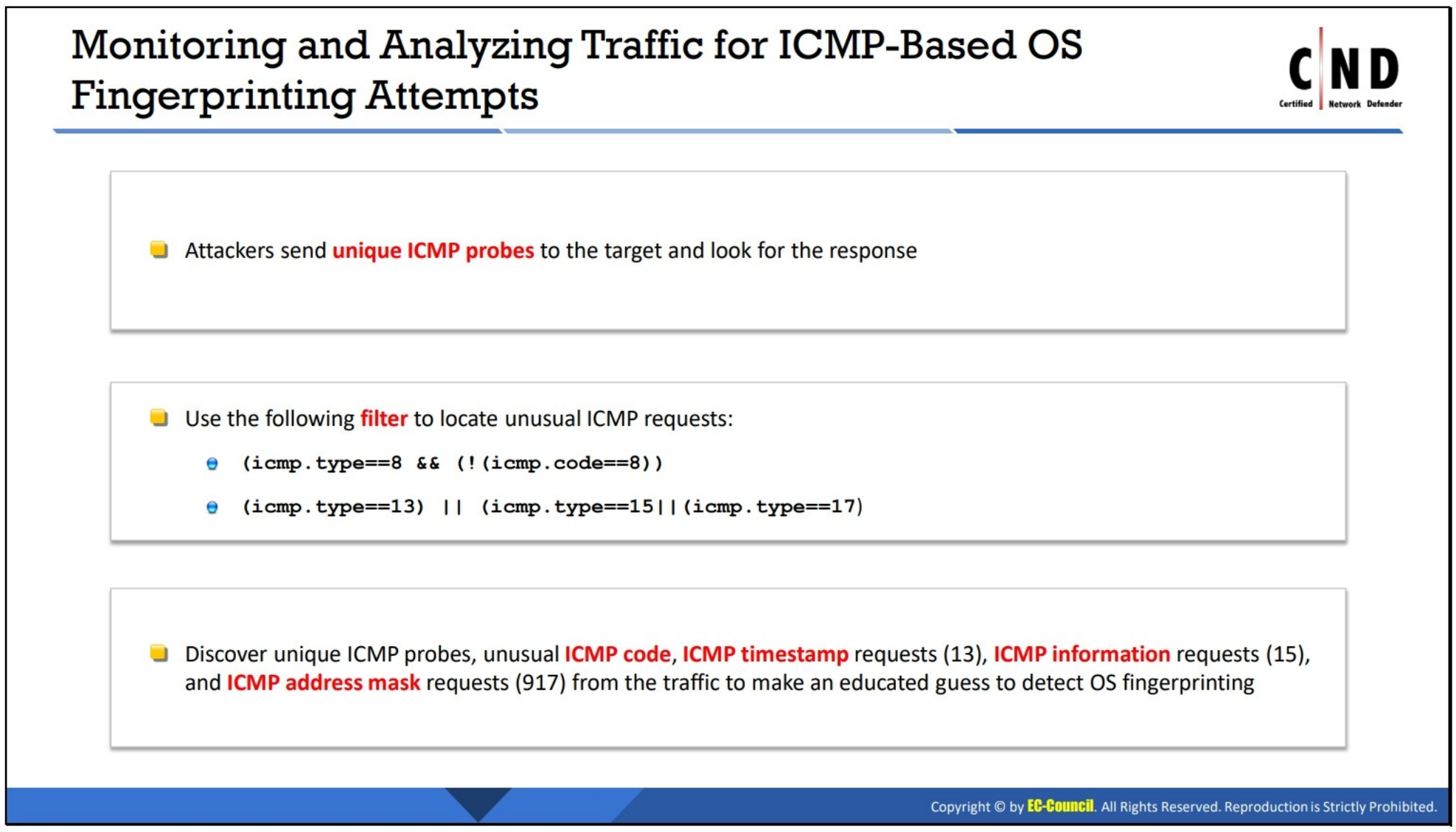
In active OS fingerprinting, an attacker sends packets to the target and waits for a reply. There are two ways to perform active OS fingerprinting: using either ICMP probes or TCP probes. The attacker analyzes the reply received from the target and makes an educated guess to determine the OS.

Active OS fingerprinting attempts are much easier to detect than passive OS fingerprinting attempts. Specific Wireshark filters can be used to filter out OS fingerprinting traffic.

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

https://t.me/learningnets

Technet24



Monitoring and Analyzing Traffic for ICMP-Based OS Fingerprinting Attempts

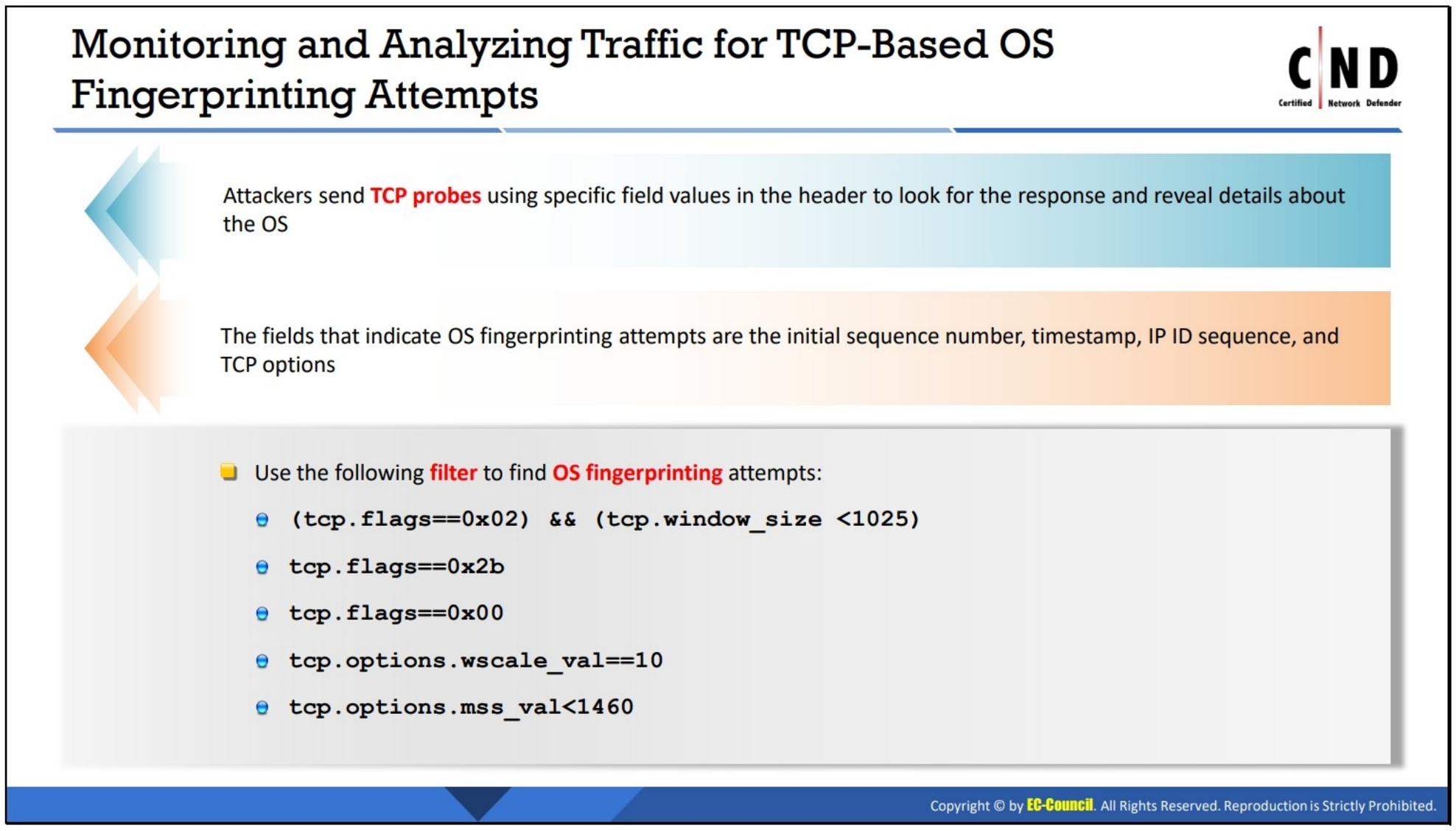
An attacker can use various tools to perform ICMP-based fingerprinting. These tools send a specific ICMP probe to the target. The tools manipulate the ICMP probe in different ways to detect the target OS:

- Some tools use unique ICMP probes.
- Some tools use ICMP echo requests with an unusual ICMP code.
- Some tools use ICMP timestamp requests (13), ICMP information requests (15), ICMP address mask requests (17), etc.

The network defenders can use various traffic filters on ICMP and check for these types of ICMP requests being received from the outside.

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

https://t.me/learningnets



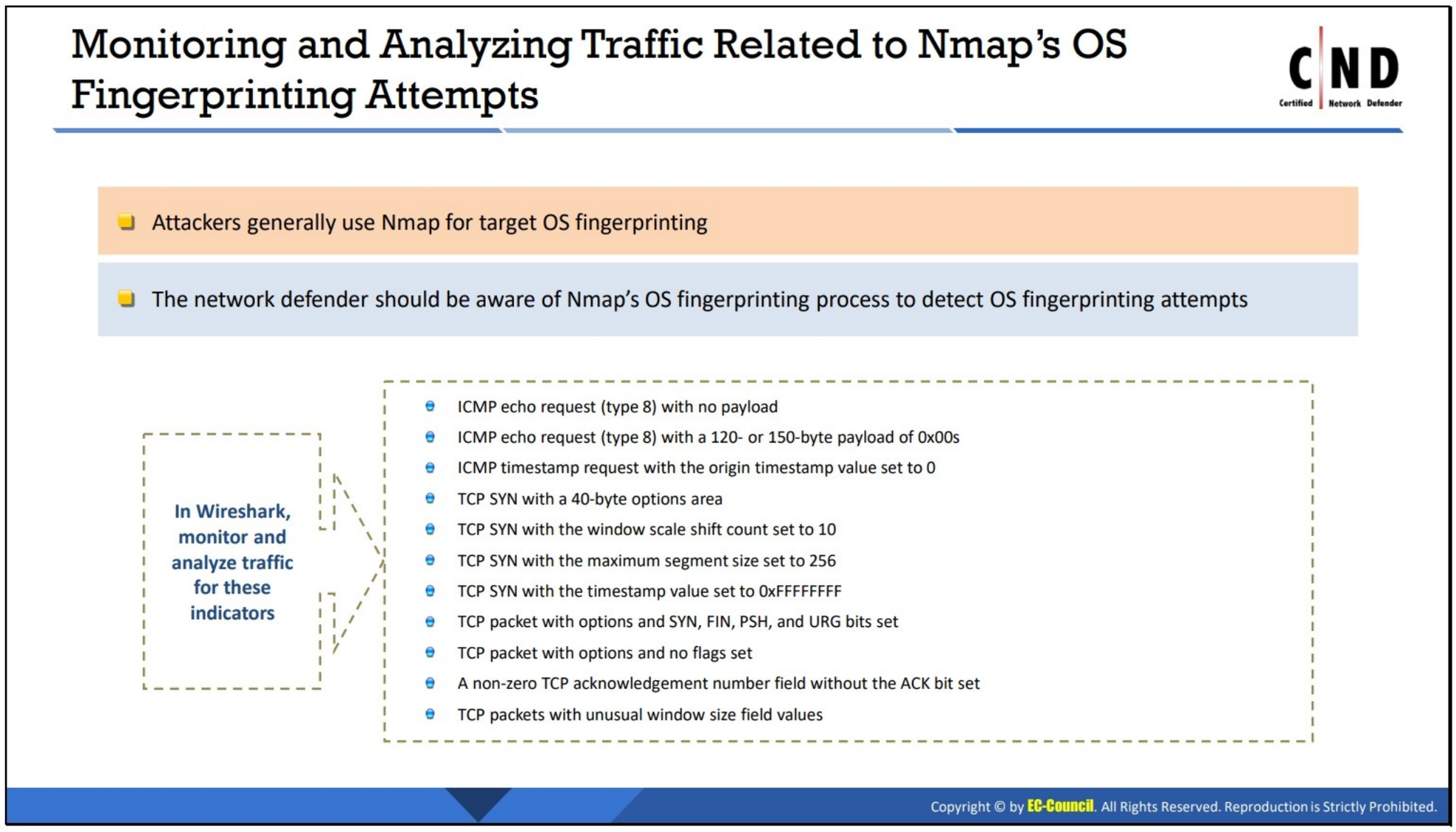
Monitoring and Analyzing Traffic for TCP-Based OS Fingerprinting Attempts

In TCP-based OS fingerprinting, an attacker sends TCP probe packets to the target and then waits for a response. Based on the response received from the target, the attacker makes an educated guess to determine the OS. To perform TCP-based fingerprinting, an attacker may use various tools such as Nmap and Queso. The attacker sends different types of TCP probes, and based on the response received, they can detect the OS running on the target.

- **FIN probe**: The attacker sends a FIN packet without an ACK or a SYN flag to an open port. Many broken OS implementations such as Microsoft Windows, Berkeley Software Design Inc. (BSDI), Cisco, Hewlett Packard Unix (HP/UX), Multiple Virtual Storage (MVS), and IRIX reply to a FIN probe with RESET.
- **BOGUS flag probe**: The attacker sends a SYN packet with an undefined TCP "flag" in the TCP header. The Linux OS versions prior to 2.0.35 respond to this packet with the flag set.
- **TCP initial window**: The attacker checks the size of the window field in the response.
- **TCP initial sequence number (ISN) sampling**: The attacker sends a connection request and then finds specific patterns in the ISNs of the response.
- **Interface pointer identifier (IPID) sampling**: The attacker checks the IPID value for each packet in the response. Most OSes increment a system-wide IPID value.
- **TCP timestamp**: The attacker checks the TCP timestamp option values in the response. It may be at frequencies of 2, 100, or 1000 Hz, and still others return 0.
- **Do-not-fragment bit:** Some OSes set a "do not fragment" bit in the response.
- **ACK value:** The attacker checks the ACK field in the response.

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

https://t.me/learningnets
Technet24



Monitoring and Analyzing Traffic Related to Nmap's OS Fingerprinting Attempts

Generally, attackers use Nmap to perform target OS fingerprinting. It is necessary to understand how Nmap is used to perform OS fingerprinting. Knowing the Nmap process for OS fingerprinting will help in identifying OS detection attempts made using Nmap.

Nmap Process for OS Fingerprinting

OS fingerprinting is one of the main features of Nmap. Nmap sends a series of TCP and UDP packets to remote hosts and examines every bit in the response. Nmap compares the results for all the fields tested with its database **nmap-os-db**. If the database finds a match for the tested fields, it gives the OS information. The database has a complete description of the OS, including the vendor name, OS generation, OS type, and device type. The Nmap process depends on the response from the devices. The responses received vary each time. If Windows OS receives the response as a TCP ACK frame, the response of Linux for the same frame will be different. With these minor differences in responses, Nmap builds detailed fingerprints for different OSes.

Nmap investigates the TCP/IP stack of systems by sending them eight different packets. Once the target machines receive the packets, they respond with either different TCP/IP stacks or the same TCP/IP stack.

This test allows Nmap to determine accurate information on the OS running on the target machine and its version. The tests sent by the machine running Nmap are as follows:

- **Tseq:** The machine sends a series of SYN packets to the targets to analyze their TCP sequence numbers.
- **T1:** A SYN packet with the options (WNMTE) is sent to an open TCP port.

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

https://t.me/learningnets

- **T2:** A NULL packet with the options (WNMTE) is sent to an open TCP port.
- **T3:** A SYN, FIN, PSH, and URG packet with the options (WNMTE) is sent to an open TCP port.
- **T4:** An ACK packet with the options (WNMTE) is sent to an open TCP port.
- **T5:** A SYN packet with the options (WNMTE) is sent to a closed TCP port.
- **T6:** An ACK packet with the options (WNMTE) is sent to a closed TCP port.
- **T7:** A FIN, PSH, and URG packet with the options (WNMTE) is sent to a closed TCP port.
- **PU:** A packet is sent to a closed UDP port.

Attackers use several methods to determine the target OS. The following are some examples:

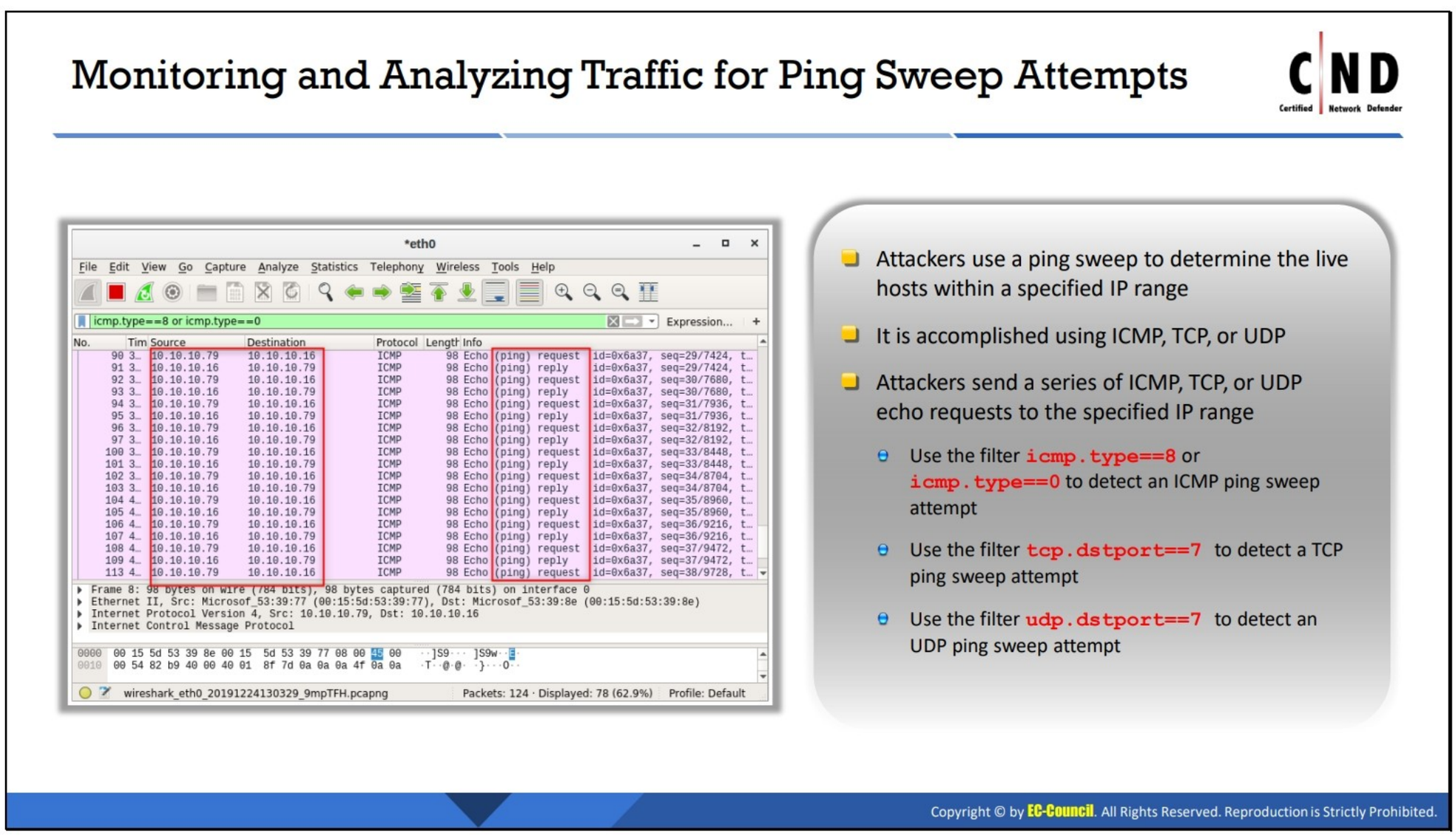
- Did the target host respond?
- Did the target host have the "do not fragment" bit set?
- What is the window size of the target host?
- What is the status of the ACK number for the TCP packet sent to Nmap?
- Which flags are set in the TCP packet?

These methods can be applied to any version of any OS. All the matched OS fingerprints are saved in a text file in Nmap called nmap-os-fingerprints.

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

https://t.me/learningnets

Technet24



Monitoring and Analyzing Traffic for Ping Sweep Attempts

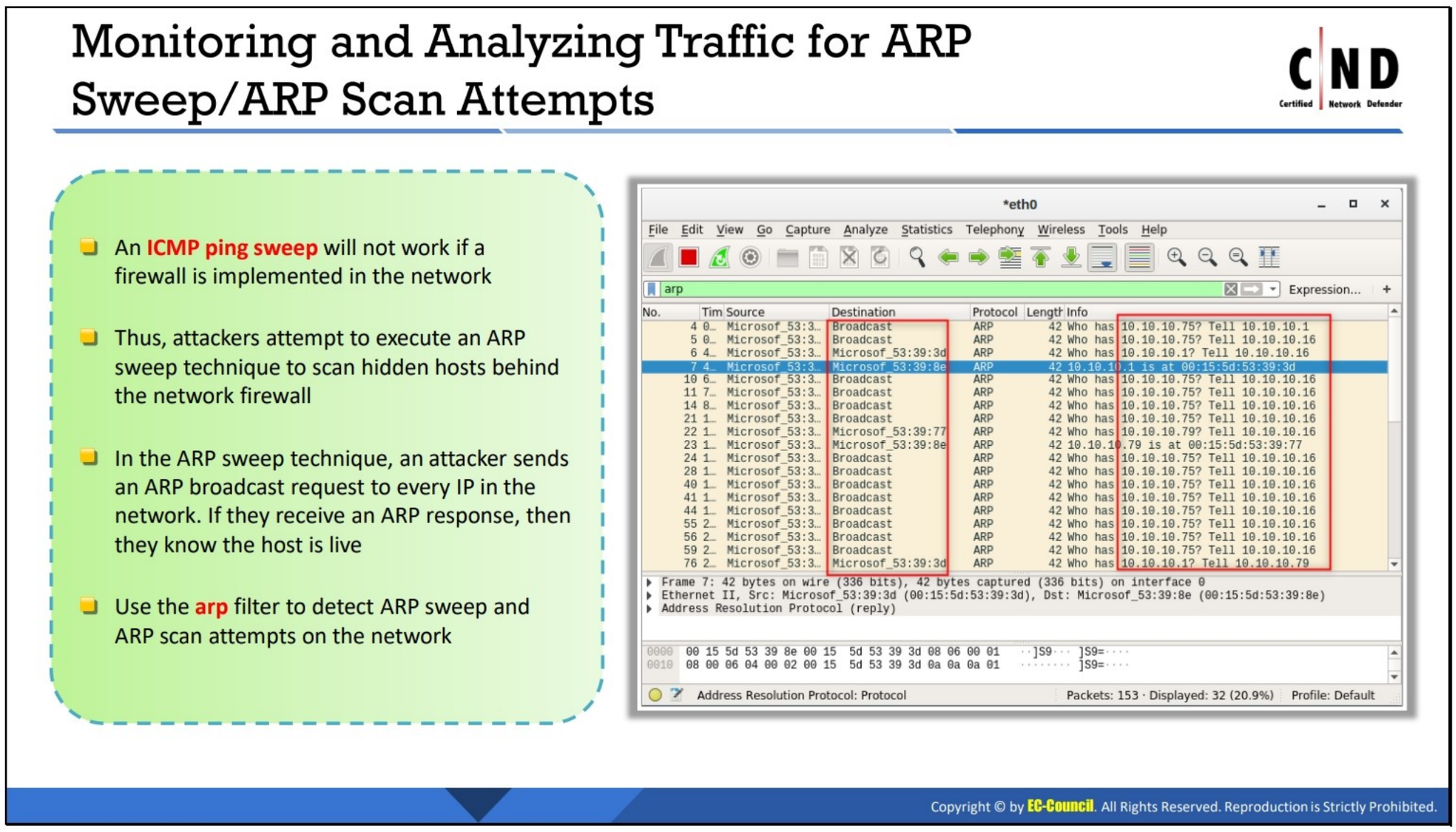
A ping sweep scan helps attackers discover active systems in a network. It involves sending multiple ICMP, TCP, or UDP echo requests to target ports and then analyzing the echo reply obtained from the port.

In an ICMP ping sweep, the attacker sends an ICMP type-8 echo request followed by an ICMP type-0 request and analyzes the echo reply. To detect the ICMP ping sweep, the network defenders must find the ICMP type-8 and ICMP type-0 echo requests in the network traffic. The use of a filter is recommended to accomplish this task. The filter **icmp.type==8** or **icmp.type==0** can be used to detect an ICMP ping sweep attempt.

In a TCP/UDP ping sweep, an attacker sends an echo request packet to TCP/UDP port 7. To detect the TCP/UDP ping sweep attempt, the TCP echo request packets going to port 7 and the UDP echo request packets going to port 7 must be detected in the network traffic. The filter **tcp.dstport==7** can be used to detect the TCP ping sweep and the filter **udp.dstport==7** can be used to detect the UDP ping sweep attempts. If the target port does not support an echo reply, then this technique will not work.

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

https://t.me/learningnets



Monitoring and Analyzing Traffic for ARP Sweep/ARP Scan Attempts

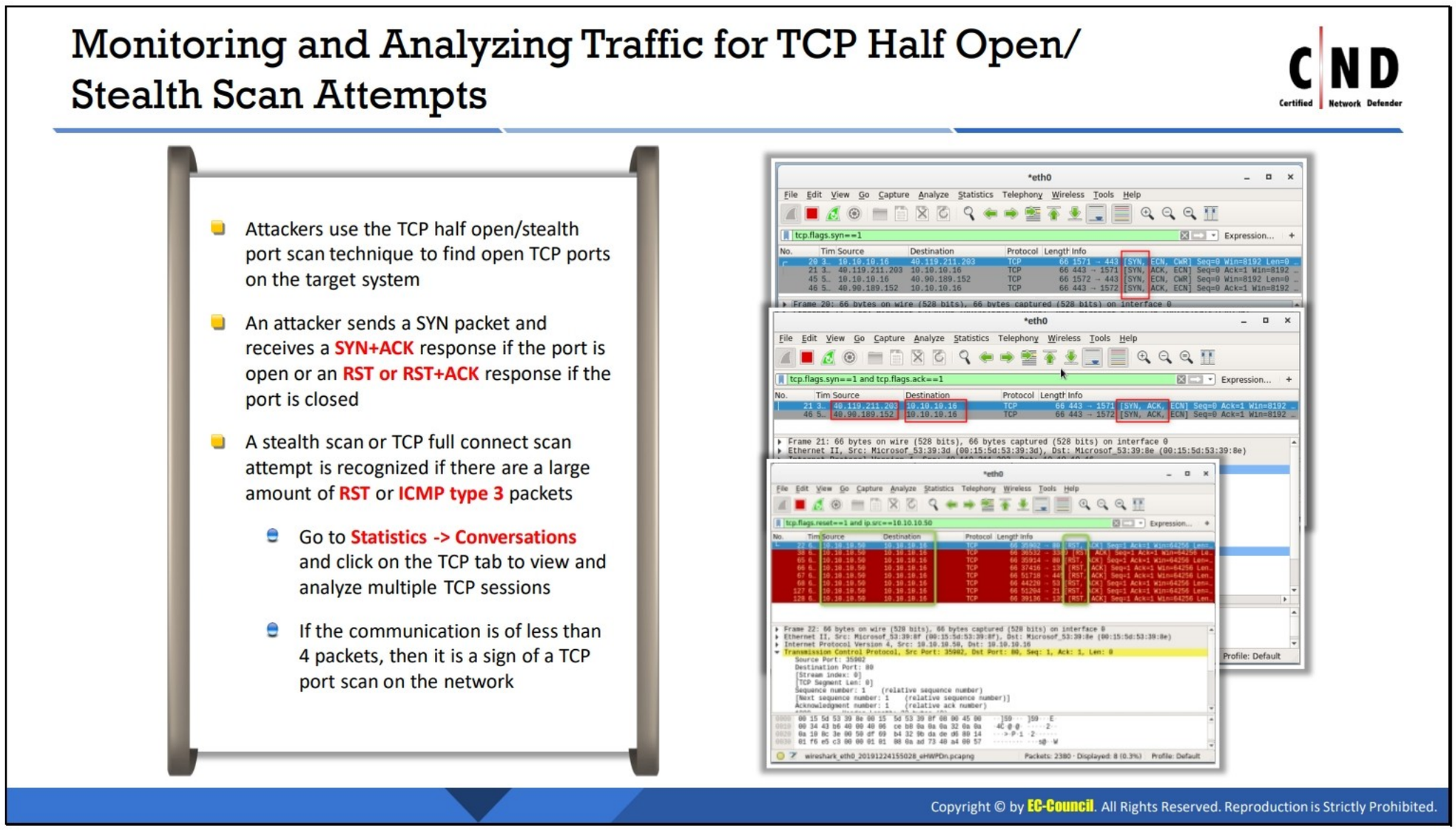
Similar to a ping sweep scan, an attacker can also use an ARP sweep/ARP scan to locate active IPs in the network. Attackers use this method especially when a firewall is implemented between them and the target network, in which case the ping sweep method will not work. In an ARP sweep, an attacker broadcasts ARP packets to all the hosts in the selected subnet and waits for a response. If an ARP response is received from a specific host, then the host is live.

ARP communications cannot be disabled to restrict an ARP sweep attempt on the network as all TCP/IP communication is based on it. However, network defenders can easily monitor and detect this type of attempt using an ARP filter in Wireshark. An unexpected number of broadcast ARP requests indicates an ARP sweep attempt on the network.

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

https://t.me/learningnets

Technet24



Monitoring and Analyzing Traffic for TCP Half Open/ Stealth Scan Attempts

An attacker can use a TCP half open/stealth scan to detect open or closed TCP ports on the target system. This scan involves sending a SYN packet to the target port exactly like normal TCP communication and waiting for a response. If a SYN+ACK packet is received in the response, the target port is open. If an RST or RST+ACK packet is received in the response, the port is closed. If the target port is behind a firewall, the response will be an ICMP type-3 packet with a code 1, 2, 3, 9, 10, or 13.

The TCP half connection can act as an open gate for attackers to enter the network. It is necessary for network defenders to detect a TCP half open connection. Excessive RST packets or ICMP type-3 response packets in Wireshark indicate a TCP half open/stealth scan attempt on the network.

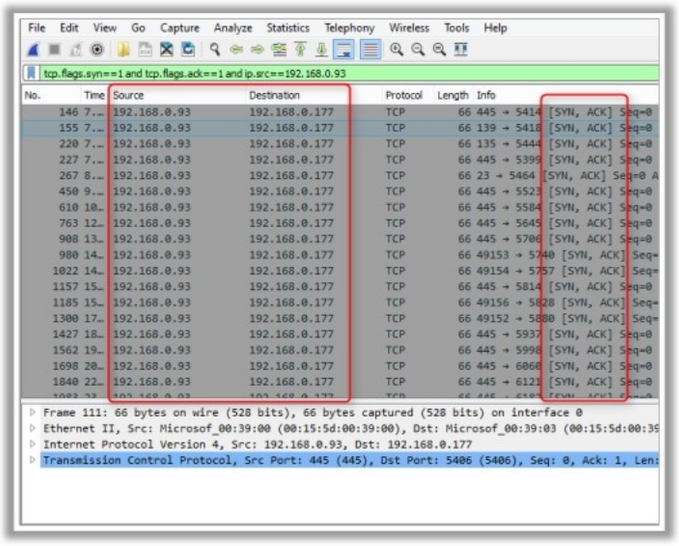
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

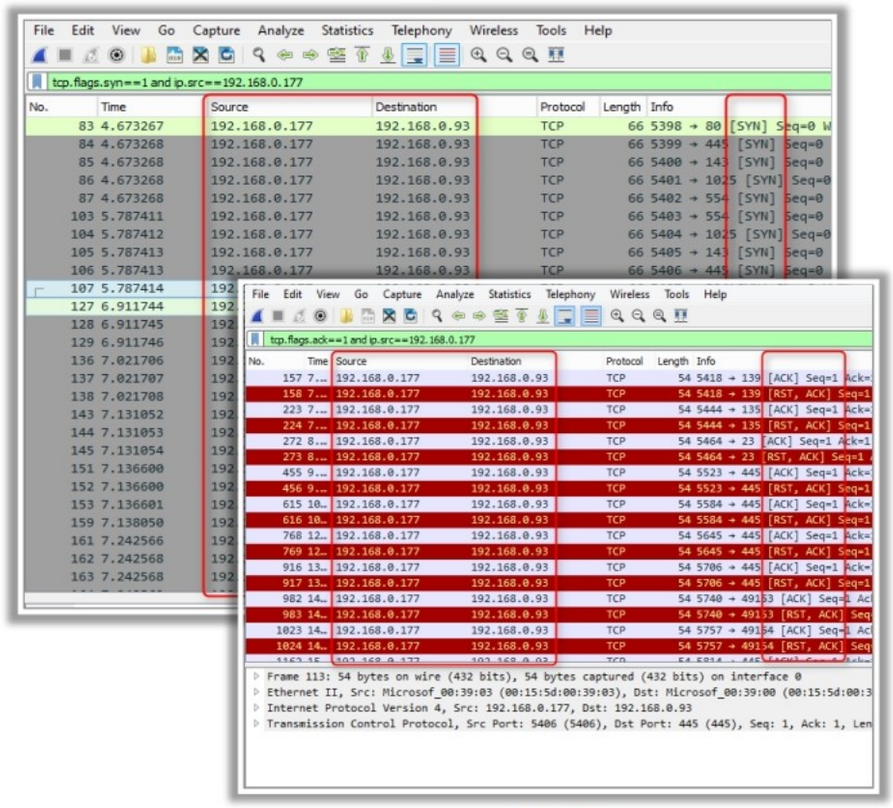
Monitoring and Analyzing Traffic for TCP Full Connect Scan Attempts

- In a TCP full connect scan, the attacker performs a complete three-way handshake to find open ports on the target system
- A TCP full connect scan is recognized using the same methods as those used to detect a stealth scan
- Check for **SYN+ACK**, **RST**, and **RST+ACK** packets or **ICMP type 3** packets

SYN+ACK



SYN

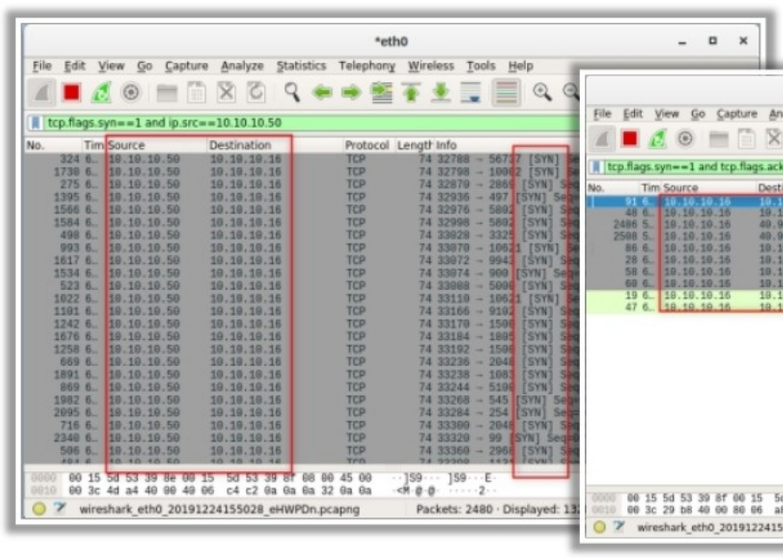


RST+ACK

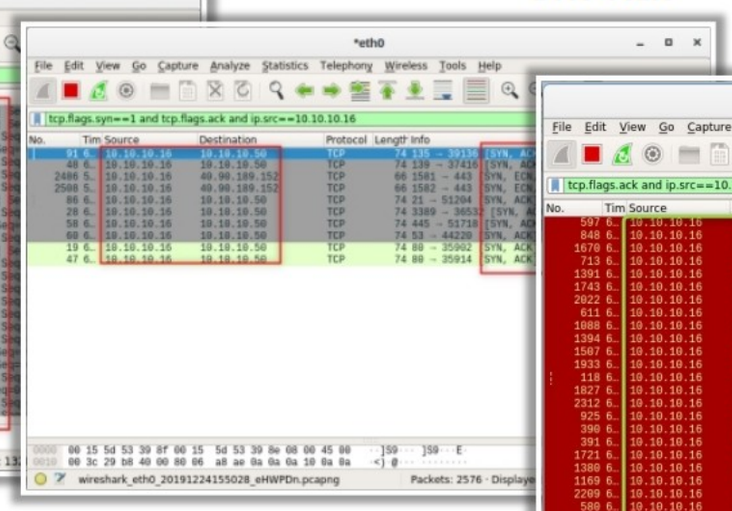
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Monitoring and Analyzing Traffic for TCP Full Connect Scan Attempts (Cont'd)

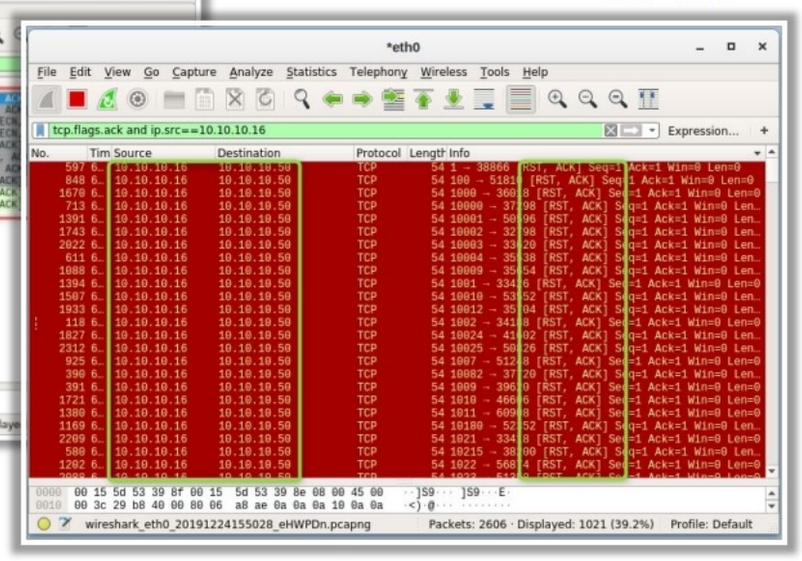
SYN



SYN+ACK



RST+ACK



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

Monitoring and Analyzing Traffic for TCP Full Connect Scan Attempts

A TCP full connect scan or a TCP connect scan is the default scan that establishes a complete three-way handshake connection. A successful three-way handshake implies that the port is open. To establish a TCP full connect scan, the attacker sends a SYN probe packet to the target port. If the port is open, the attacker receives a SYN/ACK packet in the response, indicating that the target port is open. The attacker completes the communication by sending an ACK flag and

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

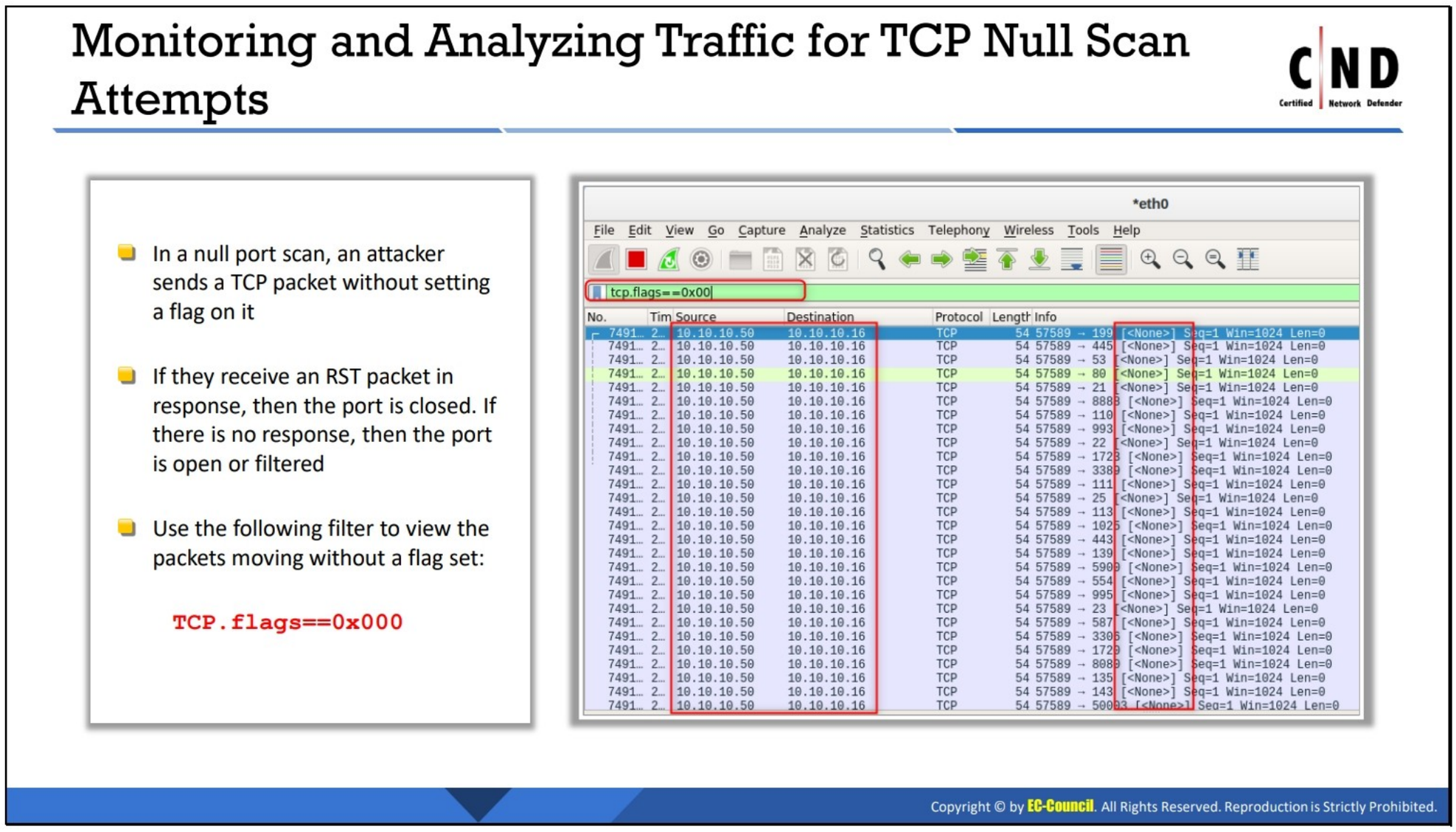
https://t.me/learningnets

Technet24

receiving an RST flag to terminate the session. If the port is closed, the attacker receives RST/ACK as the response. If the target port is behind a firewall, they receive an ICMP type-3 packet with a code 1, 2, 3, 9, 10, or 13 as the response.

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

https://t.me/learningnets



Monitoring and Analyzing Traffic for TCP Null Scan Attempts

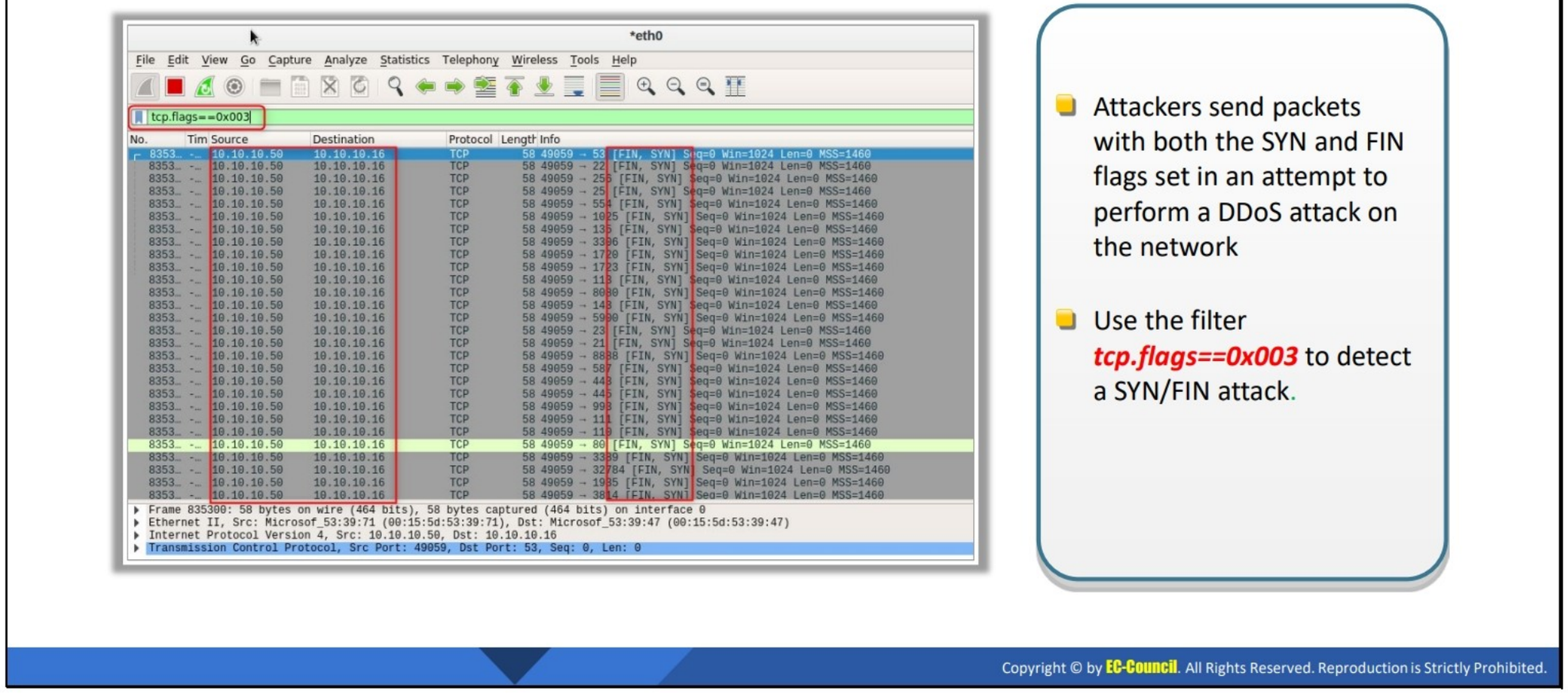
A TCP null scan helps attackers identify listening ports in the network. A TCP null scan is a series of TCP scan packets containing a sequence number of 0 and no set flag. Since the null scan does not contain any set flags, it can penetrate a router and a firewall that filter incoming packets with particular flags set.

