EC-Council

Building A Culture Of Security

C|ND

Certified Network Defender

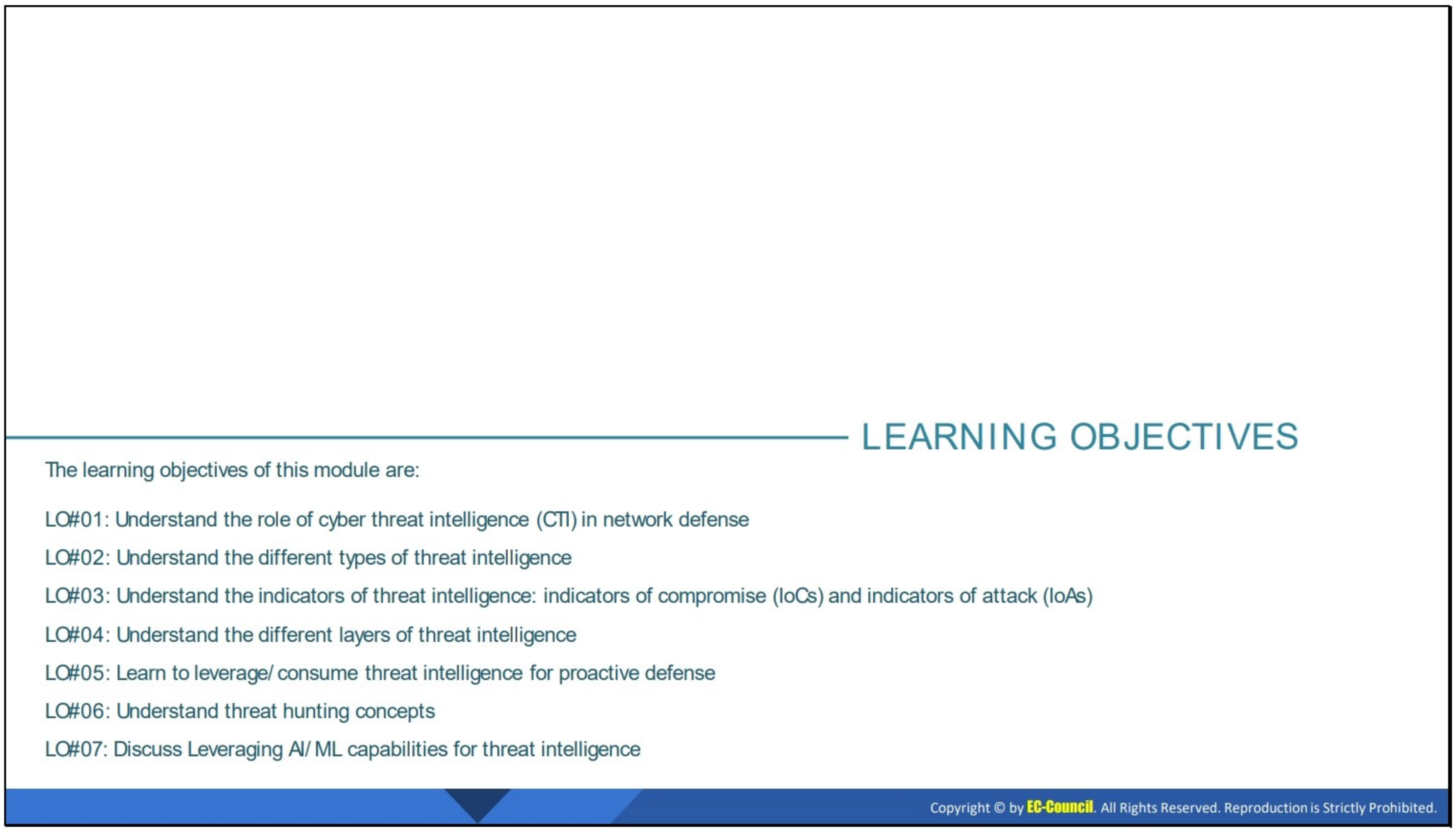
Certified Network Defender v3

MODULE 20

THREAT PREDICTION WITH CYBER THREAT INTELLIGENCE

EC-Council Official Curricula

This page is intentionally left blank.



LEARNING OBJECTIVES

The learning objectives of this module are:

LO#01: Understand the role of cyber threat intelligence (CTI) in network defense

LO#02: Understand the different types of threat intelligence

LO#03: Understand the indicators of threat intelligence: indicators of compromise (IoCs) and indicators of attack (IoAs)

LO#04: Understand the different layers of threat intelligence

LO#05: Learn to leverage/ consume threat intelligence for proactive defense

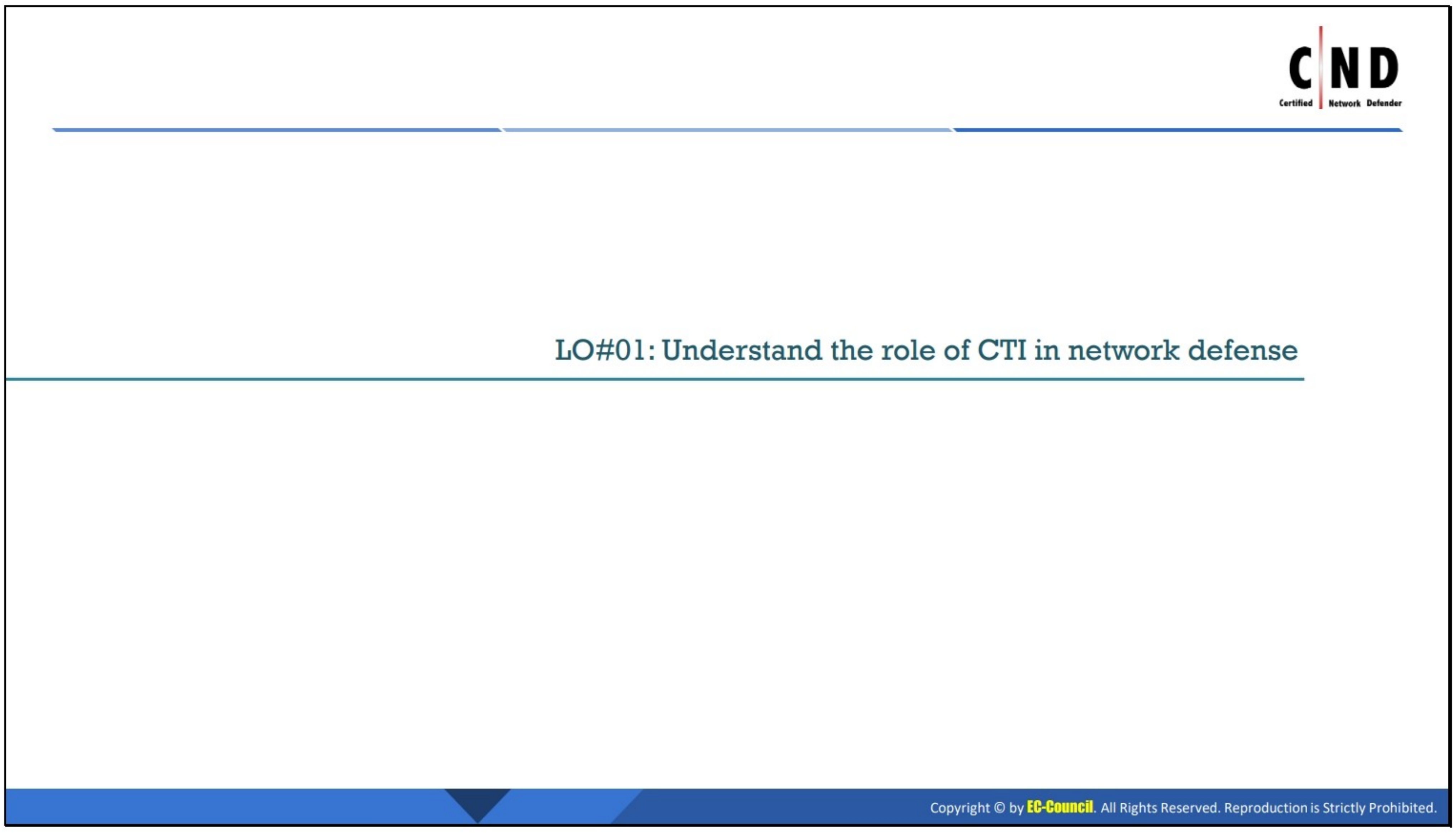
LO#06: Understand threat hunting concepts

LO#07: Discuss Leveraging AI/ ML capabilities for threat intelligence

Learning Objectives

Network defenders should analyze and filter threat intelligence feeds, or raw data about emerging or existing threat actors collected from various sources, to keep organizations' networks secure and protect against possible risks of advanced persistent threats, zero-day threats, and exploits. Threat intelligence provides the ability to respond quickly, decisively, and effectively to emerging threats. The learning objectives of this module are as follows:

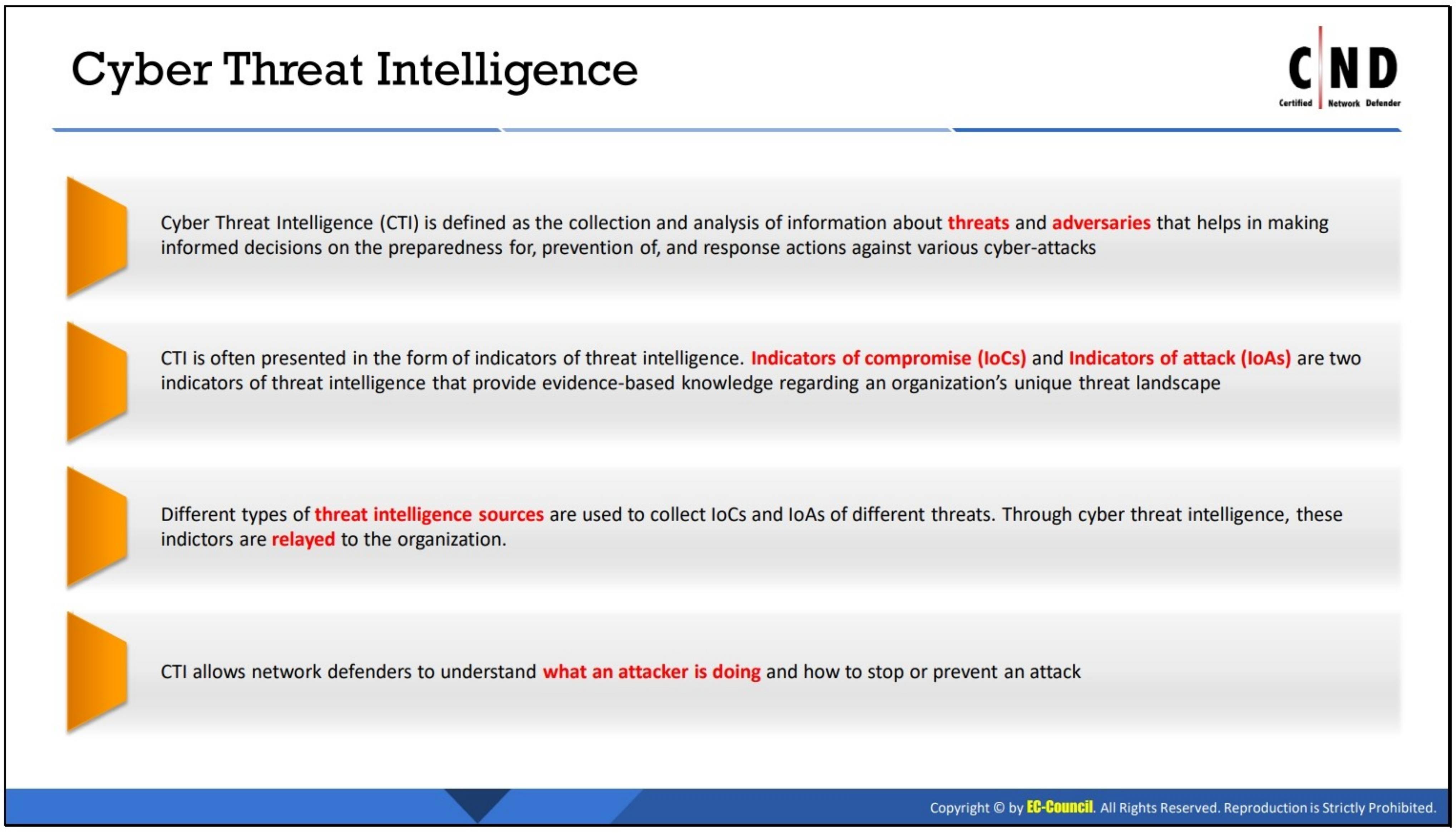
- Understand the Role of Cyber Threat Intelligence (CTI) In Network Defense
- Understand the Different Types of Threat Intelligence
- Understand the Indicators of Threat Intelligence: Indicators of Compromise (IoCs) and Indicators of Attack (IoAs)
- Understand the Different Layers of Threat Intelligence
- Learn to Leverage/Consume Threat Intelligence for Proactive Defense
- Understand threat hunting
- Leveraging AI/ML capabilities for threat intelligence



LO#01: Understand the role of CTI in network defense

LO#01: Understand the Role of CTI in Network Defense

Cyber threat intelligence (CTI) enables network defenders to predict future attacks by providing insight into the mechanisms and implications of threats. Further, it helps them understand their readiness status and reduce their attack surface. CTI gives the network defender better visibility of cyber threats and their risk to the organization’s security infrastructure. The objective of this section is to impart an understanding of the importance and role of CTI in network defense.



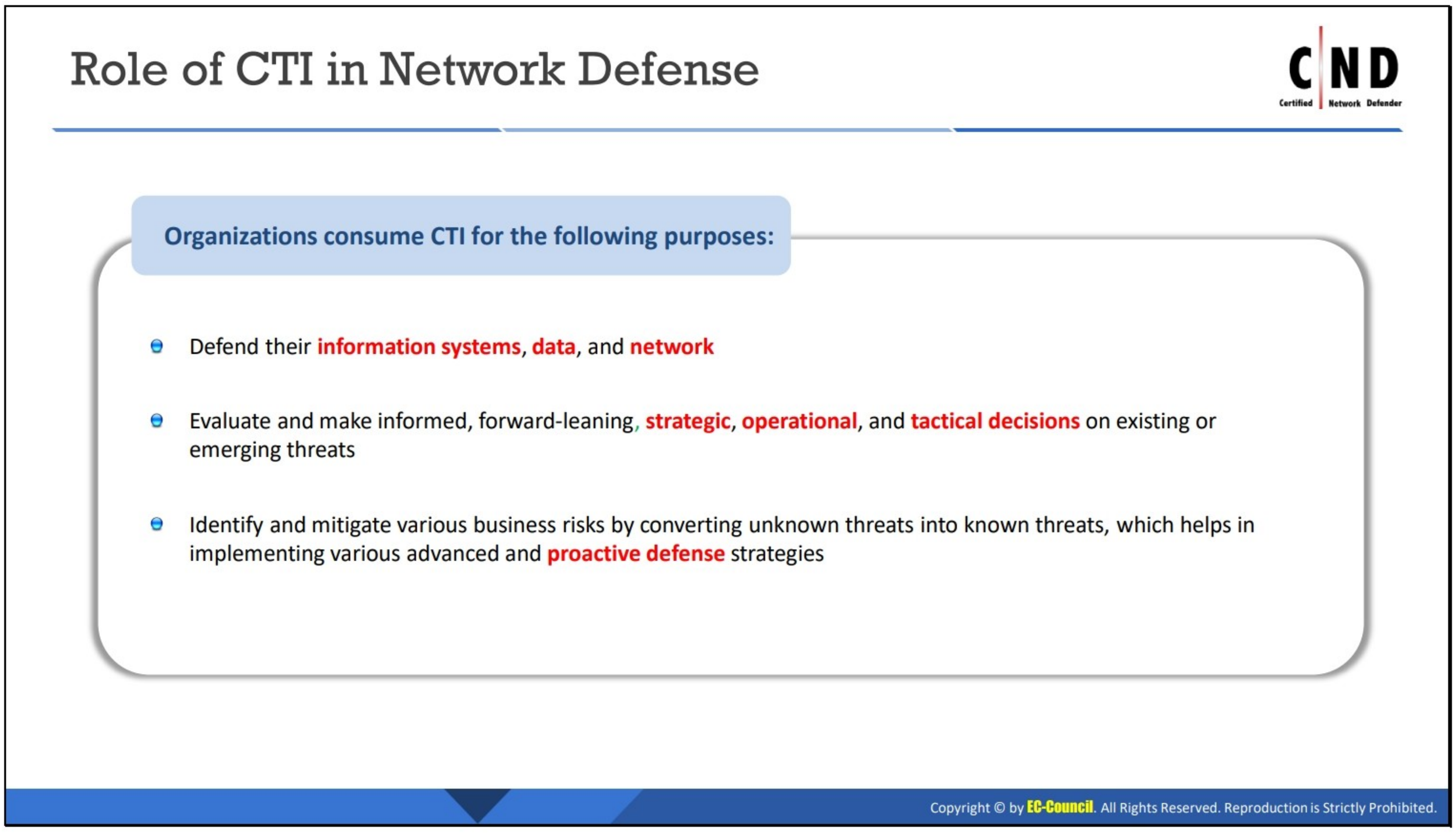
Cyber Threat Intelligence

- Cyber Threat Intelligence (CTI) is defined as the collection and analysis of information about **threats** and **adversaries** that helps in making informed decisions on the preparedness for, prevention of, and response actions against various cyber-attacks
- CTI is often presented in the form of indicators of threat intelligence. **Indicators of compromise (IoCs)** and **Indicators of attack (IoAs)** are two indicators of threat intelligence that provide evidence-based knowledge regarding an organization's unique threat landscape
- Different types of **threat intelligence sources** are used to collect IoCs and IoAs of different threats. Through cyber threat intelligence, these indictors are **relayed** to the organization.
- CTI allows network defenders to understand **what an attacker is doing** and how to stop or prevent an attack

Cyber Threat Intelligence

CTI is defined as the collection and analysis of information about threats and adversaries and drawing patterns to facilitate informed decisions on the preparedness for, prevention of, and response actions against various cyber-attacks. It is the process of recognizing or discovering any "unknown threats" that an organization can face so that necessary defense mechanisms can be applied to avoid them. It involves collecting, researching, and analyzing trends and technical developments in the field of cyber threats (i.e., cybercrime, hacktivism, espionage, etc.). Any knowledge about threats that can help an organization make plans and decisions to handle the threats can be termed threat intelligence. The main aim of the CTI is to make the organization aware of existing or emerging threats and prepare the organization to develop a proactive cybersecurity posture before these threats affect it. This process, in which unknown threats are converted into possibly known ones, helps in anticipating an attack and ultimately results in a better and secure system in the organization. Thus, threat intelligence is useful in achieving secure data sharing and transactions among organizations globally.