In a TCP null scan, the attacker sends a TCP packet to the target port. If the port is closed, they receive an RST flag. If the port is open, the port will not respond, because the packet lacks a flag. A TCP null scan sets all the TCP headers (ACK, FIN, RST, SYN, URG, and PSH) to NULL. network defenders can detect a TCP null scan on Unix servers by applying the filter **tcp.flags==0x000** in Wireshark. TCP null scans do not support Windows.

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

https://t.me/learningnets

Technet24



Monitoring and Analyzing Traffic for SYN/FIN DDoS Attempts

In a SYN attack, the attacker sends a succession of SYN requests to the target's system to make the system unavailable for legitimate users. It exploits a known weakness in the TCP connection.

A typical TCP communication is established in the following manner (TCP three-way handshake):

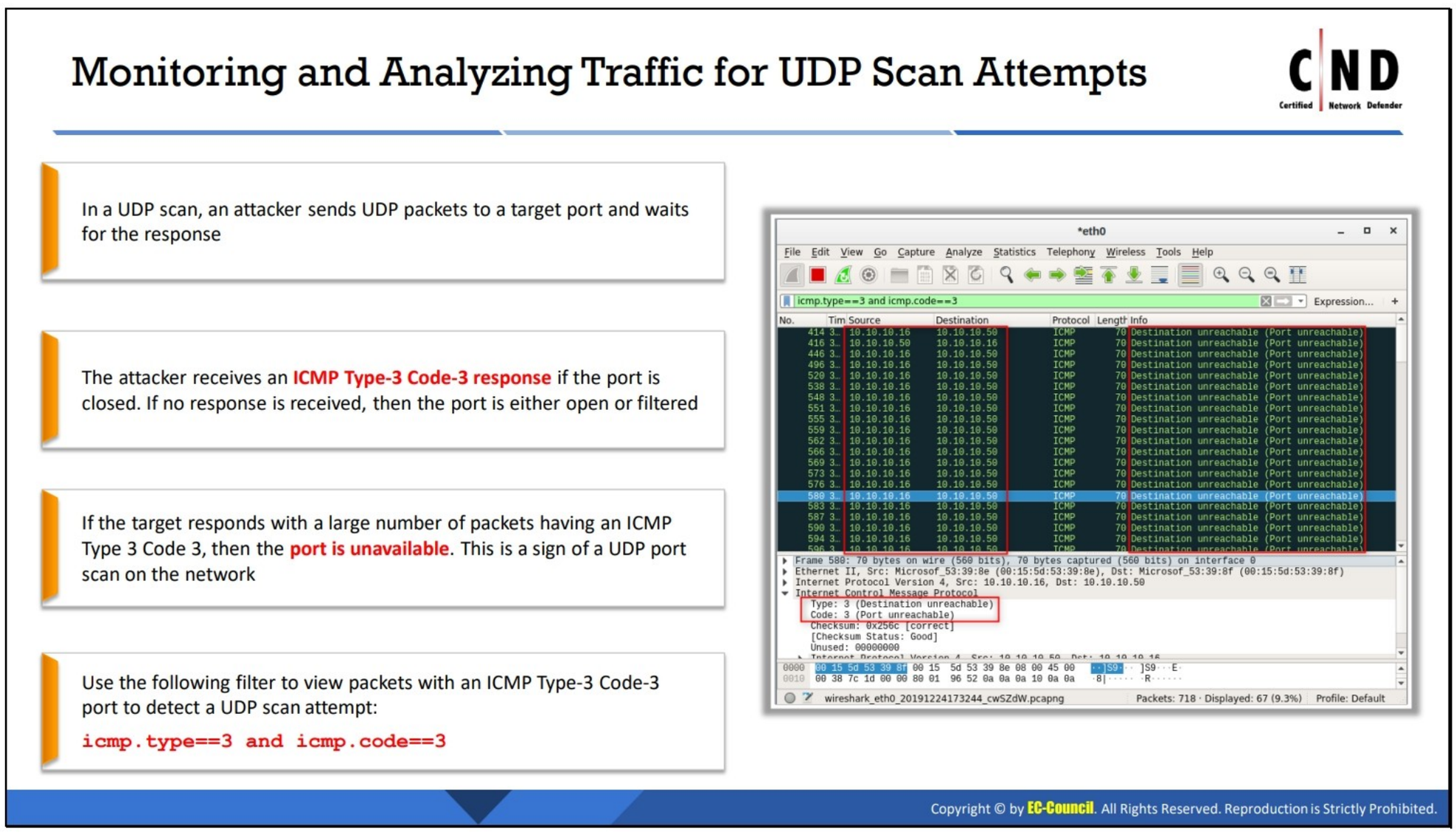
1. The client sends a SYN packet to request a connection.
2. The server responds with SYN/ACK.
3. The client then responds with an ACK to establish the connection.

A SYN flood attack is initiated by not responding to the server with an ACK as expected in the last step of the TCP three-way handshake. The server waits indefinitely for the ACK, causing network congestion.

The SYN flag establishes a connection, while the FIN flag terminates a connection. In a SYN/FIN DDoS attempt, the attacker floods the network by setting both SYN and FIN flags. In a typical TCP communication, SYN and FIN are not set simultaneously. Traffic with both SYN and FIN flags set is a sign of a SYN/FIN DDoS attempt, which can exhaust the firewall on the server by regularly sending packets. To detect such suspicious attacks, the network defenders should use the filter **tcp.flags==0X003** to determine whether these traffic entries are in the same packet.

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

https://t.me/learningnets



Monitoring and Analyzing Traffic for UDP Scan Attempts

The UDP service can receive packets without establishing a connection. When an attacker sends a UDP packet to the target, either of the following can occur:

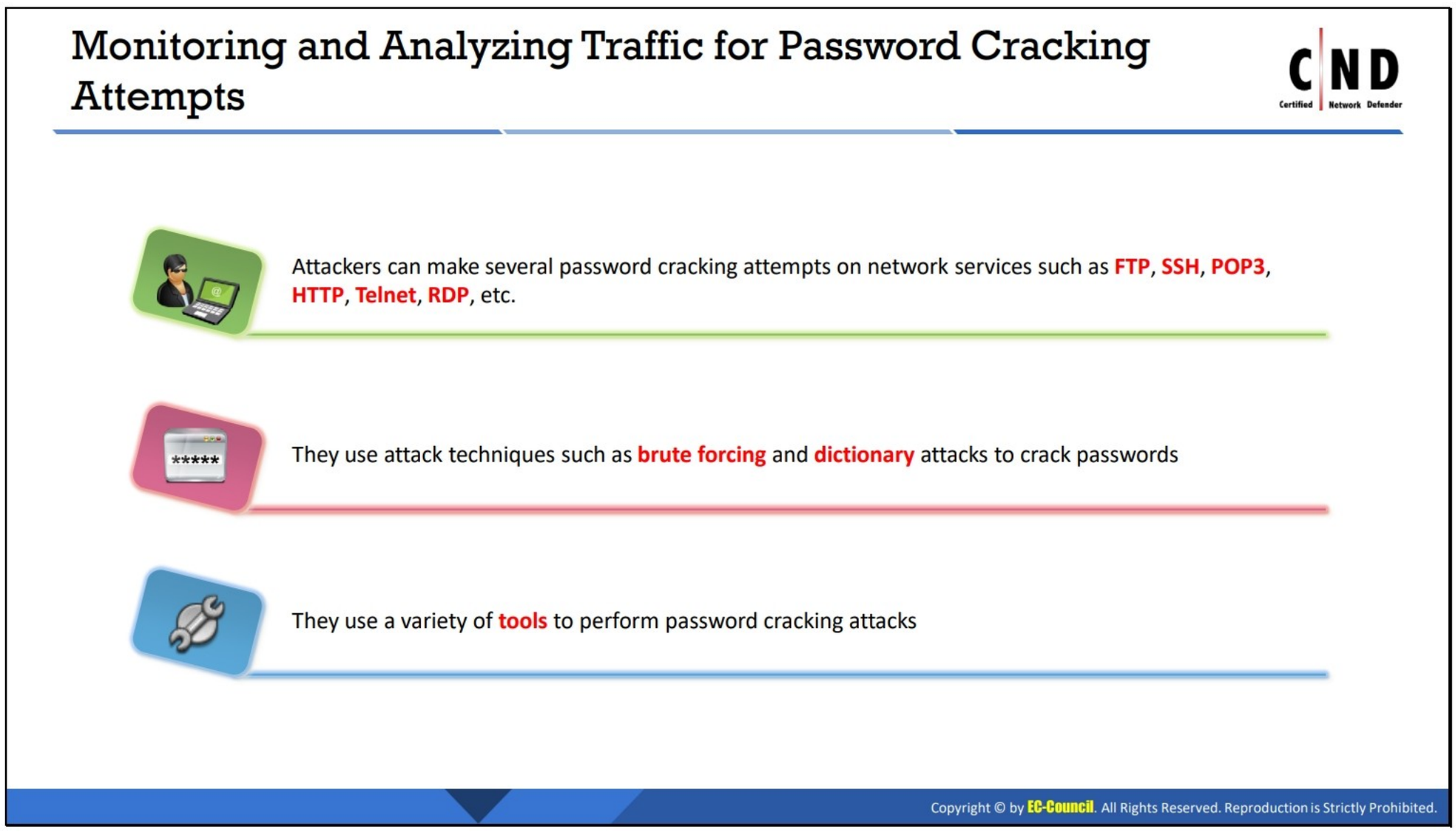
- If the UDP port is open, the target accepts the packet and does not send any response.
- If the UDP port is closed, an ICMP packet is sent in response.

UDP scanning is more difficult to probe than TCP scanning as it does not depend on the acknowledgements received. A UDP scan gathers all the ICMP errors received from closed ports. Network defenders should take proper measures to handle open UDP ports to avoid any intrusion in the network. While monitoring, if any machine replies with bulk ICMP type-3 responses, it is a sign of a UDP scan attempt on the network. To identify UDP scan attempts, the filters **icmp.type==3** and **icmp.code==3** should be used in Wireshark.

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

https://t.me/learningnets

Technet24



Monitoring and Analyzing Traffic for Password Cracking Attempts

Password cracking is a process of gaining or recovering passwords either through trial and error or by making password guessing attempts with the most commonly used passwords; these techniques are called brute-force attacks and dictionary attacks, respectively.

Brute-force Attack

Though brute-force attacks can be a lengthy process, attackers use various tools to implement them on networks.

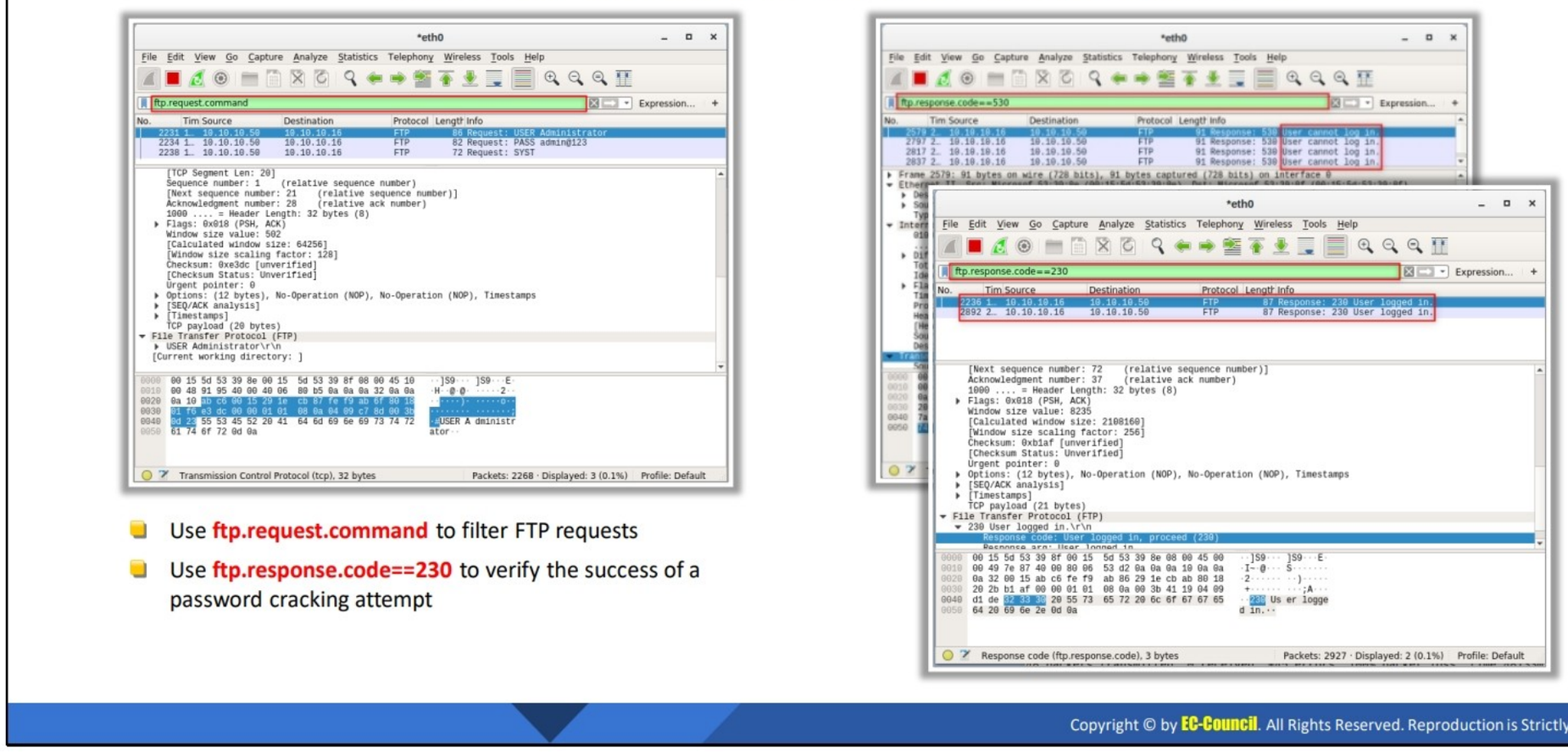
Dictionary Attack

In this technique, the attacker uses a limited set of words. It is easier for attackers to perform a dictionary attack with SSH services running in the network. SSH dictionary attacks rely on log files or network traffic. A dictionary attack can be accomplished easily on an account that has a weak password. This type of attack is performed on a single target machine or on a network.

Network defender can detect this type of attack by monitoring the number of login attempts made from the same IP address or username.

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

https://t.me/learningnets



Monitoring and Analyzing Traffic for Password Cracking Attempts (Cont'd)

FFTP is a standard protocol to transmit files between systems over the Internet using the TCP/IP suite. FTP is a client server protocol relying on two communication channels between a client and server. One manages conversations, and the other is responsible for the actual content transmission. A client initiates a session with a download request, to which the server responds with the requested file.

An FTP session requires the user to login to the FTP server with their username and password. In an FTP password attack, the attacker attempts to gain the user's password.

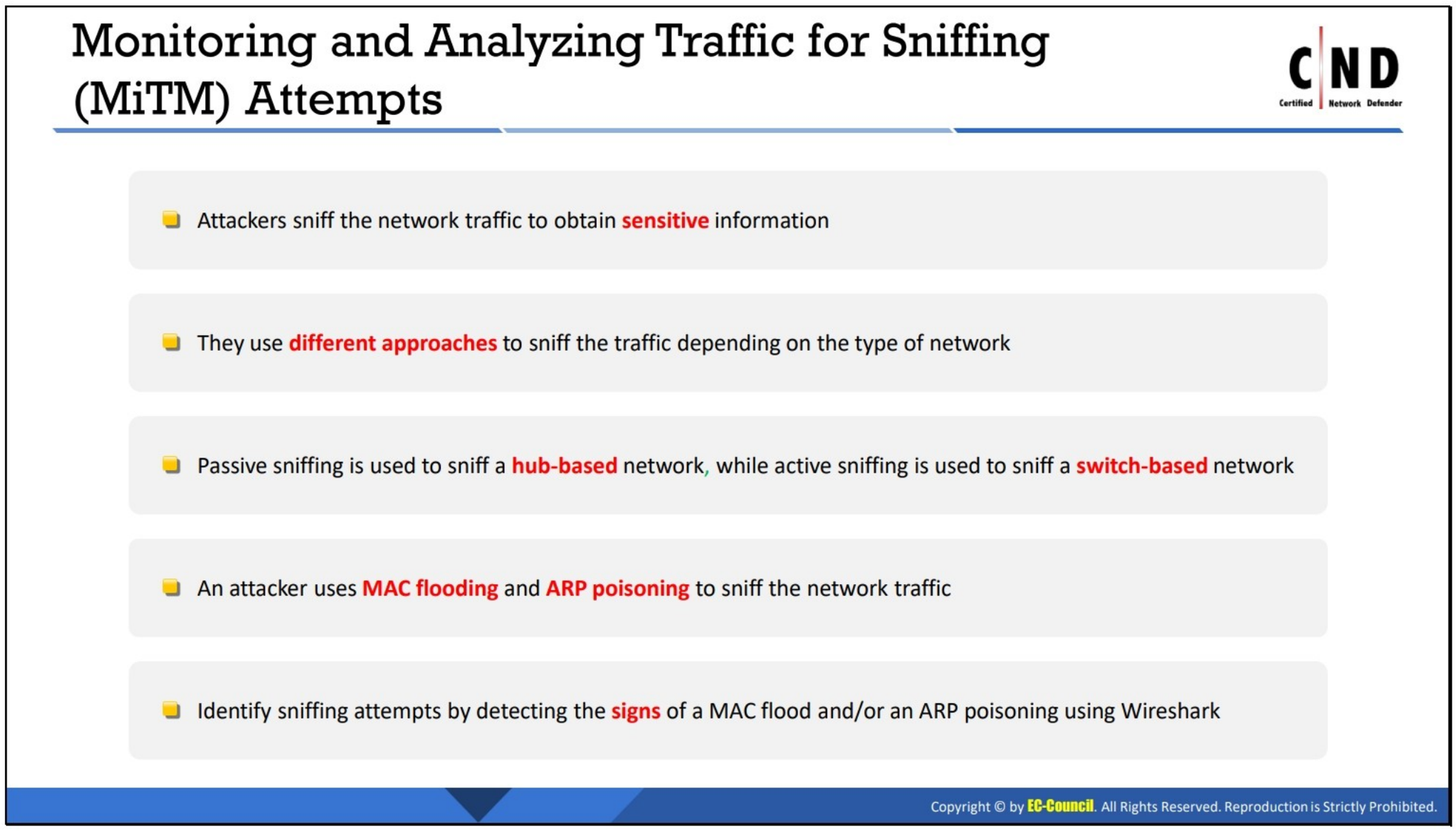
The filter **ftp.request.command** in Wireshark can be used to detect an FTP password cracking attempt in the network. Furthermore, the filter **ftp.request.command** shows all the FTP requests made in the network. It also displays the number of attempts made by an attacker to gain access to the FTP server.

- To check for successful FTP password cracking attempts, apply the filter **ftp.response.code = = 230**
- To check for unsuccessful FTP password cracking attempts, apply the filter **ftp.response.code = = 530**

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

https://t.me/learningnets

Technet24



Monitoring and Analyzing Traffic for Sniffing (MiTM) Attempts

Sniffing or man-in-the-middle (MITM) attacks are a form of eavesdropping in which an attacker captures packets by placing themselves between a client and server. Sniffing is performed using either an active form or a passive form.

Active Sniffing

Sniffing performed over a switched network is called active sniffing. In this type of sniffing, the attacker injects packets into the network traffic to gain information from the switch, which maintains its own ARP cache known as content addressable memory (CAM).

Passive Sniffing

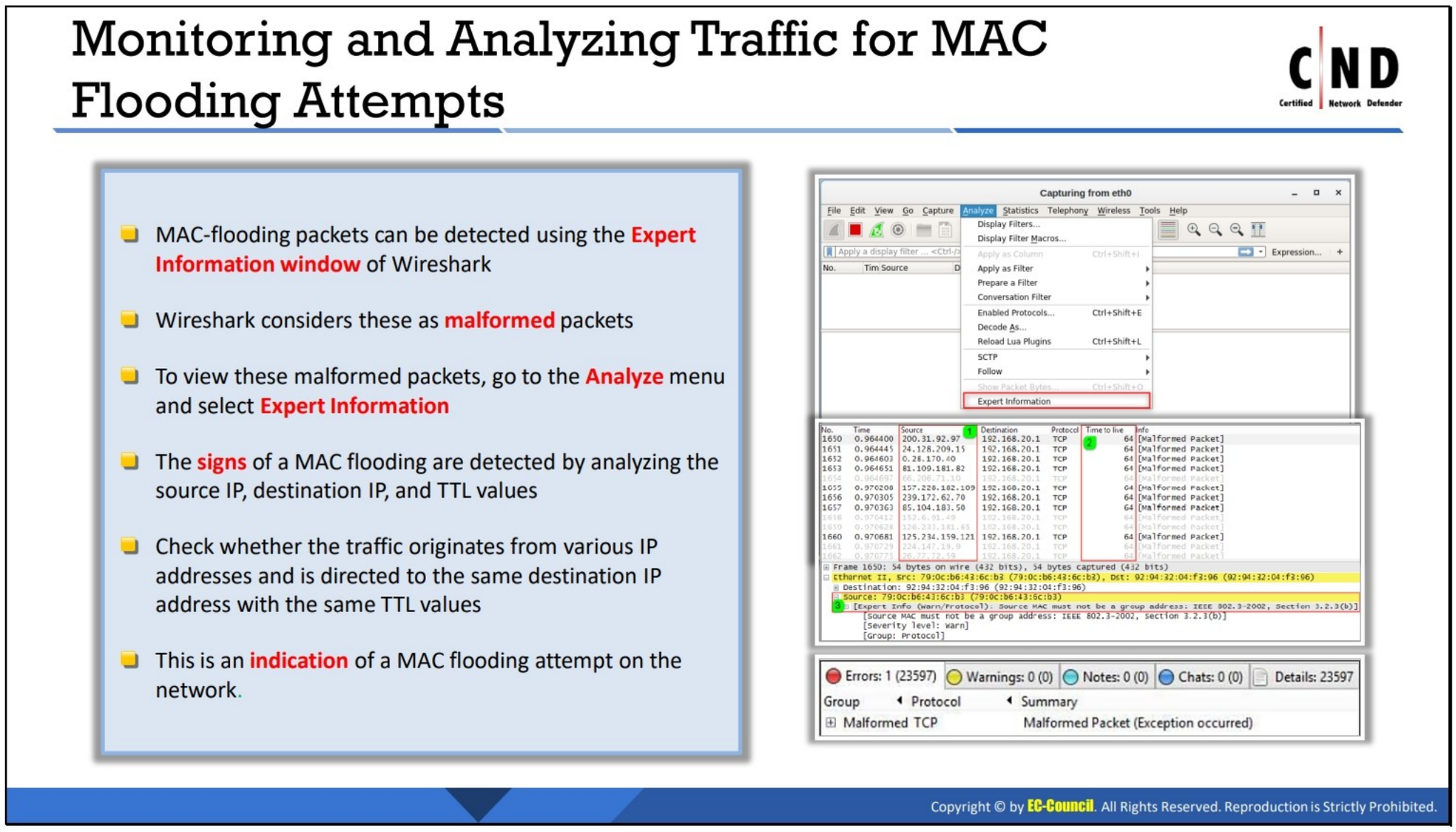
Sniffing performed on the hub is called passive sniffing. Since a hub broadcasts all packets, an attacker only has to initiate a session and wait for someone else to send packets on the same collision domain.

The following methods are used in sniffing:

- MAC flooding
- ARP poisoning

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

https://t.me/learningnets



Monitoring and Analyzing Traffic for MAC Flooding Attempts

MAC flooding is an active sniffing method in which the attacker connects to a port on a switch and sends a flurry of Ethernet frames with various fake MAC addresses. Through MAC flooding, the attacker attempts to gain access to the content addressable memory (CAM) table maintained by the switch. This attack is also known as CAM flooding.

A MAC flooding attempt can be detected in Wireshark by carefully analyzing a packet's source and destination addresses along with its time to live (TTL).

For analyzing packets in Wireshark after capture, go to the Analyze tab and click on Expert Information from the drop-down context menu, as shown in Figure 14.6.

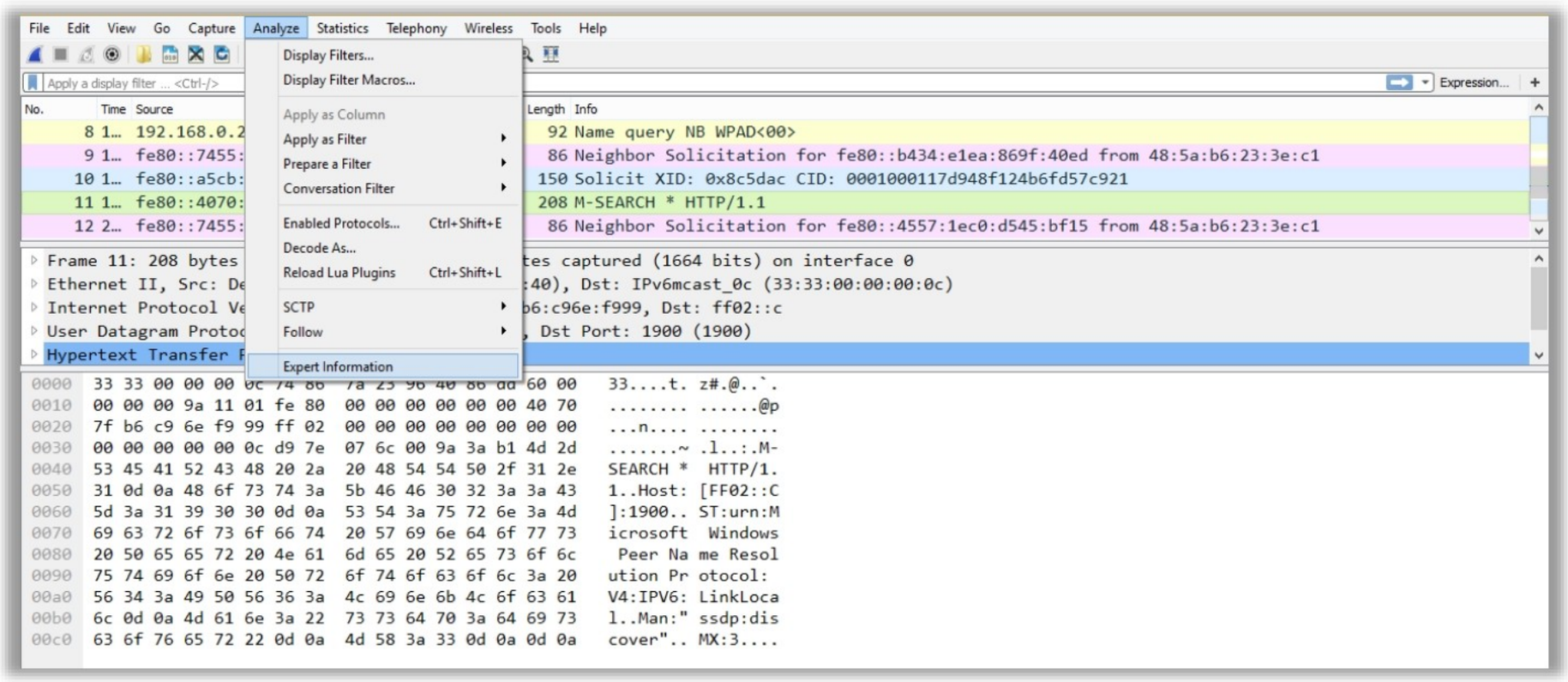


Figure 14.6: Selecting Expert Information from the Analyze Tab in Wireshark

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

https://t.me/learningnets

Technet24

Then, look for malformed packets in the Expert Information tab, as shown in Figure 14.7.

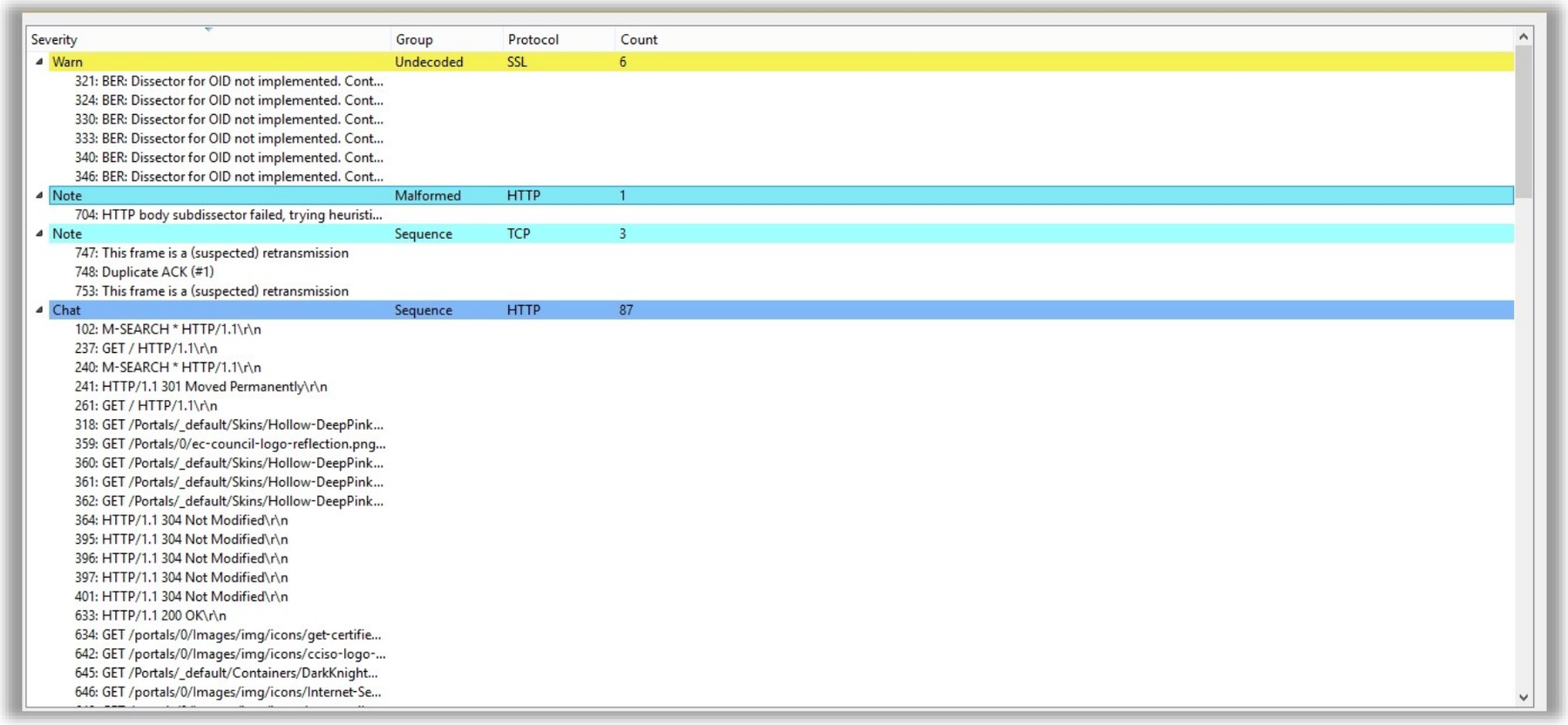


Figure 14.7: Malformed Packets in the Expert Information Tab in Wireshark

There are various reasons for malformed packets, and they are not necessarily due to MAC flooding attempts. To accurately detect a MAC flooding attempt, the network defender must check whether several packets are destined towards the same machine but originate from different sources.

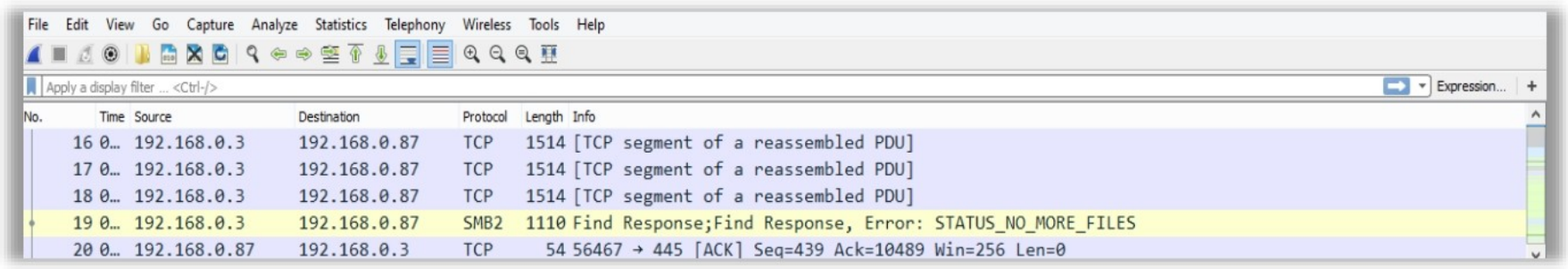


Figure 14.8: MAC Flooding Attempt

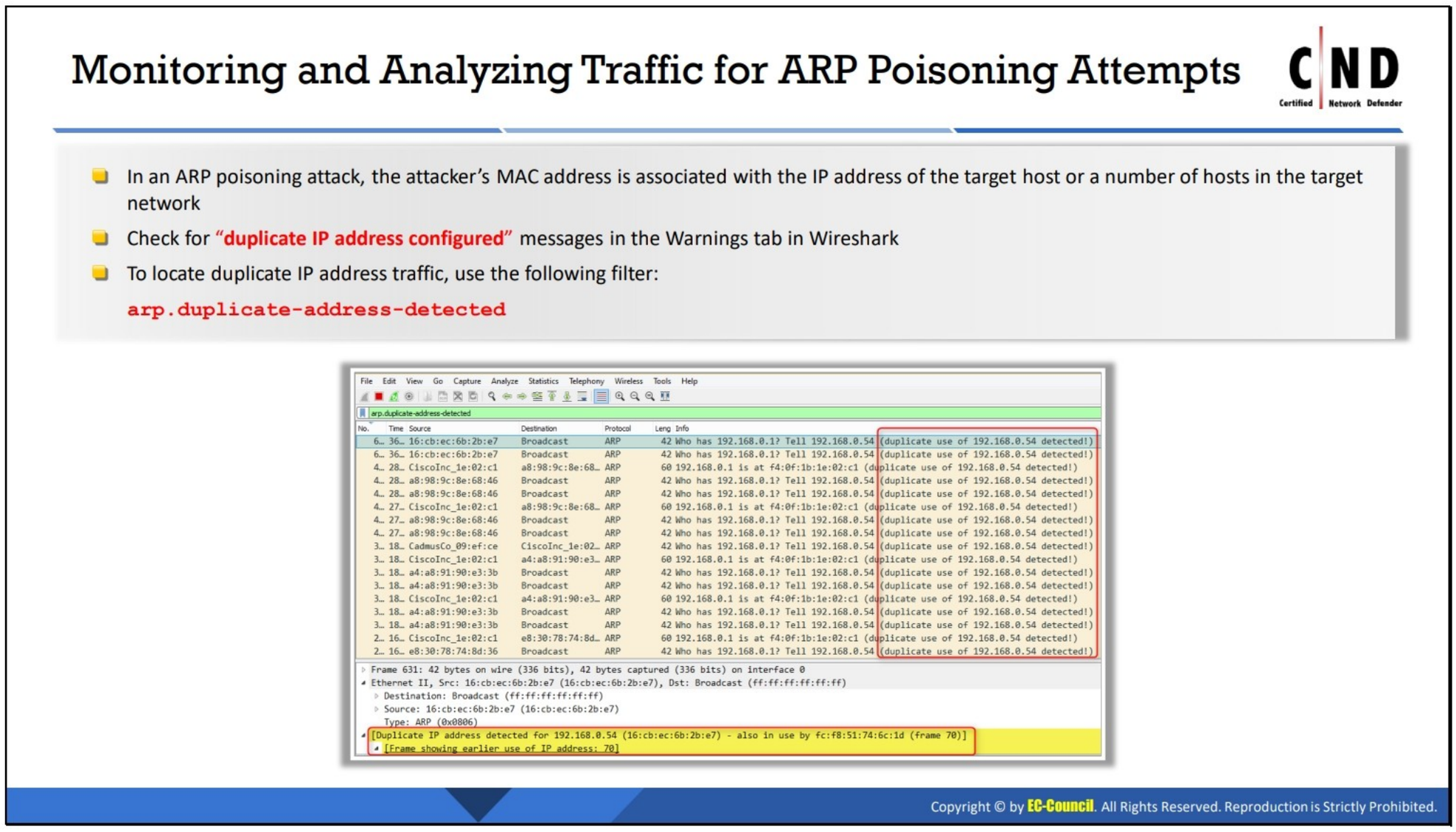
Although the destination address is the same in Figure 14.8, it should be noted that the source address is also the same, which implies that the packets were sent from a legitimate source. Network defender can also verify the TTL values for each packet. If every source has the same TTL values and all the packets are directed towards the same machine, then there may be a MAC flooding attempt on the network.

Preventing MAC Flooding

- MAC flooding can be avoided using the built-in port security feature of Cisco switches. Port security limits the number of MAC addresses and creates a small MAC address table instead of the larger ones created conventionally.
- The implementation of authentication, authorization, and accounting (AAA) by vendors minimizes the risk of MAC flooding.
- The implementation of IEEE suites allows packet filtering rules to be installed by an AAA server.

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

https://t.me/learningnets



Monitoring and Analyzing Traffic for ARP Poisoning Attempts

The address resolution protocol (ARP) maps a MAC address to an IP address. In an ARP poisoning attack, an attacker changes the MAC address of the target system to their MAC address. Consequently, all packets destined to the target system are transmitted to the attacker's machine. Through an ARP poisoning attack, an attacker can monitor the data flow in a network, forge more than one device on the network, and have all their packets directed towards them. An ARP poisoning attack can be detected in Wireshark by looking for a warning message that reads "duplicate IP address configured." Network defender can use the filter **arp.duplicate-address-detected** after capturing the packets to view packets with these messages, as shown in Figure 14.9. These messages are an indication of an ARP poisoning attempt on the network.

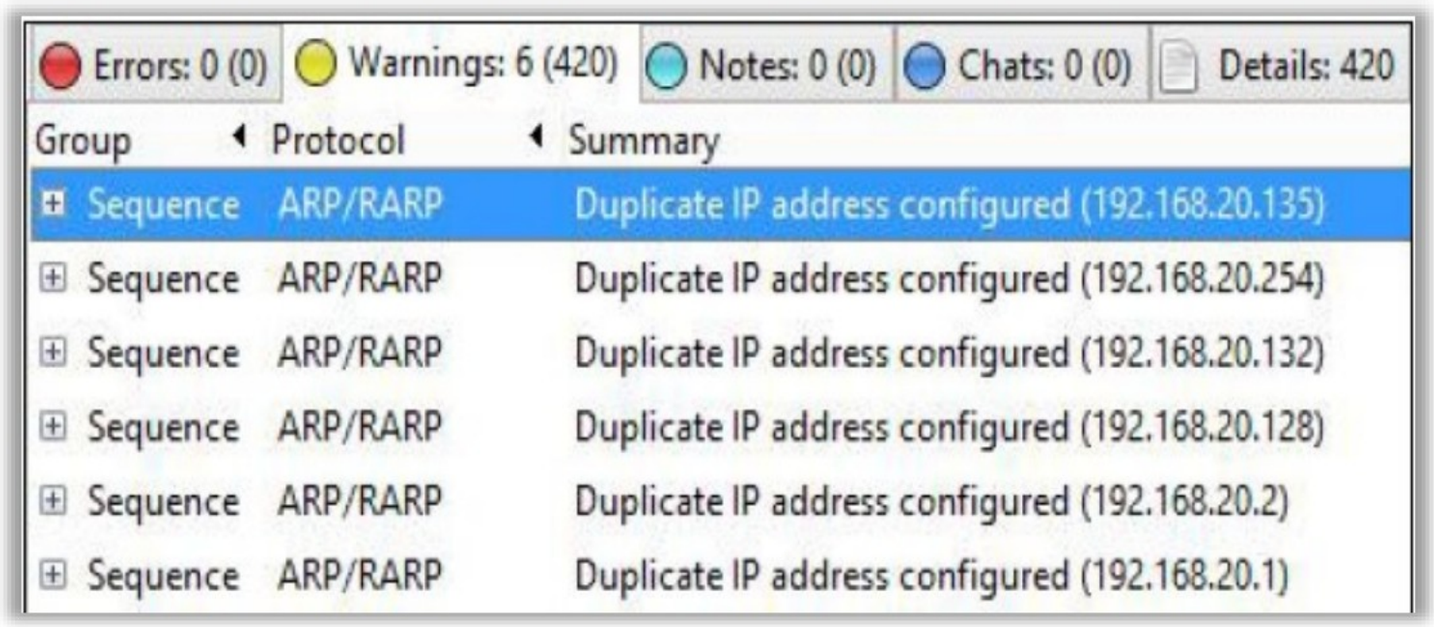
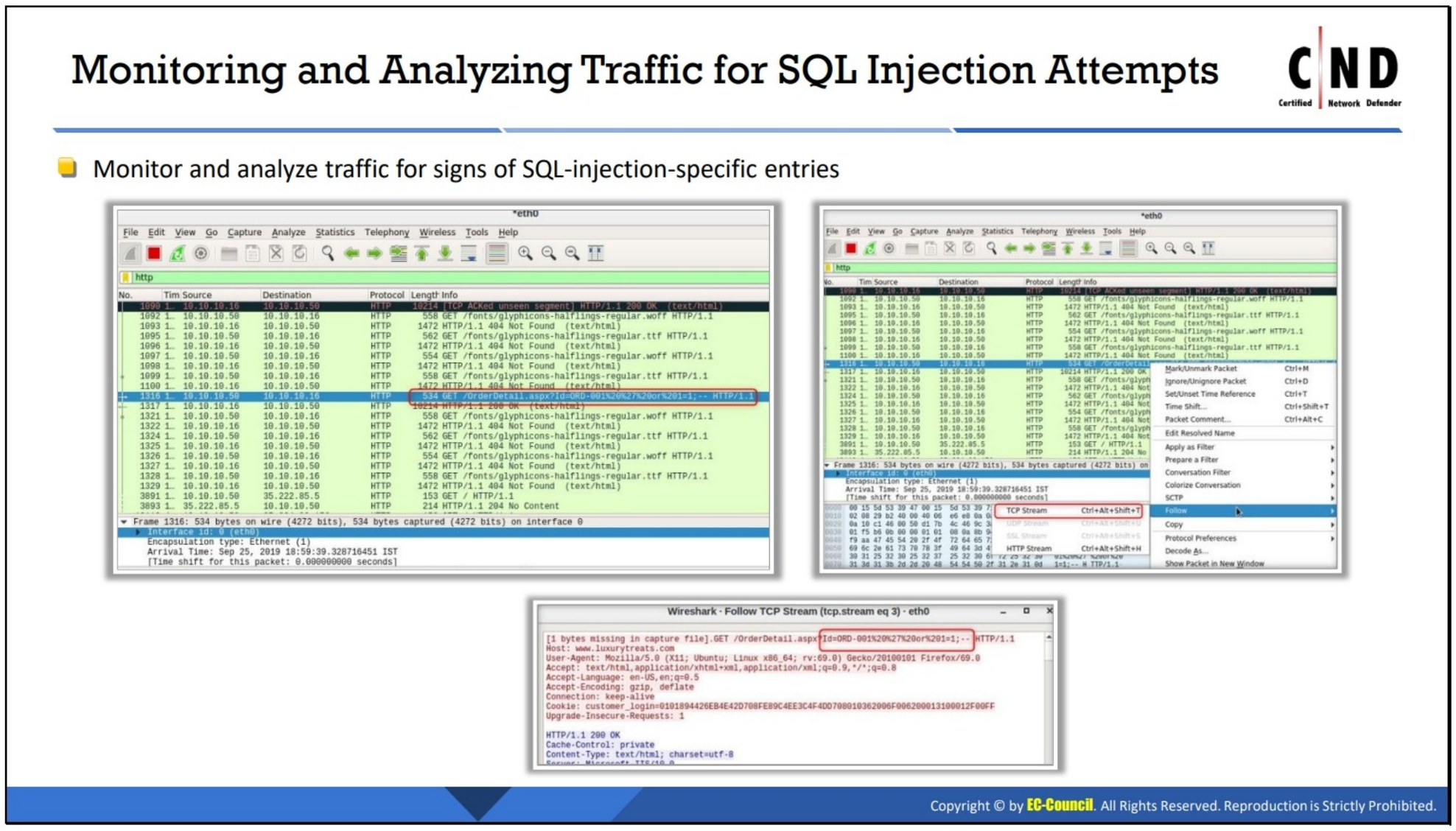


Figure 14.9: ARP Poisoning Attempt

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

https://t.me/learningnets

Technet24



Monitoring and Analyzing Traffic for SQL Injection Attempts

Wireshark can also be used to detect various application-level attacks such as SQL injection and cross-site scripting (XSS). To detect such attempts, the network defender must inspect traffic and look for patterns specific to these types of attacks.

For example, to detect SQL injection attacks, the network defender should look for traffic that contains characters specific to SQL injection such as OR, --, ‘, and =.

Figure 14.10 shows an indication of an SQL injection attempt.

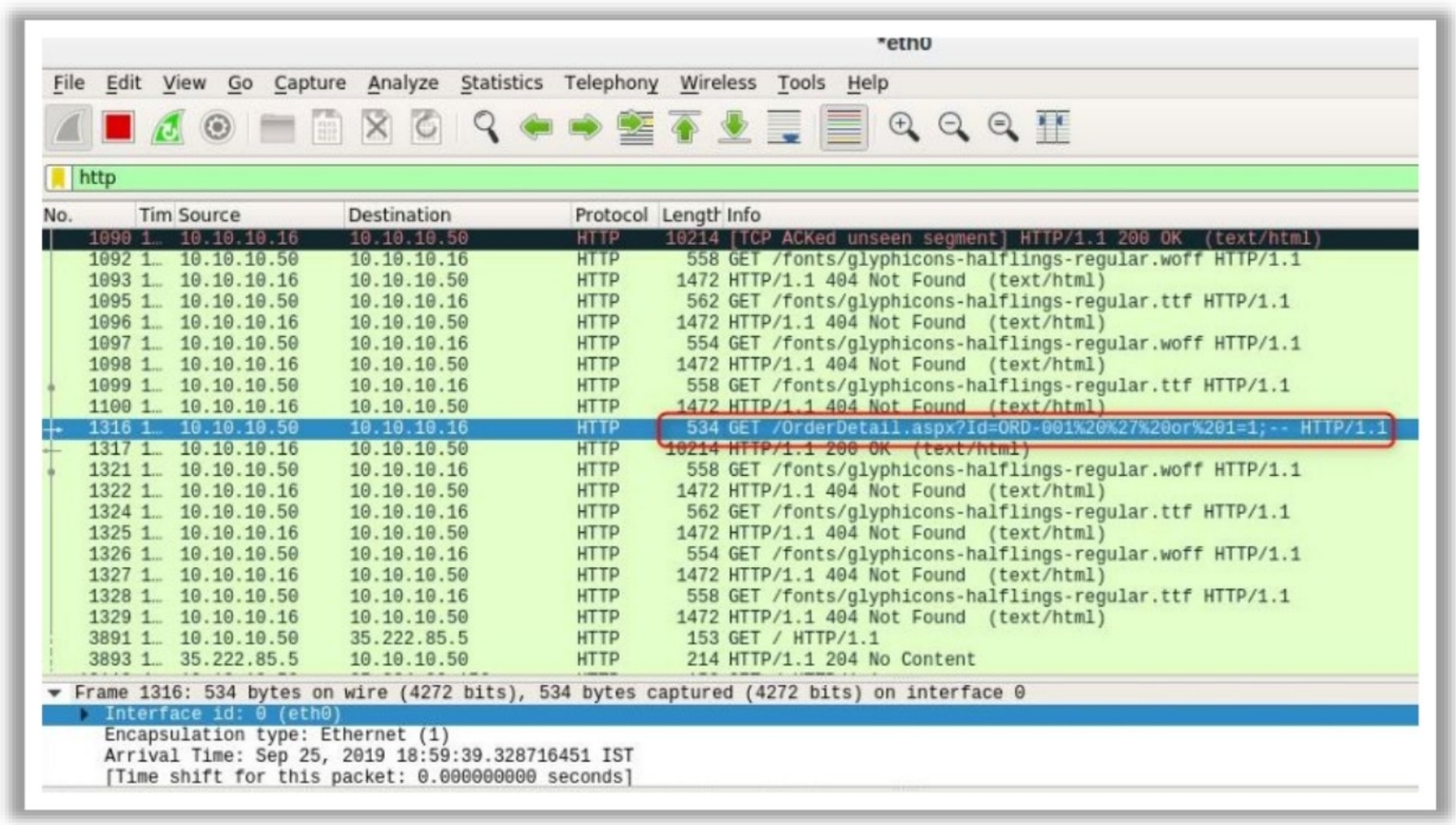


Figure 14.10: SQL Injection Attempt

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

https://t.me/learningnets

These SQL injection attack patterns can be detected by following the stream, as shown in Figure 14.11.

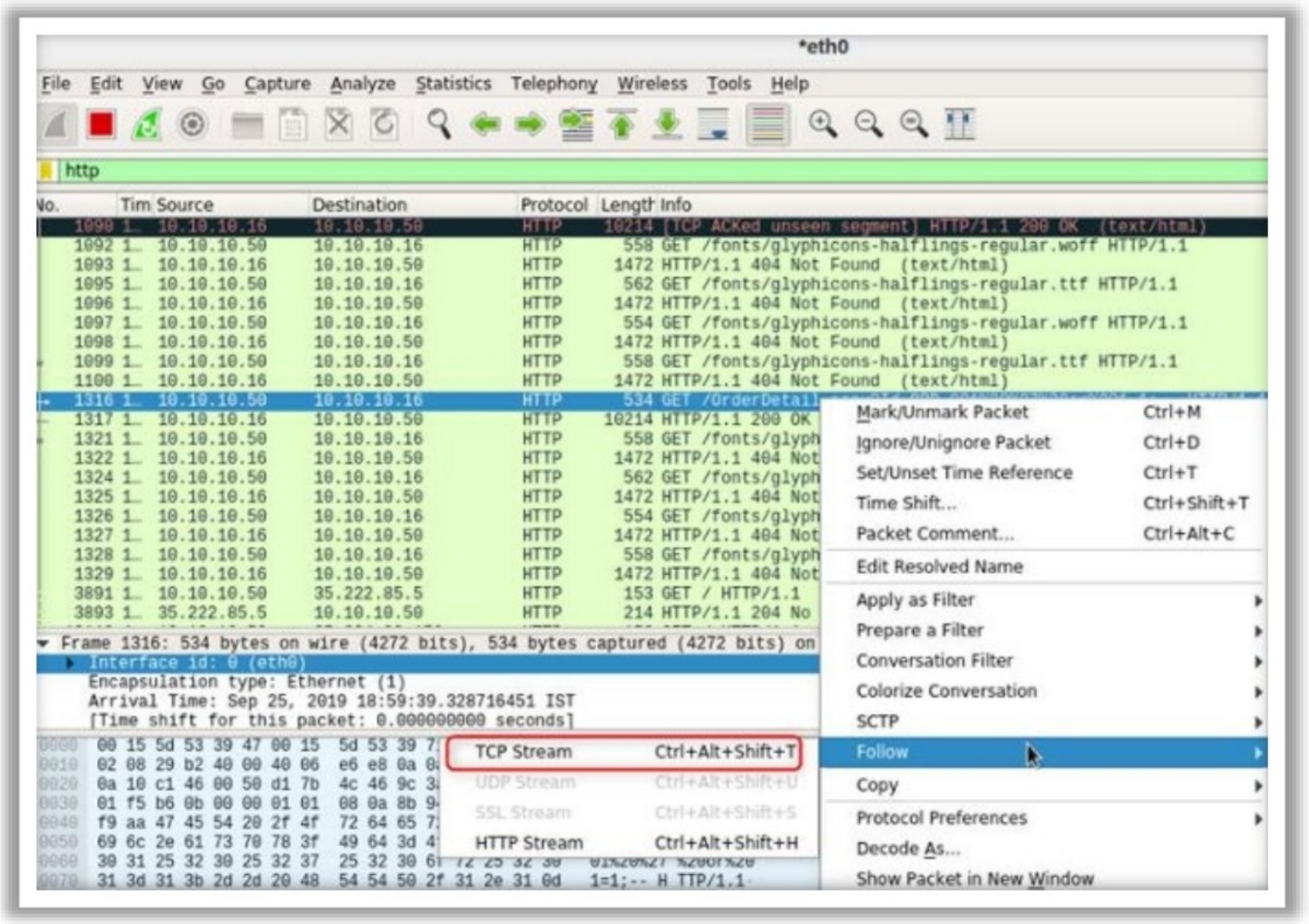


Figure 14.11: Following the Stream to Detect SQL Injection Attack Patterns

By analyzing the traffic details, one can even determine whether the attack was successful, as shown in Figure 14.12.



Figure 14.12: Analysis of Traffic Details to Determine whether an SQL Injection Attempt was Successful

Similarly, XSS exploits can be recognized by finding malicious data (XSS injection string patterns) in the web-page POST, as shown in Figure 14.13.

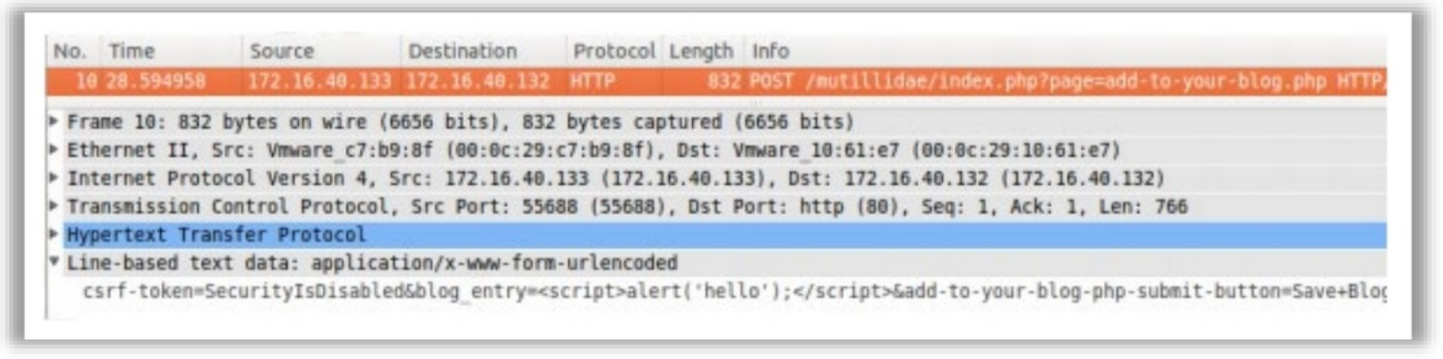
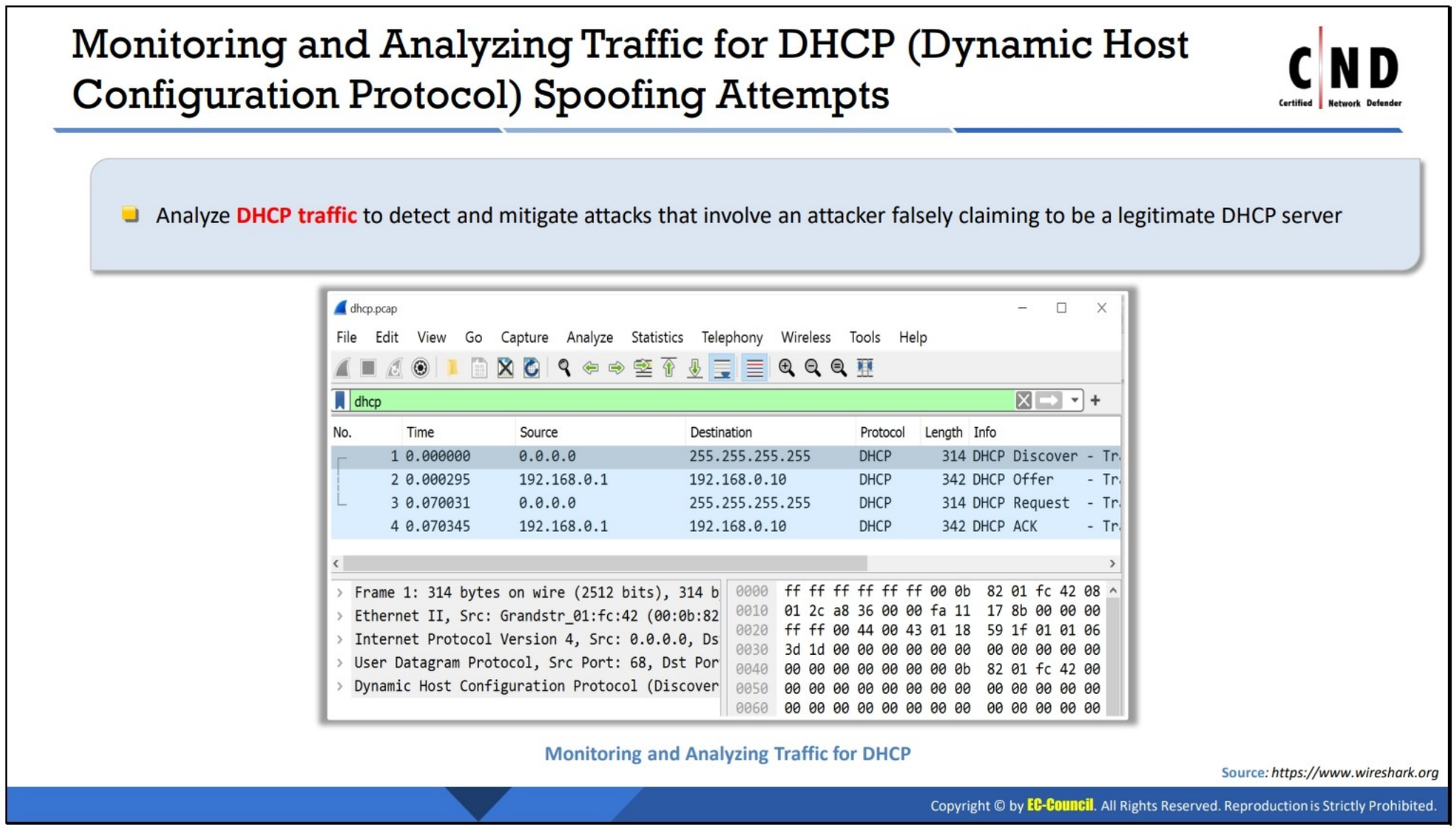


Figure 14.13: XSS Injection String Patterns in the web-page POST

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

https://t.me/learningnets

Technet24



Monitoring and Analyzing Traffic for DHCP Spoofing Attempts

Dynamic Host Configuration Protocol (DHCP) spoofing is a technique attackers use to compromise network security. By employing DHCP spoofing, they distribute rogue IP addresses to clients. This can result in various attacks, such as eavesdropping, network disruption, and man-in-the-middle attacks. DHCP employs the client/server protocol BOOTP as its transport protocol. To filter out DHCP spoofing attacks, use the filter **dhcp**.

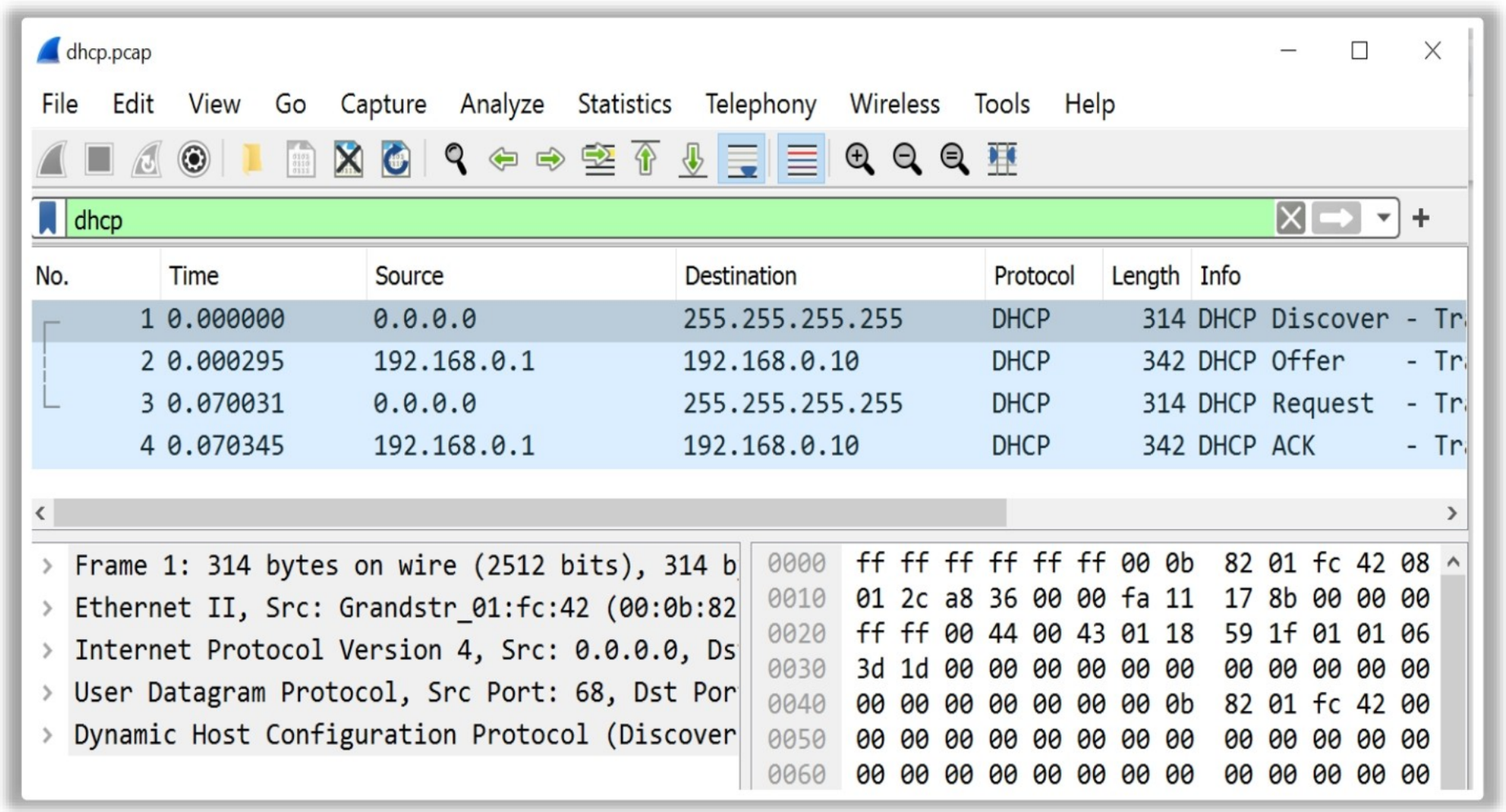
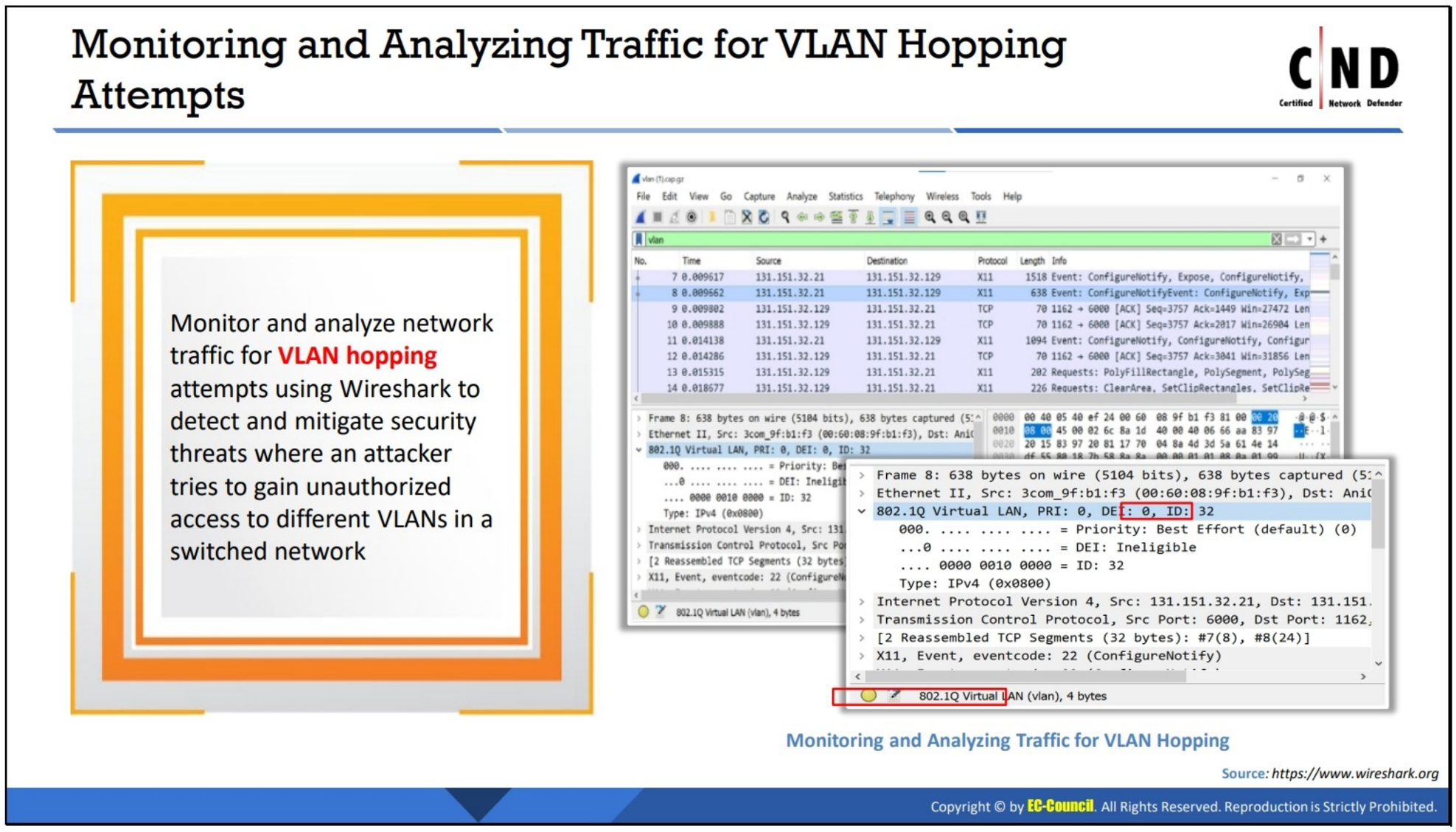


Figure 14.14: Identifying DHCP Traffic

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

https://t.me/learningnets



Monitoring and Analyzing Traffic for VLAN Hopping Attempts

VLAN hopping is an attack where the attacker sends traffic from one VLAN to another, bypassing Network Access Controls (NAC) to access different VLANs. This attack exploits misconfigurations in switches to steal protected information. The presence of DTP packets or packets tagged with multiple VLAN tags indicates a VLAN hopping attack. To detect VLAN hopping on a network, use the Wireshark filter **vlan**.

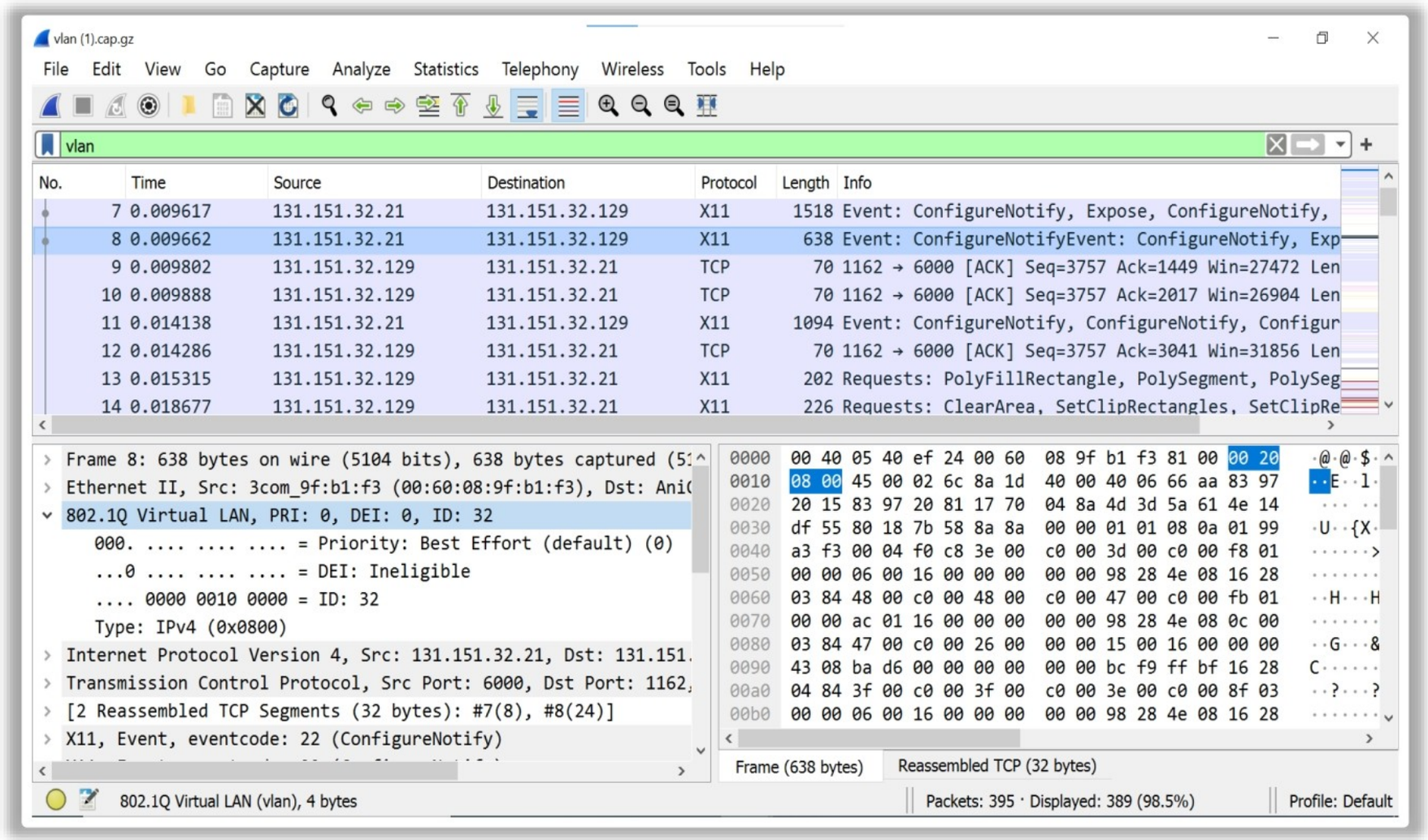
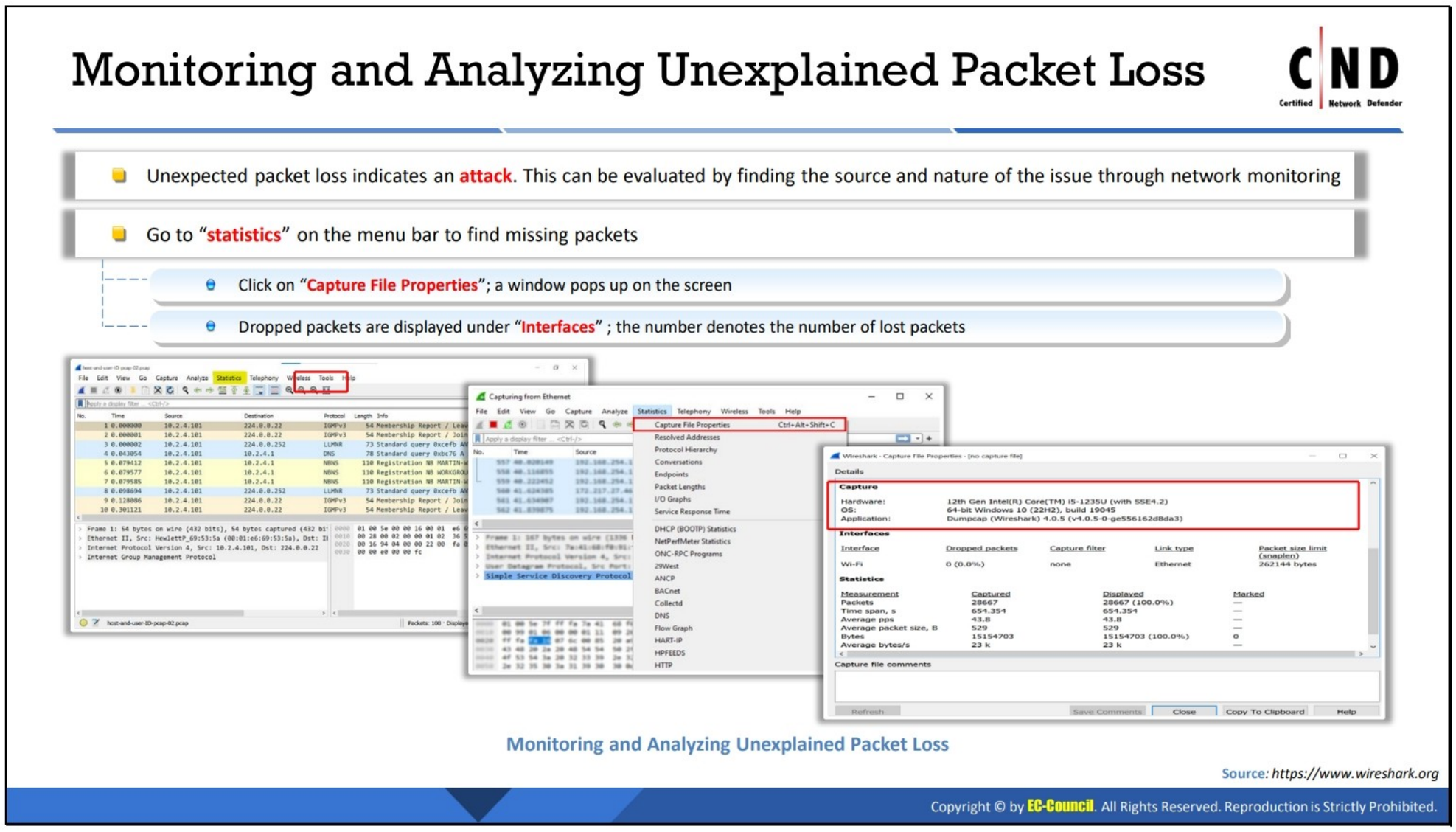


Figure 14.15: Identifying VLAN Hopping Traffic

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

https://t.me/learningnets

Technet24



Monitoring and Analyzing Unexplained Packet Loss

Monitoring and Analyzing Unexplained Packet Loss

Monitoring and analyzing unexplained packets is crucial for identifying network attacks, such as distributed denial of service (DDoS) attacks or packet injection attempts. Observing patterns of packet loss and scrutinizing the associated network traffic assists in detecting security incidents. This acts as an early warning system for potential attacks, enabling prompt responses to limit the damage to the organization.

Unexplained packet loss adversely affects network performance, leading to poor user experience, increased latency, and reduced throughput. By monitoring this unexplained packet loss, you can determine the nature of the attack and its impact on specific network segments or devices. This information is essential for taking necessary actions to enhance network performance.

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

https://t.me/learningnets

To determine if there are dropped packets using Wireshark,

- Click **Statistics** in the menu bar.

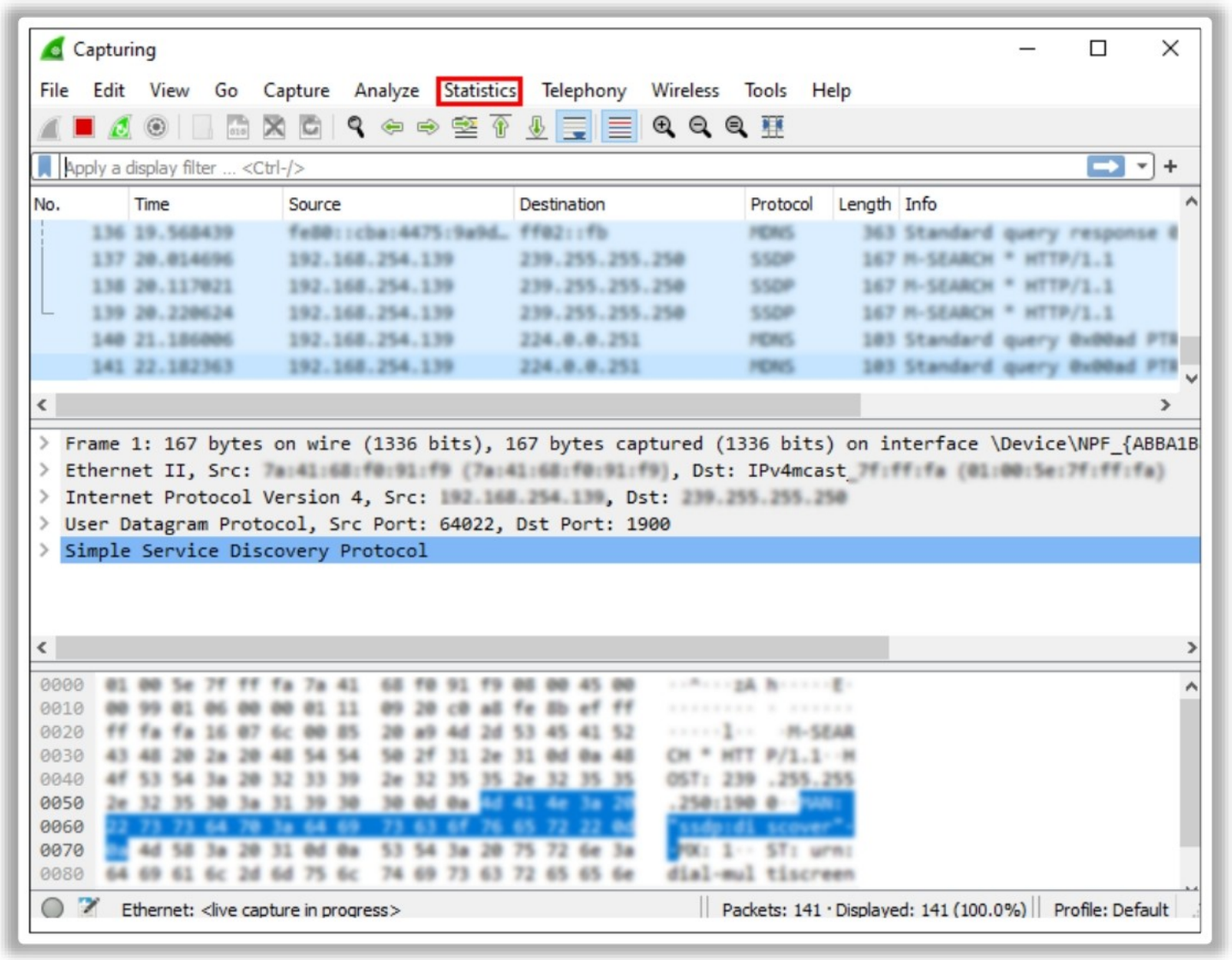


Figure 14.16: Wireshark – Capturing Mode

- Select **Capture File Properties**. A new window will open.

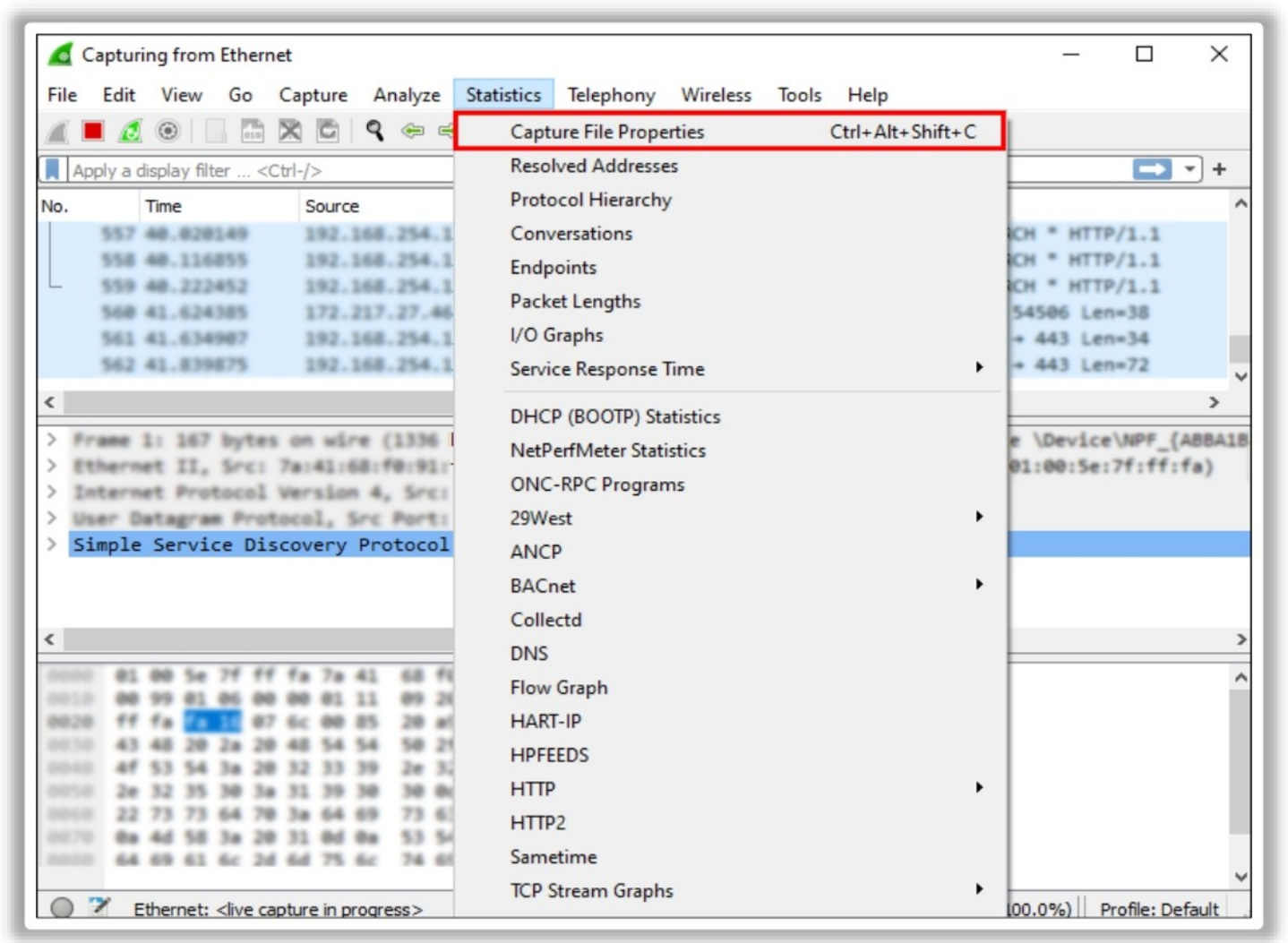


Figure 14.17: Wireshark – Capturing Dropped Packets

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

https://t.me/learningnets

Technet24

- Under **Interfaces**, see the **Dropped packets** and the number underneath it will tell how many packets were not captured.

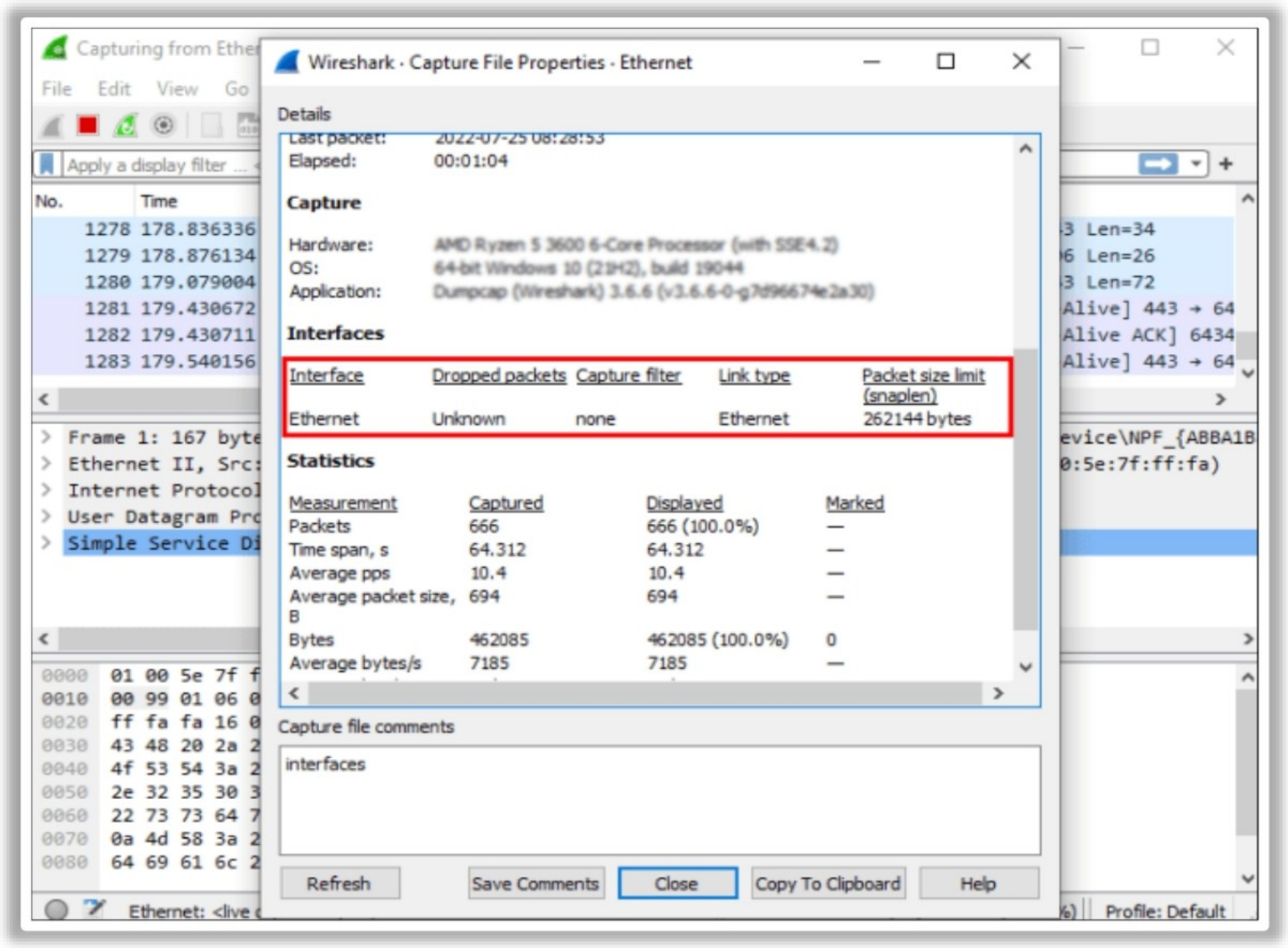
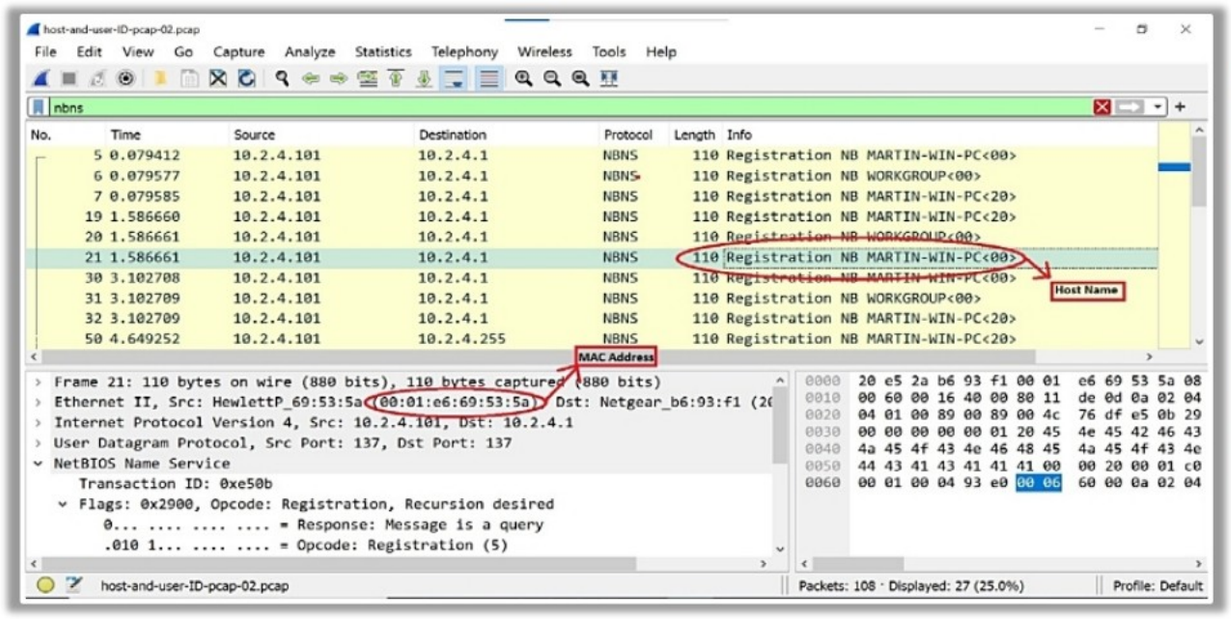


Figure 14.18: Wireshark – Capturing Dropped Packets

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

https://t.me/learningnets

Monitoring and Analyzing Host Information from NetBIOS Name Service (NBNS) Traffic



Monitoring and Analyzing Host Information

- NBNS is a **legacy protocol** used for NetBIOS name resolution, and its traffic can reveal valuable information about devices and hosts on the network. It gives information such as hostname on the network, IP/MAC addresses, and the services they are offering
- Monitoring NBNS traffic can help in host discovery, detecting rogue devices and in identifying **misconfigured devices**
- NBNS traffic works on **UDP/TCP** port 137
- Use the **nbns** filter to check host information from NETBIOS

Source: *https://www.wireshark.org*

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

Monitoring and Analyzing Host information from NetBIOS Name Service (NBNS) Traffic

NBNS (NetBIOS Name Service) is a protocol utilized for NetBIOS name resolution, which reveals significant information about network devices and hosts. It discloses critical details such as host names, IP and MAC addresses, and the services provided by these entities.