The threat intelligence process can be used to identify the risk factors responsible for malware attacks, SQL injections, web-application attacks, data leaks, phishing, and denial-of-service (DoS) attacks. Such risks, once filtered, can be placed on a checklist and handled appropriately. CTI helps an organization to handle cyber threats through effective planning and execution along with a thorough analysis of the threat; it also strengthens the organization's defense system, creates awareness about impending risks, and aids in responding to such risks.



Role of CTI in Network Defense

Organizations consume CTI for the following purposes:

- Defend their **information systems**, **data**, and **network**
- Evaluate and make informed, forward-leaning, **strategic**, **operational**, and **tactical decisions** on existing or emerging threats
- Identify and mitigate various business risks by converting unknown threats into known threats, which helps in implementing various advanced and **proactive defense** strategies

Role of CTI in Network Defense

Many organizations use threat intelligence to enhance aspects such as network security, incident response, and risk management. Threat intelligence helps in enhancing, implementing, and managing various security controls to protect IT assets from emerging threats. The inclusion of threat intelligence in cybersecurity programs can assist and improve the threat assessment process and provide accurate information on which security controls need to be incorporated to thwart emerging threats in an enterprise environment.

Discussed below are the organizational objectives for threat intelligence:

- **Enhanced and automated incident prevention**

  Many organizations use threat intelligence to improve and automate their incident prevention mechanisms. Organizations consume and analyze external threat intelligence to improve internal security controls to thwart evolving threats. Organizations must assess and craft well-informed, proactive choices pertaining to both current and emerging threats, encompassing strategic, operational, tactical, and technical decisions.

- **Automation of security operations and remediation activities**

  Organizations use threat intelligence to automate and enhance their security operations and remediation activities. Threat intelligence guides organizations in the decision-making process of cybersecurity investigations by focusing on people and process aspects.

- **Guidance to cybersecurity activities**

  Many organizations establish a threat intelligence center or service to provide guidance and monitor various cybersecurity activities of smaller sections within the organization.

- **Improved risk management**

  Many organizations consume threat intelligence to improve the efficiency of the risk management process. Threat intelligence is used to enhance risk-management metrics and mitigation strategies.

- **Improved incident detection**

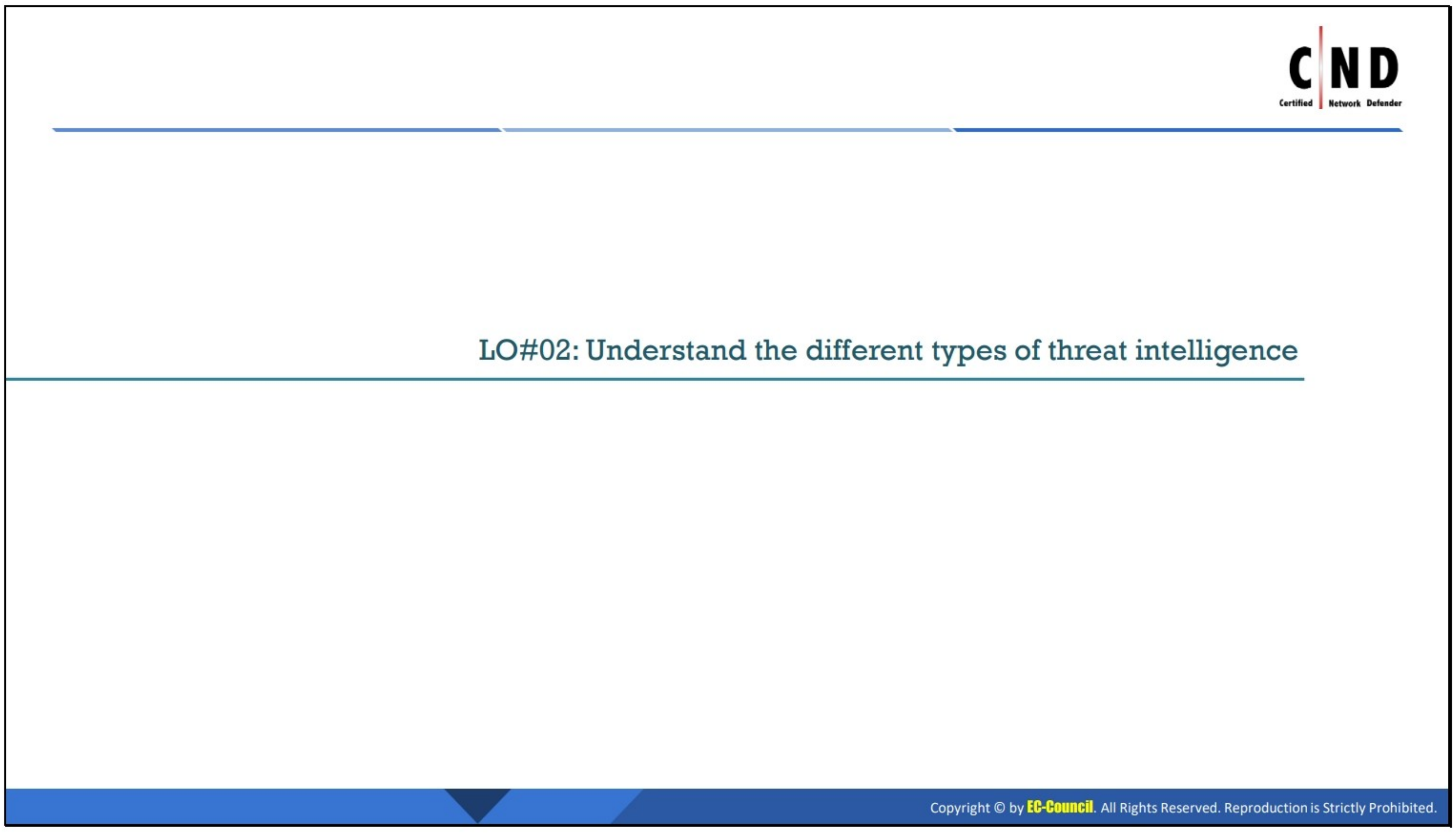
  In many organizations, network defender utilizes threat intelligence to enhance incident detection mechanisms in various security systems of the organization. Many malware detection systems use threat intelligence to detect malicious files entering the organization's network. The network defender uses threat intelligence to identify internal threats by extracting information such as IoCs; threat actors; and tactics, techniques, and procedures (TTPs).

With innovative TTPs, cyber threats are becoming major risks to any business sector. To prevent these threats, it is important for organizations to incorporate and leverage actionable threat intelligence to strengthen their current security posture.

Threat intelligence can be effectively leveraged to enhance the following areas of cybersecurity:

- **Identify and protect**
  - The monitoring of internal and external threats reveals unknown threats and vulnerabilities that pose risks to the organization.
  - Threat intelligence aids in adapting the current security strategy to the attacker's TTPs to prevent evolving threats.
  - A prepared assessment helps organizations evaluate their capability to leverage and operationalize the threat intelligence.
- **Detect**
  - Real-time threat monitoring and intelligence help organizations detect attacks rapidly and efficiently.
  - Threat intelligence helps analysts discover and focus on attacks at an early stage and reduces irrelevant and false-positive alerts.
  - Reliable intelligence feeds provide indicators of threats that help organizations uncover ongoing hidden intrusions.
- **Respond**
  - Threat intelligence provides contextual information about the attacks, including IoCs and TTPs, which helps the organization prevent the propagation of the attacks, reduce their impact, reduce their duration, and provide appropriate mitigations.
  - Threat intelligence supports the decision-making process with relevant details, which lead to enhanced incident response activities.

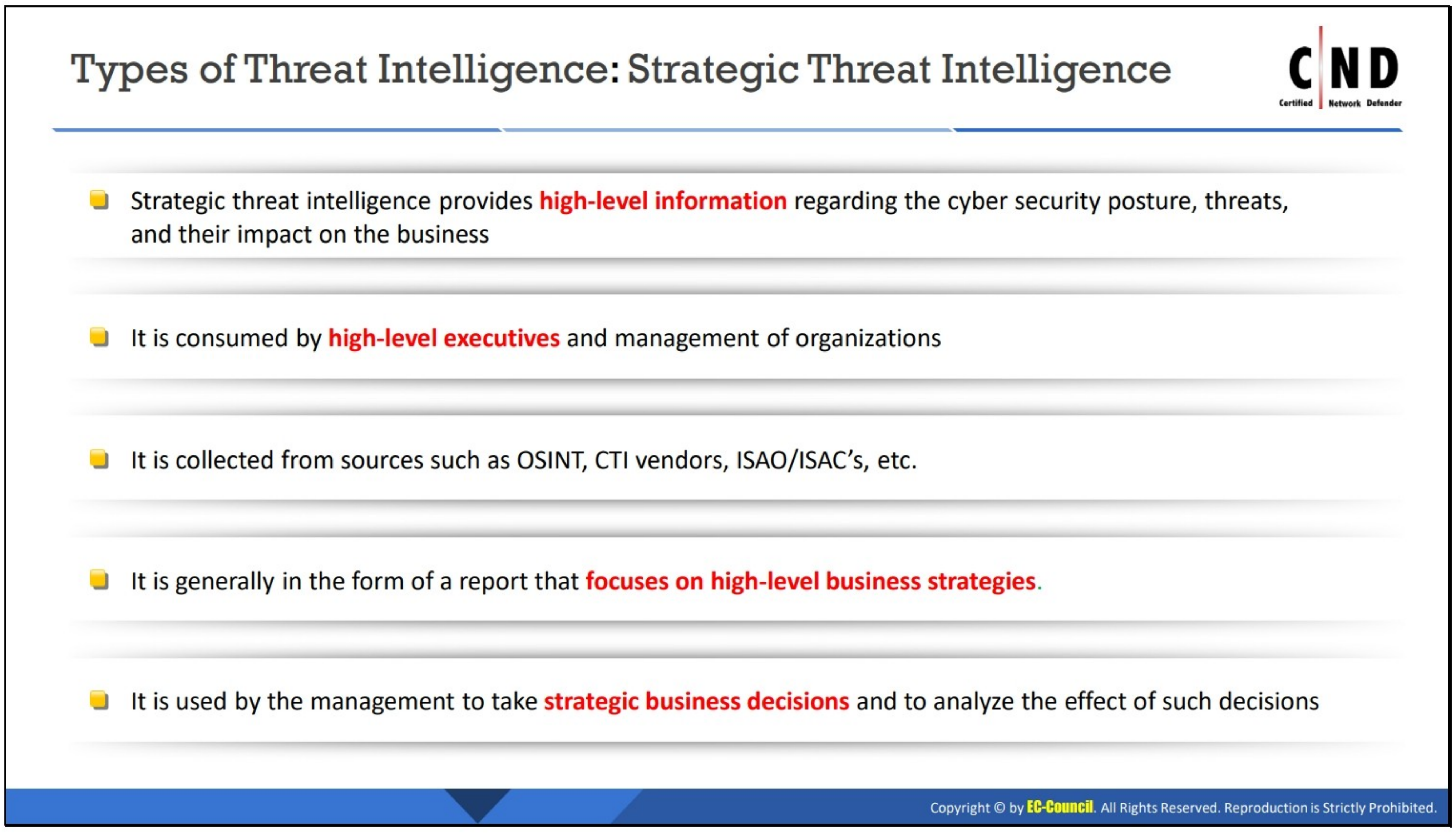
- **Recover**
  - Threat intelligence detects and removes persistent mechanisms of threat actors, such as malicious files installed on the systems, leading to rapid and efficient recovery from attacks.
  - Incorporating threat intelligence helps organizations meet compliance requirements.
  - Threat intelligence, by prioritizing security investments, helps in enhancing existing security mechanisms.



LO#02: Understand the different types of threat intelligence

LO#02: Understand the Different Types of Threat Intelligence

Threat intelligence is categorized based on the initial intelligence requirements, sources of information, and intended audience. This section discusses strategic threat intelligence, tactical threat intelligence, and operational threat intelligence.



Types of Threat Intelligence: Strategic Threat Intelligence

- Strategic threat intelligence provides **high-level information** regarding the cyber security posture, threats, and their impact on the business
- It is consumed by **high-level executives** and management of organizations
- It is collected from sources such as OSINT, CTI vendors, ISAO/ISAC's, etc.
- It is generally in the form of a report that **focuses on high-level business strategies**.
- It is used by the management to take **strategic business decisions** and to analyze the effect of such decisions

Types of Threat Intelligence: Strategic Threat Intelligence

Threat intelligence is contextual information that describes threats and guides organizations in taking various business decisions. It is extracted from a huge collection of sources and information. It provides operational insight by looking outside the organization and issuing alerts on evolving threats to the organization. For the efficient management of information collected from different sources, it is important to subdivide threat intelligence into different types. This subdivision is performed based on the consumers and goals of the intelligence. Based on the consumption, threat intelligence is divided into three types: strategic, tactical, and operational threat intelligence. These three types differ in terms of data collection, data analysis, and intelligence consumption.