Monitoring NBNS traffic is crucial for network security, aiding in host discovery, detecting rogue devices, and identifying misconfigurations in network infrastructure. NBNS traffic, operating on UDP/TCP port 137, is a vital component of network communication.

Security experts often use specialized tools and filters, such as NBNS filters, to extract and analyze this data, uncovering essential details about the hosts in question. Utilizing NBNS, administrators enhance their ability to maintain network integrity and swiftly identify issues. In Wireshark, use the filter **NBNS** to examine host information from NETBIOS.

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

https://t.me/learningnets

Technet24

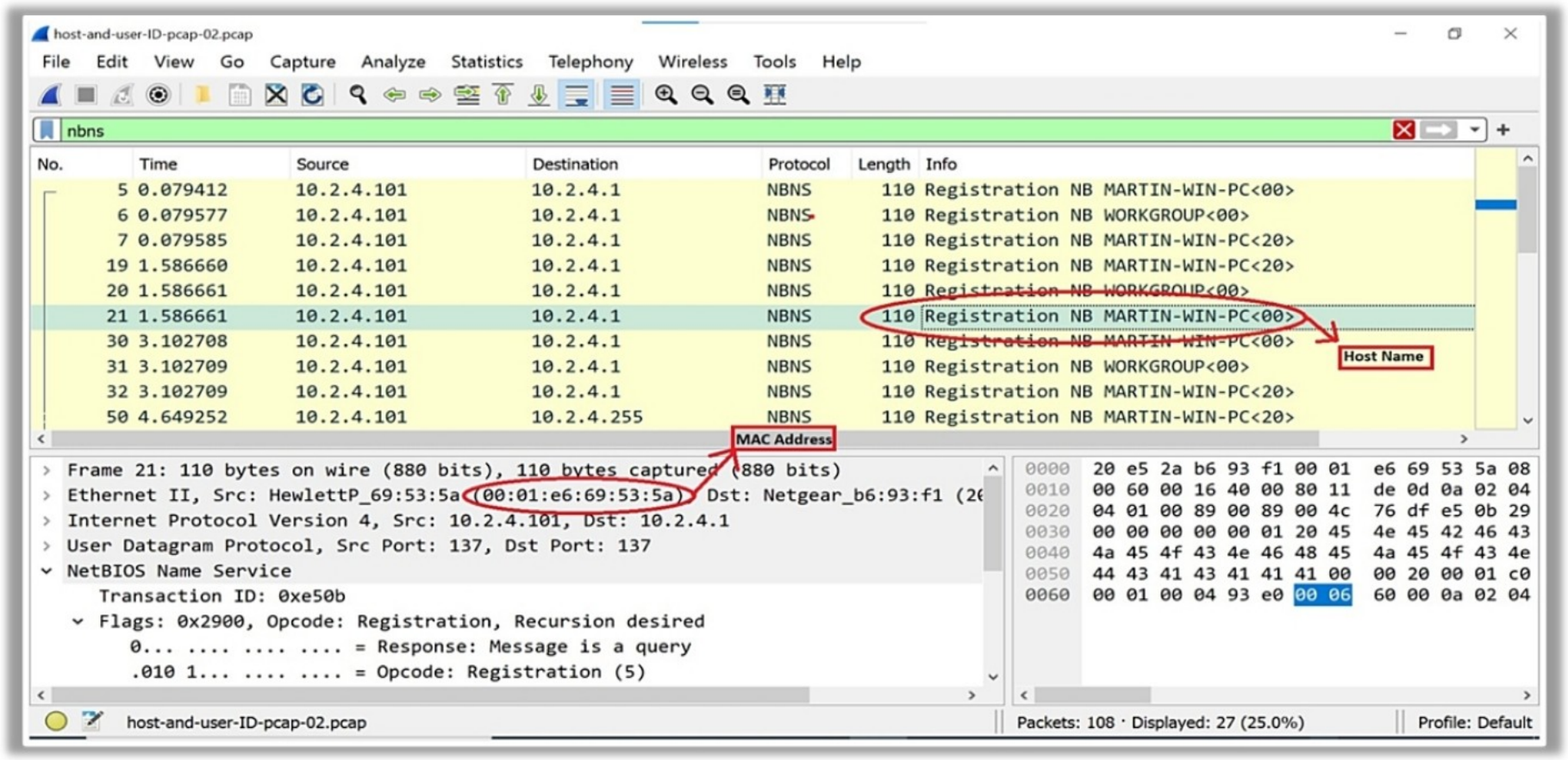
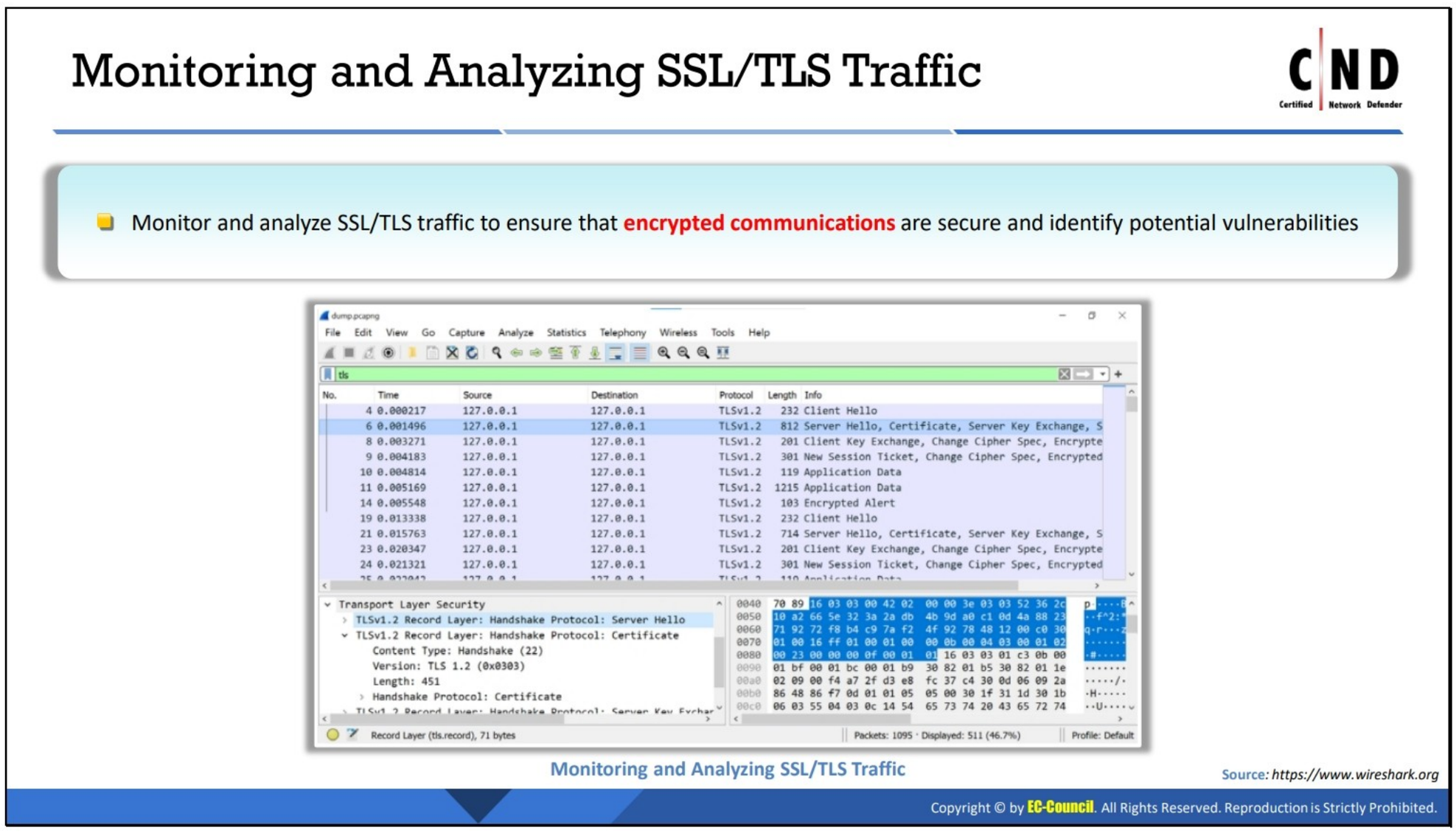


Figure 14.19: Identifying NBNS Traffic

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

https://t.me/learningnets



Monitoring and Analyzing SSL/TLS Traffic

Transport layer security (TLS) secures internet traffic by encrypting data transmitted over the internet, making it challenging for attackers to intercept and read. Secure Sockets Layer (SSL), its predecessor, is now considered insecure. To find a complete list of TLS display filter fields, use the "tls" filter in Wireshark. Remember, you cannot filter TLS protocols directly while capturing; instead, filter on the default TCP port 443.

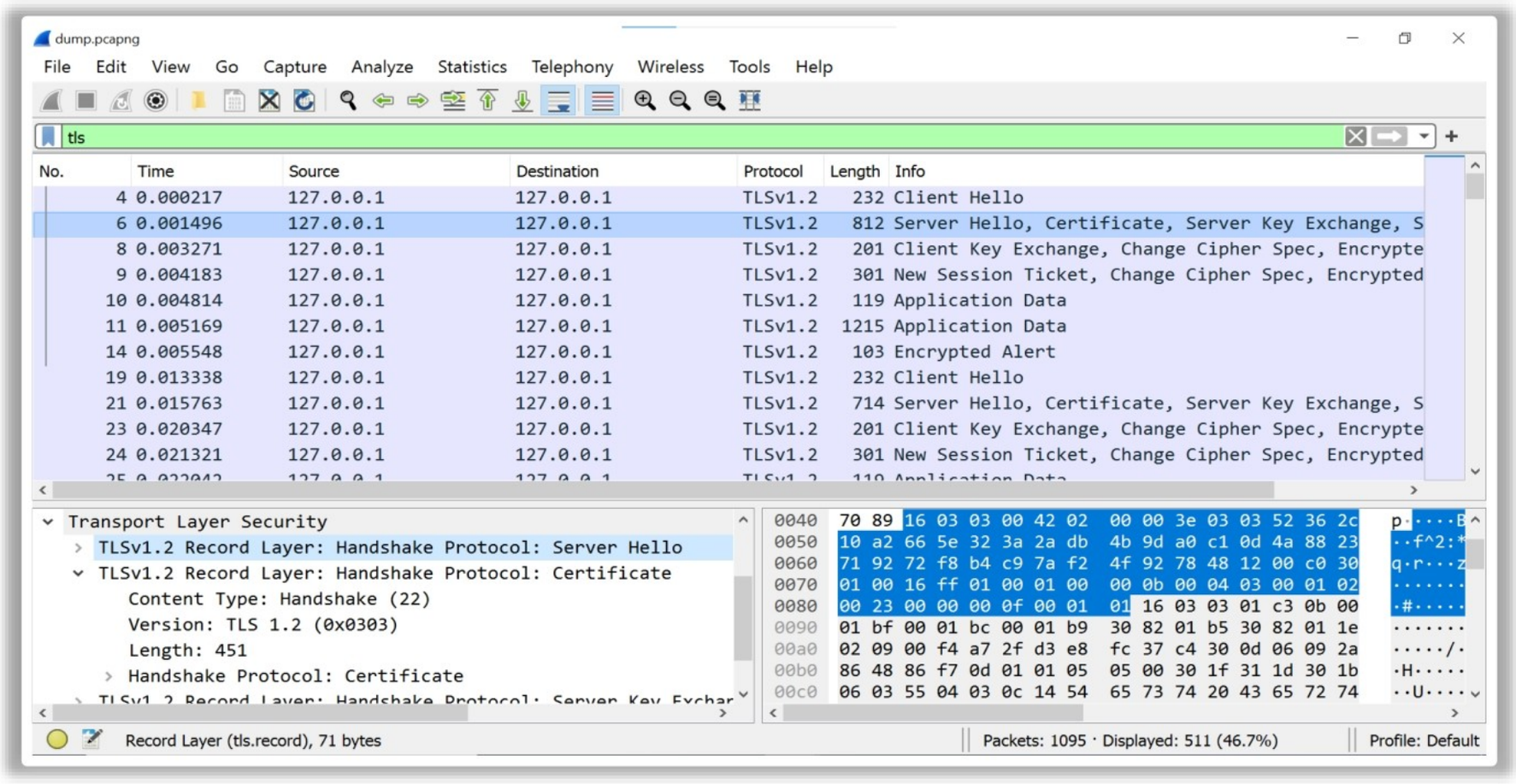


Figure 14.20: Identifying SSL/TLS Traffic

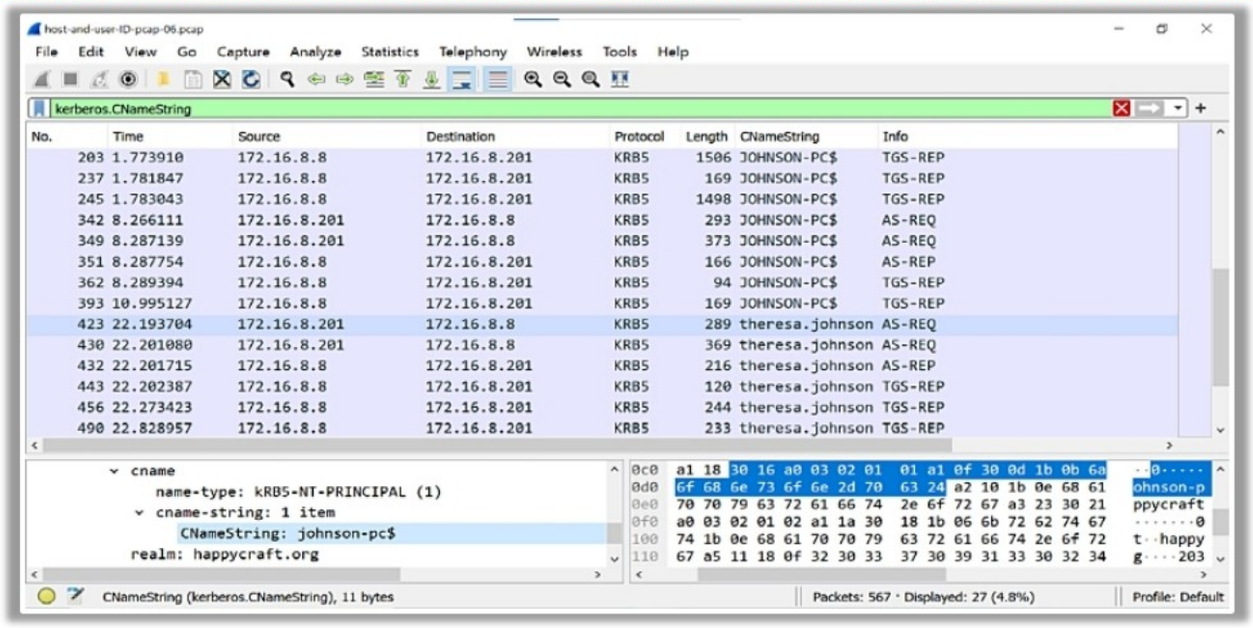
Certified Network Defender Copyright © by **EC-Council**
All Rights Reserved. Reproduction is Strictly Prohibited.

https://t.me/learningnets

Technet24

Monitoring and Analyzing Kerberos Traffic

- Monitor and analyze Kerberos traffic to detect potential security threats related to **Kerberos authentication**
- Apply the **kerberos.CNameString** filter in Wireshark to obtain a Windows/Linux user account and hostname



Monitoring and Analyzing Kerberos Traffic

Source: *https://www.wireshark.org*

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

Monitoring and Analyzing Kerberos Traffic

Kerberos is designed to provide secure authentication by encrypting authentication messages between clients and servers using shared secret keys. It facilitates mutual authentication between users and services in a network. The default port for Kerberos is 88. Monitoring and analyzing Kerberos traffic is crucial for identifying potential security issues, thereby enhancing the overall security of a network. In Wireshark, use the filter **'kerberos.CNameString'** to obtain a Windows/Linux user account and hostname.

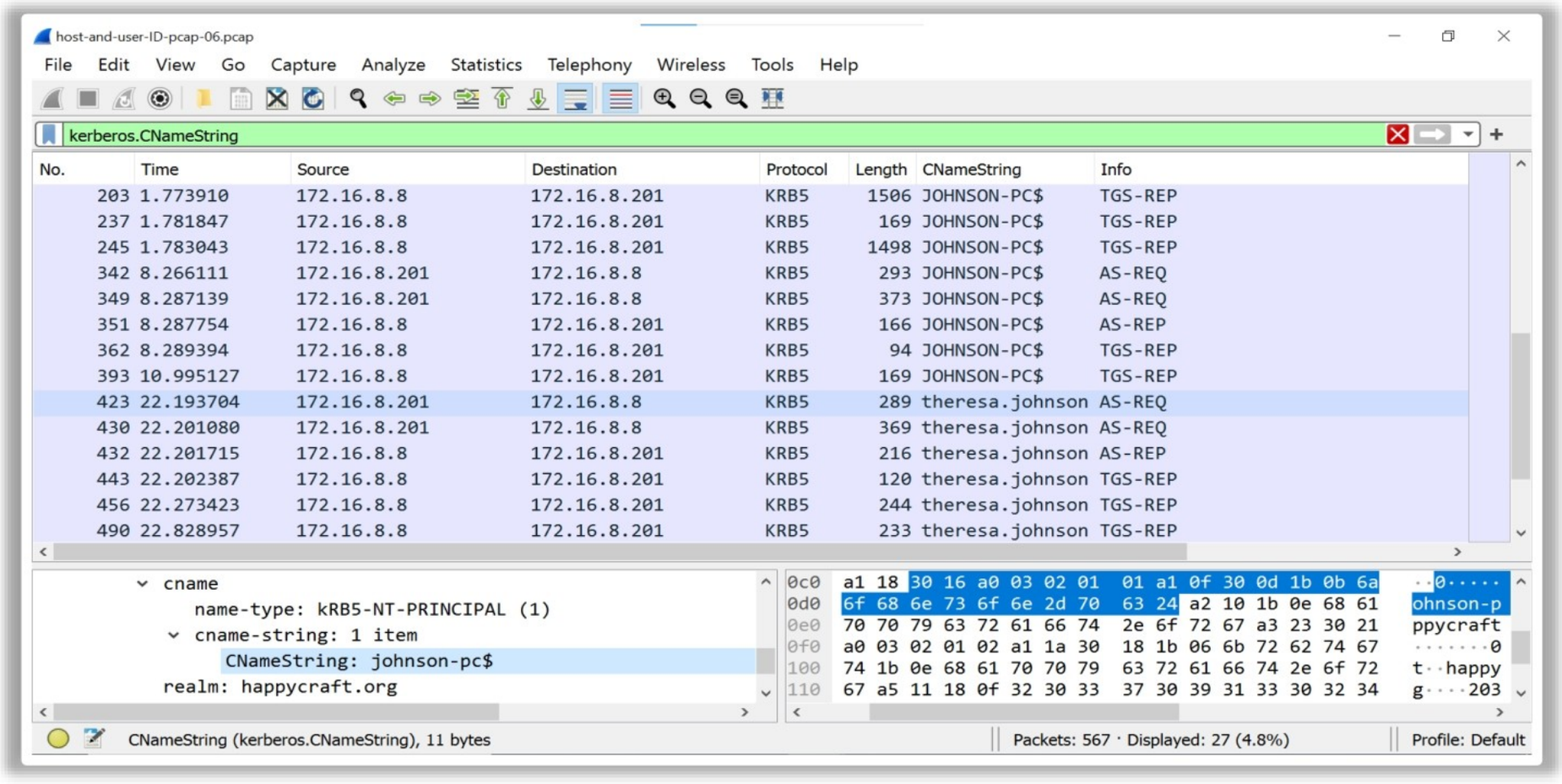
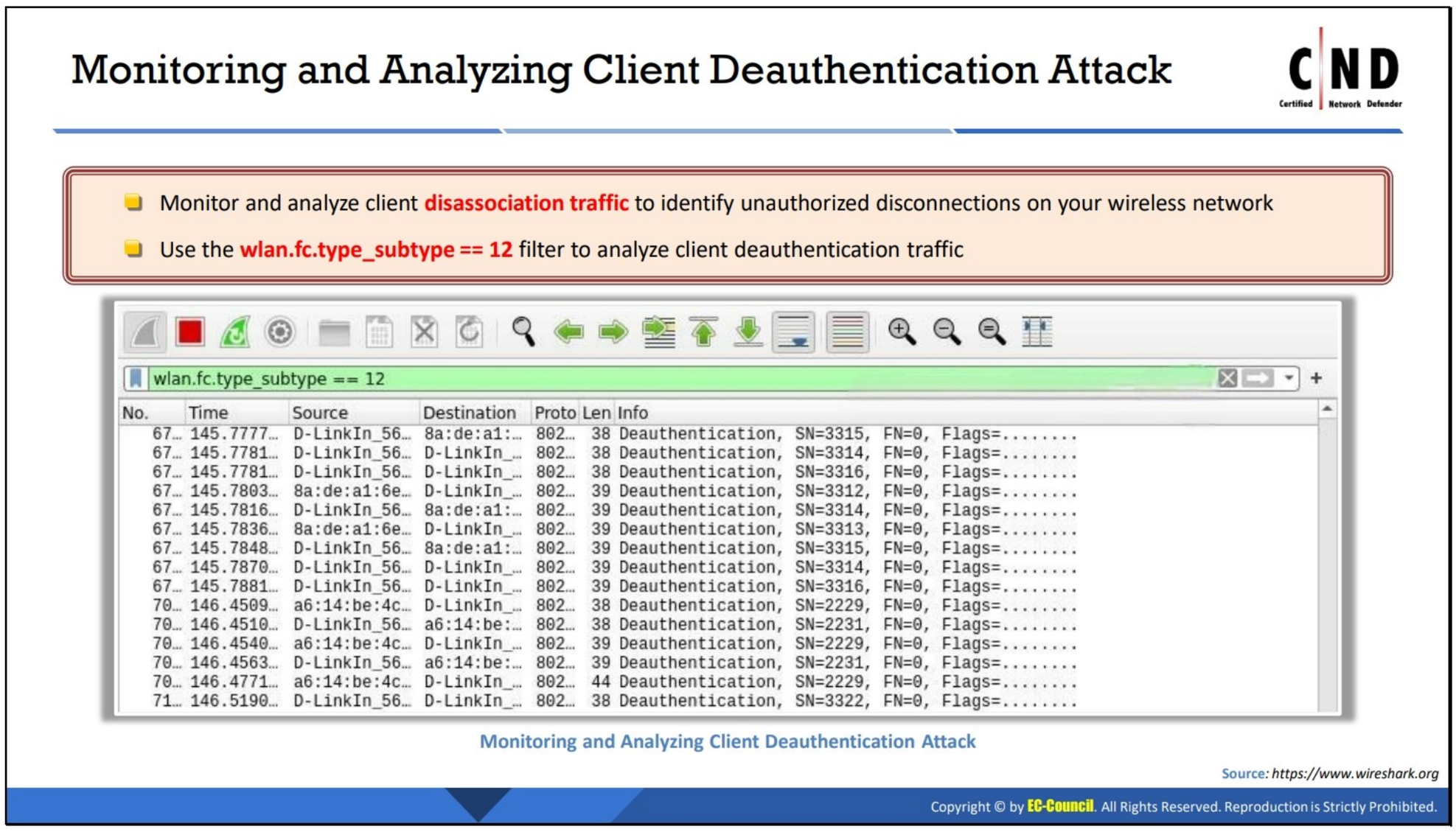


Figure 14.21: Identifying Kerberos Traffic

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

https://t.me/learningnets



Monitoring and Analyzing Client Deauthentication Attack

A client deauthentication attack is a wireless attack used to disconnect clients from a network by sending forged deauthentication frames. This attack can force clients to reconnect, potentially exposing sensitive authentication information like passwords. It can disrupt a wireless network, cause denial of service (DoS) for legitimate users, or enable other attacks such as man-in-the-middle.

To identify a client deauthentication attack, use the Wireshark filter **wlan.fc.type_subtype == 12**'. This filter captures deauthentication packets, allowing for the analysis of the information they contain. Wireshark captures and analyzes the 802.11 management frames sent during a deauthentication attack, revealing the source and destination MAC addresses of the attacker and victim devices, as well as the reason code for the deauthentication.

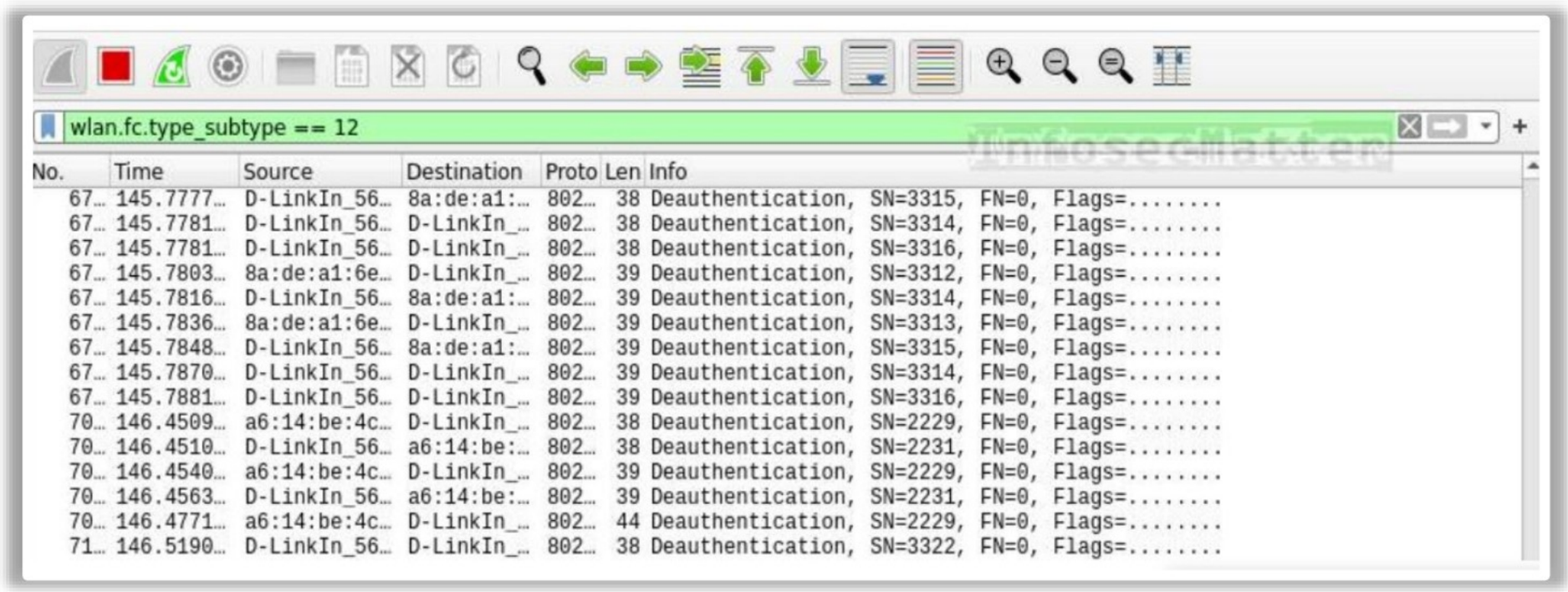
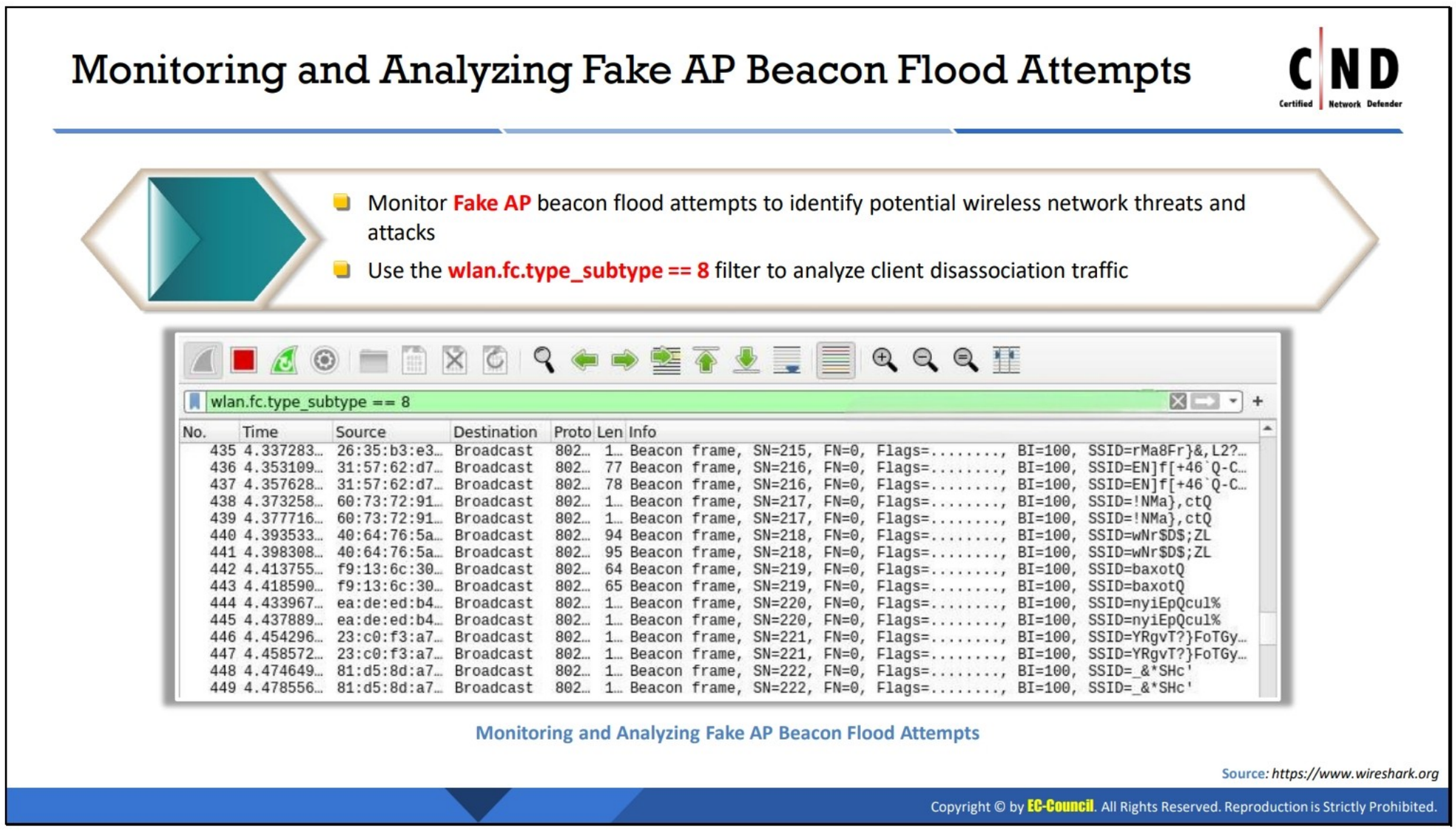


Figure 14.22: Identifying Deauthentication Traffic

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

https://t.me/learningnets

Technet24



Monitoring and Analyzing Fake AP Beacon Flood Attempts

The fake AP beacon flood is an attack where an attacker transmits a large number of false beacon frames within the wireless range of a targeted Wi-Fi network. These frames, normally used by Wi-Fi devices to find and connect to networks, can be overrun by the attacker's false frames. This leads to confusion among devices and potentially disables wireless connectivity. The attack floods the area with fake access point beacons, causing connectivity issues (jamming) or even crashing some clients' networks (DoS), ultimately leading to a network crash.

Monitoring and analyzing fake AP beacon flood attempts is crucial for identifying vulnerabilities in a wireless network. It aids in recognizing weak security setups, understanding attack patterns, and implementing additional security measures for protection. In Wireshark, use the filter wlan.fc.type_subtype == 8 to analyze client Disassociation traffic, which is instrumental in identifying such attacks.

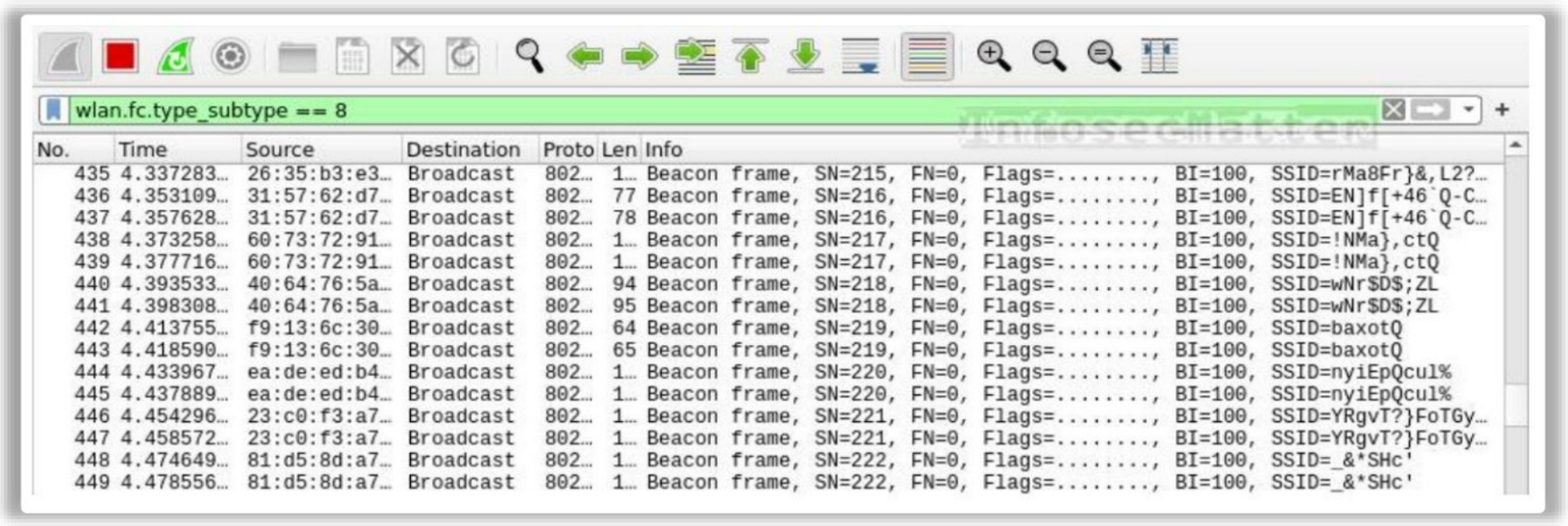
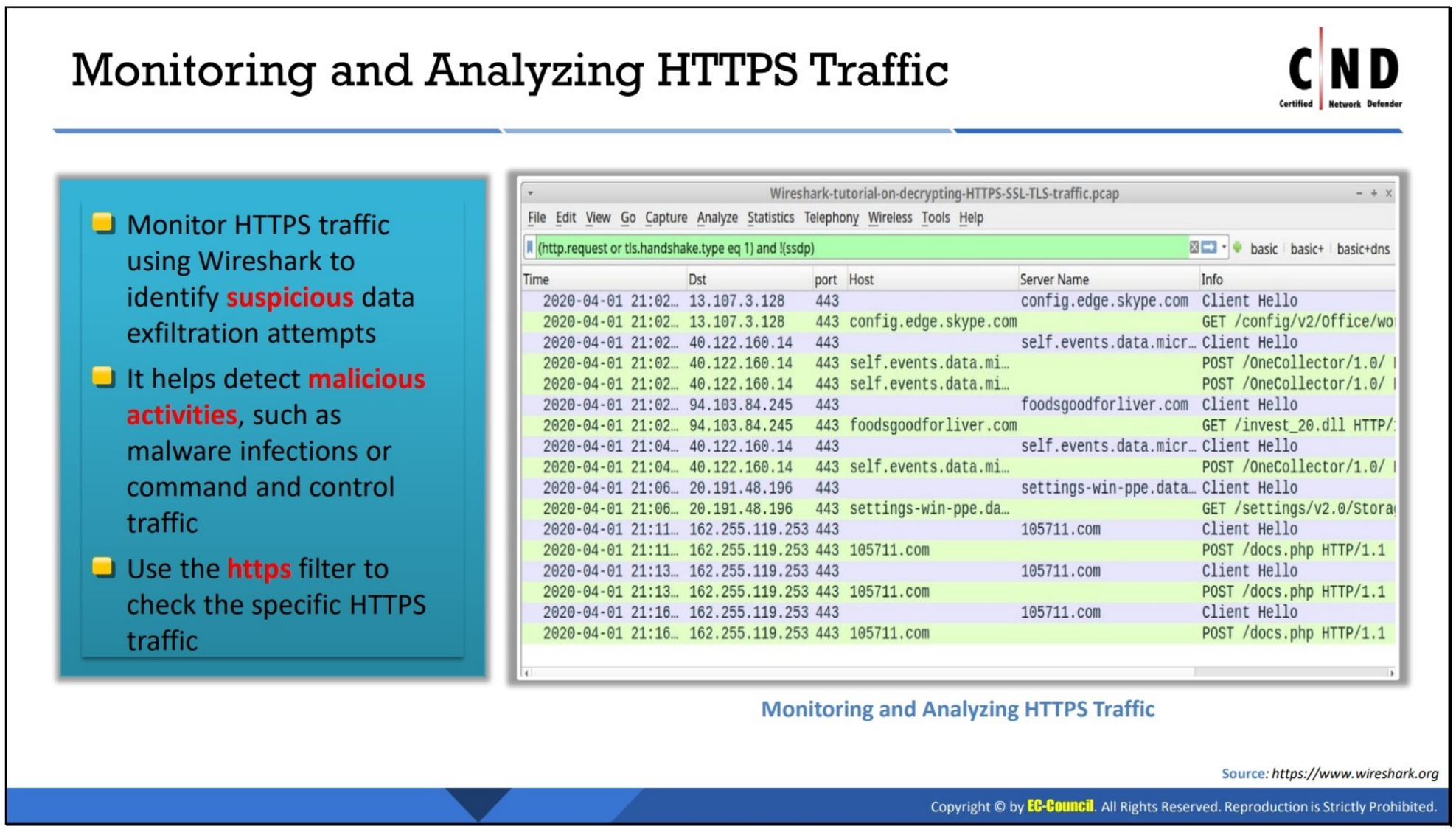


Figure 14.23: Identifying Fake AP beacon Traffic

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

https://t.me/learningnets



Monitoring and Analyzing HTTPS Traffic

Hypertext Transfer Protocol Secure (HTTPS) secures the communication between a user's website and web browser within a network. HTTPS traffic typically operates on port 443. In Wireshark, while it is impossible to directly analyze the content of encrypted HTTPS communications, you can still monitor metadata like source/destination IP addresses, ports, packet sizes, and timing details, which can provide valuable insights.

If you are using a proxy server, decrypting the traffic with the proxy's SSL/TLS keys is possible. Poorly encrypted HTTPS traffic is vulnerable to attacks, potentially allowing attackers to perform man-in-the-middle attacks and intercept network traffic.

Monitoring and analyzing HTTPS traffic is crucial for several reasons: to ensure sensitive information is not sent over HTTP, to detect malicious traffic, to check compliance with policy violations, and to identify applications using unnecessary or restricted services. In Wireshark, use the filter https to examine specific HTTPS traffic.

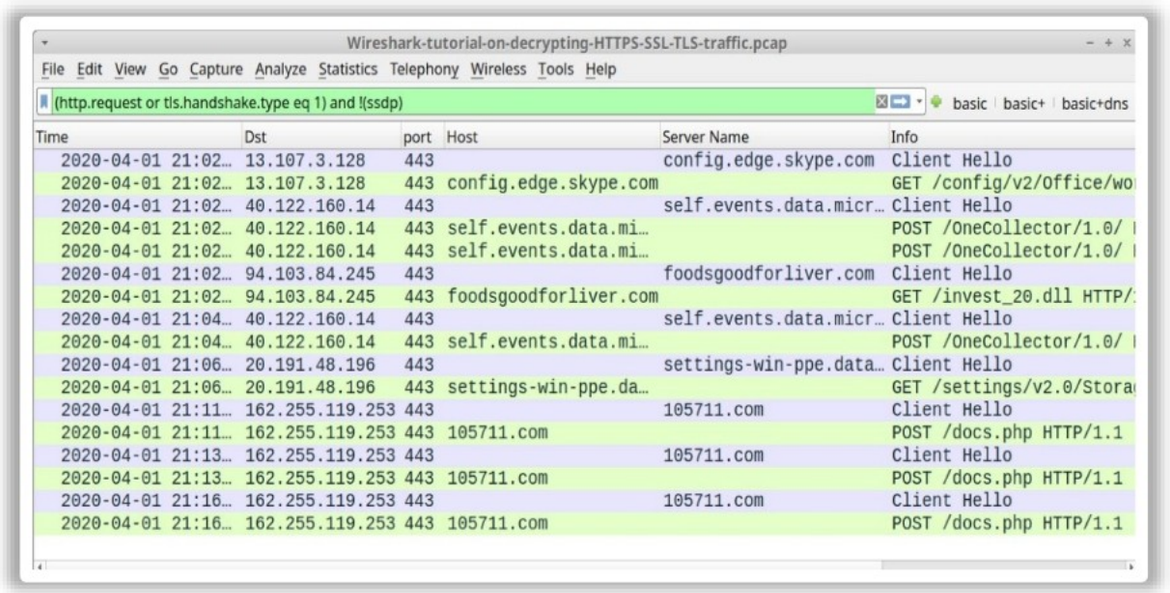
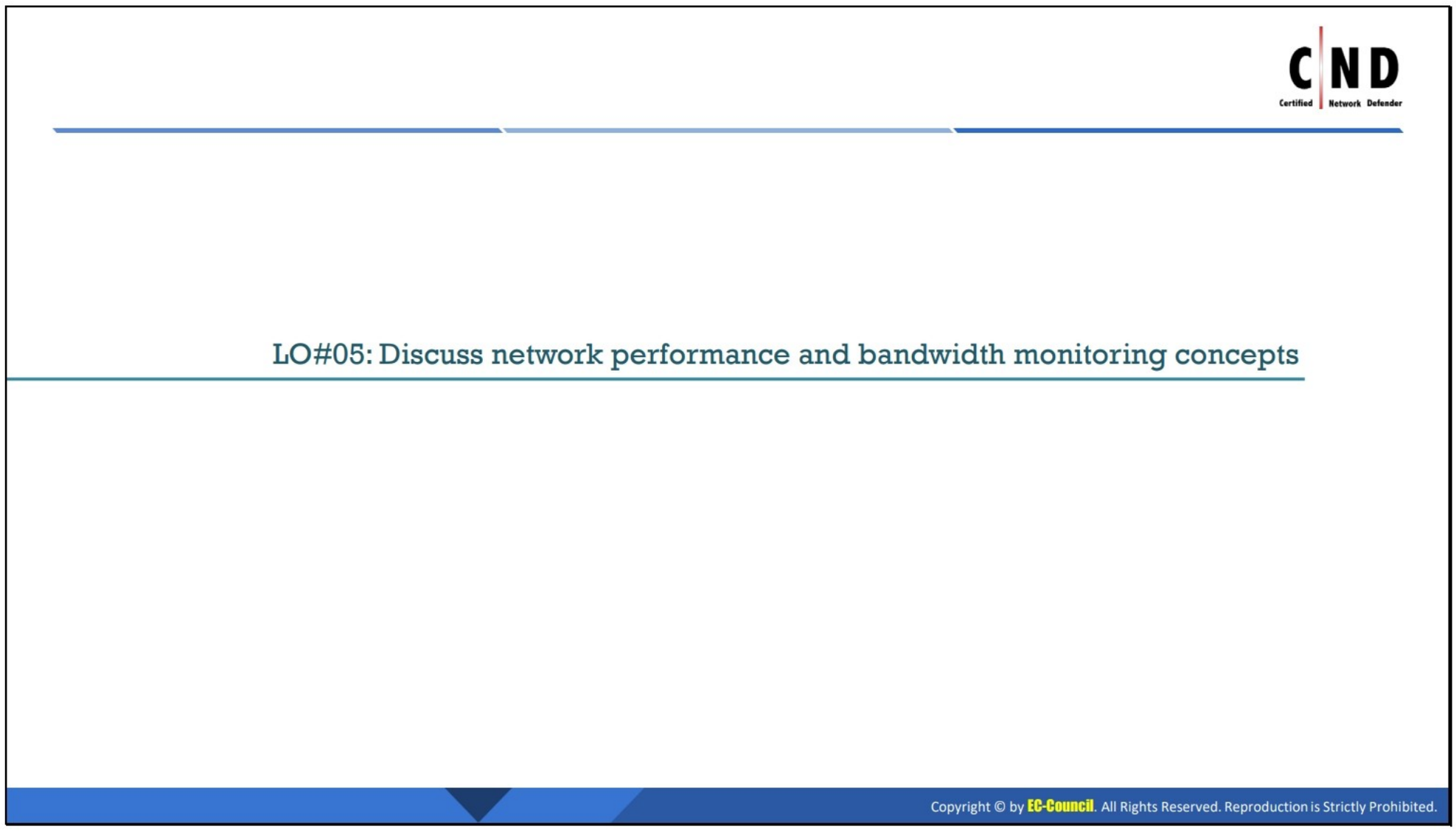


Figure 14.24: Filtering HTTPS Traffic

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

https://t.me/learningnets

Technet24

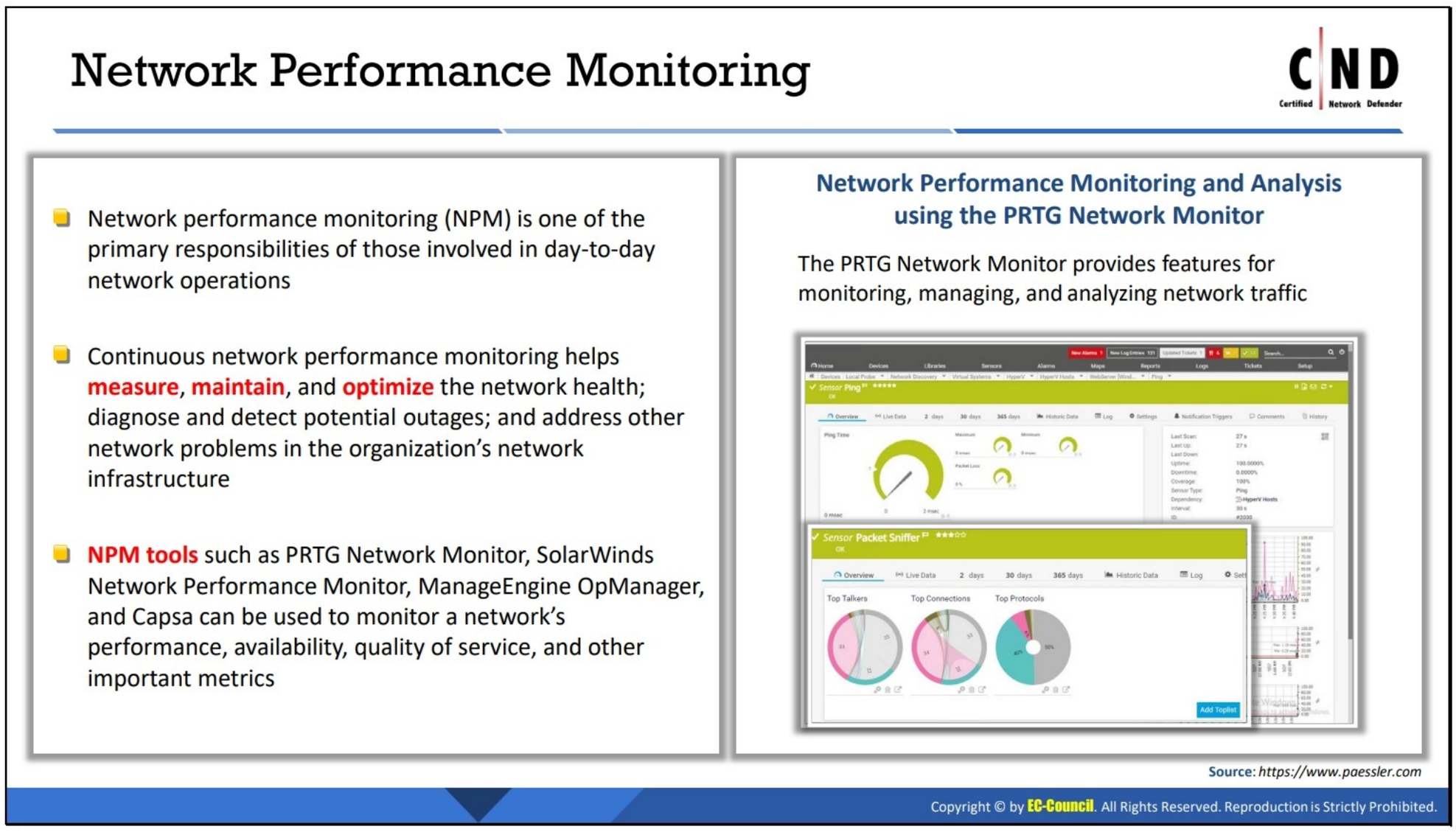


LO#05: Discuss Network Performance and Bandwidth Monitoring Concepts

The objective of this section is to explain how to monitor network performance and bandwidth. It describes various network performance and bandwidth monitoring tools as well as best practices for bandwidth monitoring.

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

https://t.me/learningnets



Network Performance Monitoring

Network performance monitoring is one of the primary responsibilities of those involved in day-to-day network operations. Continuous network performance monitoring helps measure, maintain, and optimize network health; diagnose and detect potential outages; and address other network problems in the organization's network infrastructure.

Network performance monitoring tools such as PRTG Network Monitor, SolarWinds Network Performance Monitor, ManageEngine OpManager, and Capsa can be used to monitor a network's performance, availability, quality of service, and other important metrics.

PRTG Network Monitor

Source: https://www.paessler.com

PRTG Network Monitor is a network monitoring software that supports remote management using any web browser or smartphone, various notification methods, and the monitoring of multiple locations. Network defender can use this utility for availability, usage, and activity monitoring, and it covers the entire range from website monitoring to database performance monitoring.

It helps in the following:

- Avoid bandwidth and performance bottlenecks.
- Identify applications or servers using up the available bandwidth.
- Instantly identify sudden spikes caused by malicious code.
- Reduce the costs of purchasing additional hardware and bandwidth.

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

https://t.me/learningnets

Technet24

PRTG can collect data for almost anything of interest on the network. It supports multiple protocols for collecting data:

- Simple Network Management Protocol (SNMP) and Windows Management Instrumentation (WMI)
- Packet sniffing
- NetFlow, IP Flow Information Export (IPFIX), jFlow, and sFlow

SolarWinds Network Performance Monitor

Source: https://www.solarwinds.com

SolarWinds Network Performance Monitor (NPM) is a network monitoring software that can be used to quickly detect, diagnose, and resolve network performance problems and outages.

ManageEngine OpManager

Source: https://www.manageengine.com

ManageEngine OpManager is an integrated network management software that provides real-time network monitoring and offers detailed insights into various problematic areas of a network.

Capsa Free Network Analyzer

Source: http://www.colasoft.com

Capsa is a network performance analysis and diagnostics tool that can be used to perform comprehensive packet capture and analysis.

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

https://t.me/learningnets

Bandwidth Monitoring

- Bandwidth is the amount of **information** that can be transmitted over a network in a given amount of time
- Network bandwidth **selection** plays a vital role in the design, maintenance, and performance of an organization's network
- Poor bandwidth management leads to network **congestion** and **poor performance** of the network

- Bandwidth monitoring involves **measuring** and **controlling** the traffic on a network link to avoid the overfilling of the link
- The following are factors for measuring bandwidth:
  - Determine the **amount** of available network bandwidth
  - Determine the **average** utilization required by a specific application

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

Bandwidth Monitoring (Cont'd)

- Understand the bandwidth and **resource consumption** for better network management
- Use bandwidth monitoring tools such as PRTG Bandwidth Monitor, SolarWinds Bandwidth Monitor, and ManageEngine Bandwidth Monitor to measure the bandwidth of the network link

- Focus on the following considerations to **decrease** the bandwidth requirements:
  - Server-side computing
  - Data caching
  - Data compression
  - Latency mitigation
  - Loss mitigation

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

Bandwidth Monitoring

The bandwidth is the amount data that can be transferred from one point to another. It is one of the criteria defining network performance. An effective bandwidth is one that provides the highest transmission rate. A bandwidth monitoring test identifies the maximum throughput of a system. Bandwidth monitoring tools provide the output of real-time network traffic for any

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

https://t.me/learningnets
Technet24

device. The tools provide bandwidth information at the interface and device levels. A low detected bandwidth indicates poor network functioning.

An organization works on two types of bandwidth speed: upload and download. The speed at which data are sent to a destination is called the upload speed. The speed at which data are received is called the download speed. With growing networks and huge volumes of data, organizations have started to maximize their upload and download speeds.

It is also important to consider the bandwidth capacity of a network, which involves the maximum data transfer rate of a link. With hundreds of users in a network, it is important to know the bandwidth required per day. Although it can be a tedious job for administrators to determine the bandwidth usage per day, a blueprint of the usage can help draft a proper bandwidth monitoring plan.

Bandwidth monitoring includes the monitoring of various bandwidth utilizations that are implemented in the organization. Many software tools can be used to monitor bandwidth in real time. Bandwidth monitoring has the following benefits:

- Bandwidth monitoring helps determine the network utilization of the system. Systems using high bandwidth amounts should be monitored closely as they may be performing suspicious activities or may have become a victim of suspicious activity.
- High amounts of network traffic lead to network congestion and affect the functioning of the organization. Deploying a network limit will raise an alarm when the network is about to reach the maximum bandwidth.
- If the network congestion is high, depending on the size of the organization, additional links can be added to the network. An additional link in the network will boost the network performance, reducing the network congestion.

The following set of tools can be used for bandwidth monitoring.

PRTG Bandwidth Monitor

Source: https://www.paessler.com

PRTG Bandwidth Monitor analyzes the traffic in a network and provides detailed results including tables and graphs. It monitors network devices, bandwidth, servers, applications, virtual environments, remote systems, IoT, and many more.

SolarWinds Real-Time Bandwidth Monitor

Source: http://www.solarwinds.com

With SolarWinds Real-Time Bandwidth Monitor, critical and warning thresholds can be set so that the administrator is instantly notified when usage is out of bounds.

ManageEngine Bandwidth Monitor

Source: https://www.manageengine.com

The ManageEngine Bandwidth Monitor tool shows the real-time network traffic of any SNMP device. It provides bandwidth usage details on both interface and device levels. It uses SNMP to

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

https://t.me/learningnets

fetch the bandwidth utilization details of a network interface. The details on the bandwidth utilization of a device includes a comparison of the individual traffic and its interfaces.

tbbMeter

Source: http://www.thinkbroadband.com

tbbMeter is a bandwidth meter that monitors Internet usage. It shows how much data a computer sends to and receives from the Internet in real time. It also shows how the Internet usage varies at different times of the day.

BandwidthD

Source: https://sourceforge.net

BandwidthD monitors the amount of data being received/transmitted by specific machines and/or subnets. It tracks the usage of TCP/IP network subnets and builds HTML files with graphs to display utilization.

NetWorx

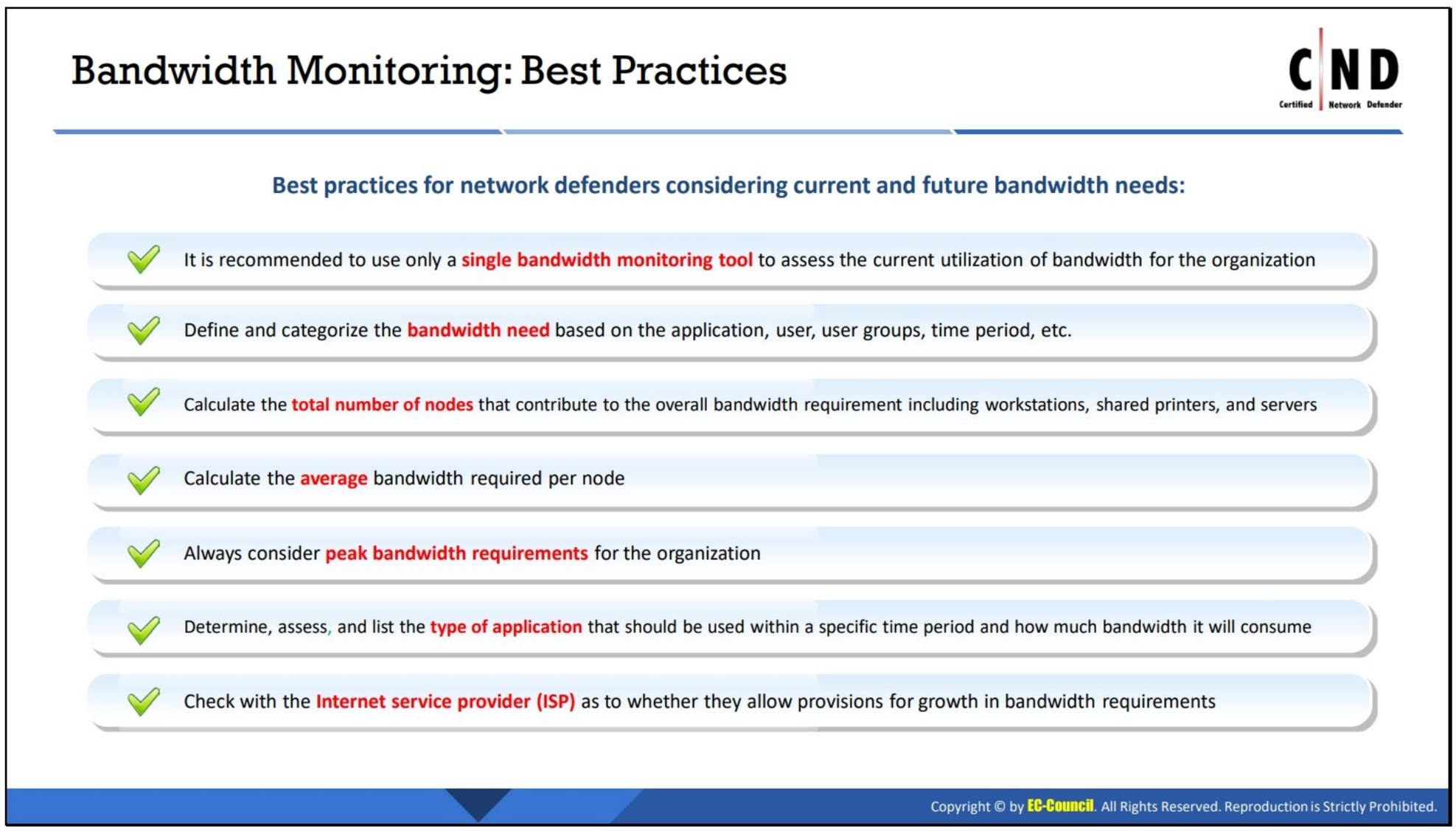
Source: https://www.softperfect.com

NetWorx monitors all the network connections or a specific network connection such as wireless or mobile broadband. The incoming and outgoing traffic is represented on a line chart and logged into a file such that the statistics about the daily, weekly, and monthly bandwidth usage and dial-up duration can always be viewed. The reports can be exported to a variety of formats such as HTML, Microsoft Word, and Microsoft Excel for further analysis.

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

https://t.me/learningnets

Technet24



Bandwidth Monitoring: Best Practices

Organizations should follow certain rules to increase bandwidth usage in their environment. The rules below depend on the size and requirement of the organization.

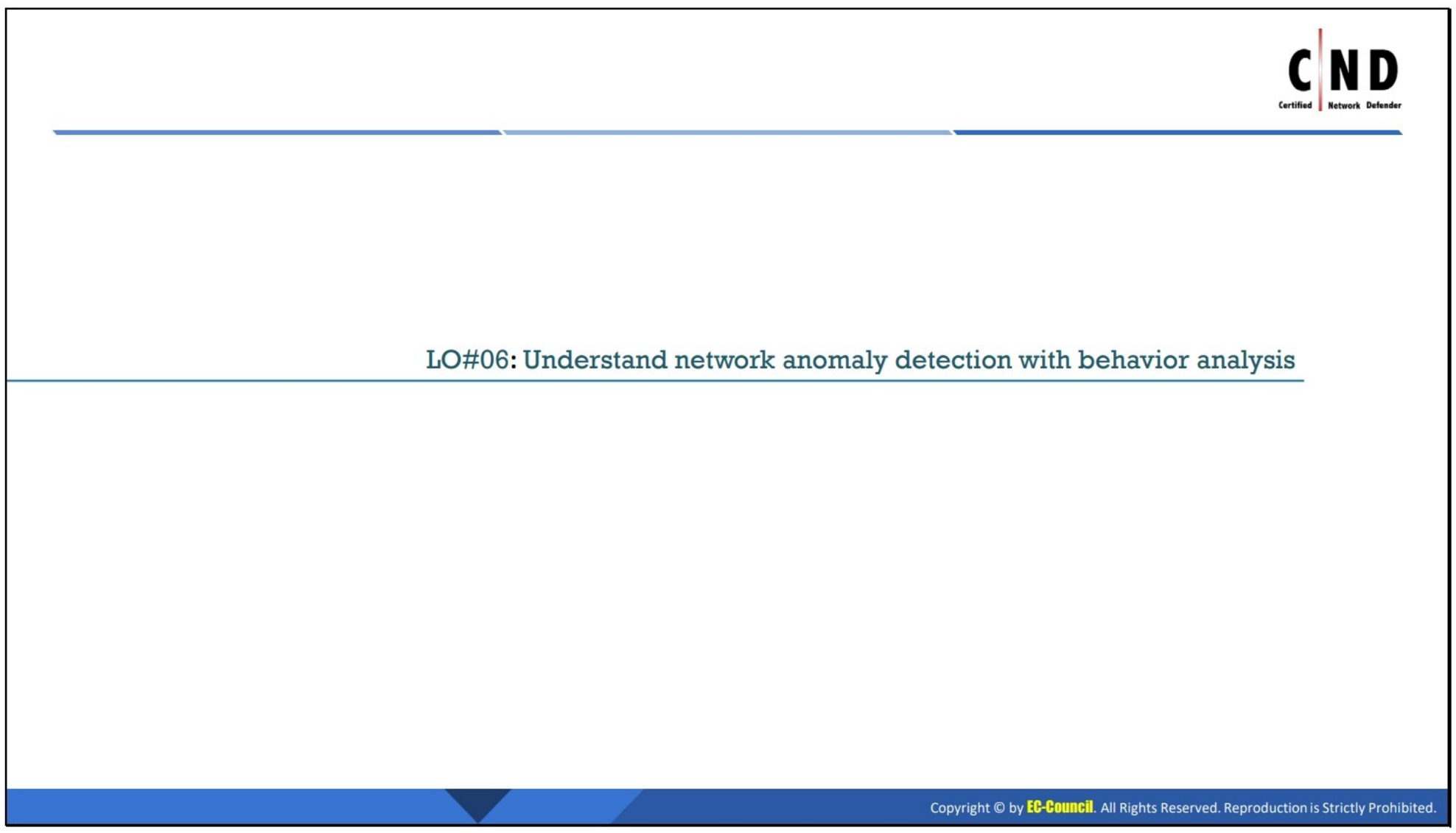
- **Limited use of media sites:** Organizations can limit their employees' access to media services such as online gaming, movies, and music. This will enhance the upload as well as download speed of the overall network.
- **Proxy cache:** When a user visits a website for the first time, the content of the site is saved (cached) on the proxy server. If the user visits the same website again, the content does not have to be downloaded again.
- **QoS:** Quality of service (QoS) is a bandwidth reservation mechanism. Since certain applications require additional bandwidth, administrators can configure the QoS for these applications. Consequently, if a user accesses these applications in the future, the QoS bandwidth will be utilized. Utilizing the QoS bandwidth will not affect the bandwidth usage for other users in the network.

In addition to above bandwidth usage recommendations, the following best practices can also be helpful in effective bandwidth monitoring:

- Provide timely education or training to employees on excessive bandwidth consumption to create awareness among them concerning bandwidth usage.
- Monitor the traffic consumed by the network components in the organization.
- Implement a QoS policy to prioritize bandwidth usage as per application requirements.
- Optimize the WAN capacity to increase the network bandwidth.
- Backup the devices configured on the network. During a power failure or network failure, these backups act as a good configuration and keep the bandwidth stable.

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

https://t.me/learningnets



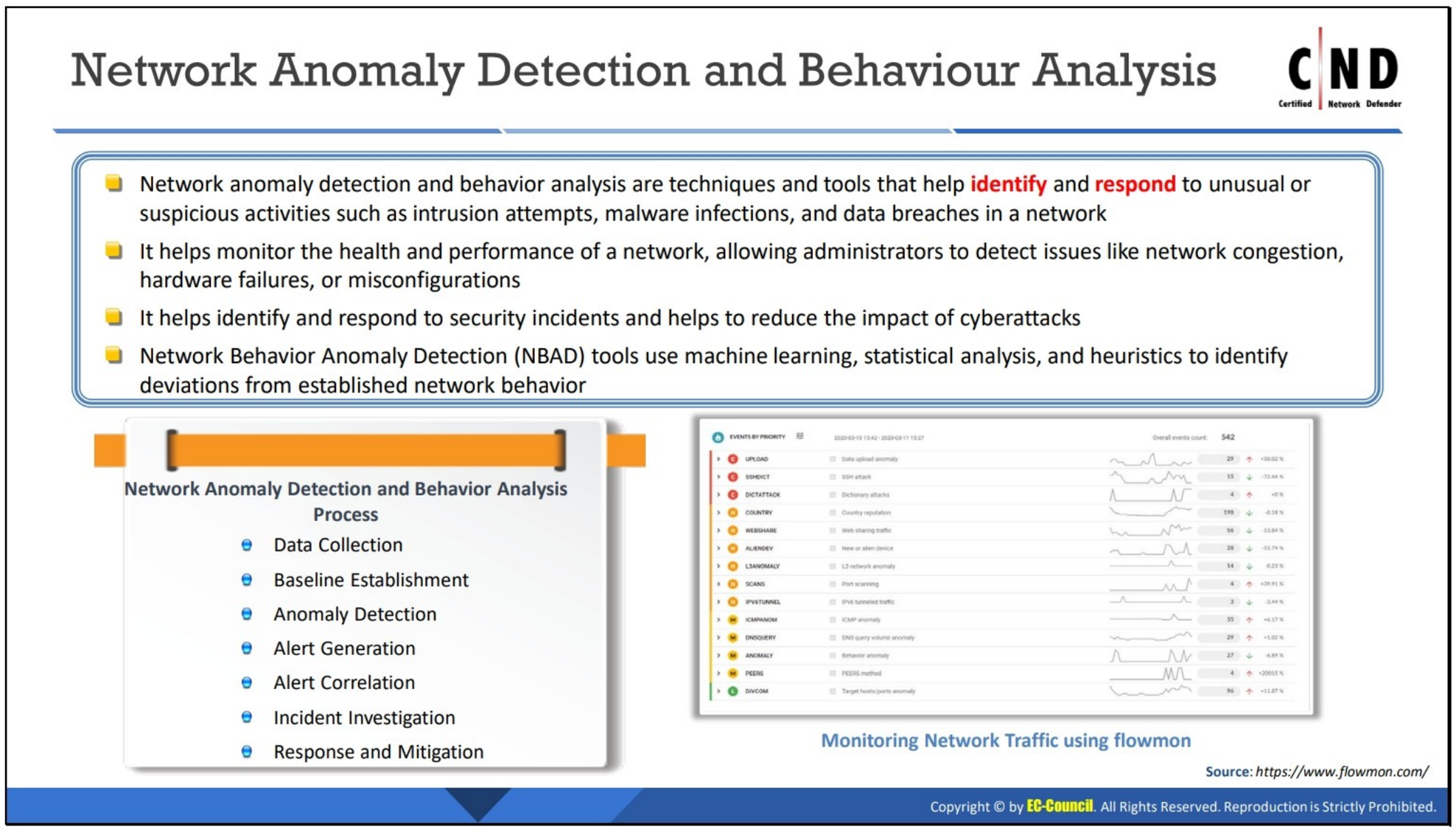
LO#06: Understand Network Anomaly Detection with Behavior Analysis

Understand the role of network anomaly detection and behavior analysis (NADBA) in network monitoring and security. NADBA plays a crucial role in identifying abnormal or suspicious activities within a network. It helps organizations detect and respond to security incidents by identifying patterns or deviations from normal network behavior. NADBA aids in maintaining the integrity, availability, and security of networks. These systems are often complemented by other security measures, such as firewalls, intrusion detection systems (IDS), and intrusion prevention systems (IPS), to provide comprehensive network protection.

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

https://t.me/learningnets

Technet24



Network Anomaly Detection and Behavior Analysis

A network anomaly is a sudden and brief deviation from the normal operation of a network, often caused by intruders with malicious intent. Network Anomaly Detection is a security technique that monitors the network for abnormal behavior, relying on network behavior analysis. These tools, used in addition to perimeter security systems like firewalls and antivirus software, provide an extra layer of security. They detect suspicious activities that could compromise network operations through data theft, hidden infections, or system infection. Network Anomaly Detection operates by identifying abnormal network behaviors, such as high traffic flow, intrusion attempts, malware infections, and data breaches.

Administrators are tasked with detecting various issues in networks, such as congestion, misconfigurations, and hardware failures, to maintain the health and performance of the network. Keen monitoring ensures efficiency and accuracy. Network anomaly detection and behavior analysis (NBAD) plays a vital role in detecting network behavior anomalies on a large scale by keeping track of packets, bandwidth, bytes, traffic volume, and protocol usage. Every suspicious event is recorded in a report with its timestamp, relevant ports, protocols, and originating and destination IP addresses. NBAD focuses on three crucial aspects: traffic flow patterns, passive traffic analysis, and network performance data, to identify a range of threats. It employs machine learning, statistical analysis, and heuristics to pinpoint abnormal behavior and deviations from established network norms.

The process for Network Anomaly Detection and Behavioral Analysis involves several key steps:

- **Data collection:** This involves collecting and analyzing data from multiple sources to understand and analyze trends.

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

https://t.me/learningnets

- **Baseline Establishment:** Establishing a baseline over a longer period improves accuracy and usefulness of the collected behavior data, aiding in analyzing the current situation.
- **Anomaly detection:** This step involves identifying factors such as data points, events, and observations that deviate from the expected dataset behavior.
- **Alert Generation:** When suspicious activities are detected within the environment, notifications are sent out.
- **Alert correlation:** This process involves collecting multiple alerts, warnings, and notifications and correlating them to understand the larger scope of the situation.
- **Incident Investigation:** This is the process of identifying the reasons and root cause of any detected security breach.
- **Response and mitigation:** The response strategy is structured to react to threats, while mitigation involves processes to limit the impact of the threat.

Network behavior anomaly detection (NBAD) tools leverage machine learning, statistical analysis, and heuristics to identify deviations from established network behavior.

Example NBAD tool: flowmon

Source: https://www.flowmon.com/

Flowmon NBAD provides insights into network activities, enabling detection and response to targeted attacks, botnets, unknown malware, insider threats, data leakage, and more. It utilizes network traffic statistics exported by routers, switches, or network probes. These statistics are gathered using various flow data standards such as NetFlow, jFlow, IPFIX, and NetStream. By analyzing this data, Flowmon NBAD can effectively detect malicious behavior within the network.

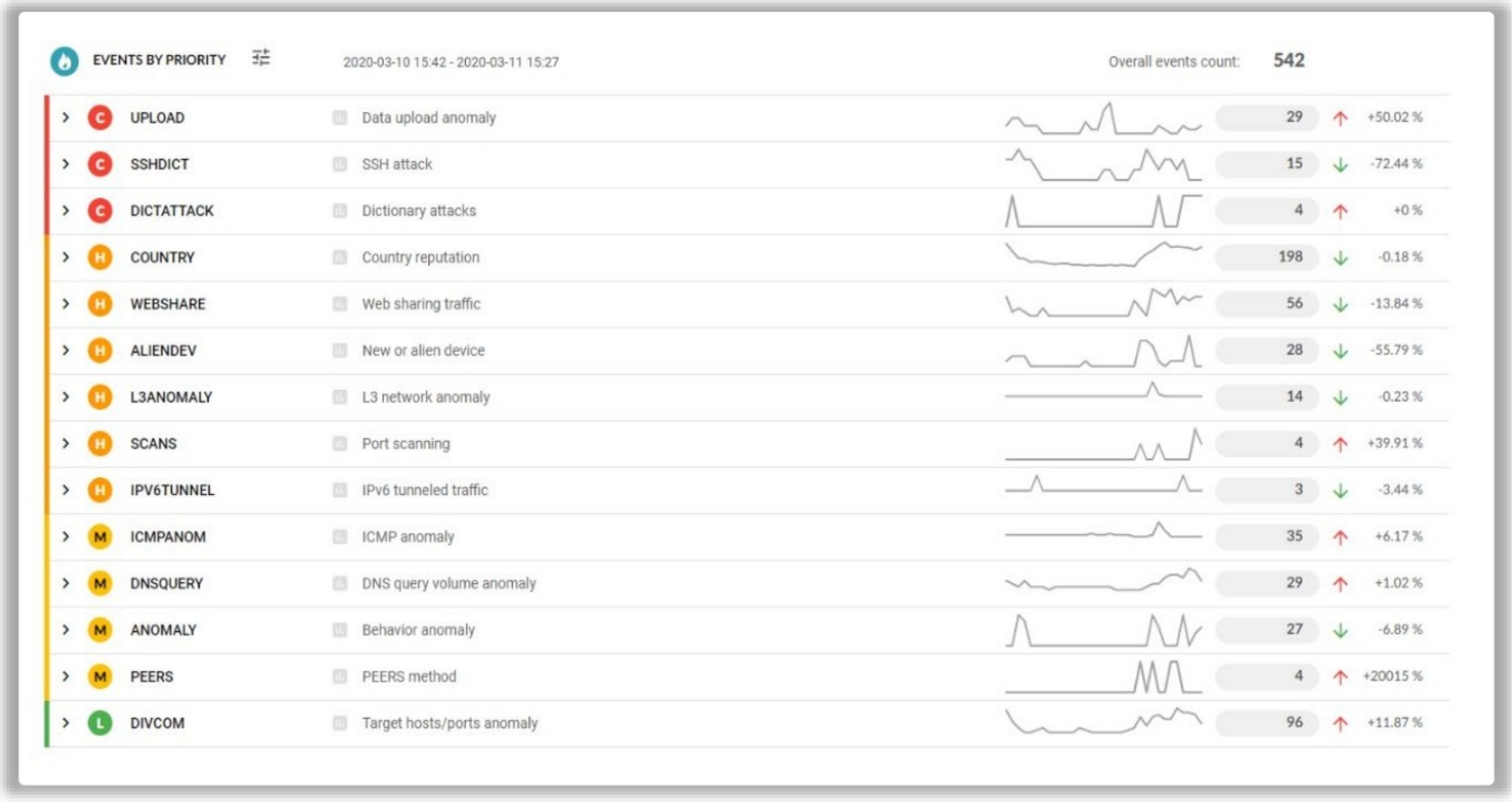
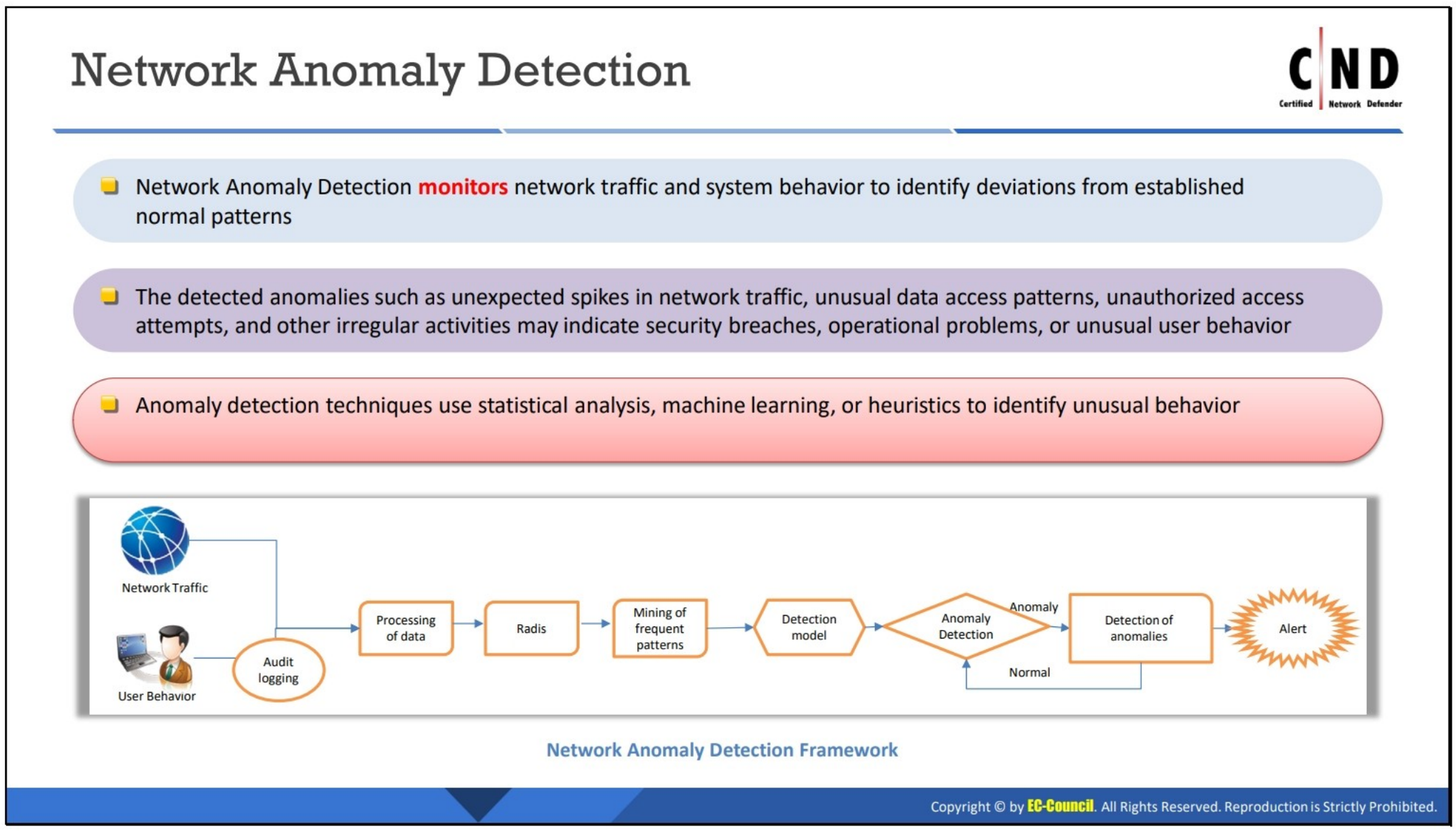


Figure 14.25: Using Statistics to Monitor Network Traffic using Flowmon

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

https://t.me/learningnets

Technet24



Network Anomaly Detection

Network anomaly detection involves identifying abnormal or unexpected events in the network, such as data breaches, intrusions, malware injections, and other malicious activities, that cause data to deviate from its conventional pattern. It detects unnatural patterns, unauthorized access attempts, irregular activities, and unusual behavior of both the network and users.

These anomalies are analyzed and studied based on trends, historical data, and statistical analysis to detect such behaviors. This method maintains a check on the health of all devices, ensuring the integrity and security of the network. It also ensures that no regulations are violated, helping to maintain a secure and compliant network environment.

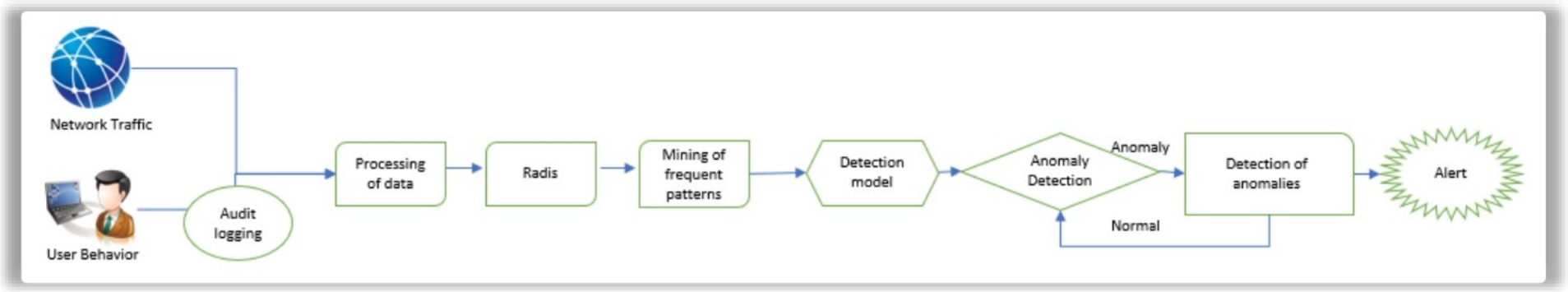
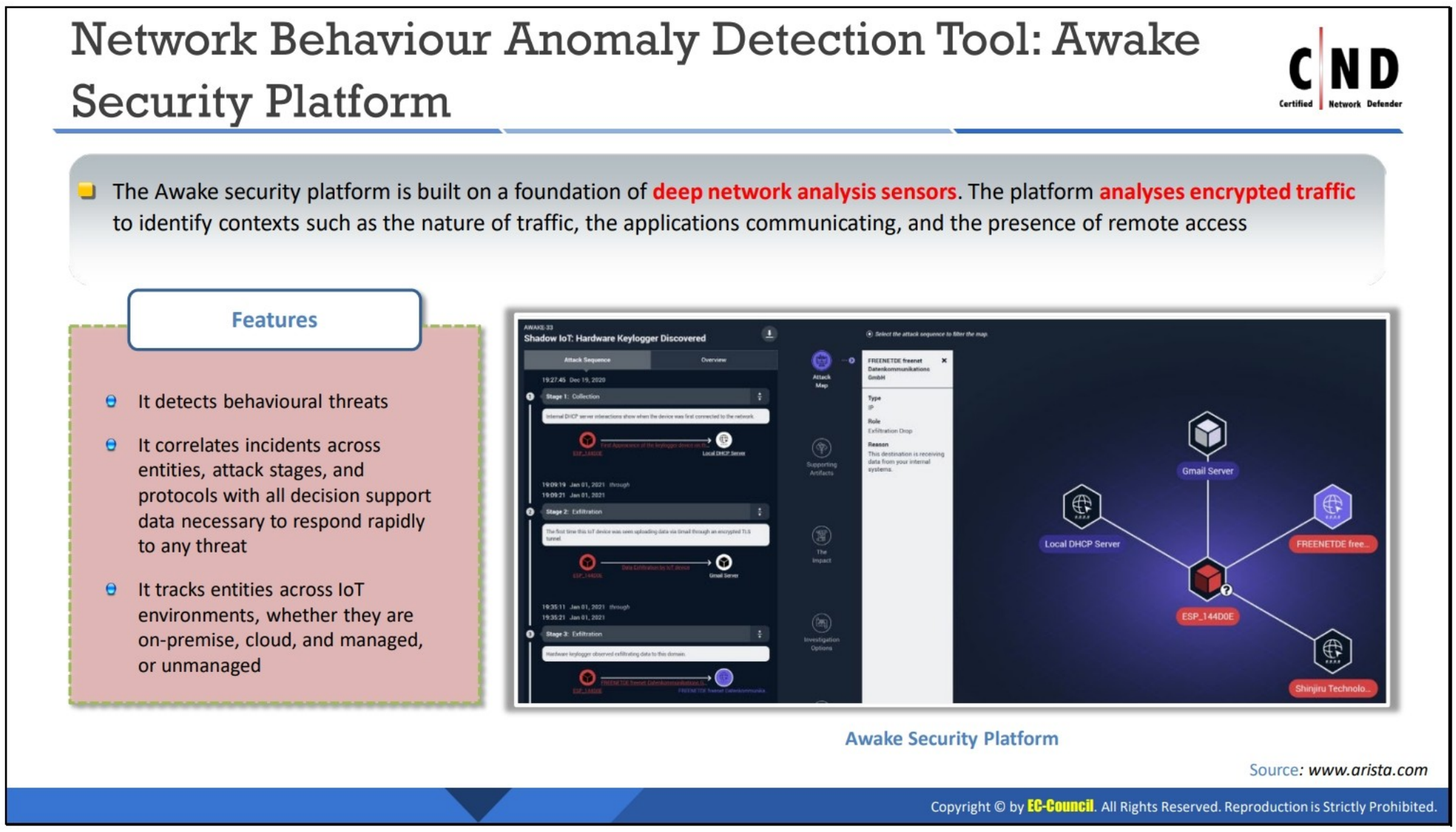


Figure 14.26: Network Anomaly Detection Framework

Network traffic encompasses all the requests and responses occurring within an environment. User behavior refers to the actions frequently performed by users to access information. This behavior is recorded in an audit logger, which is then used for data mining to detect anomalies in the environment through a specific model. If both network traffic and user behavior appear normal, no spikes or unusual patterns are detected. However, if they deviate from the norm, it is considered abnormal and potentially threatening to the environment. In such cases, alarms are triggered and sent to the business hierarchy to notify them about the detected anomaly.

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

https://t.me/learningnets



Network Behavior Anomaly Detection Tool: Awake Security Platform

Source: https://www.arista.com

The Awake Security platform is built on a foundation of deep network analysis sensors. It analyzes encrypted traffic to identify contexts such as the nature of the traffic, the applications communicating, and the presence of remote access, thereby detecting behavioral threats. The platform correlates incidents across entities, attack stages, and protocols, providing all the decision-support data necessary for a rapid response to any threat. It tracks entities across IoT environments, whether they are on-premise, in the cloud, managed, or unmanaged.