Strategic Threat Intelligence

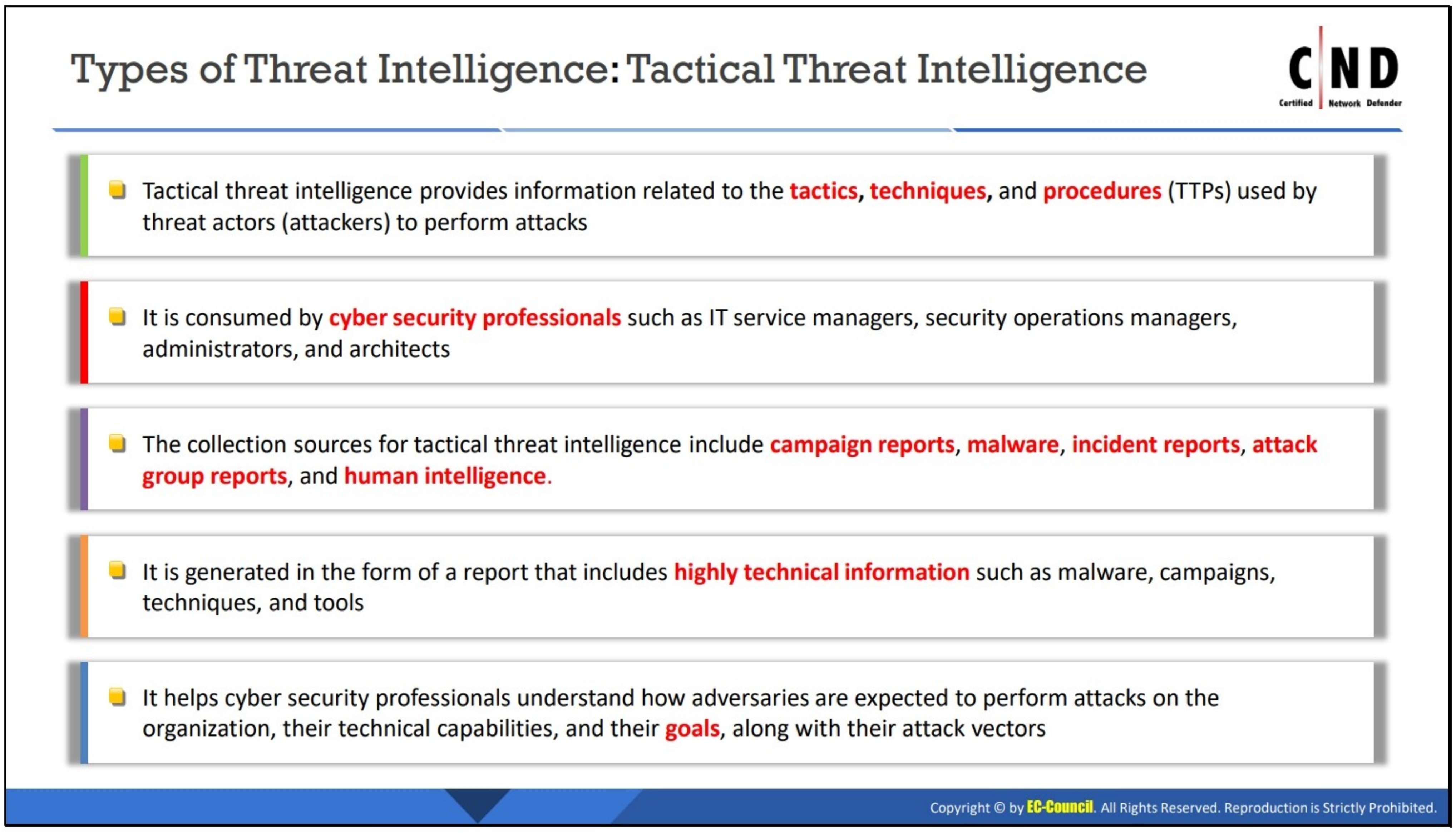
Strategic threat intelligence provides high-level information regarding cybersecurity posture, threats, details about the financial impact of various cyber activities, attack trends, and the impact of high-level business decisions. This information is consumed by high-level executives and the management of organizations, such as the IT management and chief information security officer (CISO). It helps the management in identifying current cyber risks, unknown future risks, threat groups, and the attribution of breaches. The intelligence obtained provides a risk-based view that focuses on high-level concepts of risks and their probability. It focuses on long-term issues and provides real-time alerts of threats on the organization's critical assets such as IT infrastructure, employees, customers, and applications. This intelligence is used by the management to take strategic business decisions and to analyze the effect of such decisions. Based on the analysis, the management can allocate sufficient budget and staff to protect critical IT assets and business processes.

Strategic threat intelligence is generally in the form of a report that focuses on high-level business strategies. Since strategic threat intelligence is pre-emptive in nature, data collection is related to high-level sources and requires highly skilled professionals. This intelligence is collected from sources such as open-source intelligence (OSINT), CTI vendors, and Information Sharing and Analysis Organizations (ISAOs)/Information Sharing and Analysis Centers (ISACs).

Strategic threat intelligence helps organizations identify similar incidents that might have occurred in the past, their intentions, or their attributions in order to know the adversaries of an attack, why the organization is within the scope of an attack, major attack trends, and how to reduce the risk level.

Generally, strategic threat intelligence includes the following information:

- Financial impact of cyber activity
- Attribution for intrusions and data breaches
- Threat actors and attack trends
- Threat landscape for various industry sectors
- Statistical information on data breaches, data theft, and malware
- Geopolitical conflicts of various cyber-attacks
- Information on how adversary TTPs change over time
- Industry sectors that might be impacted by high-level business decisions



Types of Threat Intelligence: Tactical Threat Intelligence

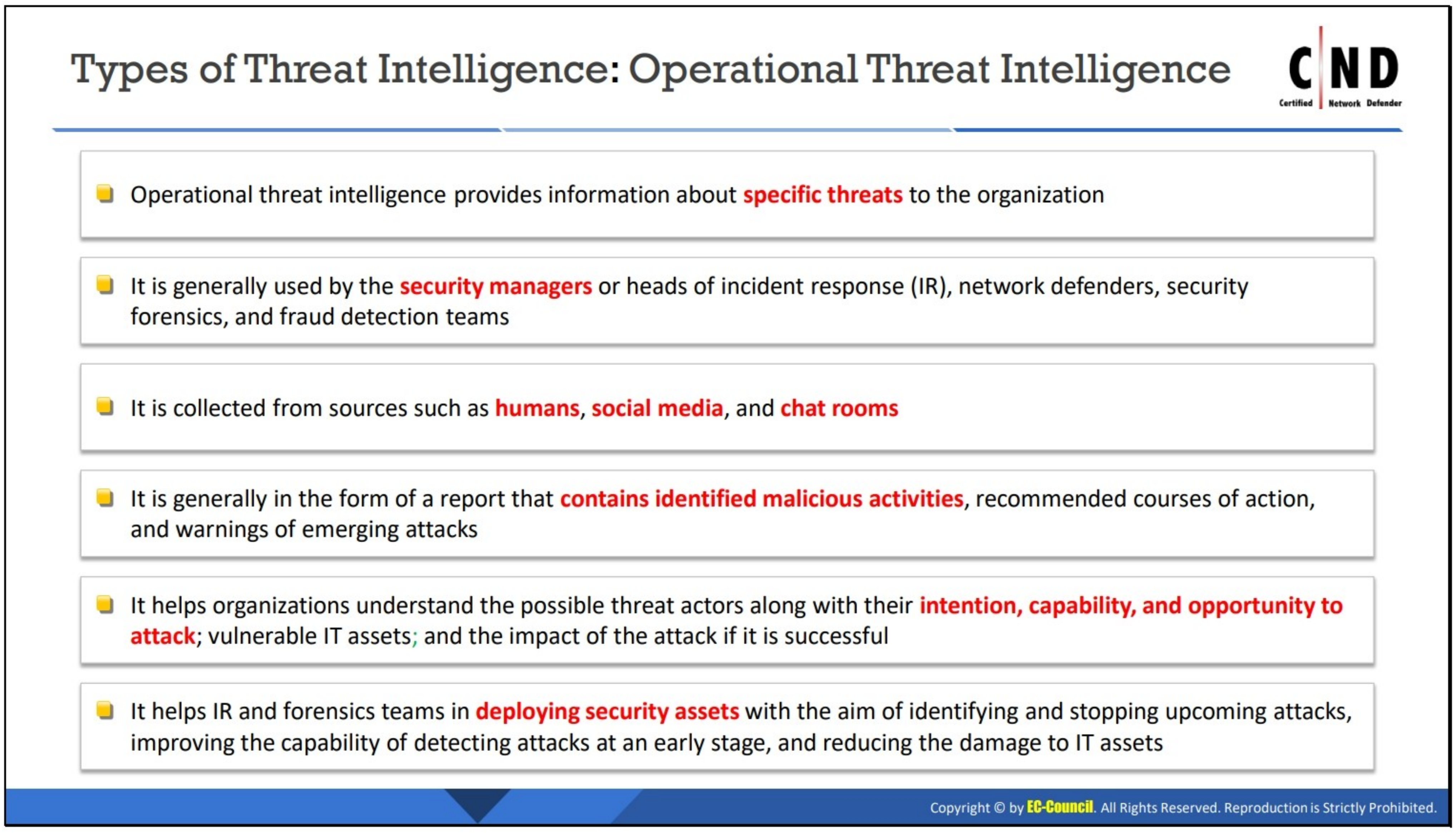
- Tactical threat intelligence provides information related to the **tactics**, **techniques**, and **procedures** (TTPs) used by threat actors (attackers) to perform attacks
- It is consumed by **cyber security professionals** such as IT service managers, security operations managers, administrators, and architects
- The collection sources for tactical threat intelligence include **campaign reports**, **malware**, **incident reports**, **attack group reports**, and **human intelligence**.
- It is generated in the form of a report that includes **highly technical information** such as malware, campaigns, techniques, and tools
- It helps cyber security professionals understand how adversaries are expected to perform attacks on the organization, their technical capabilities, and their **goals**, along with their attack vectors

Types of Threat Intelligence: Tactical Threat Intelligence

Tactical threat intelligence plays a major role in protecting the resources of an organization. It provides information related to the TTPs used by threat actors (attackers) to perform attacks. Tactical threat intelligence is consumed by cybersecurity professionals such as IT service managers, security operations managers, network operations center staff, administrators, and architects. It helps cybersecurity professionals understand how adversaries are expected to perform an attack on the organization, identify the information leakage from the organization, and the technical capabilities and goals of the attackers, along with the attack vectors. By using tactical threat intelligence, security personnel develop detection and mitigation strategies in advance by updating security products with identified indicators, patching vulnerable systems, etc.

The collection sources for tactical threat intelligence include campaign reports, malware, incident reports, attack group reports, and human intelligence. This intelligence is generally obtained by reading white/technical papers, communicating with other organizations, or purchasing intelligence from third parties. It includes highly technical information such as malware, campaigns, techniques, and tools in the form of forensic reports.

Tactical threat intelligence provides day-to-day operational support by helping analysts assess various security incidents related to events, investigations, and other activities. It also guides high-level executives of the organizations in arriving at strategic business decisions.



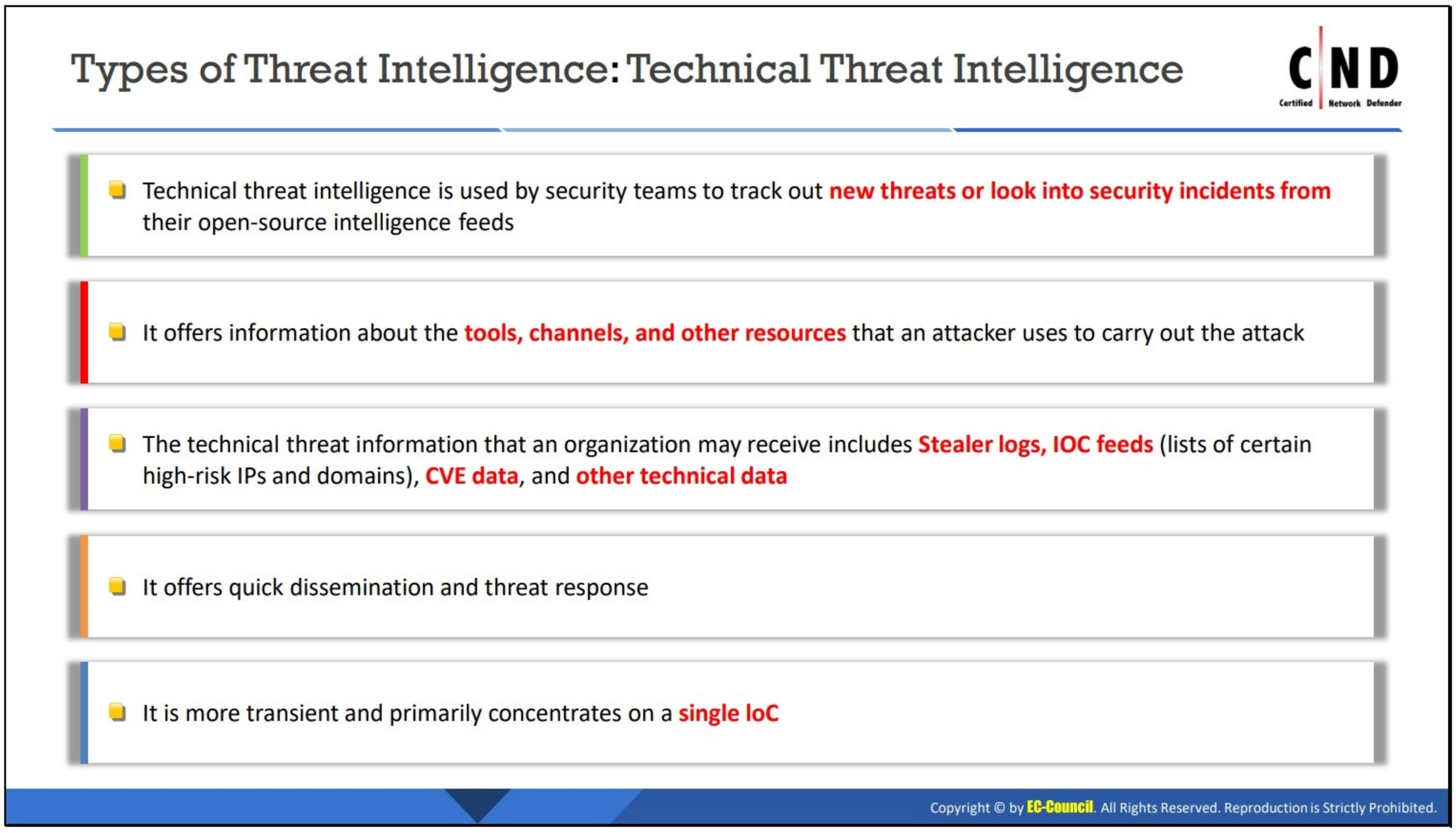
Types of Threat Intelligence: Operational Threat Intelligence

- Operational threat intelligence provides information about **specific threats** to the organization
- It is generally used by the **security managers** or heads of incident response (IR), network defenders, security forensics, and fraud detection teams
- It is collected from sources such as **humans**, **social media**, and **chat rooms**
- It is generally in the form of a report that **contains identified malicious activities**, recommended courses of action, and warnings of emerging attacks
- It helps organizations understand the possible threat actors along with their **intention, capability, and opportunity to attack**; vulnerable IT assets; and the impact of the attack if it is successful
- It helps IR and forensics teams in **deploying security assets** with the aim of identifying and stopping upcoming attacks, improving the capability of detecting attacks at an early stage, and reducing the damage to IT assets

Types of Threat Intelligence: Operational Threat Intelligence

Operational threat intelligence provides information about specific threats against an organization. It provides contextual information about security events and incidents that help defenders disclose potential risks, provide insight into attacker methodologies, identify past malicious activities, and efficiently perform investigations on malicious activity. It is consumed by security managers or heads of incident response (IR), network defenders, security forensics, and fraud detection teams. It helps organizations understand the possible threat actors and their intention, capability, and opportunity to attack; vulnerable IT assets; and the impact of the attack if it is successful. In many cases, only government organizations can collect this type of intelligence, which also helps IR and forensic teams in deploying security assets with the aim of identifying and stopping upcoming attacks, improving the capability of detecting attacks at an early stage, and reducing the damage on IT assets.

Operational threat intelligence is generally collected from sources such as humans, social media, and chat rooms, as well as from real-world activities and events that result in cyber-attacks. Further, operational threat intelligence is obtained by analyzing human behavior, threat groups, etc. This information helps in predicting future attacks and thus enhancing IR plans and mitigation strategies as required. Operational threat intelligence is generally in the form of a report that contains identified malicious activities, recommended courses of action, and warnings of emerging attacks.



Types of Threat Intelligence: Technical Threat Intelligence

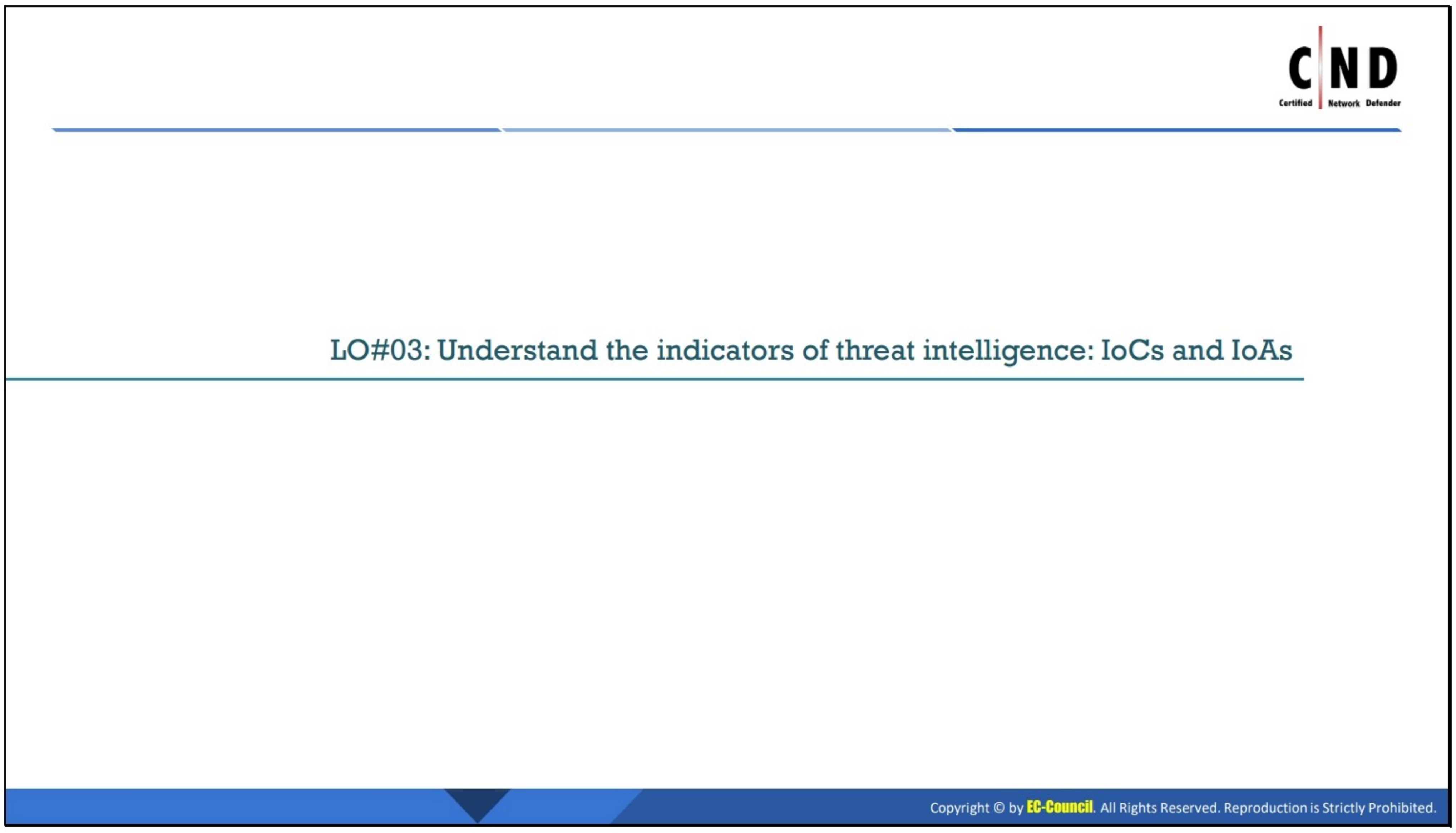
- Technical threat intelligence is used by security teams to track out **new threats or look into security incidents from** their open-source intelligence feeds
- It offers information about the **tools, channels, and other resources** that an attacker uses to carry out the attack
- The technical threat information that an organization may receive includes **Stealer logs, IOC feeds** (lists of certain high-risk IPs and domains), **CVE data**, and **other technical data**
- It offers quick dissemination and threat response
- It is more transient and primarily concentrates on a **single IoC**

Types of Threat Intelligence: Technical Threat Intelligence

Technical threat intelligence is used by security teams to track out new threats or look into security incidents from their open-source intelligence feeds. Technical threat intelligence is a vital tool for security teams, enabling them to monitor evolving threats, analyze open-source data, understand attack methods, and respond effectively. It also promotes ongoing learning and collaboration, bolstering an organization's cybersecurity defences.

It offers information about the tools, channels, and other resources that an attacker uses to carry out the attack. Technical threat intelligence provides essential insights into the tools, tactics, and communication channels employed by malicious actors in executing their attacks. This encompasses understanding the software tools and exploit methods, as well as recognizing the attack vectors, from phishing to advanced techniques. It also reveals the channels of operation, like compromised websites and command servers. The technical threat information that an organization may receive includes Stealer logs, IOC feeds (lists of certain high-risk IPs and domains), CVE data, and other technical data. Organizations can access a broad spectrum of technical threat data, encompassing detailed Stealer logs that offer insights into data theft activities. Furthermore, they have the option to utilize IOC feeds, which aggregate lists of high-risk IPs and domains, facilitating proactive measures to mitigate threats. Additionally, the availability of CVE data streamlines the process of identifying and ranking security vulnerabilities.

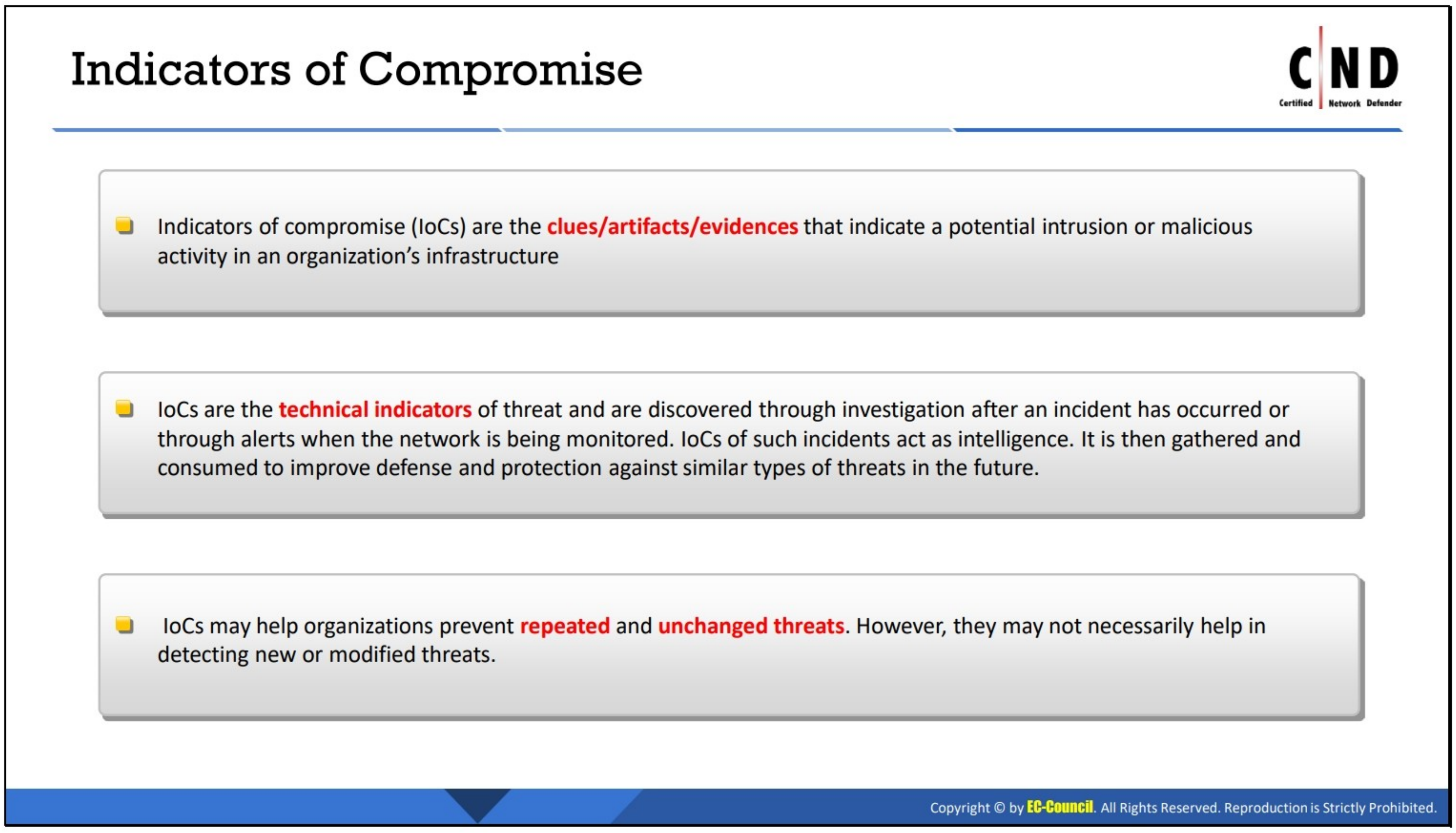
It offers quick dissemination and threat response. Furthermore, it facilitates the rapid sharing of vital information, empowering organizations to swiftly implement defensive measures and mitigate potential harm. It is more transient and primarily concentrates on a single IoC. It emphasizes pinpointing and addressing immediate threats with a narrow scope, ensuring timely and precise responses.



LO#03: Understand the indicators of threat intelligence: IoCs and IoAs

LO#03: Understand the Indicators of Threat Intelligence: IoCs and IoAs

Understanding the indicators of threat intelligence and analyzing indicators of attack (IoAs) and indicators of compromise (IoCs) enable network defenders to understand past events and identify the "how" and "why" of current events. Furthermore, understanding the difference between IoCs and IoAs is important for building a threat intelligence program for an organization. This section discusses IoCs and IoAs, as well as advantages and examples of IoCs and IoAs. In addition, the section explores the differences between IoAs and IoCs.



Indicators of Compromise

- Indicators of compromise (IoCs) are the **clues/artifacts/evidences** that indicate a potential intrusion or malicious activity in an organization's infrastructure

- IoCs are the **technical indicators** of threat and are discovered through investigation after an incident has occurred or through alerts when the network is being monitored. IoCs of such incidents act as intelligence. It is then gathered and consumed to improve defense and protection against similar types of threats in the future.

- IoCs may help organizations prevent **repeated** and **unchanged threats**. However, they may not necessarily help in detecting new or modified threats.

Indicators of Compromise

IoCs are the clues, artifacts, or evidence that indicate a potential intrusion or malicious activity in an organization's infrastructure. They are digital footprints of cyber threats or adversaries.

Any cyber-attack attempt leaves footprints indicating that an attack has occurred. These footprints (IoCs) are found in system files or log entries and help network defenders recognize malicious activities on a system or network. For instance, consider an unauthorized attempt to access a database that causes a breach. The network defenders in the organization spot the digital footprints of the unauthorized access by real-time tracking, proactive monitoring, and understanding the severity of the breach. This helps the network administrator take the required preventive measures to stop similar kinds of attacks in the future, thereby ensuring an effective system and network protection.

Anti-malware systems and threat intelligence platforms use IoCs to spot and stop malicious activities at an initial stage. Examples for IoCs include using specific registry entries, domain names of botnet command-and-control (C&C) servers, hashes of malware files, virus signatures, and Internet Protocol (IP) addresses.

IoCs have the following advantages:

- IoCs help organizations perform a complete forensic analysis. In detail, monitoring IoCs helps network defenders in organizations analyze cyber-attack attempts by providing critical threat intelligence.
- IoCs help identify cyber-attack incidents that have been overlooked by other tools.
- The recurrence of particular IoCs helps security teams update their security policies and tools to secure the organizations against future attacks.

The following is a disadvantage of IoCs:

- Although IoCs help organizations prevent repeated and persistent threats, they may not necessarily help detect new or modified threats.

Documenting IoCs and their associated threats enables organizations to share this information and enhance IR. Therefore, it is necessary to standardize IOC documentation and reporting.

IoC Formats

The following are some of the common formats used to record, define, and share different types of threat information internally and externally in a machine-digestible format.

- **OpenIOC:** OpenIOC, with its Extensible Markup Language (XML)-based framework, enables describing the complex semantics of the behavior of malware. It features definitions for specific technical details that include more than 500 indicator terms. Most of these indicator terms begin with the title names file, driver, disk, system, process, or registry. Examples for indicator terms are the file name and file MD5 hash. All these definitions are stored as an XML schema.

  Advantages of OpenIOC:

  - The XML framework of OpenIOC can be used in forensic investigation reports as it is readable by both the machine and human.
  - OpenIOC improves the reliability and repeatability of the malware forensics investigation process by providing a standard documentation syntax.
  - The derived OpenIOC indicators can be used by security tools for monitoring and detecting incidents and can also be used for configuring appropriate security controls and policies.

- **CybOX:** Cyber Observable Expression (CybOX) provides a standard for defining indicator details (observables) regarding measurable events and stateful properties. It mainly aims at automating the sharing of security information by providing more than 70 defined objects. CybOX can be used to acquire threat intelligence as well as for log management, malware characterization, IR, and forensic investigation.

- **STIX:** The Structured Threat Information Expression (STIX) defines threat information including threat details and the context of the threat. By using XML, it defines threat-related constructs. The following are the data elements (threat-related constructs) supported by STIX:

  - Observables
  - Cyber-attack campaigns
  - Exploit targets
  - Incidents
  - Indicators
  - Threat actors

- TTPs
- Adversary tactics, techniques, and procedures (attack patterns, exploits, tools, and infrastructure)

The STIX language can be used for the following:

- **Identifying and analyzing cyber threats:** Review the structured and unstructured information related to the cyber threat activity.
- **Specifying indicator patterns:** Specify measurable patterns.
- **Managing response activities:** Manage IR to prevent, detect, investigate, and respond to threats.
- **Defining and sharing threat information:** Define and share different types of threat information.

- **TAXII:** The Trusted Automated Exchange of Indicator Information (TAXII) is a set of specifications for exchanging cyber threat information over Hypertext Transfer Protocol Secure (HTTPS). TAXII uses XML and HTTP for message contents and transport, respectively. It is specially created to support the exchange of CTI represented in STIX.

  TAXII supports the following three sharing models.

  - **Hub and spoke**: One repository of information
  - **Source/subscriber**: A single source of information
  - **Peer to peer**: Sharing of information by multiple groups

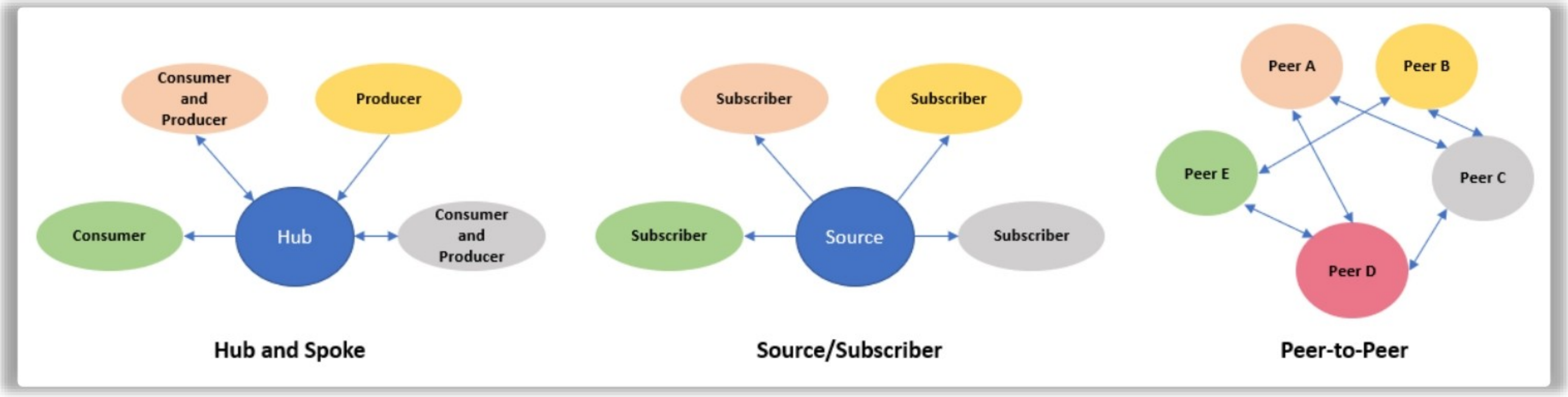


Figure 20.1: Three Sharing Models of TAXII

- **MAEC:** Malware Attribute Enumeration and Characterization (MAEC) is a standardized language to describe CTI. It defines three output formats:

  - **The MAEC bundle** captures and shares the data obtained from the analysis of a single malware instance.
  - **The MAEC package** captures and shares data for one or more malware subjects that comprise a particular malware instance's detail as well as the data derived from analysis and metadata.