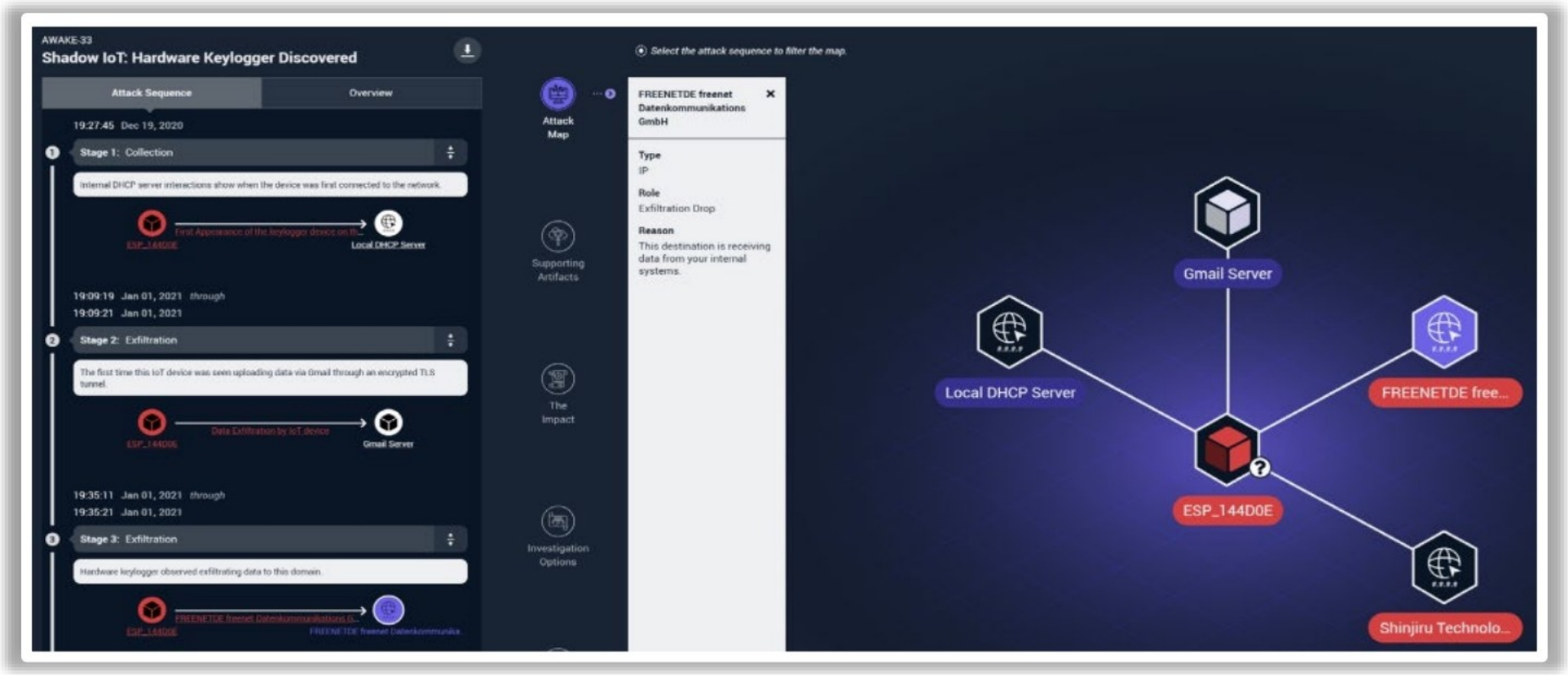
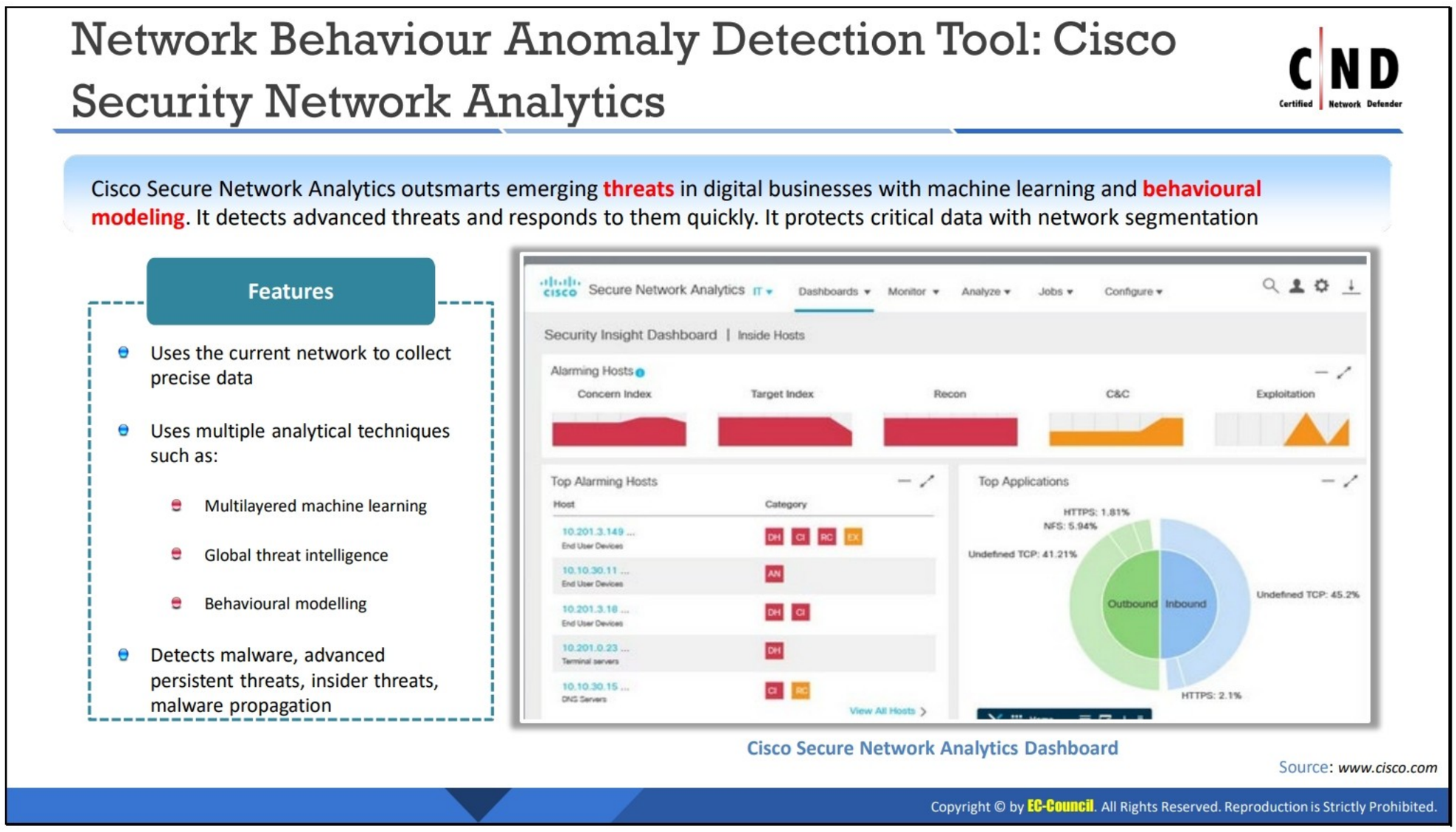


Figure 14.27: NBAD using Awake Security Platform

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

https://t.me/learningnets

Technet24



Network Behavior Anomaly Detection Tool: Cisco Secure Network Analytics

Source: https://www.cisco.com/

Cisco Secure Network Analytics informs you who is on the network and what they are doing by utilizing telemetry from your network infrastructure. It detects advanced threats and responds to them swiftly. The system also protects critical data through intelligent network segmentation. It can gather the necessary data using the existing network infrastructure. Secure Network Analytics is used to analyze encrypted traffic, enabling the detection of malware without decryption, and managing the quality of network encryption within your digital business. The system employs multiple analysis techniques, including behavioral modeling, multilayered machine learning, and global threat intelligence, to identify threats. It is capable of detecting malware in encrypted traffic without the need for decryption, as well as identifying advanced persistent threats and insider threats.

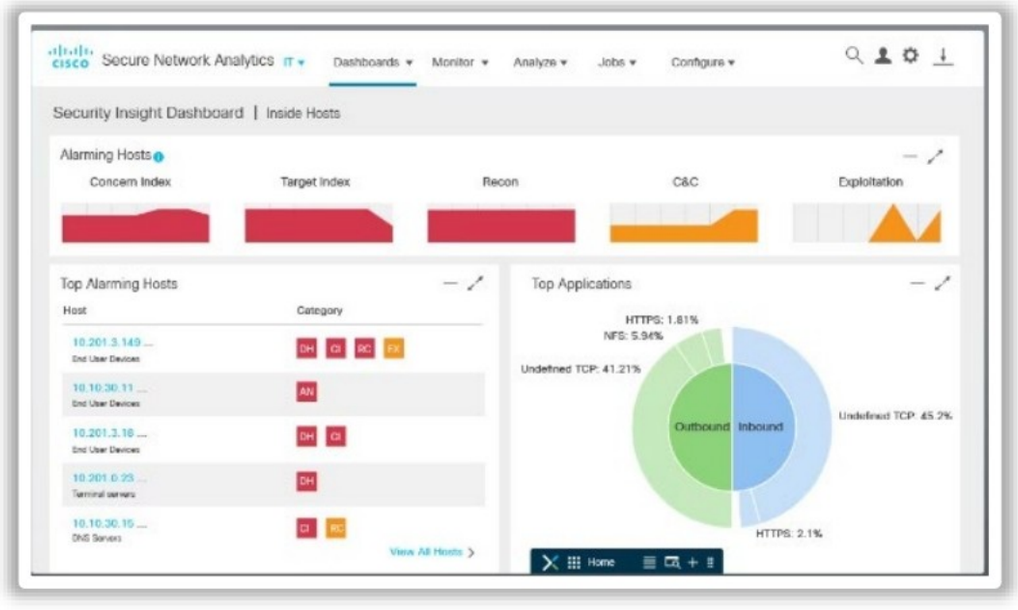
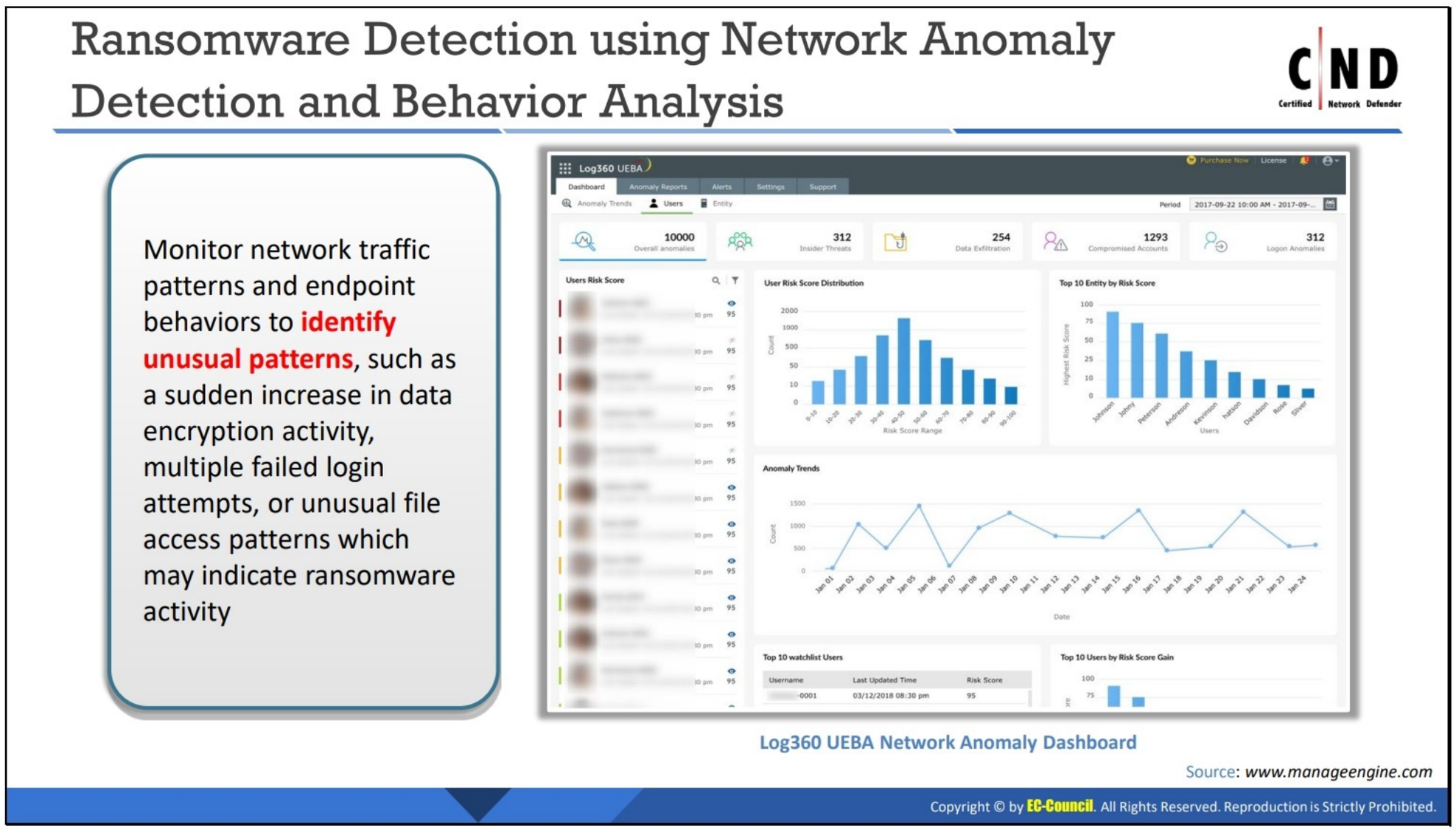


Figure 14.28: Cisco Secure Network Analytics Dashboard

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

https://t.me/learningnets



Ransomware Detection using Network Anomaly Detection and Behavior Analysis

Detect ransomware by analyzing data traffic and identifying network irregularities, such as a sudden increase in encryption activity (indicative of ransomware) or failed login attempts and accessing information through abnormal approaches.

Real-time detection of these abnormalities enables rapid countermeasures to prevent ransomware attacks from compromising critical data. This proactive approach to network security protects enterprises against emerging cyber threats. When strange patterns are observed, automatic measures can be initiated, including isolating the impacted endpoints, restricting suspect network traffic, and alerting the security team, as well as informing the business hierarchy.

Example UEBA Tool to Identify Ransomware attacks: Log360 UEBA

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

Log360 UEBA, powered by Machine Learning (ML), detects anomalies by recognizing subtle changes in user activity. It aids in identifying, qualifying, and investigating threats that might otherwise remain unnoticed, by extracting more information from logs to provide better context.

The dashboard offers a concise overview of anomalous behavior based on users and entities in the network. As it consolidates multiple data sources into a single interface, administrators can swiftly assess the status of their organization's security posture.

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

https://t.me/learningnets

Technet24

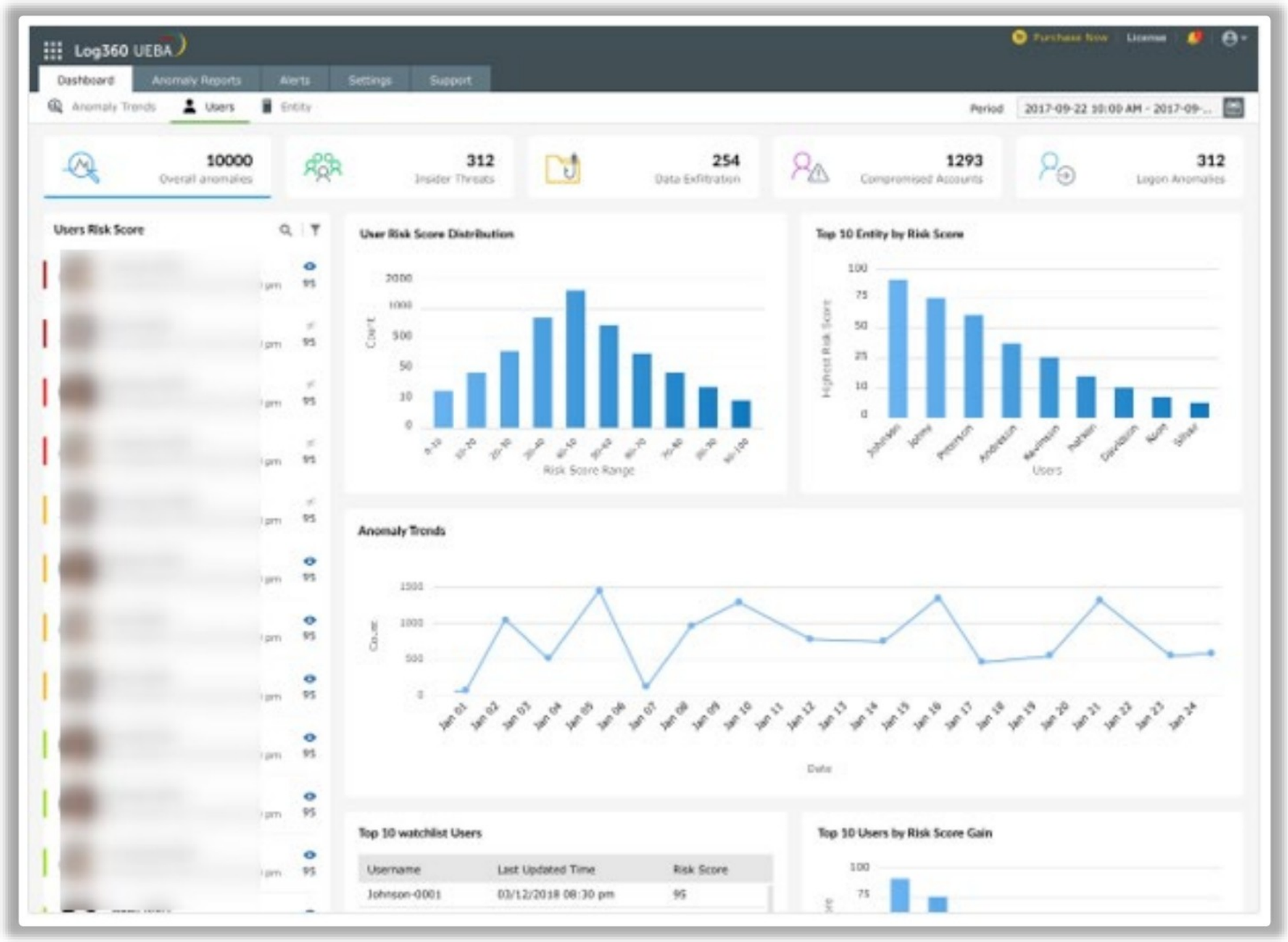
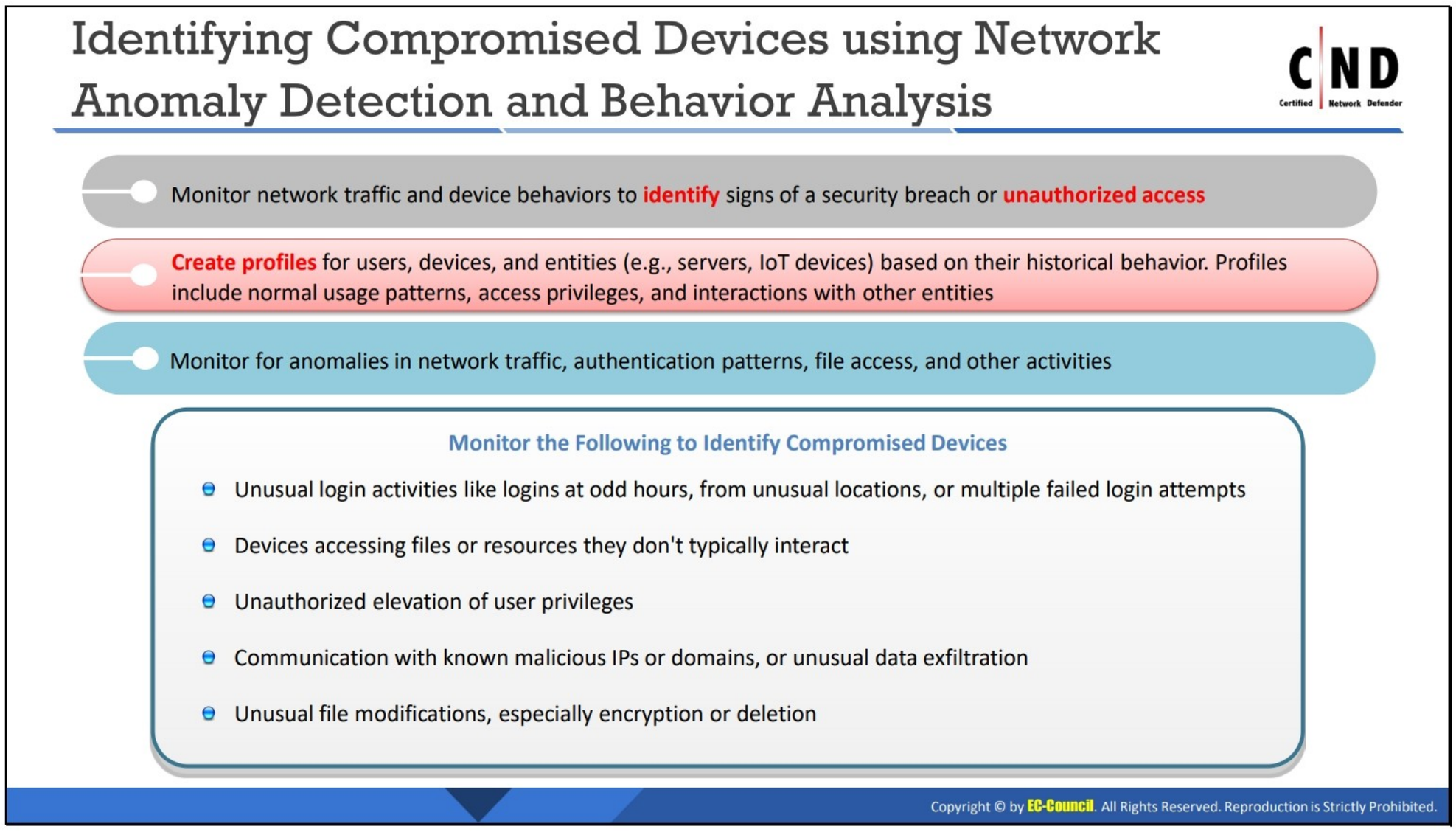


Figure 14.29: Example Ransomware Detection using Log360 UEBA

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

https://t.me/learningnets



Identifying Compromised Devices using Network Anomaly Detection and Behavior analysis

It is crucial to monitor network traffic and device behavior to detect potential security breaches or unauthorized access. To achieve this, profiles for users, devices, and entities should be established based on their historical behavior. These profiles ought to encompass normal usage habits, access rights, and interactions with third-party entities. Moreover, vigilance for any unusual patterns in network traffic, authentication, file access, or other activities is essential.

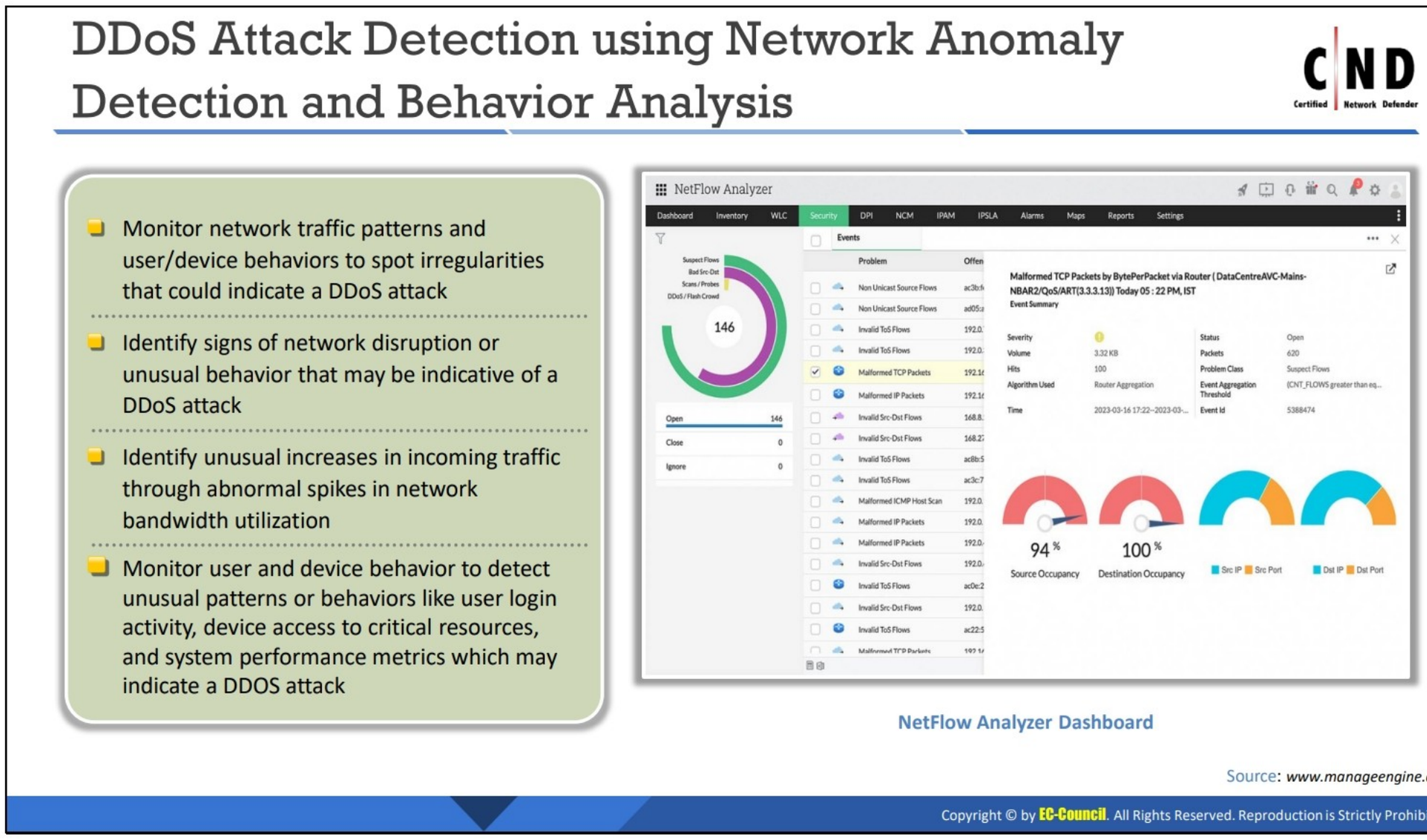
Monitor the following to identify compromised devices:

- Monitor for unusual activities such as signing in at unconventional hours or from unfamiliar locations and observe multiple login attempts. These are indicators that can help identify compromised devices.
- Monitor devices that access unusual resources.
- Monitor for unauthorized privilege escalation that could potentially lead to root access.
- Monitor for suspicious network communication, such as establishing connections with unknown IP addresses or unknown servers, which could be used to distribute malware.
- Monitor for file modifications, alterations in log files, encrypting critical resources, and deleting them, as these actions are also considered indicators of compromise.

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

https://t.me/learningnets

Technet24



DDoS Attack Detection using Network Anomaly Detection and Behavior Analysis

A DDoS attack can be detected by monitoring the network traffic of an environment. This is observed when there is a sudden spike in the flow of incoming requests, exceeding what is normally expected. Such a spike is considered abnormal or unconventional in the context of detecting a DDoS attack.

A rapid influx of connection requests can overwhelm the server, leading to reduced response times. Security systems and devices may lose their internet connection under such circumstances. These can be termed abnormal patterns that burden the network's environment. Detecting them at early stages might mitigate the attack, and it is important to frequently execute traffic filtering and redirection methods.

Subnetting on a large scale can channel the requests to different network devices. Devices might lose critical resources due to such unconventional behaviors and drastic spikes in statistics. This also reduces the system's performance, which might eventually lead to the successful execution of a DDoS attack on environments.

Example Tool for Detecting DDoS Attacks: NetFlow Analyzer

Source: *www.manageengine.com*

NetFlow Analyzer's Security module is designed to detect and analyze network security threats and anomalies. It utilizes the state-of-the-art Continuous Stream Mining Engine™ technology for pattern matching and event correlation across multiple events, thereby sensing attacks before they can compromise the entire network. The module is capable of detecting junk or anomalous traffic and classifies it into four problem classes based on predefined algorithms: suspect flows, bad source or destination, DDoS attacks, and scans/probes.

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

https://t.me/learningnets

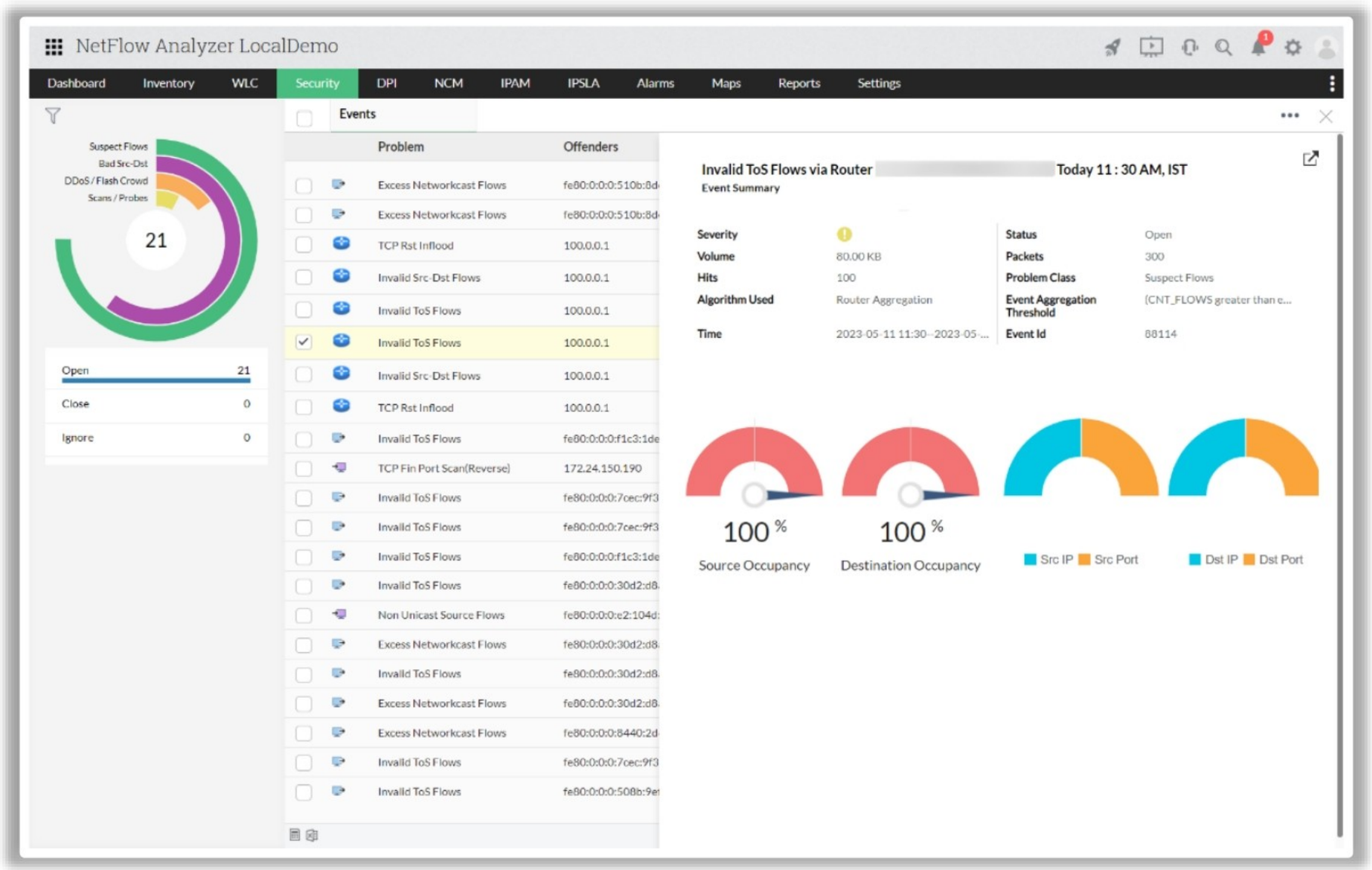
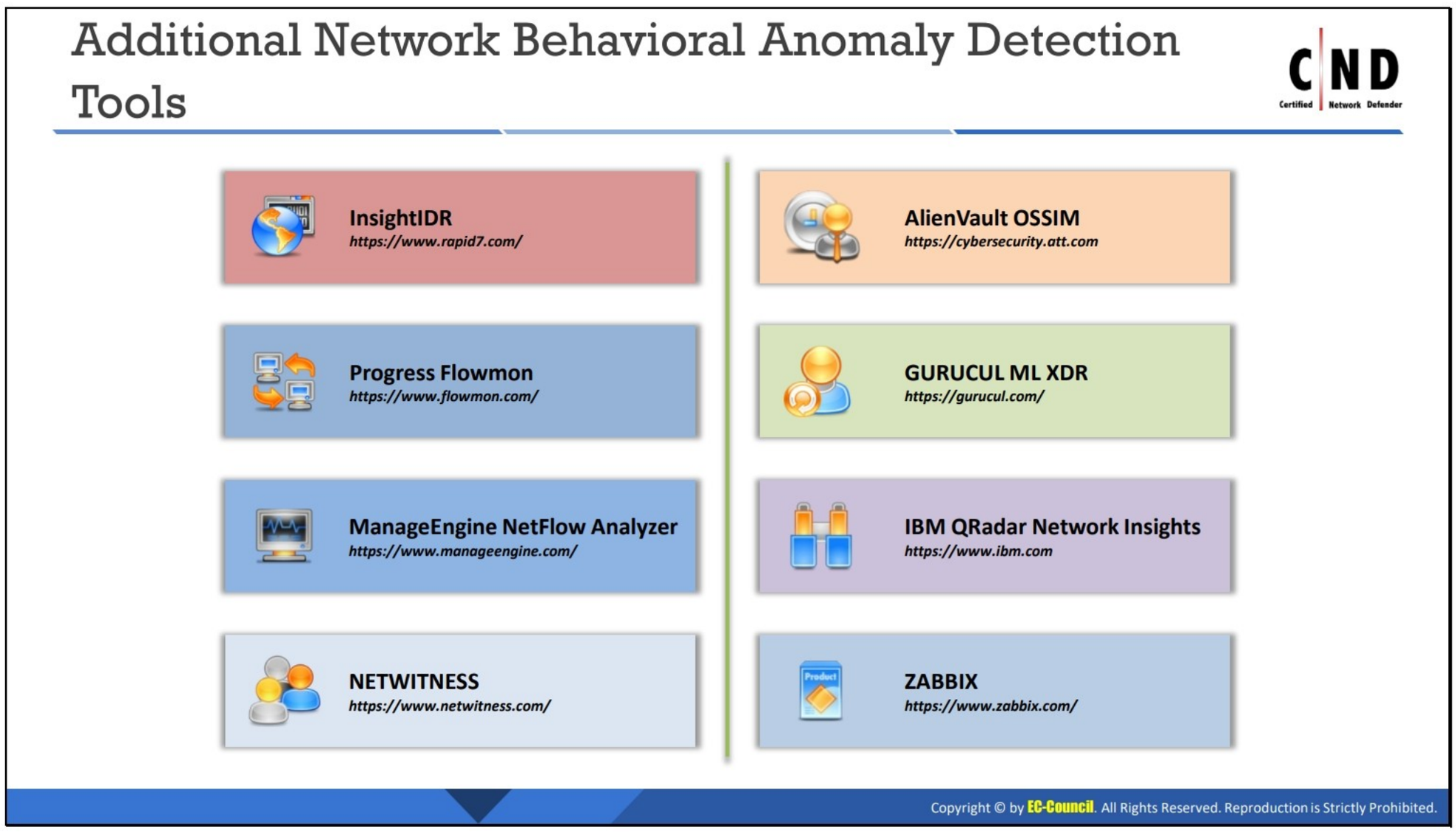


Figure 14.30: Example DDoS Attack Detection

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

https://t.me/learningnets

Technet24



Additional Network Behavioral Anomaly Detection Tools

InsightIDR

Source: https://www.rapid7.com

The InsightIDR tool is equipped with a network sensor, providing visibility and network detection for critical assets and data at rest in the environment. This tool includes lightweight tools that aid in detecting suspicious activities and policy modifications within the network. It enhances security through an IDS, which monitors malicious traffic. The IDS data is accessible on the details page, allowing users to thoroughly examine the data.

Progress Flowmon

Source: https://www.flowmon.com

This detection engine leverages behavioral algorithms to identify potential anomalies embedded in the network, exposing threats and enabling their mitigation. It also helps the network recognize indicators of compromise and vulnerabilities, thereby securing the business with advanced network detection and response. This tool adds a network-centric layer to the environment.

ManageEngine NetFlow Analyzer

Source: https://www.manageengine.com

ManageEngine NetFlow Analyzer is a traffic analysis tool that enhances the visibility of an organization's critical assets and offers a detection mechanism for the network's bandwidth utilization. It is capable of optimizing various traffic patterns within the network. This tool collects records of activities in the network, monitors them, and then analyzes and reports on who is controlling and using the network bandwidth.

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

https://t.me/learningnets

NETWITNESS

Source: https://www.netwitness.com/

This tool is designed to enhance threat detection and response. It monitors, collects, and analyzes data across all access points to maintain oversight of the environment. Additionally, it enables security analysts to select and prioritize, respond to, and reconstruct plans for investigating threats in the environment.

Alien Vault OSSIM

Source: https://cybersecurity.att.com

AlienVault OSSIM is an open-source security information and event management (SIEM) tool that offers features for gathering, normalizing, and correlating events. It was developed in response to the scarcity of open-source products in the market and to address a common challenge faced by many security professionals. Additionally, it enhances security visibility.

GURUCUL ML XDR

Source: https://gurucul.com

GURUCUL ML XDR is a traffic analyzer tool that provides visibility into unknown and undetected network traffic threats based on the network's anomalous behavior. It utilizes machine learning-based network traffic analyzer entities to create behavior baselines for every device and machine on the network. These baselines are based on network flow data such as source and destination IPs/machines, protocol, bytes in/out, etc., helping the system adapt to it.

IBM QRadar Network Insights

Source: https://www.ibm.com

IBM QRadar Network Insights aids in identifying suspicious activity that coincides with regular traffic and extracts content to enhance visibility into network threat activity. It conducts comprehensive analyses of both network metadata and application content, thereby improving its capabilities in detection, analysis, and threat identification. The intelligence provided by QRadar Network Insights integrates seamlessly with conventional data sources and threat intelligence.

ZABBIX

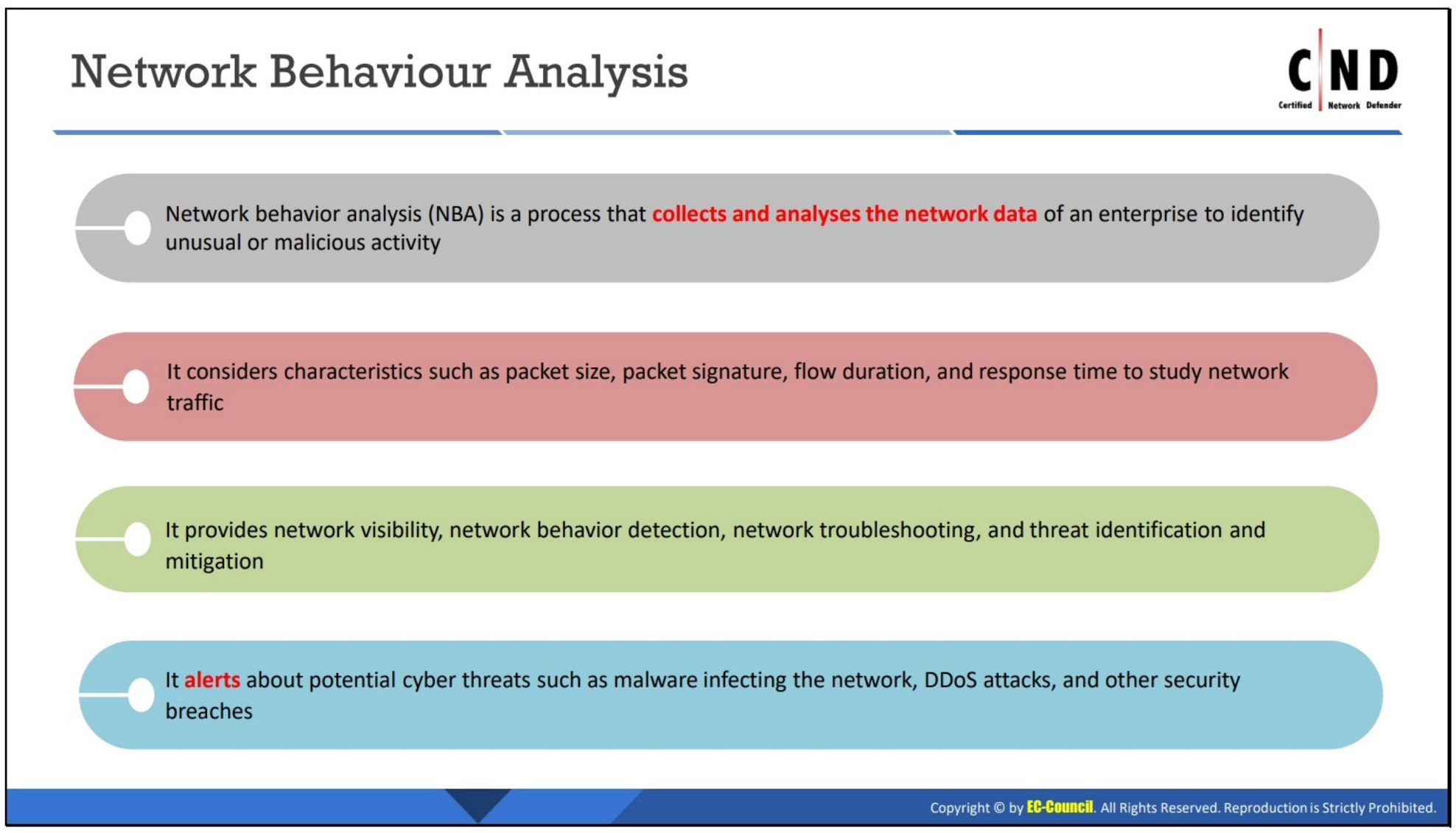
Source: https://www.zabbix.com

ZABBIX is a tool that monitors network hardware, collects, analyzes, and responds to network traffic metrics. It includes numerous parameters to monitor the health of devices and enhances monitoring and detection mechanisms.

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

https://t.me/learningnets

Technet24



Network Behavior Analysis

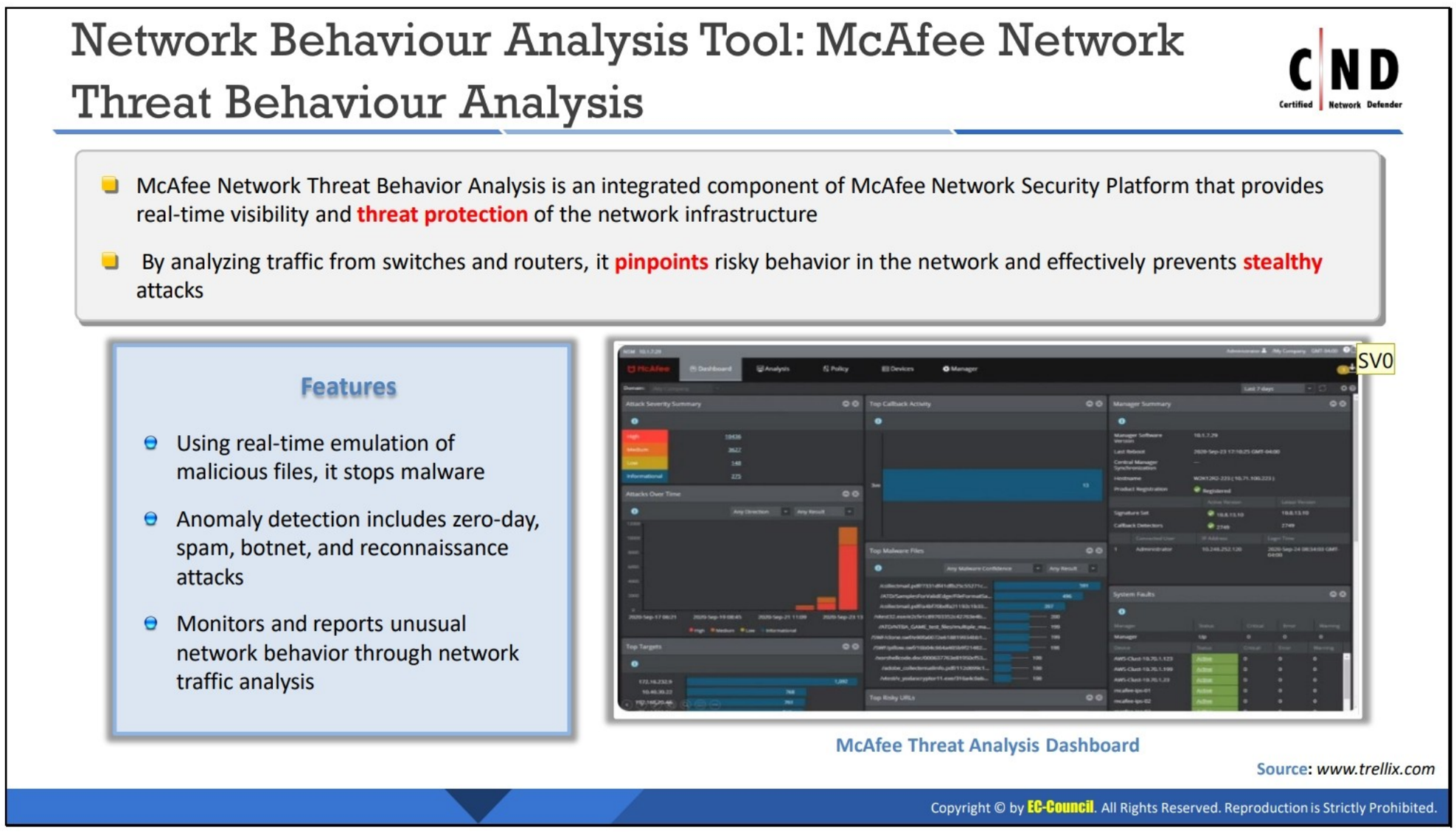
Network behavior analysis (NBA) is a process that collects and analyzes the network data of an enterprise to identify unusual or malicious activity. It utilizes advanced analytics, rule-based techniques, and machine learning to detect suspicious activities on enterprise networks.