- **The MAEC container** allows a user to share the collection of MAEC-characterized data, including one or more MAEC packages.
- **The MAEC default vocabularies** define a default set of controlled vocabularies used within MAEC.

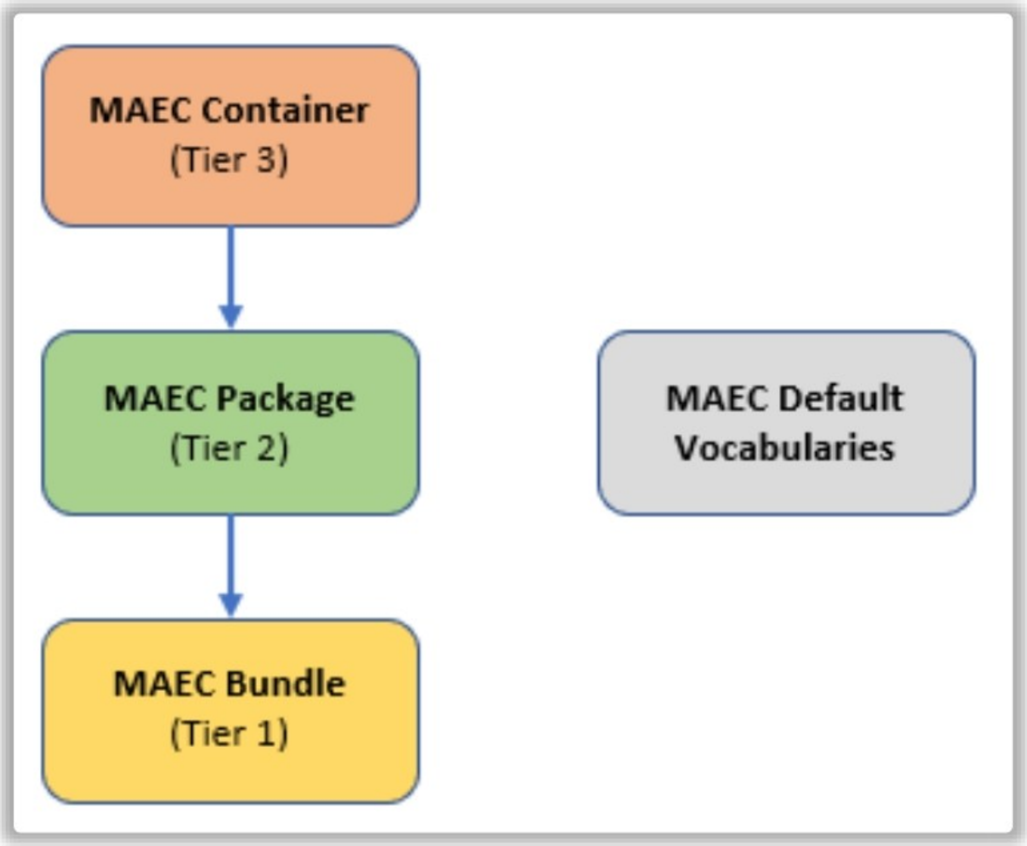
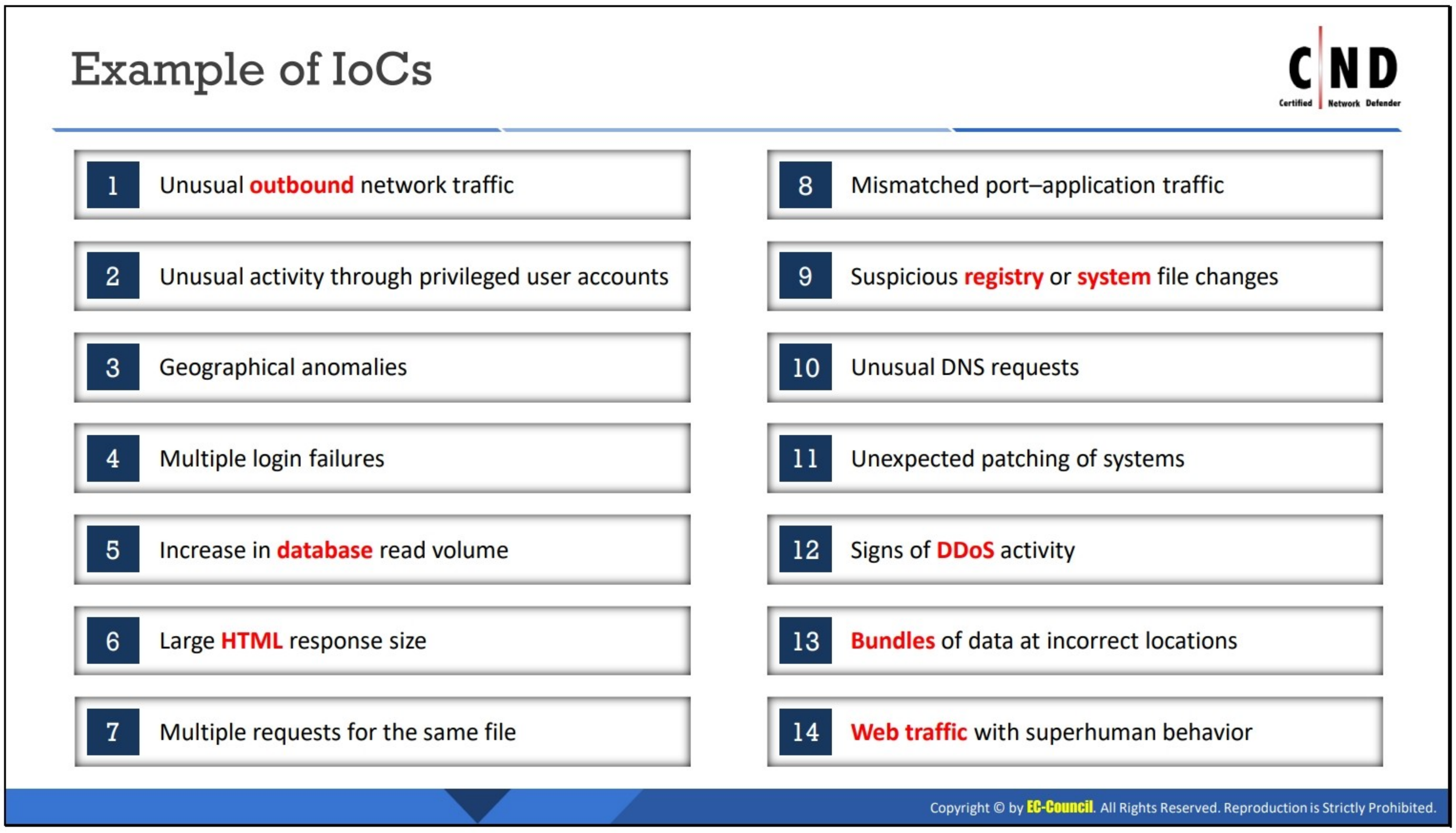


Figure 20.2: Output formats of MAEC



Example of IoCs

1 Unusual **outbound** network traffic

2 Unusual activity through privileged user accounts

3 Geographical anomalies

4 Multiple login failures

5 Increase in **database** read volume

6 Large **HTML** response size

7 Multiple requests for the same file

8 Mismatched port–application traffic

9 Suspicious **registry** or **system** file changes

10 Unusual DNS requests

11 Unexpected patching of systems

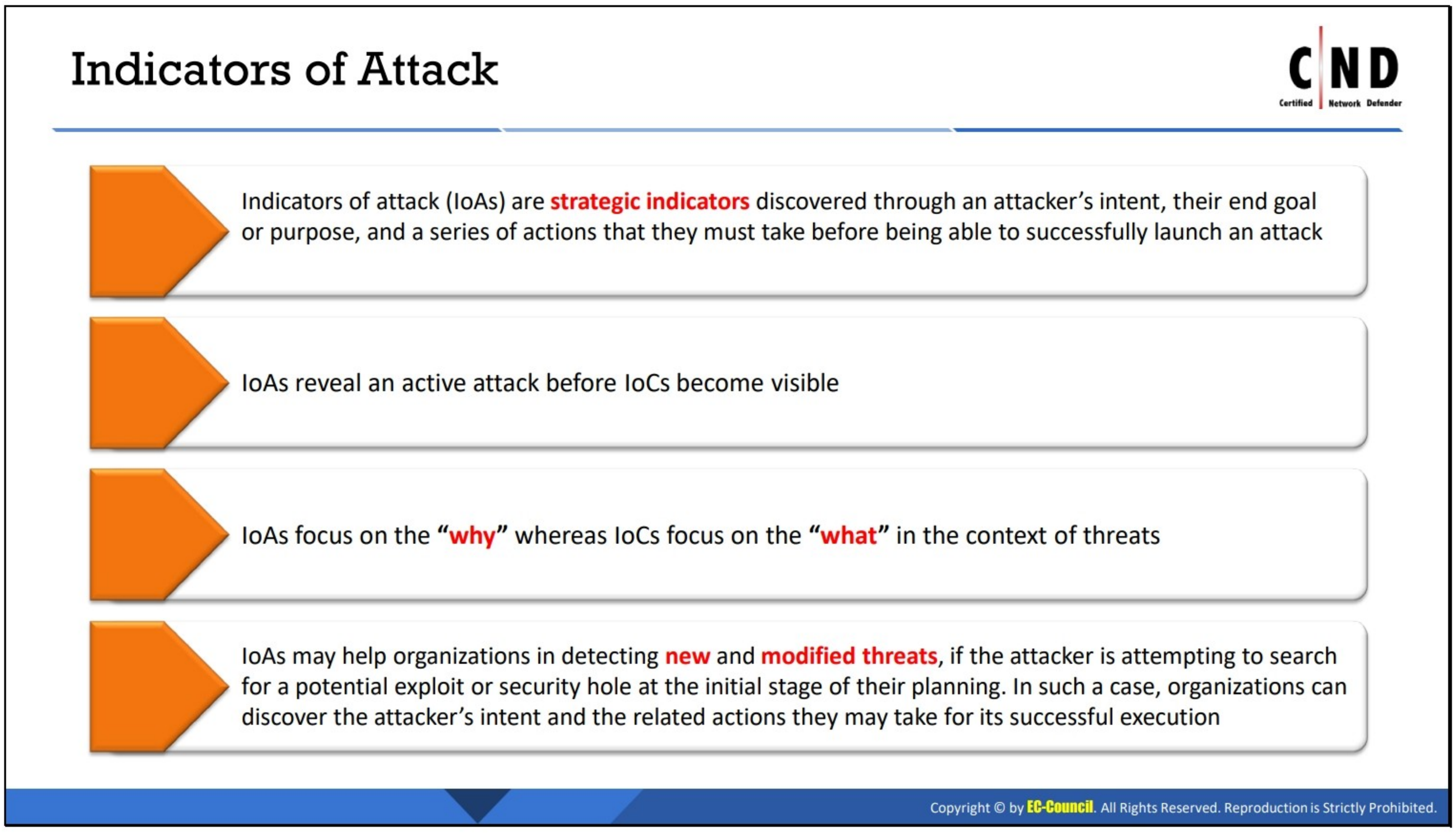
12 Signs of **DDoS** activity

13 **Bundles** of data at incorrect locations

14 **Web traffic** with superhuman behavior

Examples of IoCs

- Unusual outbound network traffic
- Unusual activity through a privileged user account
- Geographic irregularities
- Multiple login failures
- Login irregularities
- Increase in database read volume
- Large Hypertext Markup Language (HTML) response size
- Multiple requests for the same file
- Mismatched port–application traffic
- Suspicious registry or system file changes
- Unusual Domain Name System (DNS) requests
- Unexpected patching of systems
- Signs of distributed DoS (DDoS) activity
- Bundles of data at incorrect locations
- Web traffic with superhuman behavior
- MD5 hash file in the temporary directory



Indicators of Attack

- Indicators of attack (IoAs) are **strategic indicators** discovered through an attacker's intent, their end goal or purpose, and a series of actions that they must take before being able to successfully launch an attack
- IoAs reveal an active attack before IoCs become visible
- IoAs focus on the **"why"** whereas IoCs focus on the **"what"** in the context of threats
- IoAs may help organizations in detecting **new** and **modified threats**, if the attacker is attempting to search for a potential exploit or security hole at the initial stage of their planning. In such a case, organizations can discover the attacker's intent and the related actions they may take for its successful execution

Indicators of Attack

IoAs are strategic indicators discovered through the attackers' intention and end goal as well as a series of actions that an attacker must take before being able to successfully launch an attack. It reveals an active attack before IoCs become visible. In the context of threats, IoAs focus on the "why," whereas IOCs focus on the "what."

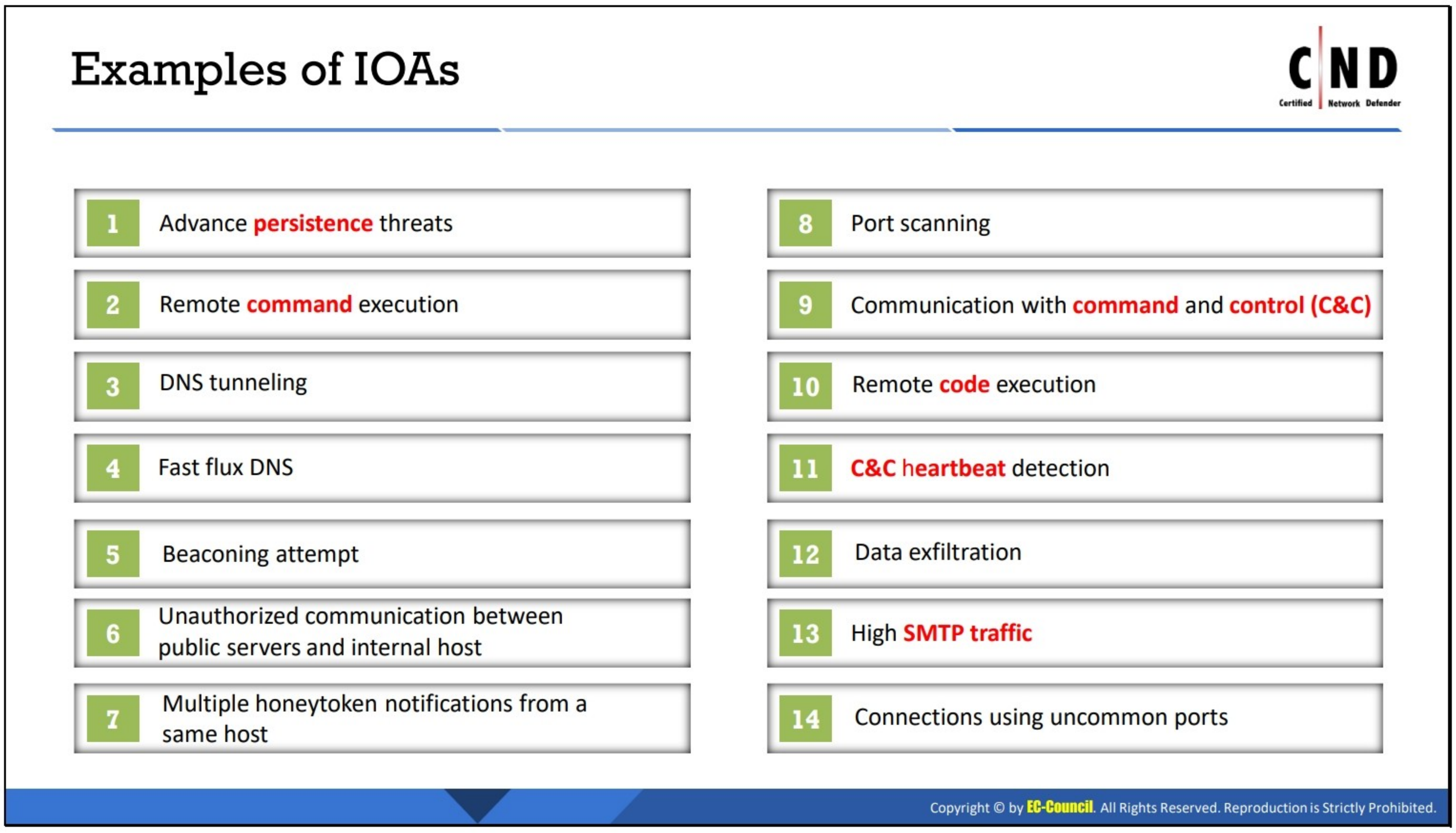
IoAs include the following types of data:

- Real-time behavior that includes endpoint behavioral analytics (EBA)
- Persistent and stealth components used in attacks
- Actions taken
- Sequence of events
- Use behavior in relationship to the digital threat
- Calling of dynamic-link libraries (DLLs)
- TTPs linked to hostile data (malware) used in attacks
- Code-execution metadata

IoAs help an organization detect new and modified threats if an attacker is attempting to search for a potential exploit or security hole at the initial stage of their planning. In such a case, the organization can discover the attacker's intent and related actions they may take for its successful execution. By monitoring the attack execution points and collecting the indicators, the network defenders decide how an actor attempts to gain network access, and thus, the network defender can infer intent. In this case, IoCs (knowledge of tools and malware) are not required.