It allows for the following:

- Tracking and recording bandwidth and protocol usage patterns.
- Gathering data about network operations from various sources, employing machine learning to recognize data patterns, so any sudden change suggests the presence of malicious activity.
- Detecting new malware and zero-day vulnerabilities by considering characteristics like packet size, packet signature, flow duration, and response time.
- Enhancing network visibility, network behavior detection, network troubleshooting, threat identification, and mitigation.
- Notifying of emerging cyber threats, such as malware taking hold of part of the network and spreading its presence, unfolding DoS attacks, or a hacker attempting to infiltrate the enterprise network.

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

https://t.me/learningnets



Network Behavior Analysis Tool: McAfee Network Threat Behavior Analysis

Source: https://www.softwareadvice.com/

McAfee Network Security Platform is designed to help businesses identify and block vulnerability threats across virtual environments, data centers, and both private and public clouds. It enables IT teams to analyze business risks and monitor unusual network behavior through a unified platform.

McAfee Network Threat Behavior Analysis, an integrated component of the McAfee Network Security Platform, provides real-time visibility and threat protection for network infrastructure. Anomaly detection includes zero-day, spam, botnet, and reconnaissance attacks.

By analyzing traffic from switches and routers, it pinpoints risky behavior in the network and effectively prevents stealthy attacks.

The features of the McAfee Network Threat Behavior Analysis tool are as follows:

- Enhanced security through integration with McAfee
- Effortless sorting and analysis of network traffic
- Anomaly detection includes zero-day, spam, botnet, and reconnaissance attacks
- External host visibility with detailed host threat Factor ratings
- Factor ratings

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

https://t.me/learningnets

Technet24

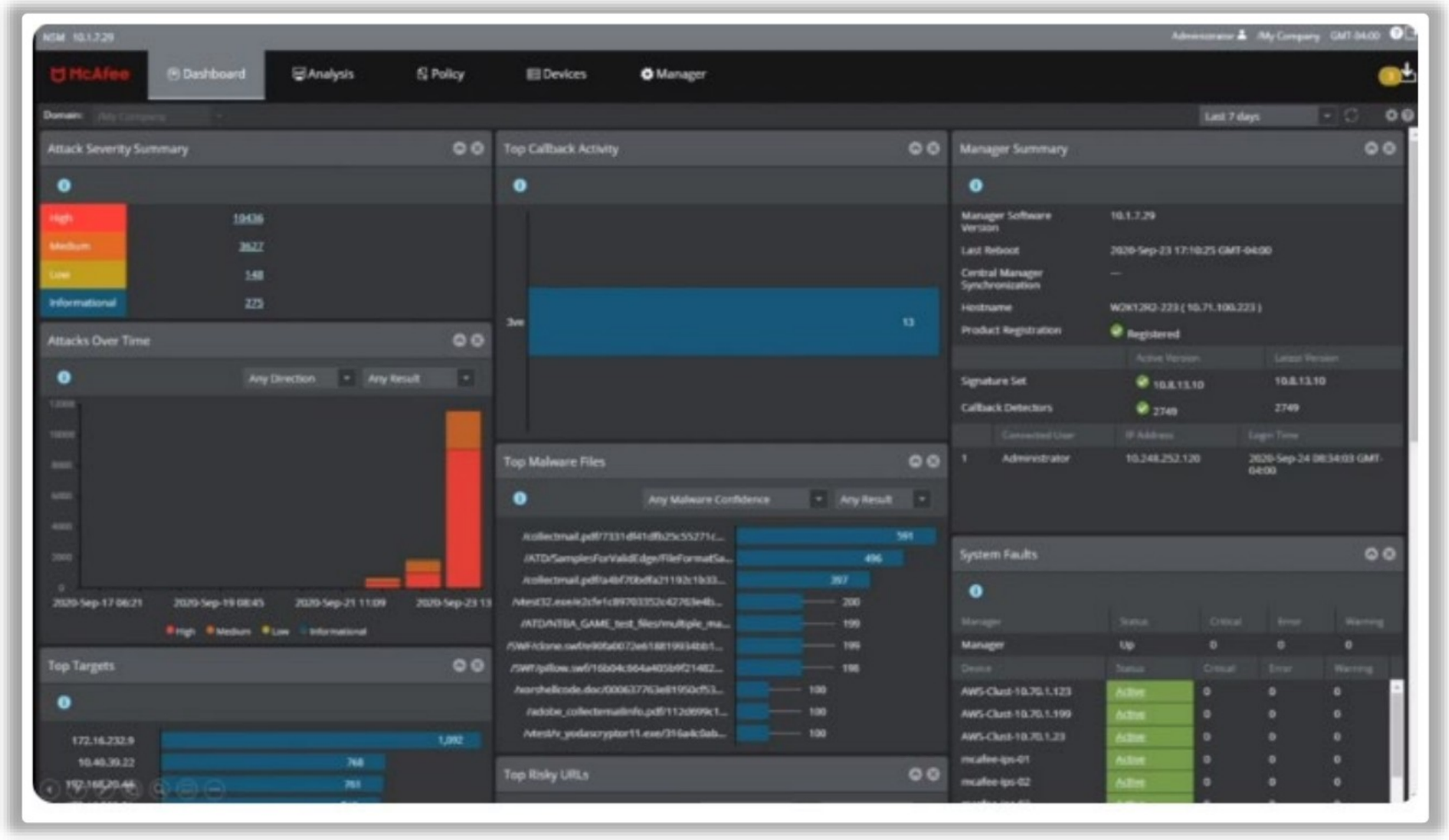
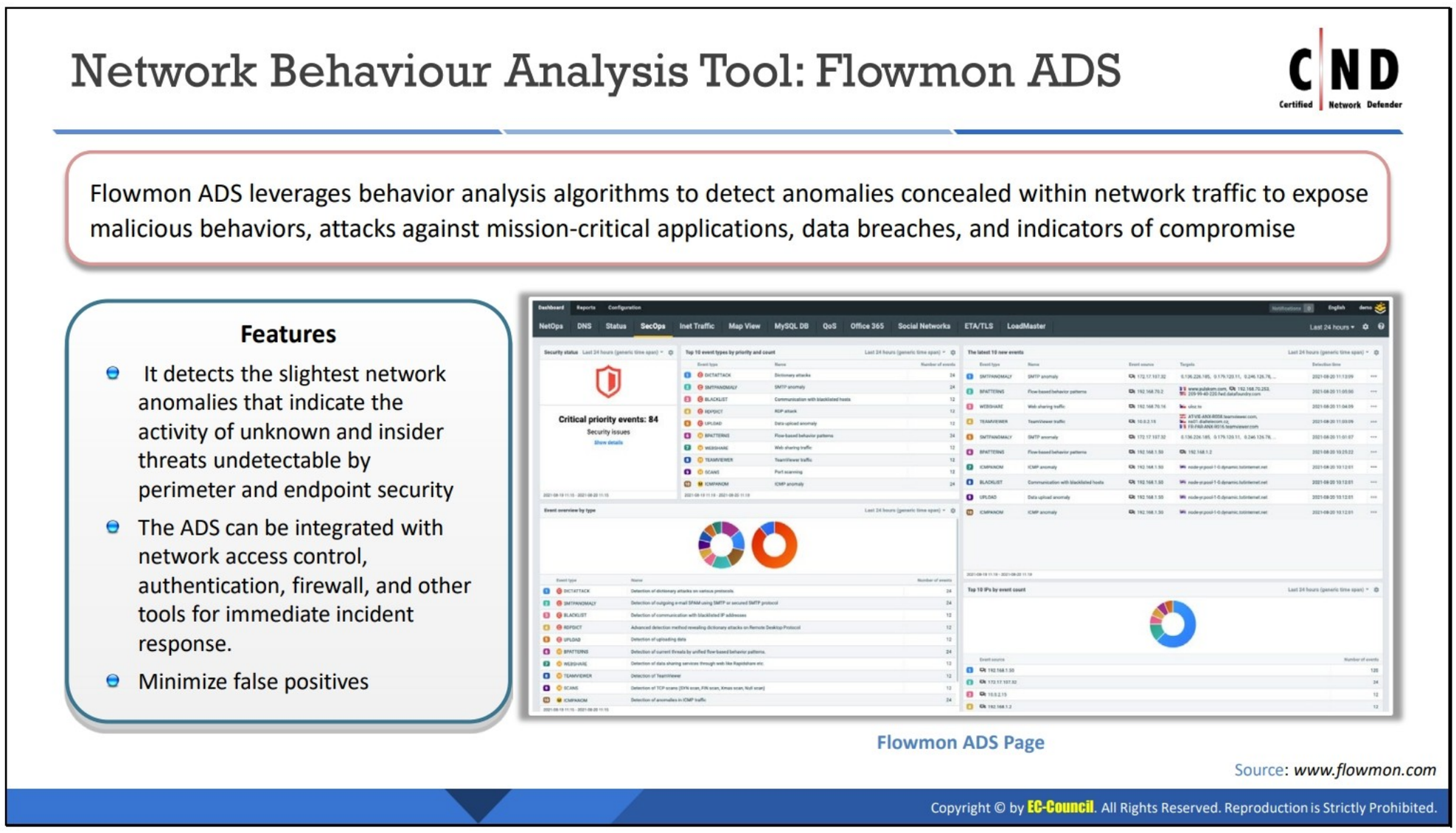


Figure 14.31: McAfee Threat Analysis Dashboard

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

https://t.me/learningnets



Network Behavior Analysis Tool: Flowmon ADS

Source: https://www.flowmon.com/

Flowmon ADS leverages behavior analysis algorithms to detect anomalies concealed within network traffic, exposing malicious behaviors, attacks against mission-critical applications, data breaches, and indicators of compromise.

The features of Flowmon ADS are as follows:

- **Behavior patterns**: Detect misuse and suspicious behavior of users, devices, and servers. Understanding protocols such as DNS, DHCP, ICMP, and SMTP can reveal data exfiltration, reconnaissance, lateral movement, and other unwanted activities.
- **Attack evidence and analysis**: Understand every suspicious event in its complexity. Context-rich evidence, visualization, network data, or full packet traces for forensics allow for prompt decisive actions.
- **Prioritization and reporting**: Utilize out-of-the-box prioritization and severity rules at a global, group, or user level. Create custom dashboards for security, networking, IT helpdesk, or managers based on their interests.
- **Advanced action triggering**: Respond to attacks automatically through script-based integration with network or authentication tools. For example, when detecting an event, Flowmon can connect to Cisco ISE through pxGrid and quarantine the malicious IP address.
- **Configuration wizard**: The system comes with predefined configurations for a variety of network types and automatically adjusts the settings after the initial setup using a simple wizard. Then, by managing false positives, maximize the relevance of detected events.

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

https://t.me/learningnets

Technet24

The ADS can be integrated with network access control, authentication, firewall, and other tools for immediate incident response.

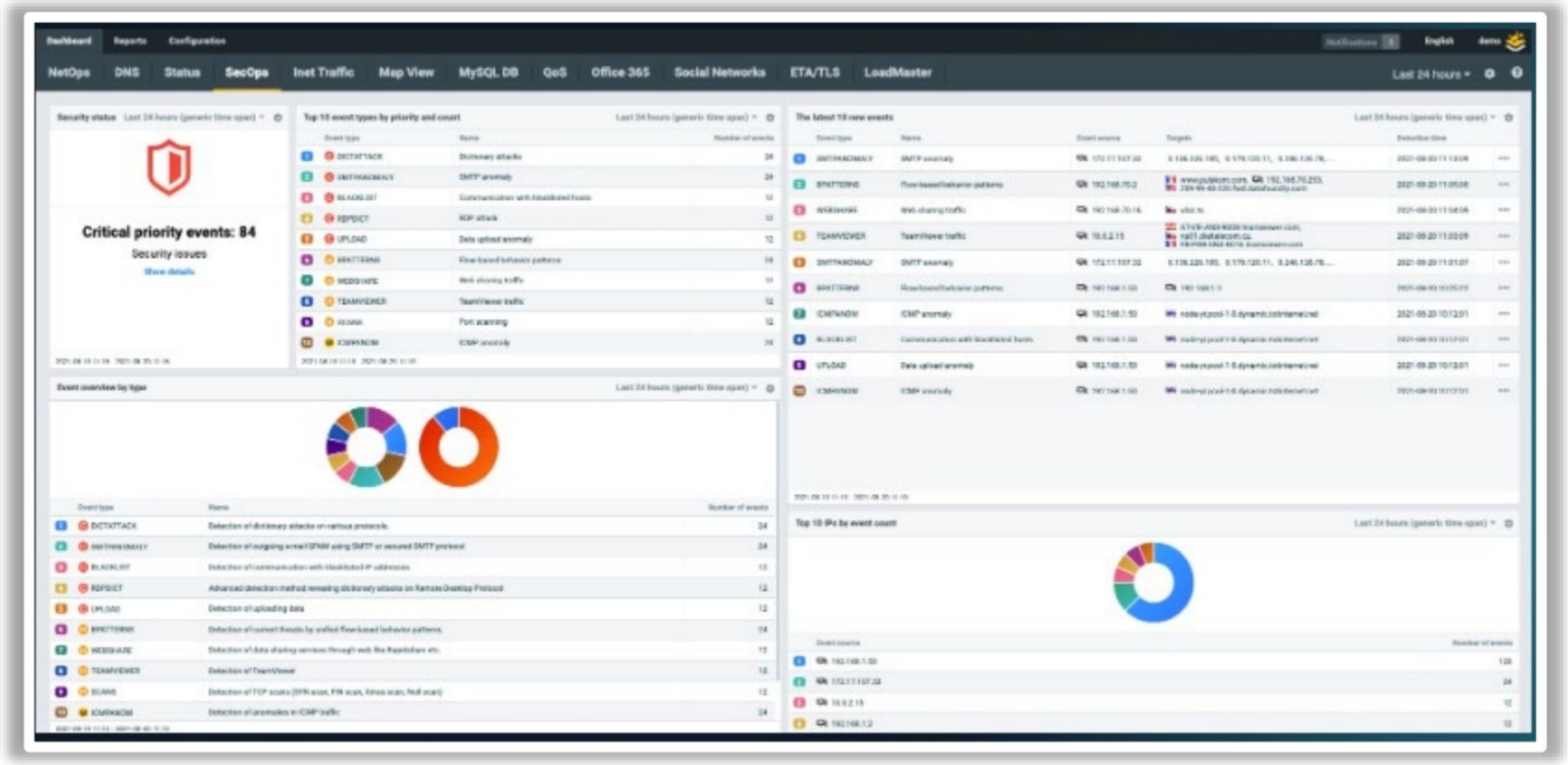
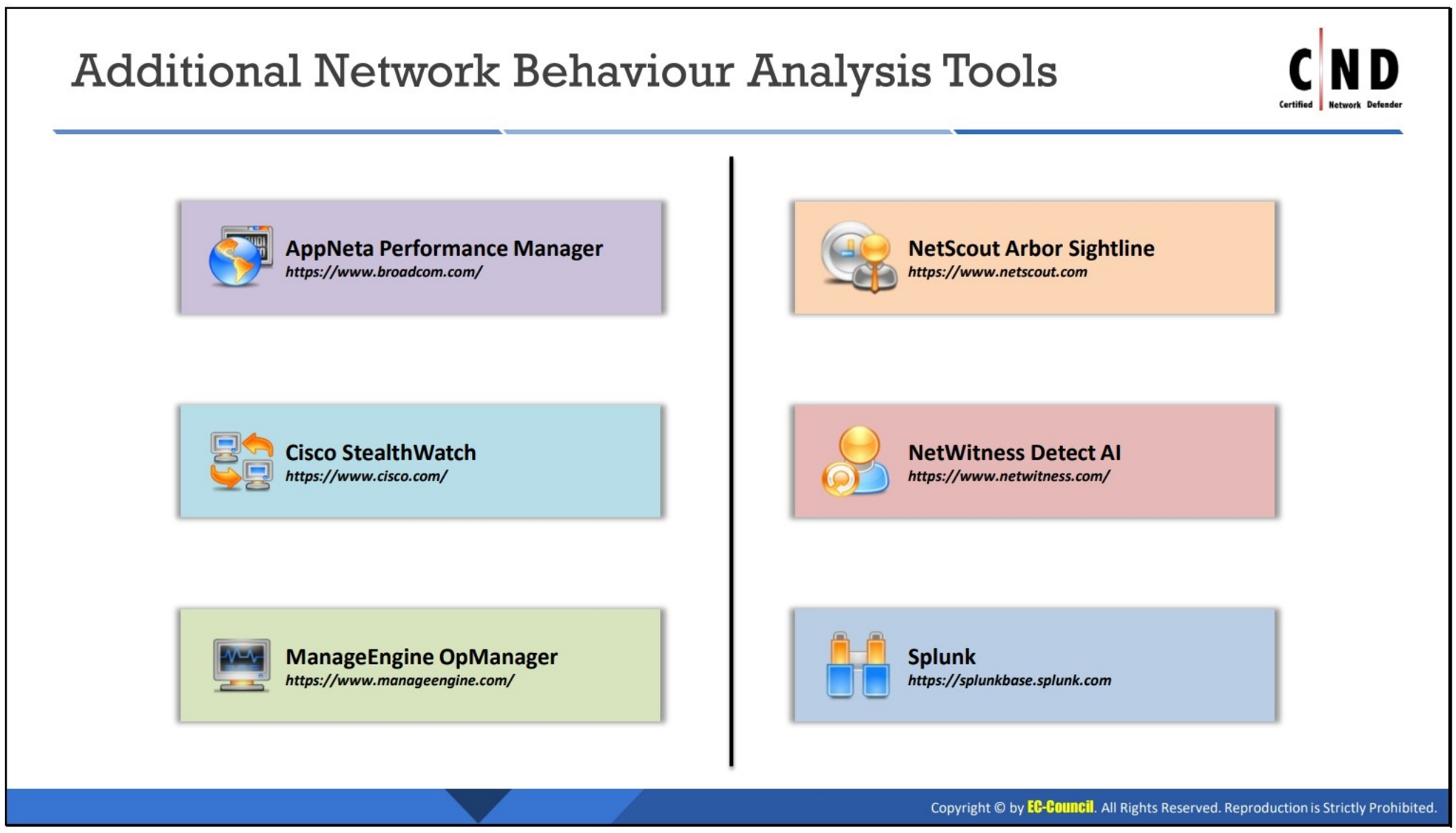


Figure 14.32: Flowmon ADS Page

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

https://t.me/learningnets



Additional Network Behavior Analysis Tools

AppNeta Performance Manager

Source: https://www.broadcom.com

AppNeta is a network performance monitoring tool that delivers visibility into the end-user experience of any application, from any location, at any time. It helps identify the cause of network problems and determines the critical traffic in the network by identifying the apps running on it.

The features of AppNeta Performance Manager are as follows:

- **Active and passive monitoring**: AppNeta's 4-dimensional monitoring helps customers quickly solve complex network problems, allowing employees to return to business-critical activities that drive revenue.
- **Critical network data collection:** AppNeta collects critical network data without impacting overhead, resulting in lower internal resource costs and faster issue resolution, which gets knowledge workers back to revenue-producing activities quickly.
- **Flexible deployment:** With remote deployment and management of Monitoring Points, AppNeta minimizes the impact on remote locations with quicker deployment and less effort than competing solutions, ultimately driving a faster return on investment.

Cisco StealthWatch

Source: https://www.cisco.com

Outsmart emerging threats in the digital business with industry-leading machine learning and behavioral modeling provided by Secure Network Analytics (formerly StealthWatch). Know who

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

https://t.me/learningnets
Technet24

is on the network and what they are doing using telemetry from the organization's network infrastructure. Detect advanced threats and respond to them quickly. Protect critical data with smarter network segmentation.

The features of Cisco StealthWatch are as follows:

- **Get comprehensive visibility and analytics-** Detect attacks across the dynamic network with high-fidelity alerts enriched with context, including user, device, location, timestamp, and application.
- **Speed up incident response-** Quickly detect unknown malware, insider threats like data exfiltration, policy violations, and other sophisticated attacks using advanced analytics.
- **Simplify network segmentation-** Define smarter segmentation policies without disrupting the business. Create custom alerts to detect any unauthorized access and ensure compliance.

ManageEngine OpManager

Source: https://www.manageengine.com

ManageEngine OpManager is a network monitoring software that offers deep visibility into the performance of routers, switches, firewalls, load balancers, wireless LAN controllers, servers, VMs, printers, and storage devices. It is an easy-to-use and affordable network monitoring solution that enables organizations to drill down to the root cause of an issue and resolve it.

The features of ManageEngine OpManager are as follows:

- **Network monitoring-** Monitor network services and visualize system performance with OpManager.
- **Physical & virtual server monitoring-** Ensure servers are up and running at their optimum performance level, 24x7.
- **Wireless network monitoring-** Provide comprehensive in-depth wireless network stats for access points, wireless routers, switches, Wi-Fi systems, etc.

NetScout Arbor Sightline

Source: https://www.netscout.com/

NetScout Arbor Sightline is a DDoS attack detection solution that offers powerful features ranging from network-wide capacity planning to the identification and management of the mitigation and detection of DDoS and other threats to the network.

The features of NetScout Arbor Sightline are as follows:

- **Network peering analysis**: Peering analysis helps determine which traffic can transfer off expensive transit links to either free peering or even become revenue-generating as a new customer.
- **Network capacity management**: The organization can use Arbor Sightline to monitor the capacity of network infrastructure, allowing for the avoidance of saturation and the re-engineering of network traffic for more efficient utilization.

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

https://t.me/learningnets

- **Threat detection:** Through proactive detection of network or service availability threats, Sightline can quickly diagnose and detect DDoS attacks.

NetWitness Detect AI

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

NetWitness Detect AI is a cybersecurity solution that utilizes artificial intelligence (AI) and machine learning (ML) technologies to enhance threat detection and response capabilities within an organization's network. It collects and analyzes data across all capture points (logs, packets, NetFlow, endpoint, and IoT) and computing platforms (physical, virtual, and cloud), enriching the data with threat intelligence and business context.

The features of NetWitness Detect AI are as follows:

- An innovative, dynamic statistical risk scoring model produces high-fidelity alerts with meaningful insights.
- Intelligent peer grouping of anomalies provides additional context for understanding suspicious behavioral activity.
- Patented unsupervised machine learning and behavioral analytics drive advanced and highly automated threat detection.

Splunk

Source: www.splunk.com

Splunk is a data analytics and visualization platform used for monitoring, searching, and analyzing machine-generated data, such as logs, events, and metrics. It collects data from various sources, including servers, applications, and devices, providing real-time insights and actionable intelligence. Splunk helps organizations gain valuable insights from their data, enabling them to make informed decisions and improve operational efficiency.

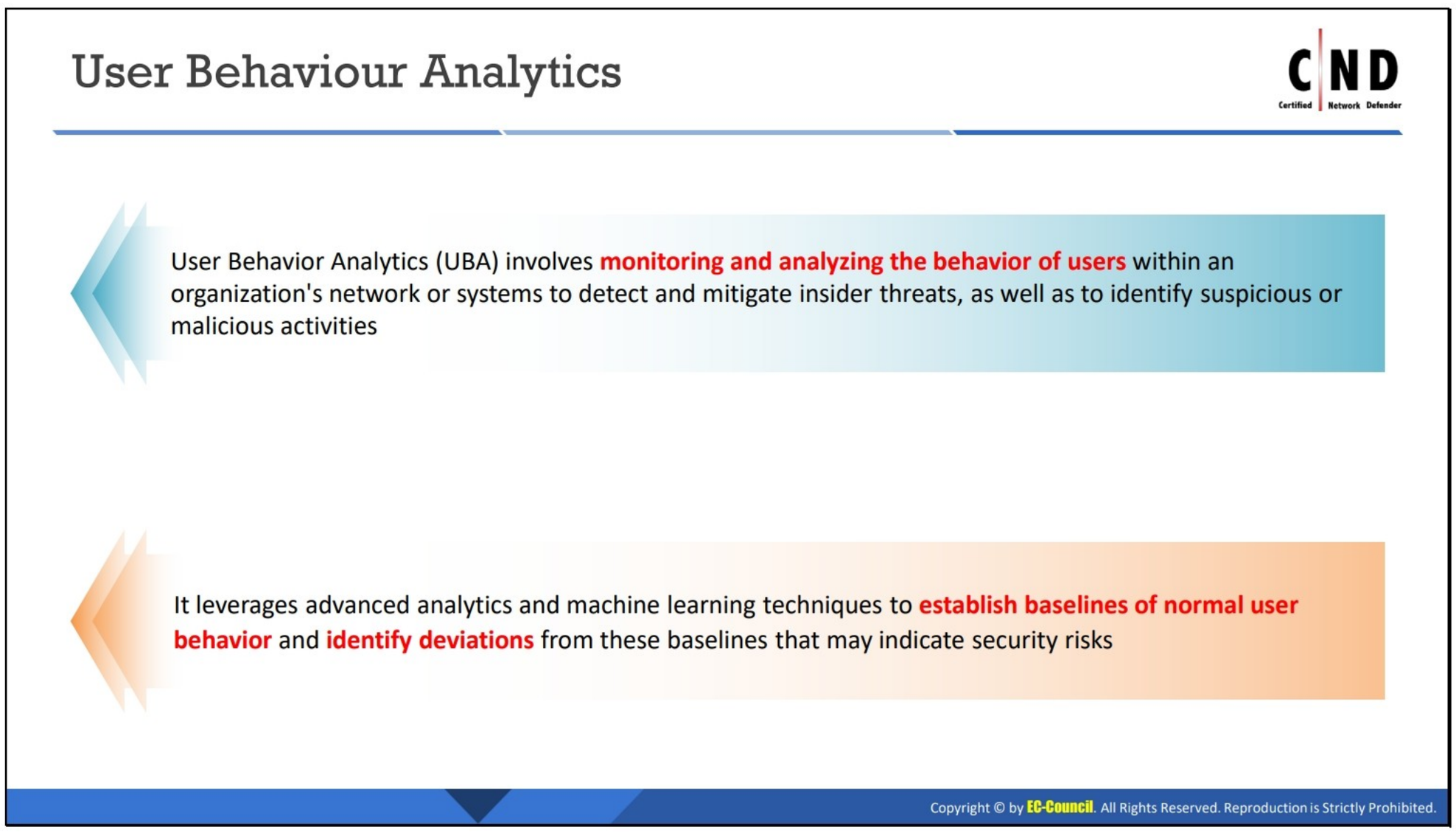
The features of Splunk tool are as follows:

- **Advanced threat detection:** Detect advanced threats with machine learning and 1400+ out-of-the-box detections for frameworks such as MITRE ATT&CK, NIST, CIS 20, and Kill Chain.
- **Risk-based alerting**: Attribute risk to users and systems, map alerts to cybersecurity frameworks, and trigger alerts when risk exceeds thresholds, helping to conquer alert fatigue.
- **Rapid response security content:** Receive automatic security content updates directly from the Splunk Threat Research Team to help the organization stay on top of new and emerging threats.

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

https://t.me/learningnets

Technet24



User Behavior Analytics

User Behavior Analytics (UBA) is a security process that detects abnormal user activities on the network. UBA leverages machine learning and data science to develop insights into the behavioral patterns of users in real time in each environment. It analyzes data, authentication, and network logs stored in security information and event management systems (SIEM) and log management to identify traffic patterns caused by user behavior. UBA creates baselines for user activities and highlights any deviations from these baselines. These anomalies may serve as indicators of potential threats or security breaches. It tracks and analyzes data, which may include files accessed, emails sent and read, apps opened, network activity, etc. UBA spots irregularities such as data breaches and identifies potential security threats and unauthorized access attempts.

How UBA Works?

UBA collects diverse data on a user from multiple sources and locations within the environment, which may include log files, network traffic, and application usage. Through the process of behavioral profiling, UBA creates a baseline of the user's typical behavior, encompassing regular activities, interactions, and even passive information like the user's geographic location. UBA utilizes machine learning, statistical modeling, and other sophisticated analytics to identify deviations from either the user's established baseline or the behavior of their peers. These anomalies may suggest unauthorized access attempts or other security threats. By scrutinizing these deviations, UBA assesses their potential risks and assigns risk scores based on the severity of the detected anomalies. It generates an alert upon potentially malicious activity.

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

https://t.me/learningnets

Use Cases of UBA

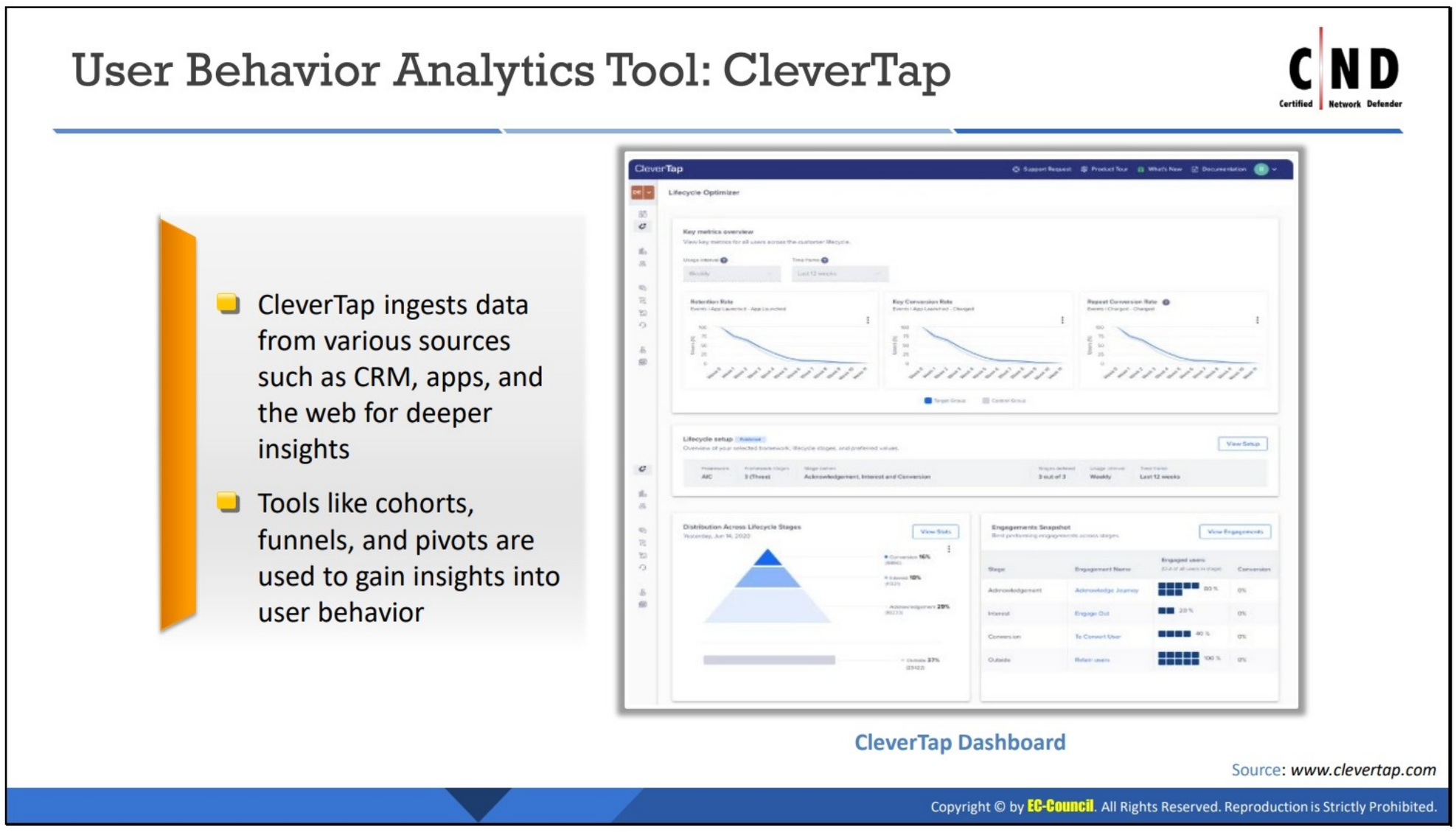
Use cases of UBA include the following:

- **Insider threats:** Many employees have access to crucial data. If an employee goes rogue, it can be challenging to stop them from accessing this data. In such cases, UBA helps in detecting when their behavior deviates from the norm.
- **Data theft:** UBA is effective in mitigating data theft by promptly identifying instances where a user attempts to download information beyond their authorized permissions. While the alert might be triggered after unauthorized access and data download have occurred, it enables administrators to swiftly respond by promptly disabling the account's access, thereby preventing any further data theft.
- **Compromised user accounts:** A valuable use case for UBA arises when a user's account gets compromised. In such instances, UBA can identify abnormal activities, like unauthorized access to sensitive information that the user typically does not attempt to access. Once detected, the system alerts a security analyst, prompting an immediate investigation.
- **Compromised hosts:** Beyond detecting compromised user accounts, UBA can identify compromised hosts, whether they are servers or personal devices, such as in the case of a malware infection. When a compromised host exhibits abnormal behavior, UBA triggers an alert, prompting cybersecurity personnel to conduct a thorough investigation.

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

https://t.me/learningnets

Technet24



User Behavior Analytics Tool: CleverTap

Source: https://clevertap.com/

CleverTap ingests data from various sources like CRM, apps, and the web for deeper insights. Tools like cohorts, funnels, and pivots are used to gain insights into user behavior. It creates micro-segments based on past behavior, real-time actions, and interests. It identifies at-risk customers based on recency and frequency.

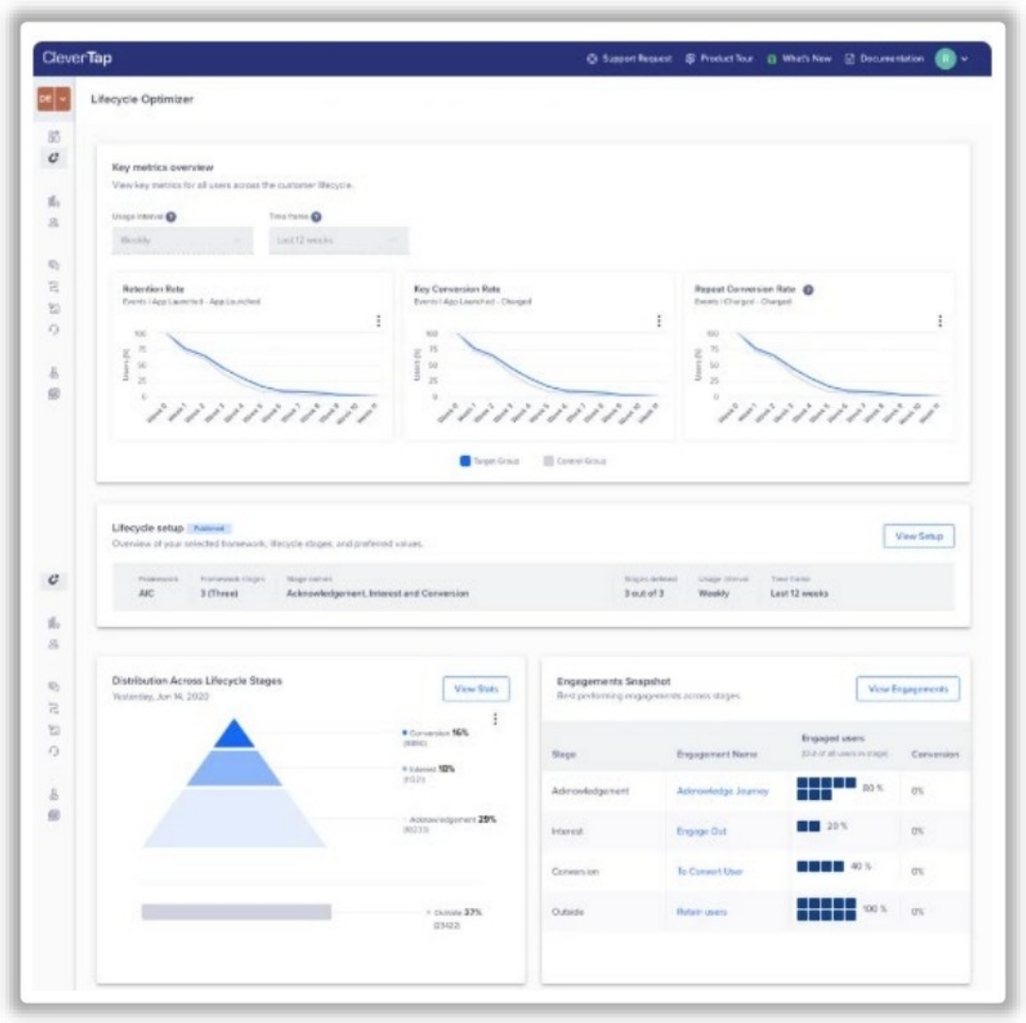


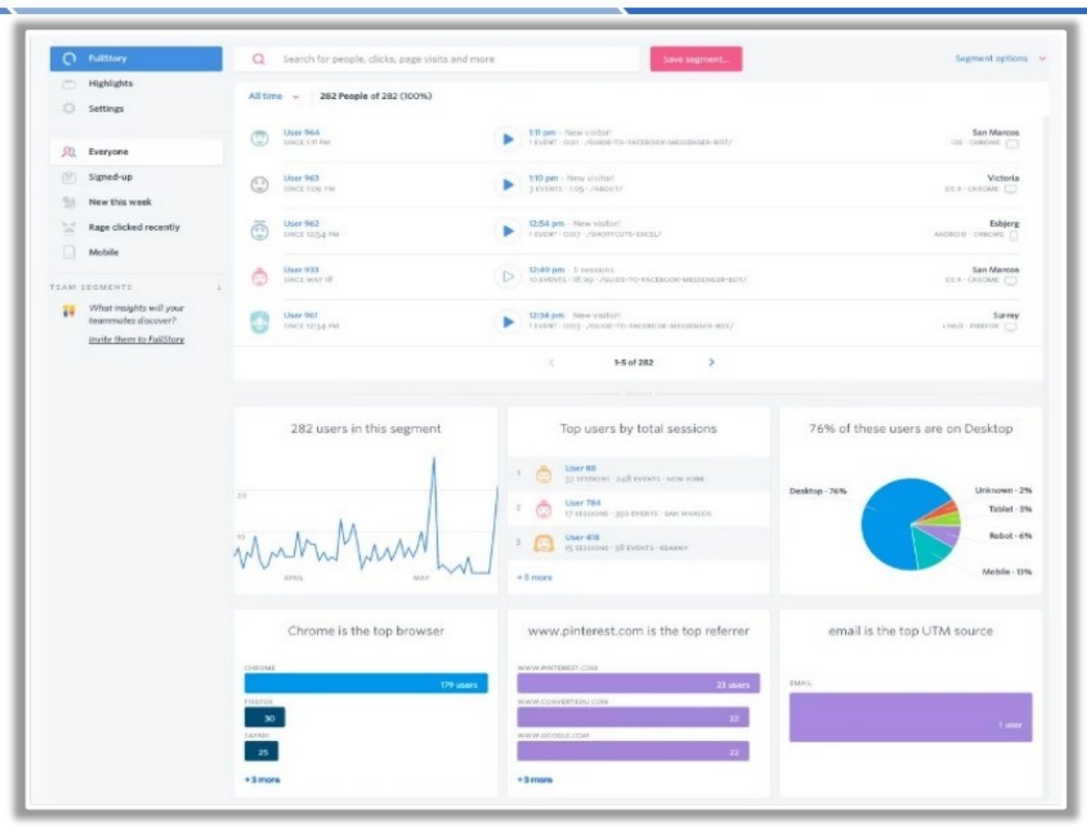
Figure 14.33: Lifecycle View of User Behavior using ClearTap

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

https://t.me/learningnets

User Behavior Analytics Tool: FullStory

- FullStory is an analytics platform that helps organizations **track and monitor user activity**
- Session playbacks provide a complete view of the user's journey



FullStory Dashboard

Source: *www.fullstory.com*

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

User Behavior Analytics Tool: FullStory

Source: https://www.fullstory.com/

FullStory is an analytics platform that helps organizations track and monitor user activity. Session playbacks provide a complete view of the user's journey, with everything automatically indexed, from clicks to page transitions. It assists organizations in tracking and monitoring user activity, inspecting customer activity, and creating funnels.