IoAs have the following advantages:

- IoAs provide a strategic view of the tactics, techniques, and procedures (TTPs) of a threat actor or group. They can proactively identify new unknown threats and defensive strategies against them.
- An IoA-based system is perfect for preventing attackers before they enter the network as an attacker does not need malware to compromise a system.
- An IoA-based system does not require any tools to identify attacks.
- IoAs provide indicators of the actions taken during each stage of an attack.
- IoAs help develop a strong game plan for a company's defense.
- IoAs help gain an understanding of the internal environment and identify probable targets for threat actors.



Examples of IOAs

1. Advance **persistence** threats
2. Remote **command** execution
3. DNS tunneling
4. Fast flux DNS
5. Beaconing attempt
6. Unauthorized communication between public servers and internal host
7. Multiple honeytoken notifications from a same host
8. Port scanning
9. Communication with **command** and **control (C&C)**
10. Remote **code** execution
11. **C&C heartbeat** detection
12. Data exfiltration
13. High **SMTP traffic**
14. Connections using uncommon ports

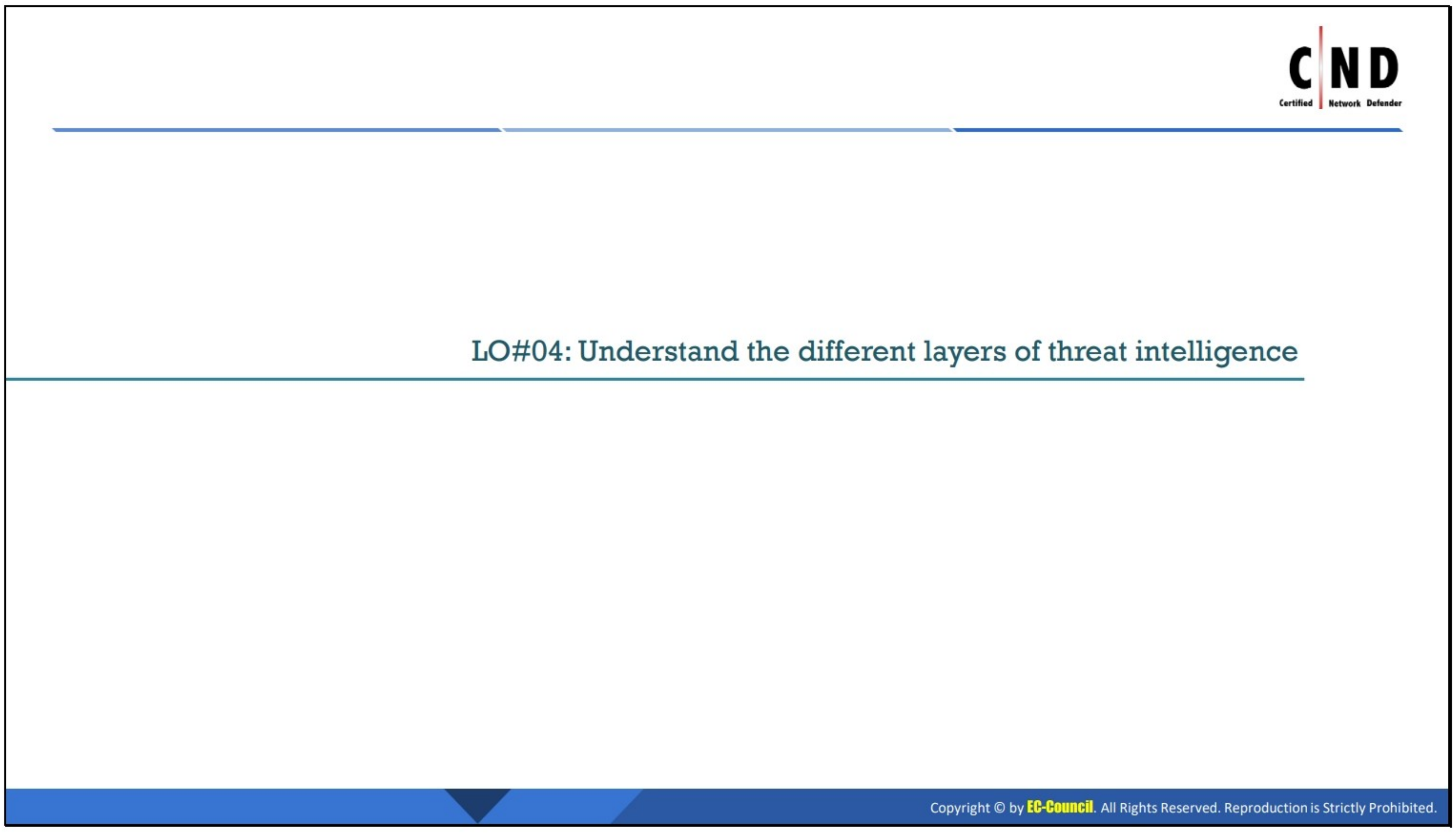
Examples of IoAs

- Advance persistence threats
- Remote command execution
- DNS tunneling
- Fast flux DNS
- Beaconing attempt
- Unauthorized communication between public servers and internal host
- Multiple honeytoken notifications from a same host
- Port scanning
- Communication with command and control (C&C)
- Remote code execution
- C&C heartbeat detection
- Data exfiltration
- High SMTP traffic
- Connection using uncommon ports

Table 20.1 lists the key differences between IoCs and IoAs.

Indicators of Compromise (IoCs)	**Indicators of Attack (IoAs)**
Monitoring “what (who) we know”	Monitoring “what (whom) we do not recognize yet”
Reactive indicators of compromise	Proactive indicators of attack
Can be used only after a point in time	Used in real time
Focus on malware, signatures, exploits, vulnerabilities, an IP addresses	Focus on code execution, persistence, stealth, command and control, and lateral movement
May not necessarily help detect new or modified threats	Identify new unknown threats and defensive strategies proactively
Known, universal bad news	Become bad news only based on what they mean to the organization and the situation
Examples: ▪ Malware ▪ Signatures ▪ Exploits ▪ IP addresses ▪ Vulnerabilities	Examples: ▪ Code executions ▪ User behavior ▪ Malware behavior ▪ Persistence ▪ Stealth

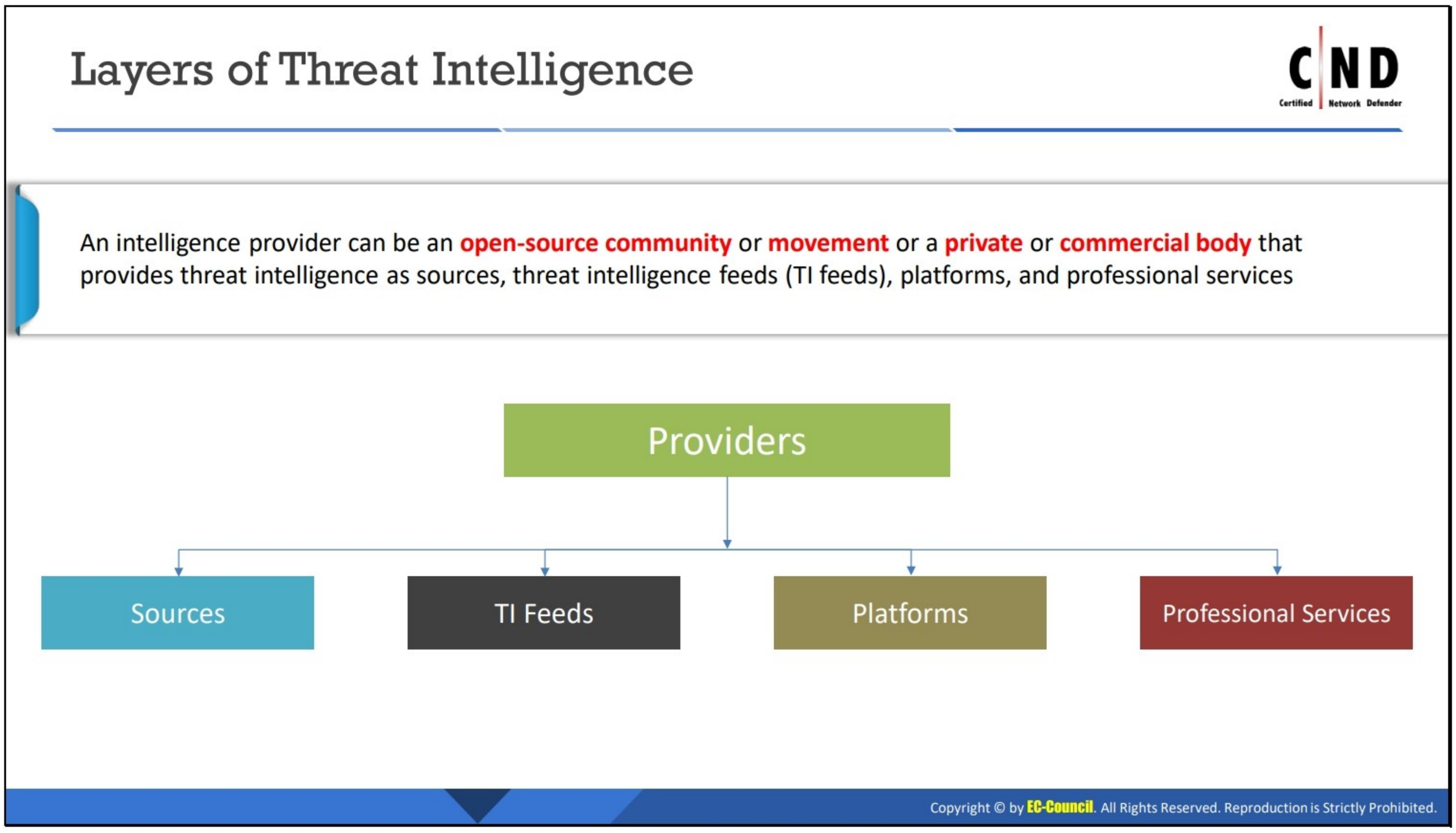
Table 20.1: Differences between IoCs and IoAs



LO#04: Understand the different layers of threat intelligence

LO#04: Understand the Different Layers of Threat Intelligence

Threat intelligence comprises four layers. These layers allow organizations to use threat data to identify malicious activity in a network. This section discusses these four layers of threat intelligence in detail.



Layers of Threat Intelligence

An intelligence provider can be an **open-source community** or **movement** or a **private** or **commercial body** that provides threat intelligence as sources, threat intelligence feeds (TI feeds), platforms, and professional services

Providers

Sources

TI Feeds

Platforms

Professional Services

Layers of Threat Intelligence

An intelligence provider can be an open-source community, a movement, a private body, or a commercial body that provides threat intelligence as sources, feeds, platforms, and professional services. Threat intelligence providers are categorized based on the way they deliver or organize threat-related content. A threat intelligence provider is a body that provides a few or all four layers of threat intelligence. Threat intelligence is provided by commercial providers, government institutes, and independent research bodies.

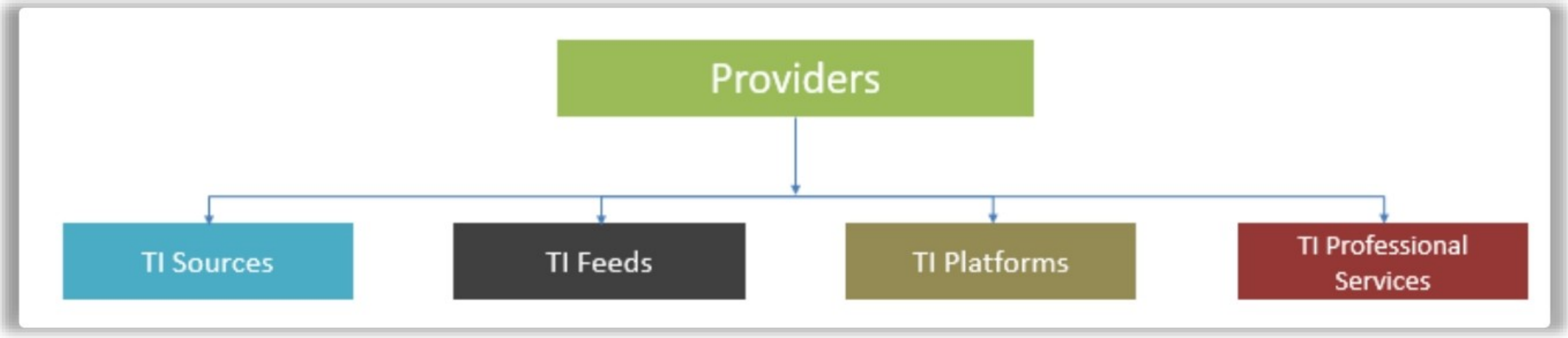
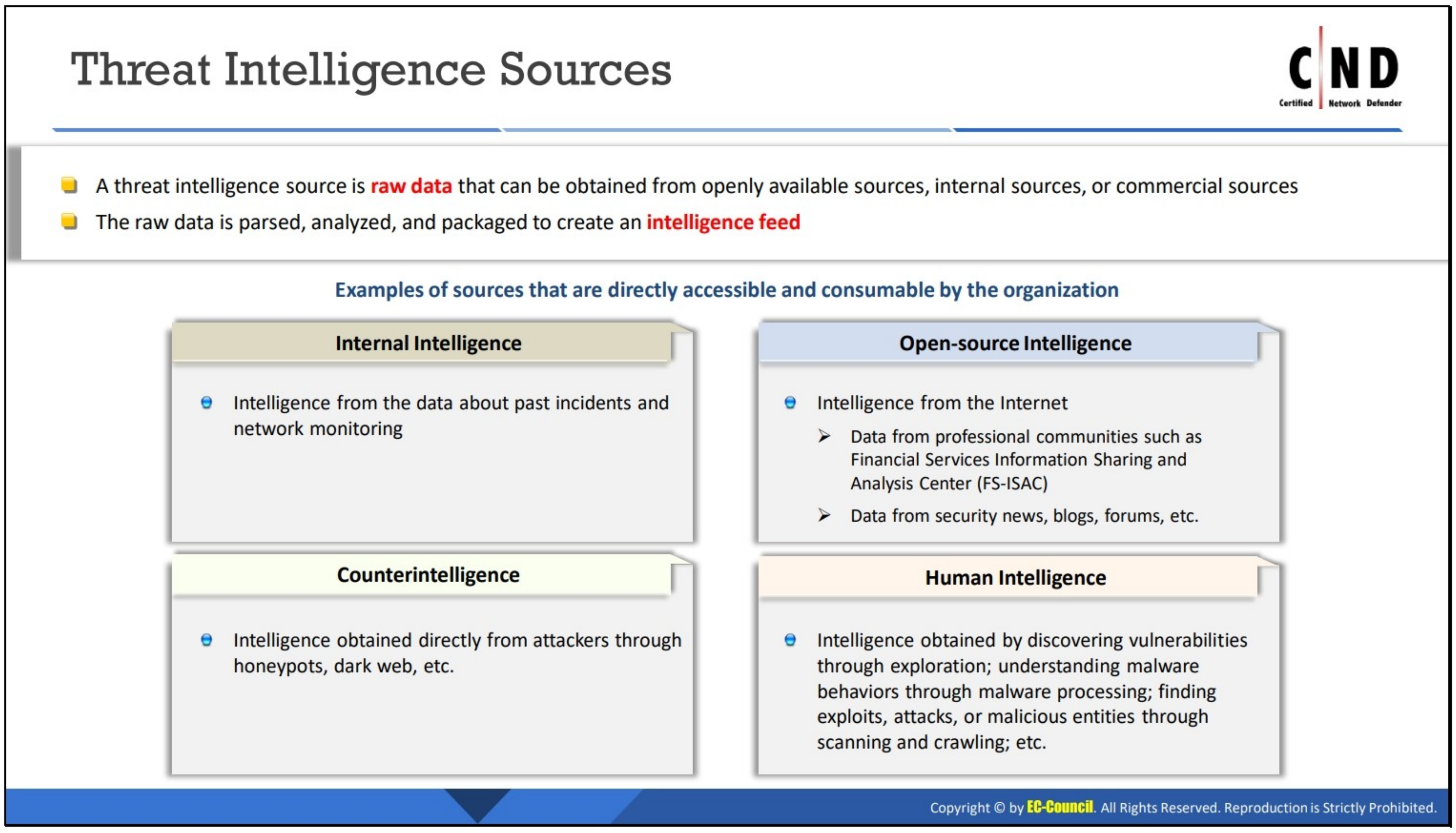


Figure 20.3: Layers of Threat Intelligence



Threat Intelligence Sources

CND
Certified Network Defender

- A threat intelligence source is **raw data** that can be obtained from openly available sources, internal sources, or commercial sources
- The raw data is parsed, analyzed, and packaged to create an **intelligence feed**

Examples of sources that are directly accessible and consumable by the organization

Internal Intelligence

- Intelligence from the data about past incidents and network monitoring

Open-source Intelligence

- Intelligence from the Internet
  - Data from professional communities such as Financial Services Information Sharing and Analysis Center (FS-ISAC)
  - Data from security news, blogs, forums, etc.

Counterintelligence

- Intelligence obtained directly from attackers through honeypots, dark web, etc.

Human Intelligence

- Intelligence obtained by discovering vulnerabilities through exploration; understanding malware behaviors through malware processing; finding exploits, attacks, or malicious entities through scanning and crawling; etc.

Threat Intelligence Sources

Threat intelligence could be obtained from a several sources, but an efficient intelligence strategy is one that has relevant, minimal sources. While choosing the sources, two points must be considered:

- The intelligence from the source should help in developing a long-term intelligence strategy.
- The intelligence from the source should be relevant to the plan.

Sources that do not satisfy the points mentioned above are best avoided. Threat intelligence could be obtained from a wide variety of sources such as vendors and the public sector. The following are typical sources of intelligence:

- Internal intelligence
- Open-source intelligence (OSINT)
- Counterintelligence
- Human intelligence (HUMINT)

Internal Intelligence

Internal intelligence is the intelligence gathered from internal employees who are well aware of cyber threats. Whenever any unexpected incident or anonymous phishing attack occurs, the employees must identify it and report it to the security team, instead of replying to the email or addressing the security incident themselves. In this regard, organizations must provide proper awareness about security concepts to both technical and nontechnical employees. This helps organizations handle and respond to the security incidents efficiently. Thus, employees are a good source of intelligence about internal threats and incidents.

Apart from the employees, event monitoring solutions such as security information and event management (SIEM) tools also provide huge volumes of intelligence about the organization. IoCs and honeypots are also good sources of internal intelligence.

Open-source Intelligence

Open-source or passive information gathering is the easiest way to collect information about a threat vector or a target organization. It refers to the process of gathering information from open sources, that is, publicly available sources. Open sources may include newspapers, television, social networking sites (SNSs), and blogs. Information can be gathered from different sources in a variety of ways; it can even be gathered through day-to-day activities such as speaking with people. This kind of information gathering is also a part of intelligence development, and it is regarded as OSINT. This type of intelligence gathering provides an in-depth understanding at a low cost.

The following are the sources of information defined as OSINT:

- Daily newspapers, magazines, television, radio, etc.
- Search engines, blogs, forums, social networks, etc.

Counter intelligence

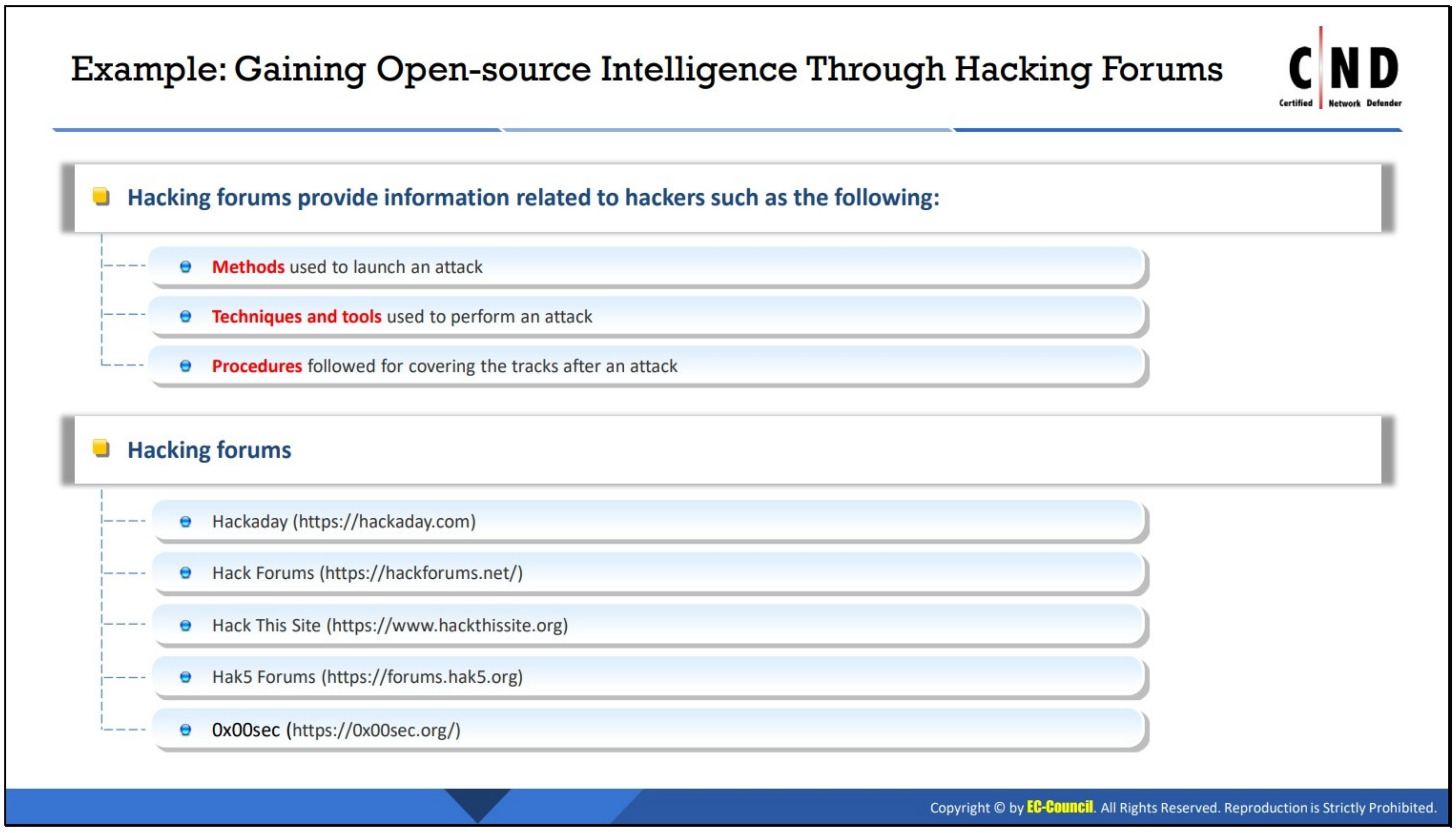
Counterintelligence is the process of intelligence gathering for protection against espionage and other intelligence attacks. It is usually designed to mislead the attacker on the wrong path to protect the system, and it can also be used to acquire information about the attacker. Counterintelligence can be used for both offensive and defensive purposes. Offensive counterintelligence refers to attacking the attacker on receiving intelligence that they are attempting to compromise the organization’s infrastructure, whereas defensive counterintelligence refers to the use of the intelligence only to protect the organization from the attacker. The process of collecting information from adversaries through counterintelligence is known as collective counterintelligence.

Human Intelligence

Human intelligence (HUMINT) could be obtained through many sources such as conversations and spying. The possibility of collecting information from human beings depends upon their nature. In addition, a person can have different moods at different times. Therefore, to acquire HUMINT effectively, the targets should be well understood first and monitored.

Some people easily provide information, whereas others hesitate to reveal information. However, successful HUMINT collection could produce a huge amount of quality information. HUMINT is one of the crucial sources for developing threat intelligence strategies.

Social engineering is regarded as the most popular intelligence gathering techniques. There are various techniques for HUMINT gathering such as dumpster diving, eavesdropping, and shoulder surfing.



Example: Gaining Open-source Intelligence Through Hacking Forums

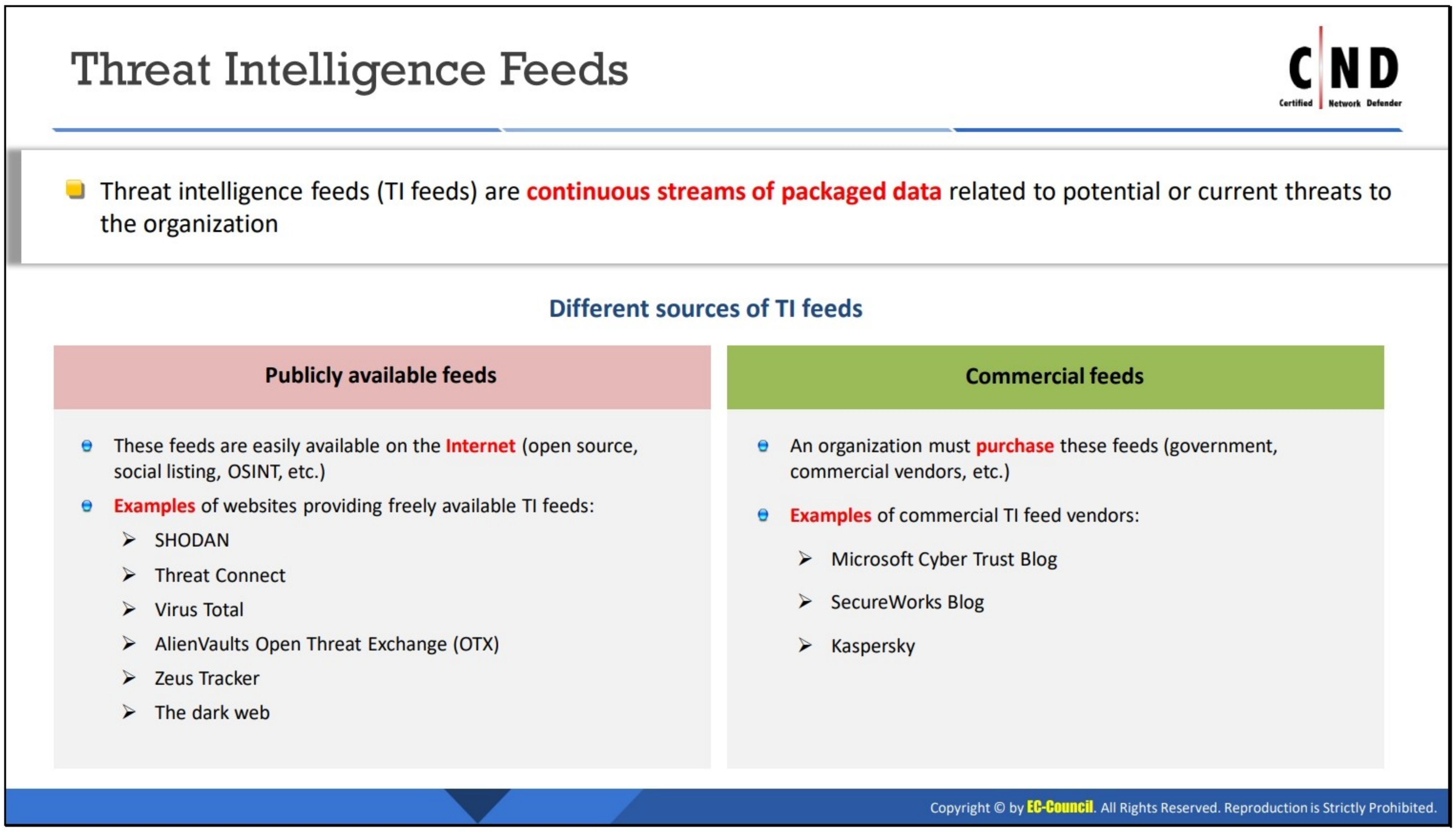
- Hacking forums provide information related to hackers such as the following:
  - **Methods** used to launch an attack
  - **Techniques and tools** used to perform an attack
  - **Procedures** followed for covering the tracks after an attack
- Hacking forums
  - Hackaday (https://hackaday.com)
  - Hack Forums (https://hackforums.net/)
  - Hack This Site (https://www.hackthissite.org)
  - Hak5 Forums (https://forums.hak5.org)
  - 0x00sec (https://0x00sec.org/)

Example: Gaining Open-source Intelligence Through Hacking Forums

Hacking forums provide information related to hackers such as the method used to launch an attack, techniques and tools used to perform an attack, and the procedures followed for covering the tracks after an attack. These forums provide detailed information related to tools, hacking procedures, stolen data, new vulnerabilities, and patches, as well as news about various cyberattacks and exploits. Network defenders can browse these hacking forums to learn such information about attacks. They help in identifying emerging threats to the organization and in implementing essential techniques to protect systems and networks from attacks.

Listed below are some popular hacking forums:

- Hack Forums (*https://hackforums.net*)
- Hackaday (*https://hackaday.com*)
- The Ethical Hacker Network (*https://www.ethicalhacker.net*)
- Hack This Site (*https://www.hackthissite.org*)
- Hak5 Forums (*https://forums.hak5.org*)
- 0x00sec (https://0x00sec.org/)
- Hack In The Box (*http://www.hitb.org*)
- The Hacker News (*https://thehackernews.com*)
- 0x00sec (*https://0x00sec.org*)
- Exploit Database (*https://www.exploit-db.com*)
- Packet Storm (*https://packetstormsecurity.com*)



Threat Intelligence Feeds

- Threat intelligence feeds (TI feeds) are **continuous streams of packaged data** related to potential or current threats to the organization

Different sources of TI feeds

Publicly available feeds

- These feeds are easily available on the **Internet** (open source, social listing, OSINT, etc.)
- **Examples** of websites providing freely available TI feeds:
  - SHODAN
  - Threat Connect
  - Virus Total
  - AlienVaults Open Threat Exchange (OTX)
  - Zeus Tracker
  - The dark web

Commercial feeds

- An organization must **purchase** these feeds (government, commercial vendors, etc.)
- **Examples** of commercial TI feed vendors:
  - Microsoft Cyber Trust Blog
  - SecureWorks Blog
  - Kaspersky

Threat Intelligence Feeds

Threat intelligence feeds (TI feeds) feature a packaged collection of data taken from different sources related to potential or current threats in an organization. Most feeds concentrate on domains, malicious IP addresses, or botnet activity. These comprise actionable information and are implemented along with technical controls to prevent cyber-attacks.

TI feeds are used by network defenders for the following purposes:

- **Coupling of TI feeds to security tools** (e.g., blocking bad IP addresses after accepting feeds by some firewalls)
- **Use of TI feeds to generate alerts** (e.g., SIEM and user and entity behavior analytics (UEBA) correlate TI feed data with internal security events to generate alerts)
- **Manual review** to investigate threats if they seem relevant to the security posture

It is recommended that organizations know their feed requirements before obtaining TI feeds. To know their requirements, they should assess themselves based on the following factors.

- Network infrastructure: how does the network infrastructure look like?
- Current security posture: What are the unique risks to the organization?
- Finance: What are the budget and resources available for implementing threat intelligence?
- The ability of threat intelligence management.
- Is the above information sufficient for building a strong strategy for the organization?

Sources of TI Feeds

Important TI feeds are obtained from the following sources.