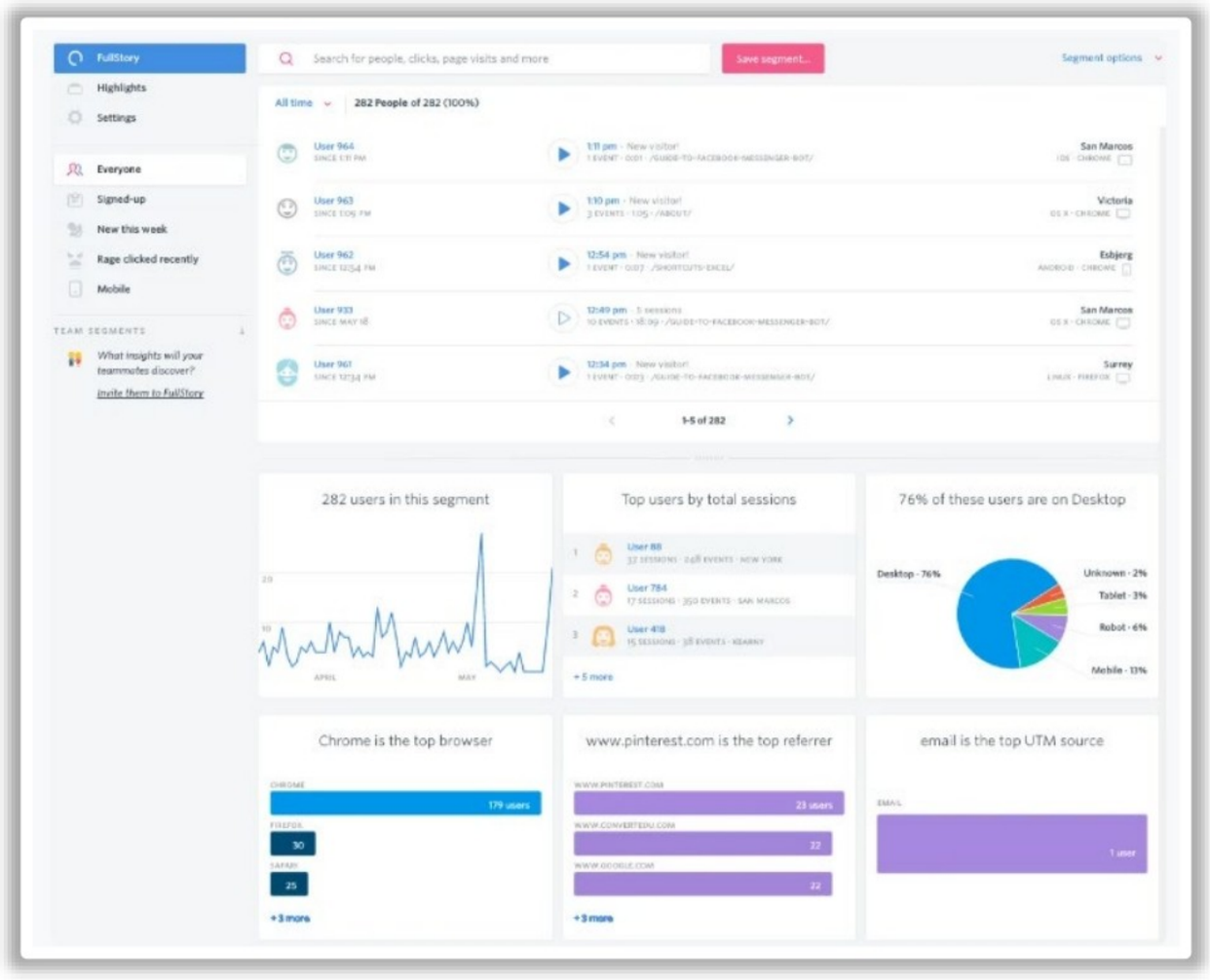
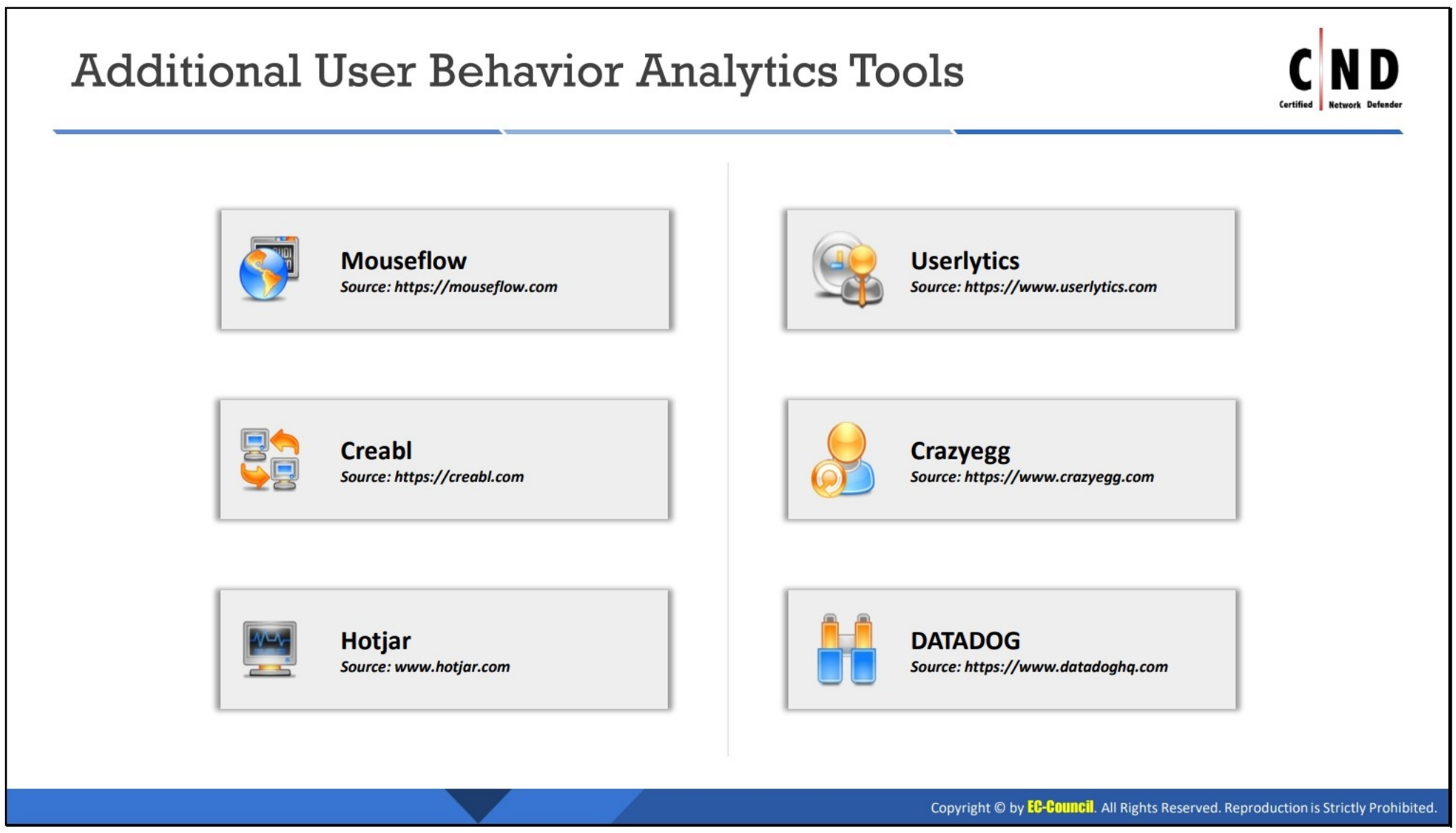


Figure 14.34: Full View of User Behavior

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

https://t.me/learningnets

Technet24



Additional User Behavior Analytics Tools

- **Mouseflow**

  Source: https://mouseflow.com/

  Mouseflow enables checkout funnel analysis to identify path-to-purchase improvements. Regardless of the conversion funnel type — eCommerce, financial services, SaaS, telehealth — Mouseflow helps streamline the user's journey. Mouseflow's website heatmap tool records 100% of your traffic by default, instead of sampling only a fraction of it.

- **Creabl**

  Source: https://creabl.com/

  Creabl records website interactions by capturing actual mouse movements as visitors navigate across pages on your website, enabling user session recording. You can observe where visitors click and how frequently they scroll up and down a page. Additionally, Creabl allows for the automatic sending of emails or the execution of other actions, based on specific events or multiple triggers, such as clicking a link or completing a form.

- **Hotjar**

  Source: https://www.hotjar.com/

  Hotjar provides an intuitive, visual way to discover, consolidate, and communicate user needs. It allows you to visualize conversion flows with funnels and understand where users are getting stuck by zooming into relevant recordings. Gain a high-level view of user data, spot issues before they become serious, identify trends, and uncover deeper insights with its dashboard.

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

https://t.me/learningnets

- **Userlytics**

  Source: https://www.userlytics.com/

  Userlytics' analytics dashboards feature tools like highlight reels, transcriptions, AI UX Analysis, and Sentiment Analysis, providing insights into your user experience. Userlytics' website usability testing helps uncover usability issues and customer pain points, enabling improvements for an optimal user experience. Additionally, Userlytics' no-download unmoderated testing feature allows for conducting shorter study sessions with more participants.

- **Crazyegg**

  Source: https://www.crazyegg.com

  Crazy Egg is an analytics platform that tracks and optimizes website visitor behavior to improve user experience, increase conversion rates, and boost the bottom line. It compares the performance of referring traffic, campaigns, and landing pages against each other.

- **Datadog**

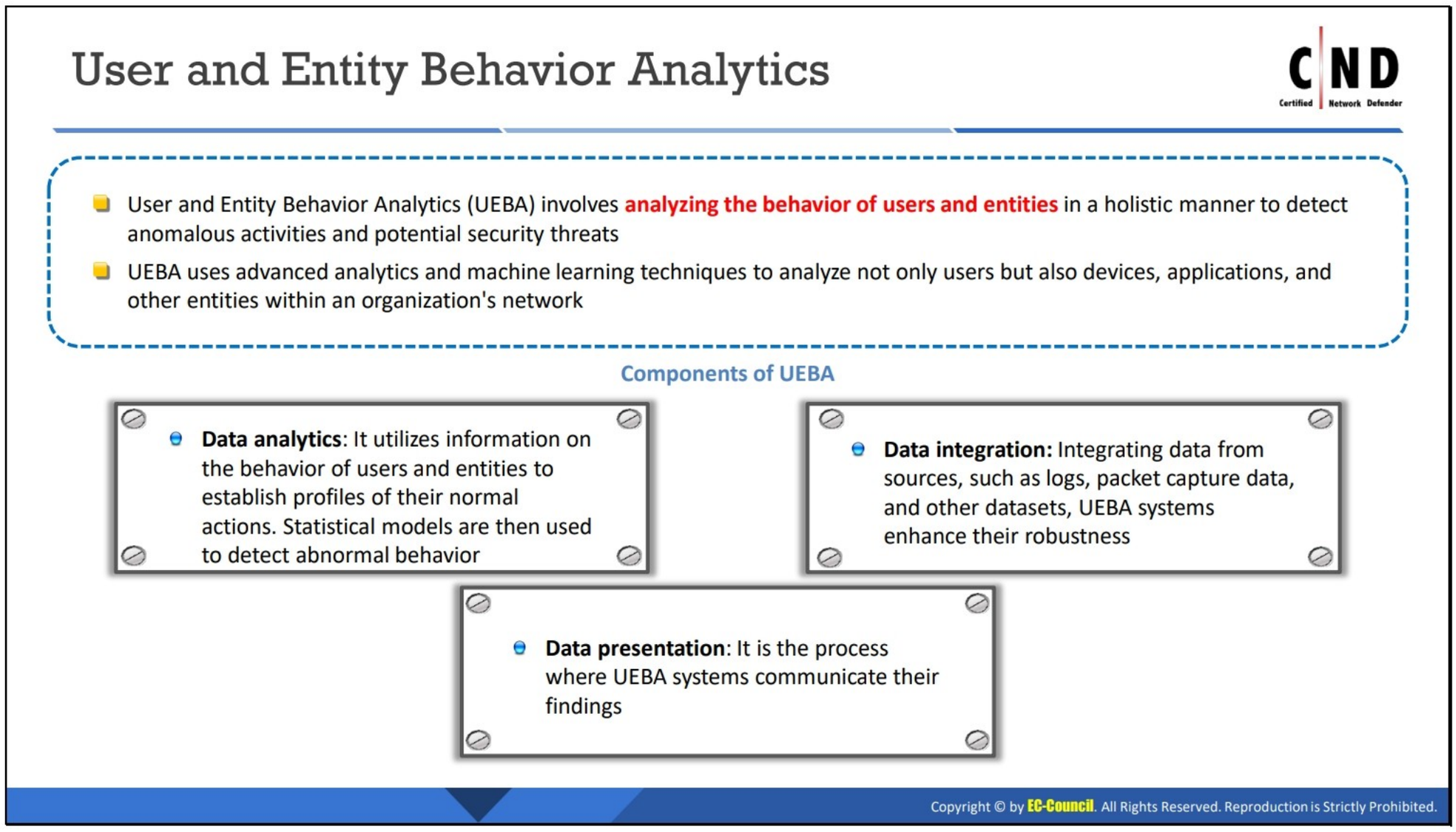
  Source: https://www.datadoghq.com/

  Datadog Real User Monitoring (RUM) offers insights into an application's frontend performance from the perspective of real users. It seamlessly correlates every user journey with synthetic tests, backend metrics, traces, logs, and network performance data. This integration allows for quick detection of poor user experiences and facilitates issue resolution with context from across the stack.

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

https://t.me/learningnets

Technet24



User and Entity Behavior Analysis

User and entity behavior analysis (UEBA) is the security process of detecting unusual anomalies in the behavior of users and entities like routers, endpoints, and servers in a network. It records the normal conduct of these entities and detects anomalous behavior when there is a deviation from the usual pattern. UEBA is primarily used to monitor and detect unusual traffic patterns, malicious activities, unauthorized data access, and movement on a network or endpoint. It employs machine learning algorithms, statistical analytics, and automation for this purpose.

How UEBA Works?

UEBA gathers, processes, and analyzes network activity using machine learning for users and entities to create a baseline behavioral reading. These readings are collected for each user or aggregated by department, role, or for the entire organization. Once the baseline is established, the algorithm identifies user and entity behaviors within the system that exceed or fall below the established baseline. When such anomalous activities are detected, the system raises an alert to inform administrators and security teams that something unusual is occurring on the network.

Components of UEBA

The components of UEBA are as follows:

- **Data analytics:** Data Analytics uses information about the typical behavior of users and entities to create profiles of their usual actions. By applying statistical models, the system can detect deviations from normal behavior and promptly notify system administrators.
- **Data** Integration**:** With integration into other security systems, UEBA can compare data gathered from various sources like packet capture data, logs, and datasets, making the system more robust.

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

https://t.me/learningnets

- **Data presentation:** This involves conveying the findings of the UEBA system and formulating an appropriate response, which can vary among organizations. Some UEBA systems generate alerts, prompting further investigation either by the employee or the IT administrator. In contrast, other UEBA systems are configured to take immediate action, like automatically cutting off network connectivity for an employee if a cyberattack is suspected**.**

Use Cases of UEBA

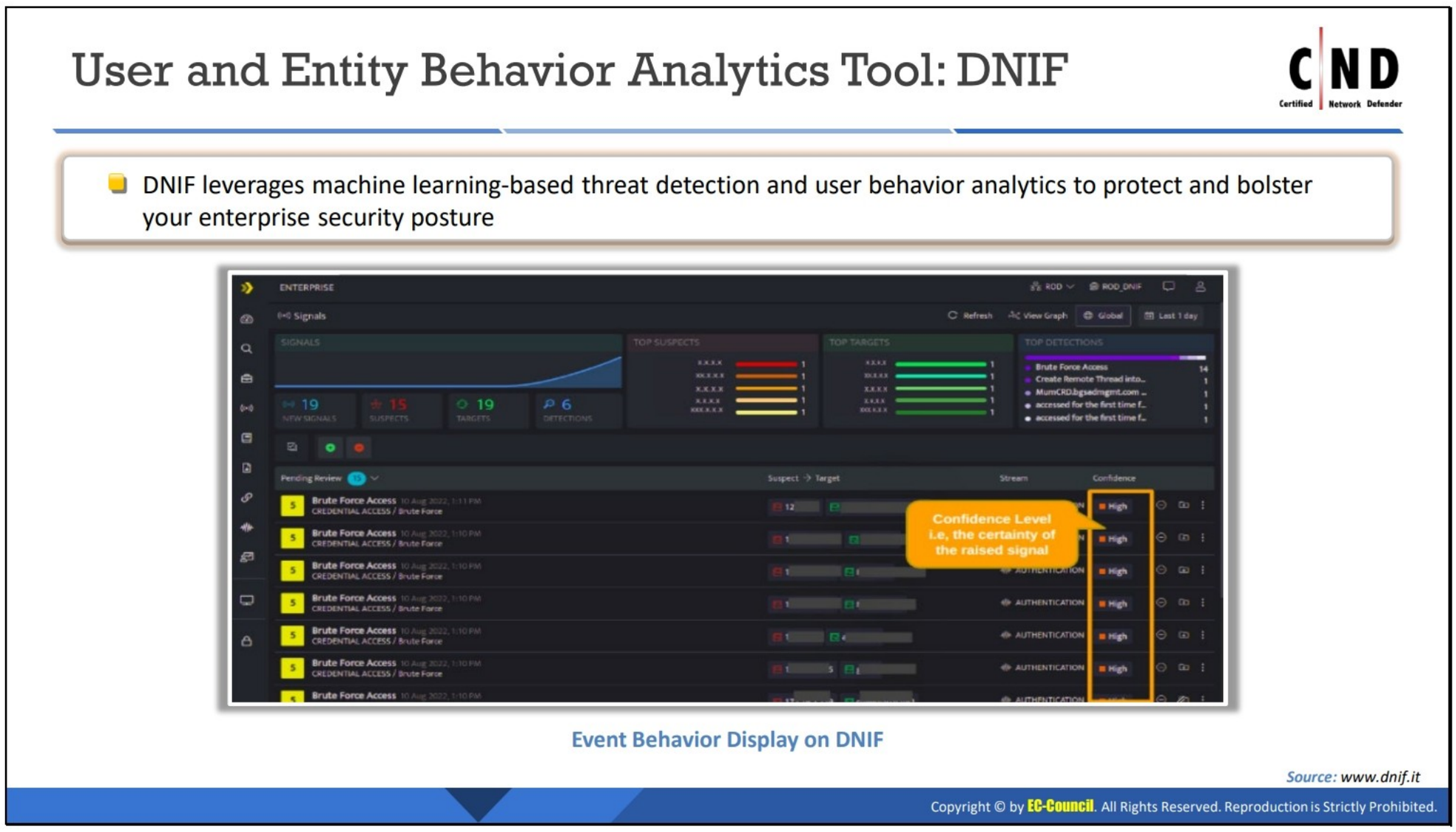
Use cases of UEBA include the following:

- **Lateral movement**: After breaching an endpoint or system, attackers can leverage it as a starting point to infiltrate other user accounts and systems. UEBA offers a holistic view across multiple systems, enabling the detection of unusual behavior throughout the network.
- **Stolen credentials**: Attackers can obtain valid user credentials. While traditional monitoring tools might not detect malicious activity carried out using these credentials, UEBA can recognize unusual behavior within the user's account.
- **Data theft**: UEBA examines data transfers to differentiate potential exfiltration attacks from legitimate activities. While some transfers might be authorized for users using external services, others could result from malicious intent with attackers using malware to exfiltrate sensitive information. UEBA evaluates the legitimacy of the destination and the appropriateness of the transmitted data based on the user's role and context.
- **Targeted devices and accounts**: UEBA assists in identifying abnormal actions on high-value assets, such as endpoint devices or accounts belonging to key executives like the CEO or CFO, which advanced attackers may specifically target.
- **Compromised hosts:** Attackers can remain undetected for extended periods, even months or years, after gaining control of a system or server within the corporate network. UEBA helps in spotting changes in system behavior and facilitates investigations to ascertain the presence of malicious activity**.**
- **Insider threats:** Malicious insiders pose a significant security challenge as they might evade detection by conventional security solutions. UEBA can detect risky or suspicious actions by users, such as transferring large data volumes, gaining higher privileges, or accessing unexpected applications or systems, which might indicate malicious intent.

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

https://t.me/learningnets

Technet24



Event Behavior Display on DNIF

User and Entity Behavior Analytics Tool: DNIF

Source: https://www.dnif.it/

DNIF leverages machine learning-based threat detection and user behavior analytics to protect and enhance your enterprise security posture. It identifies users exhibiting risky behavior, such as privileged access and atypical data movement. DNIF analyzes and detects patterns of human behavior in big data to reduce the attack surface. It learns from the anomalies that are most valuable and then screens out irrelevant detections. Historical analysis allows for the quick learning and profiling of user/entity/parameter behavior.

The features of DNIF tool are as follows:

- Identify users exhibiting risky behavior such as privileged access and atypical data movement.
- DNIF learns from the anomalies that the organization finds most valuable, and then screens out irrelevant detections.
- Leverage ML models to detect and make high-level decisions around the organization's security posture.

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

https://t.me/learningnets

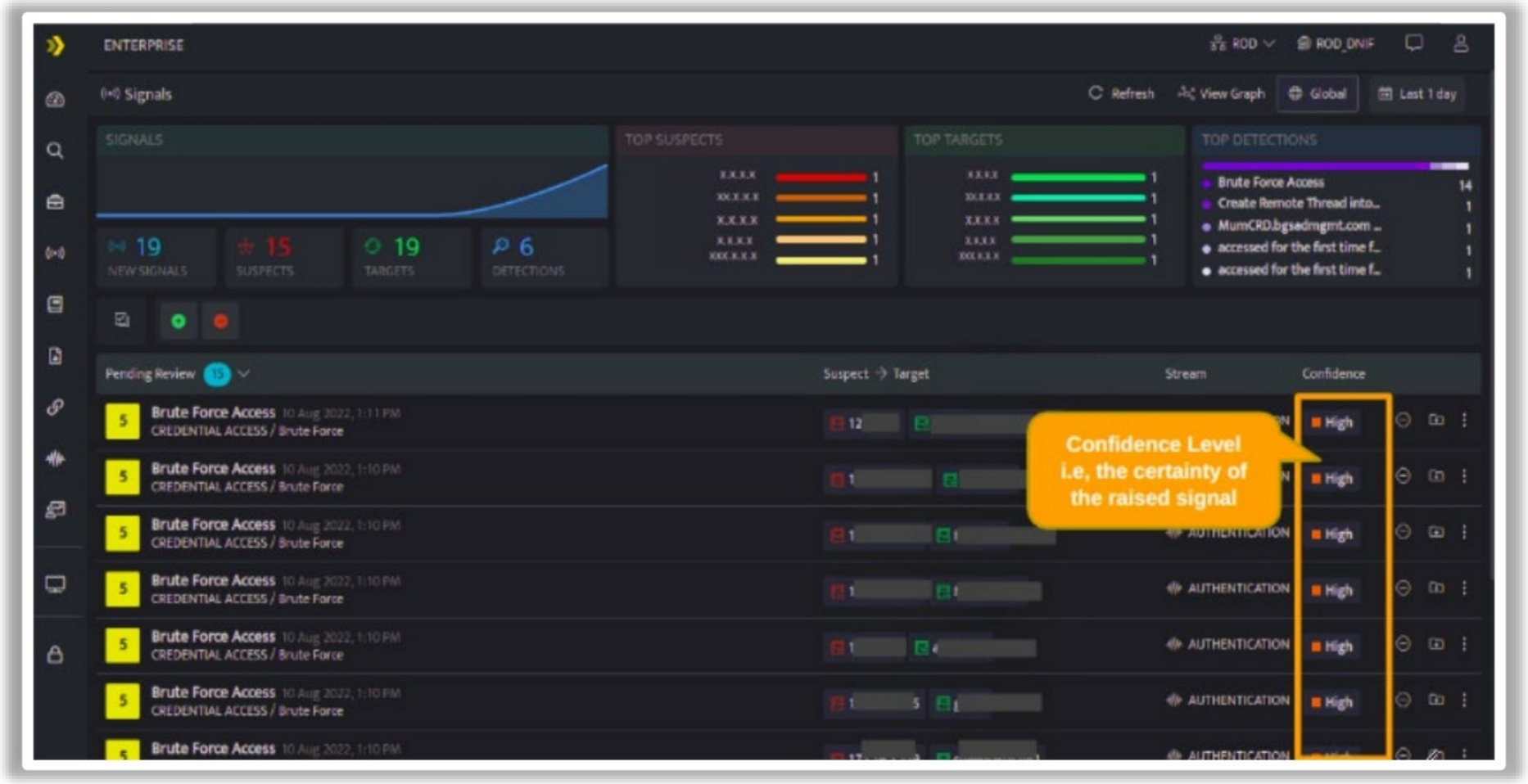
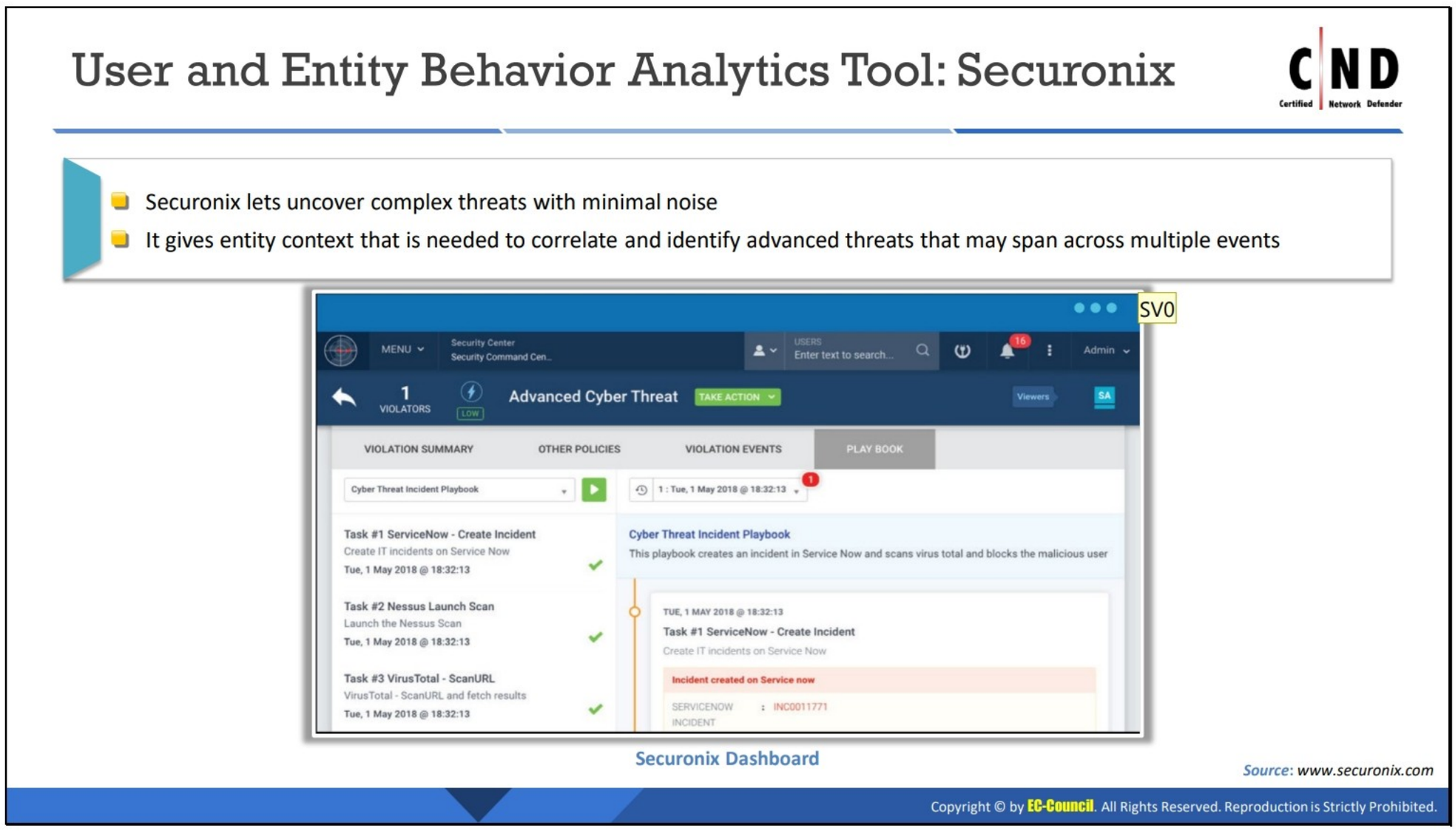


Figure 14.35: Dnif Webpage

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

https://t.me/learningnets

Technet24



User and Entity Behavior Analytics Tool: Securonix

Source: https://www.securonix.com/

Securonix helps uncover complex threats with minimal noise. It provides entity context needed to correlate and identify advanced threats that may span across multiple events. It extends security monitoring to cloud environments with built-in APIs for all major cloud infrastructure and application technologies. Securonix mitigates the risk from insiders with a UEBA that combines events with user context to alert security teams of behaviors that deviate from the established baseline. It can be quickly deployed on top of existing SIEM without having to replace it.

The features of Securonix tools are as follows:

- Mitigate the risk from insiders using UEBA that combines events with user context to alert the organization of behaviors that deviate from the established baseline.
- Extend security monitoring to the organization's cloud environment with built-in APIs for all major cloud infrastructure and application technologies.
- This UEBA can be deployed quickly on top of the organization's existing SIEM.

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

https://t.me/learningnets

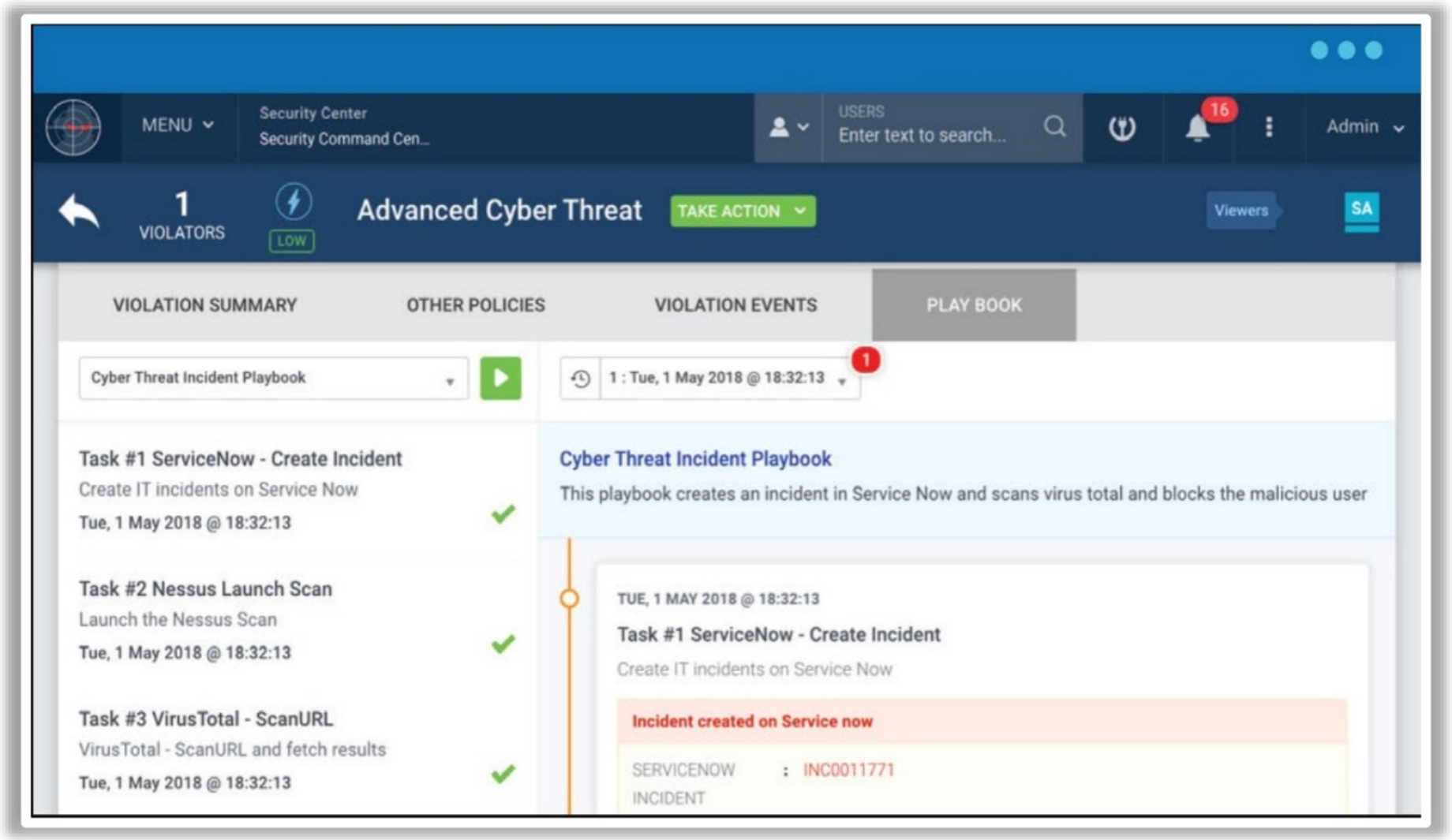
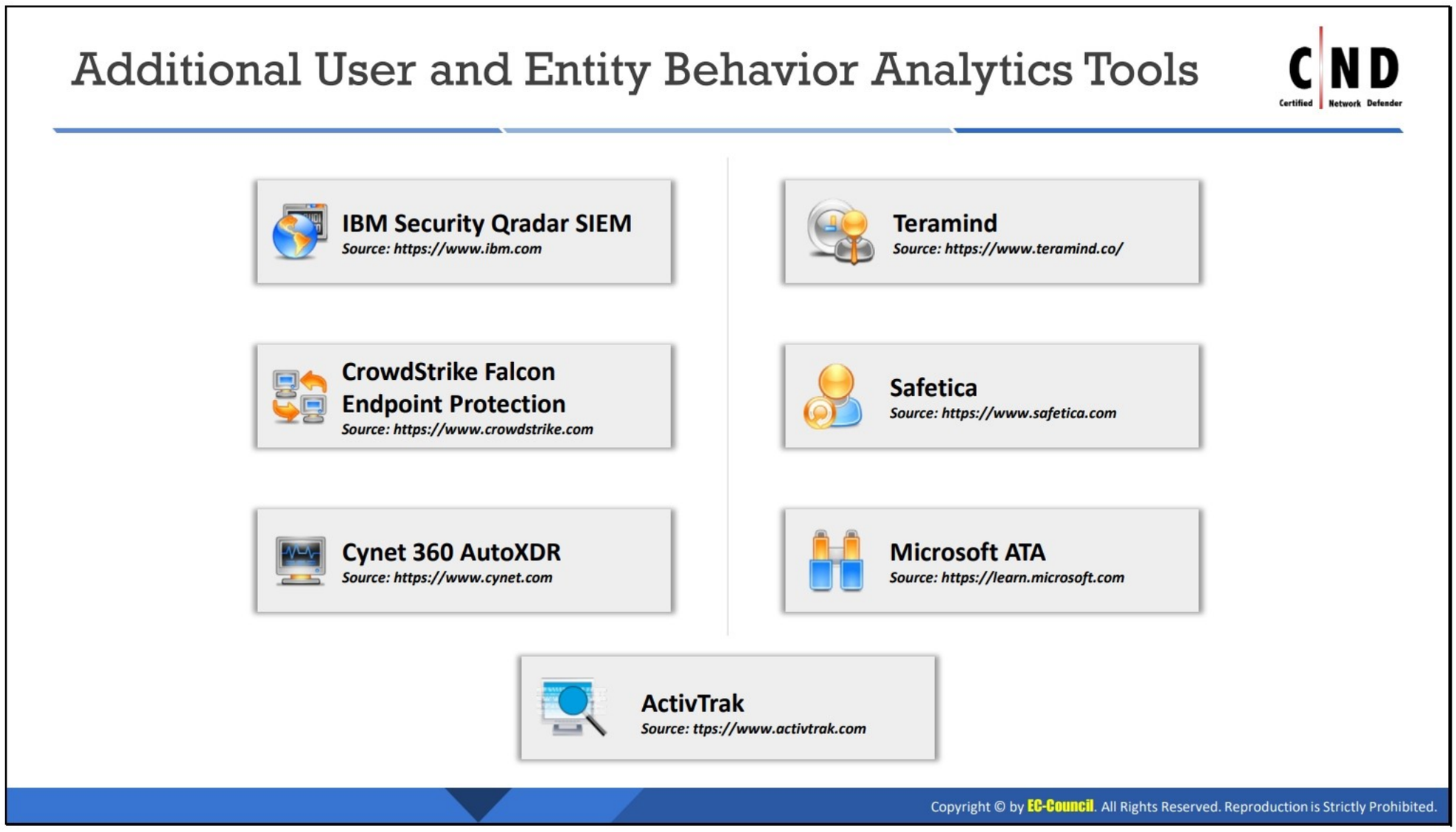


Figure 14.36: Securonix Dashboard

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

https://t.me/learningnets

Technet24



Additional User and Entity Behavior Analytics Tools

IBM Security Qradar SIEM

Source: https://www.ibm.com

This tool applies machine learning and user behavior analytics to network traffic alongside traditional logs, providing analysts with more accurate, contextualized, and prioritized alerts. QRadar SIEM makes threat detection smarter and allows for faster remediation. Run your business in the cloud and on-premises with visibility and security analytics built to rapidly investigate and prioritize critical threats.

CrowdStrike Falcon Endpoint Protection

Source: https://www.crowdstrike.com

This tool protects systems through a single lightweight sensor — there is no need for on-premises equipment to be maintained, managed, or updated, and no requirement for frequent scans, reboots, or complex integrations. CrowdStrike Falcon's single lightweight sensor makes it a fast and easy solution for protecting businesses from cyber-attacks. CrowdStrike is widely trusted by businesses of all sizes across various sectors, including financial, healthcare providers, energy, and tech companies.

Cynet 360 AutoXDR

Source: https://www.cynet.com

Cynet enables any organization to put its cybersecurity on autopilot, streamlining and automating its entire security operations. This provides enhanced levels of visibility and

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

https://t.me/learningnets

protection, regardless of the security team's size, skill, or resources, and without the need for a multi-product security stack.

Teramind

Source: https://www.teramind.co/

Teramind is a provider of insider threat management, data loss prevention, and productivity and process optimization solutions powered by user behavior analytics. Serving enterprises, governments, and SMBs, Teramind has provided organizations around the world with actionable, data-backed workforce insights that reduce risk, increase productivity, and streamline business operations. Teramind's completely customizable platform enables businesses to bring data objectivity to their decision-making and operations. Available as an on-prem, cloud, private cloud, or hybrid deployment, the Teramind platform empowers organizations to detect, prevent, and mitigate insider threats and data loss with forensic-backed evidence while providing granular behavioral data that enhance efficiency, productivity, and performance.

Safetica

Source: https://www.safetica.com/us

Safetica software offers solutions for insider threats and data loss. There are two options available: Safetica NXT (cloud-native) and Safetica ONE (on-prem). Safetica ONE protects data against human error and malicious attacks. It is an all-in-one solution that integrates seamlessly with your existing security system. Safetica NXT, on the other hand, is a cloud-based DLP solution designed for companies without in-house infrastructure. It provides low-maintenance security through its ease of use and automated features.

Microsoft ATA

Source: https://learn.microsoft.com

Minimize the risk of damage and gain a succinct, real-time view of the attack timeline with Advanced Threat Analytics. Utilize built-in intelligence to learn, analyze, and identify both normal and suspicious user or device behavior.

ActivTrak

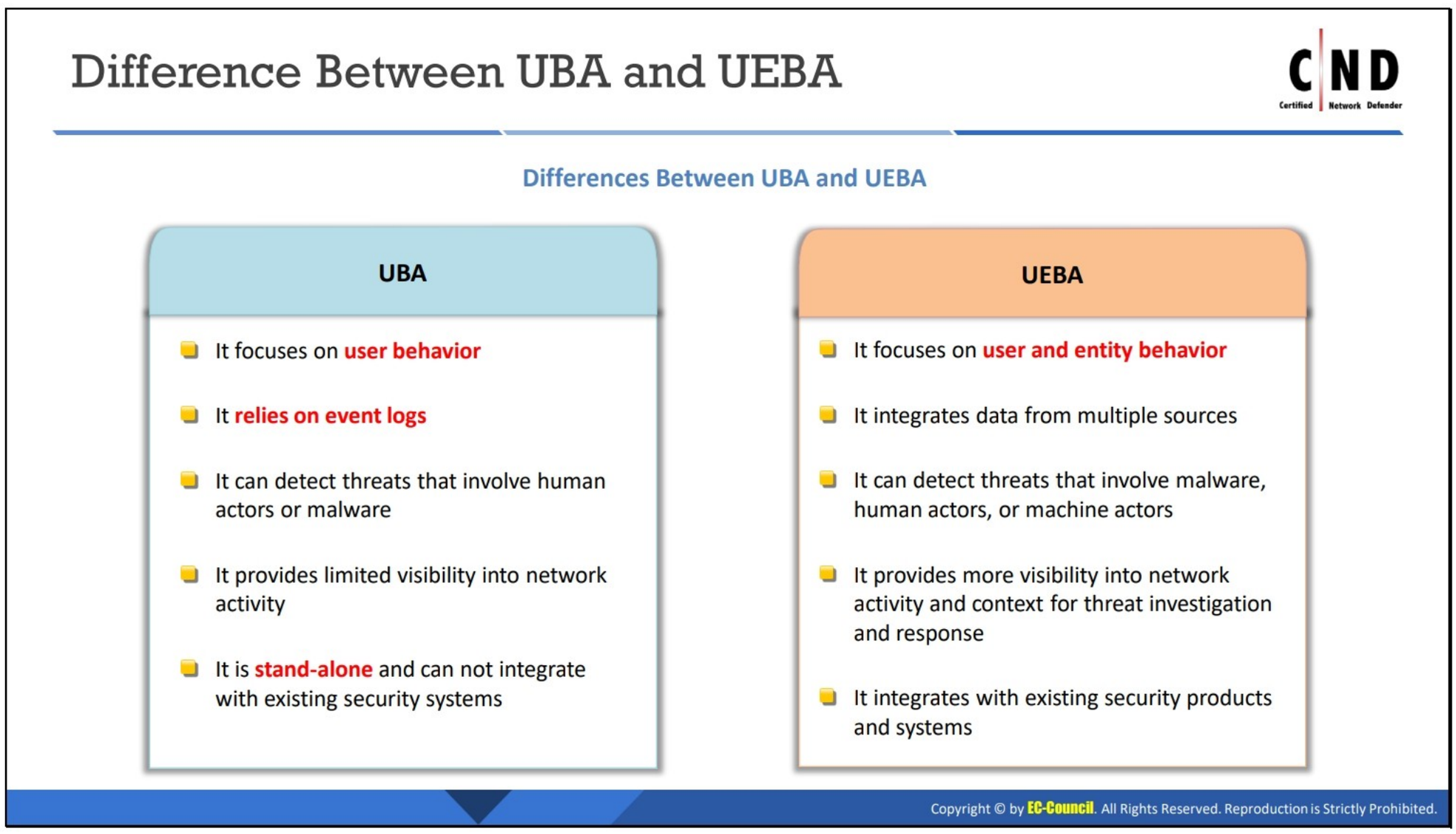
Source: https://www.activtrak.com

This workforce analytics software-as-a-service platform analyzes digital work activity data to glean insights that improve how people work, whether in the office or remotely. The workforce analytics cloud offers visibility and insights across people, processes, and technology, helping organizations inform key decisions and optimize outcomes.

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

https://t.me/learningnets

Technet24



UBA vs UEBA

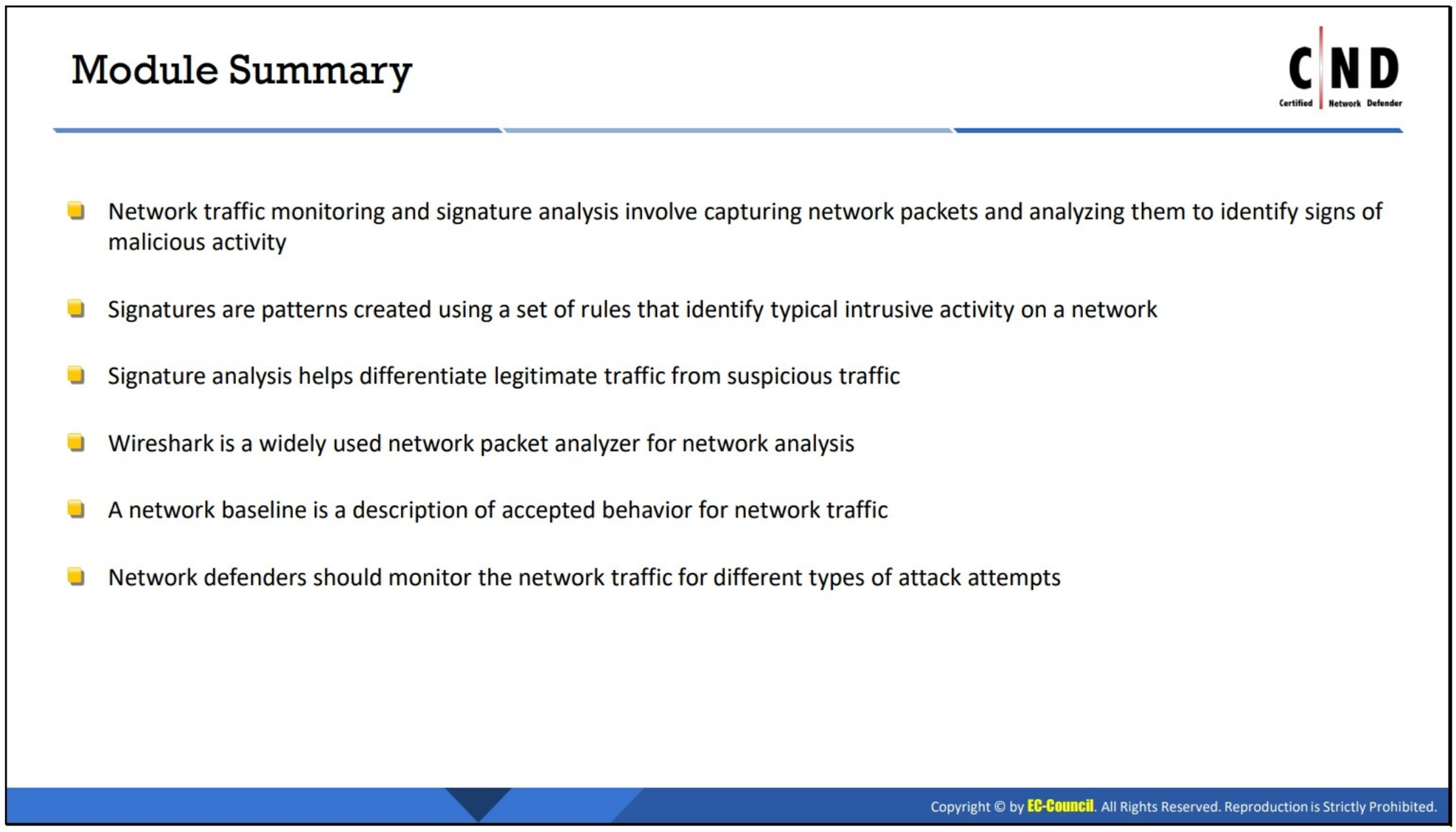
The differences between UBA and UEBA are as follows:

UBA	UEBA
It focuses on user behavior	It focuses on user and entity behavior
It relies on event logs	It integrates data from multiple sources
It can detect threats that involve human actors or malware	It can detect threats that involve malware, human actors, or machine actors
It provides limited visibility into network activity	It provides more visibility into network activity and context for threat investigation and response
It is a stand-alone and cannot integrate with existing security systems	It integrates with existing security products and systems

Table14.2: Differences Between UBA and UEBA

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

https://t.me/learningnets



Module Summary

This module covered the importance of manual network traffic monitoring, types of network signatures, network traffic baselining, network monitoring tools, and detection techniques for various types of attacks.

The key points discussed in this module are summarized as follows:

- Network traffic monitoring and signature analysis involve capturing network packets and analyzing them to identify signs of malicious activity.
- Signatures are patterns created using a set of rules that identify typical intrusive activity on a network.
- Signature analysis helps differentiate legitimate traffic from suspicious traffic.
- Wireshark is a widely used network packet analyzer for network analysis.
- A network baseline is a description of accepted behavior for network traffic.
- Network defenders should monitor the network traffic for different types of attack attempts.

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

https://t.me/learningnets

Technet24