- **Publicly available feeds**

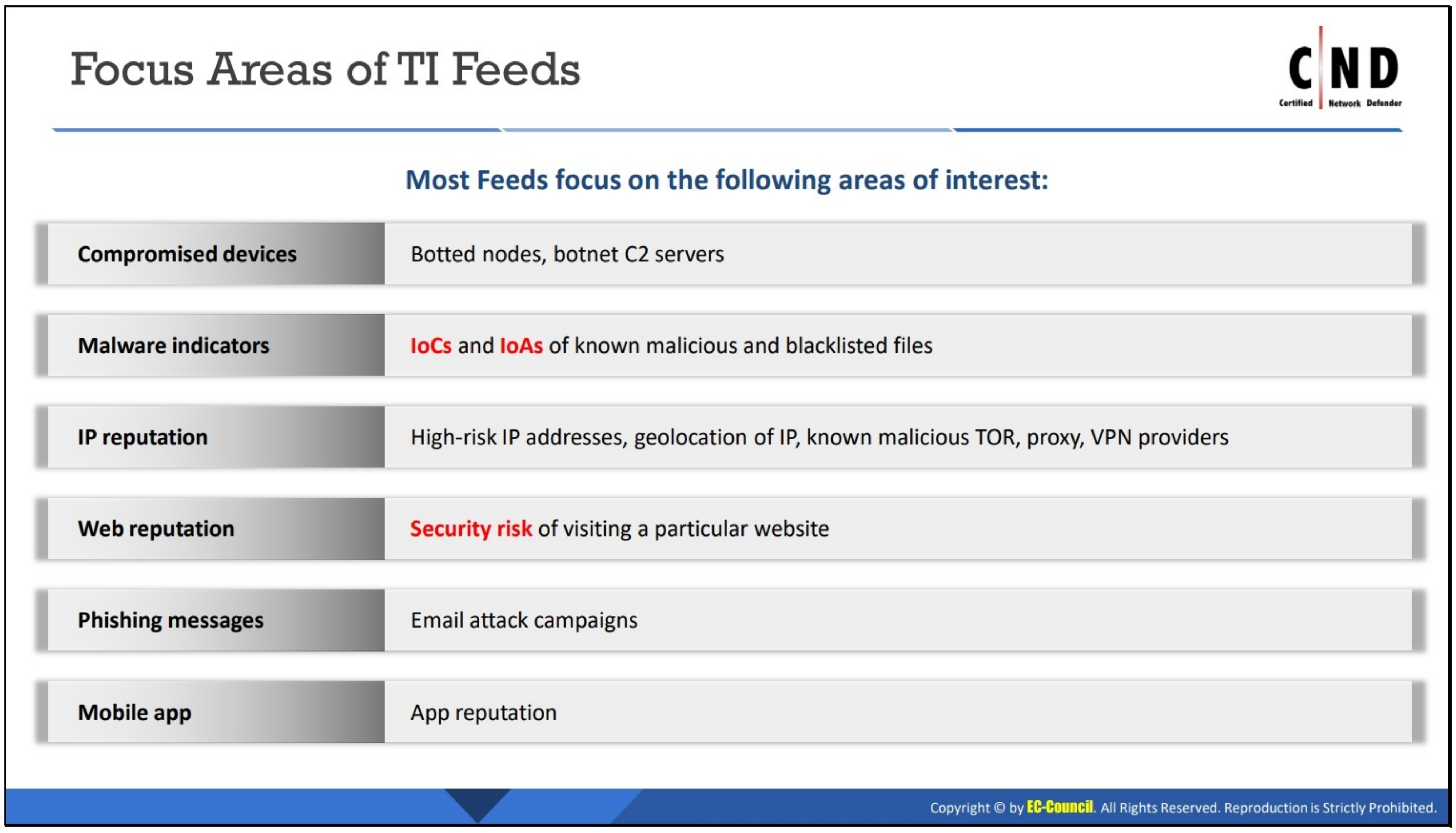
  These feeds are easily available on the Internet (open source, social listing, OSINT, etc.). Freely available TI feeds include the following:

  - SHODAN
  - Threat Connect
  - Virus Total
  - AlienVaults Open Threat Exchange (OTX)
  - Zeus Tracker
  - The dark web

- **Commercial providers**

  An organization (e.g., government and commercial vendors) needs to purchase these feeds. The following are some TI commercial feed providers:

  - Microsoft Cyber Trust Blog
  - SecureWorks Blog
  - Kaspersky Blog



Focus Areas of TI Feeds

Most Feeds focus on the following areas of interest:

Compromised devices	Botted nodes, botnet C2 servers
Malware indicators	IoCs and IoAs of known malicious and blacklisted files
IP reputation	High-risk IP addresses, geolocation of IP, known malicious TOR, proxy, VPN providers
Web reputation	Security risk of visiting a particular website
Phishing messages	Email attack campaigns
Mobile app	App reputation

Focus Areas of TI Feeds

Most TI feeds focus on the following areas of interest.

- **Compromised devices**

  Compromised devices provide external notifications to a device that participates in botnet-like activities or communicates with known malicious sites and C&Cs.

  Examples: botted nodes, botnet C2 servers, etc.

- **Malware indicators**

  Malware analysis provides an understanding of the intention of malicious code that targets devices. This process enables the identification of the malware's technical and behavioral indicators such as memory corruption, stopping of current protections, and registry changes.

  Examples: IoCs and IoAs of known malicious and blacklisted files

- **IP reputation**

  IP reputation is an indicator of maliciousness of an IP address. It provides a list of known bad/suspicious IP addresses. IP addresses from which spam or viruses originate are assigned a bad IP reputation.

- **Web reputation**

  Web reputation indicates the security risk of visiting a website and allows network defenders to finely tune security settings.

  Example: security risk of visiting a particular website

- **Command and control (C&C) networks**

  These feeds track global C&C traffic to identify malware originators, botnet controllers, and other IP addresses and sites for monitoring an environment.

  Examples: malware origination, botnet controllers, etc.

- **Phishing messages**

  The isolation and analysis of phishing email can provide information about the attackers and their tactics.

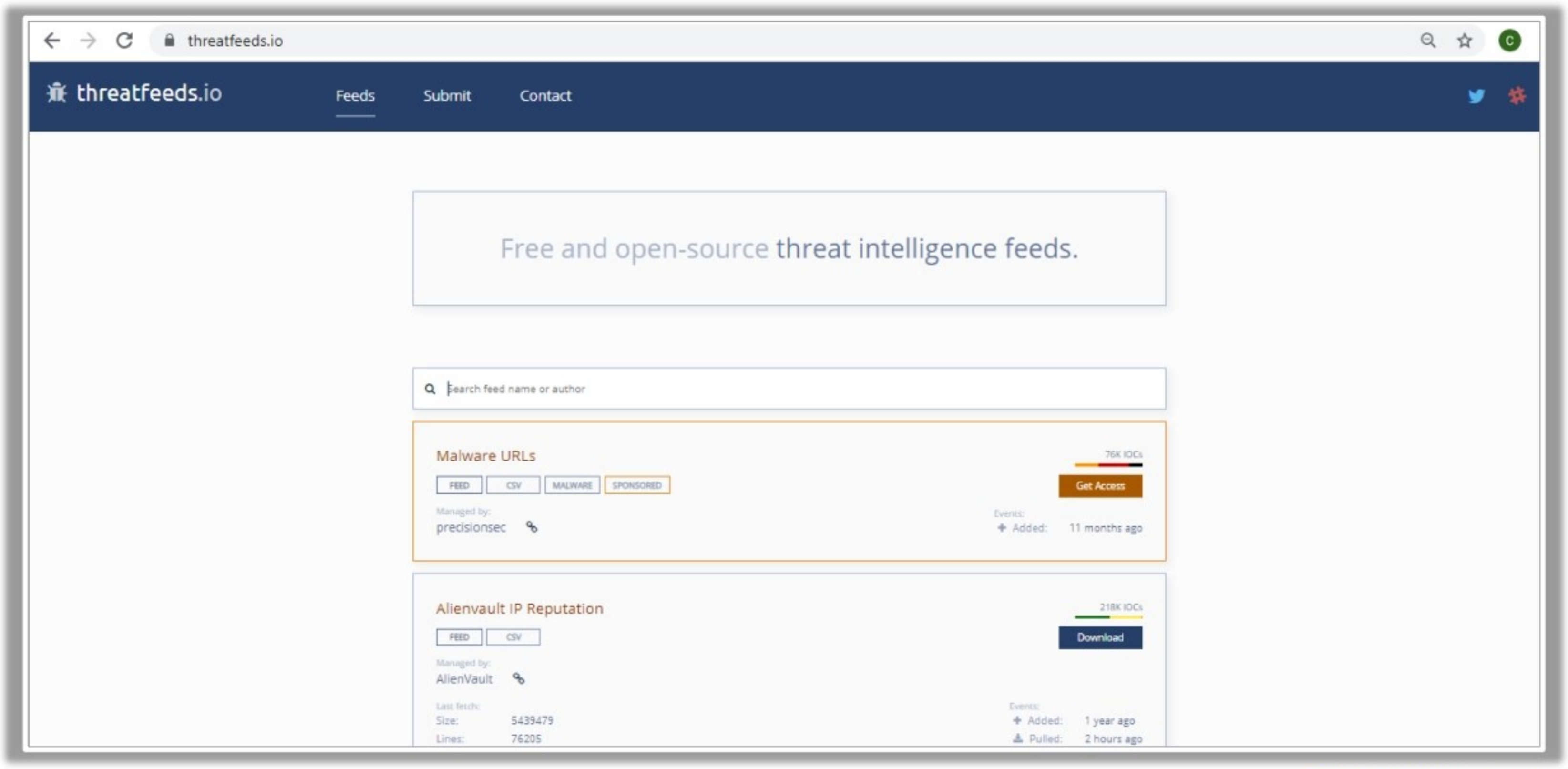
  Examples: email attack campaigns, business email compromise, etc.

- **Mobile app reputation**

  The mobile app reputation groups score apps using multi-stage analysis and advanced algorithms to ensure that the apps are safe and compliant.

  Example: app reputation

Example: Free and Open-source TI Feed Providers



Free and open-source threat intelligence feeds.

Malware URLs
76K IOCs
Managed by:
precisionsec
Events:
Added: 11 months ago

Alienvault IP Reputation
218K IOCs
Managed by:
AlienVault
Last fetch:
Size: 5439479
Lines: 76205
Events:
Added: 1 year ago
Pulled: 2 hours ago

Source: *https://threatfeeds.io*

Example: Free and Open-source TI Feed Providers

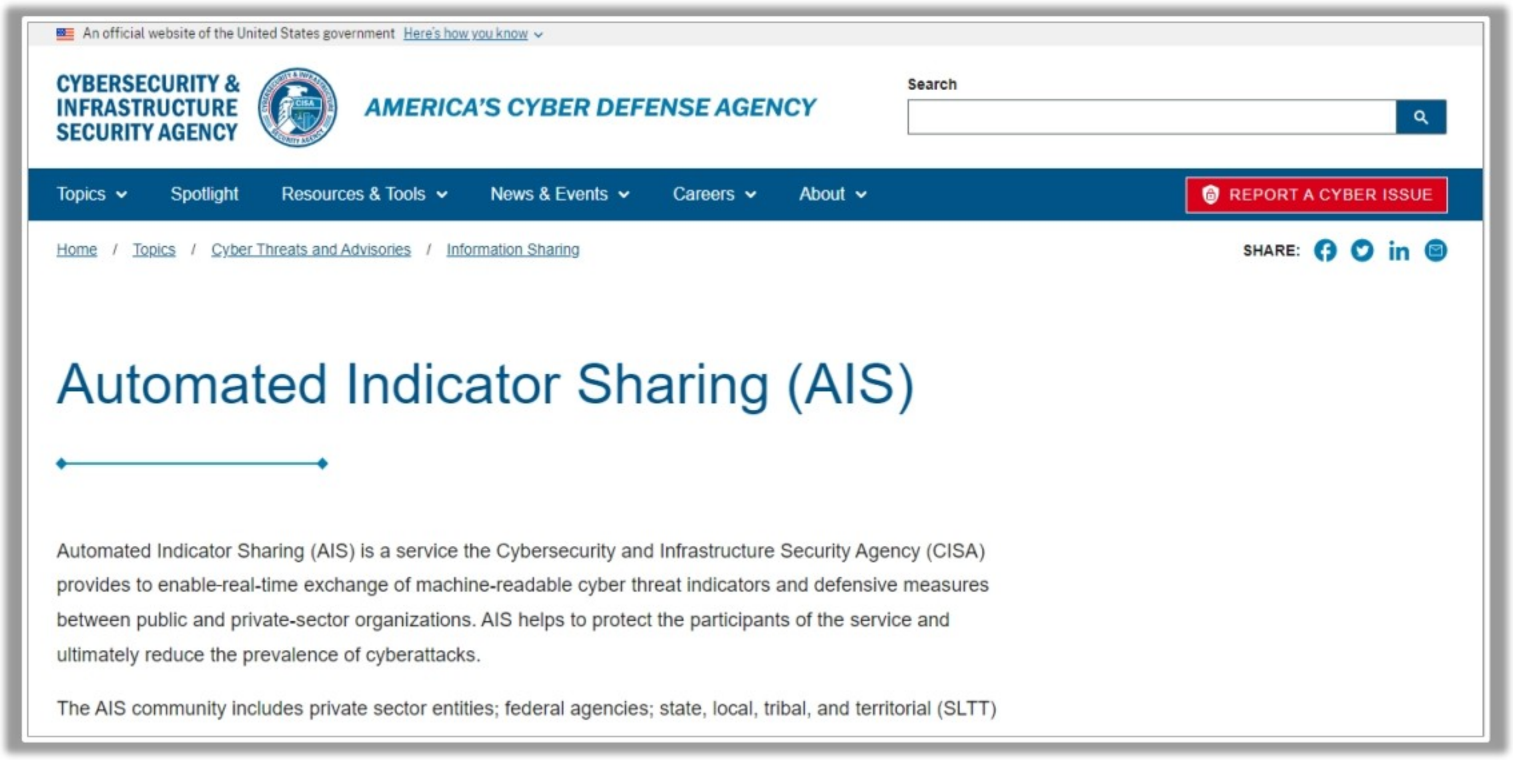
Source: https://threatfeeds.io

Threatfeeds.io is a free and open-source threat intelligence provider of popular free and open-source TI feeds and sources. It also lists links for direct downloads and live summaries.

The following are some examples of free and open-source TI feeds:

- **IPSpamList** managed by NoVirusThanks
- **Darklist** managed by Darklist
- **SSL BL** managed by abuse.ch
- **C&C Domains** managed by Bambenek Consulting
- **Botvrij.eu - ips** managed by Botvrij.eu
- **Botvrij.eu - urls** managed by Botvrij.eu
- **Malicious EXE URLs** managed by NoVirusThanks
- **Monero Miner** managed by Minerchk
- **AlienVault IP Reputation** managed by AlienVault

Example: Government TI Feed Providers



An official website of the United States government Here's how you know
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
AMERICA'S CYBER DEFENSE AGENCY
Search
Topics
Spotlight
Resources & Tools
News & Events
Careers
About
REPORT A CYBER ISSUE
Home / Topics / Cyber Threats and Advisories / Information Sharing
SHARE:

Automated Indicator Sharing (AIS)

Automated Indicator Sharing (AIS) is a service the Cybersecurity and Infrastructure Security Agency (CISA) provides to enable-real-time exchange of machine-readable cyber threat indicators and defensive measures between public and private-sector organizations. AIS helps to protect the participants of the service and ultimately reduce the prevalence of cyberattacks.

The AIS community includes private sector entities; federal agencies; state, local, tribal, and territorial (SLTT)

Source: *https://www.cisa.gov*

Example: Government TI Feed Providers

The following are the most popular government sources of TI feeds:

Automated Indicator Sharing (AIS)

Source: www.dhs.gov

The free Automated Indicator Sharing (AIS), provided by the US Department of Homeland Security (DHS), allows the exchange of cyber threat indicators between the federal government and the private sector at machine speed. Here, threat indicators are malicious IP addresses, sender addresses of phishing emails, etc.

The Department of Defense Cyber Crime Center (DC3)

Source: http://dc3.mil

DC3 is a US Department of Defense (DoD) center of excellence for digital and multimedia forensics and works under the executive agency of the Secretary of the Air Force. It delivers services for cybersecurity, critical infrastructure protection, law enforcement, counterintelligence, etc. It provides daily context on cyber threats and incidents through newsletters and its twitter feed.

US Computer Emergency Response Team (US-CERT)

Source: https://www.us-cert.gov/

US-CERT is an organization within DHS's National Protection and Programs Directorate (NPPD). It responds to threat incidents and shares information through alerts and announcements.

European Union Agency for Network and Information Security (ENISA)

Source: https://www.enisa.europa.eu/

ENISA contributes to European cybersecurity policy, supports its member states and European Union stakeholders to aid responses to cyber incidents, and contributes to the proper functioning of the Digital Single Market.

Federal Bureau of Investigation (FBI) Cyber Crime

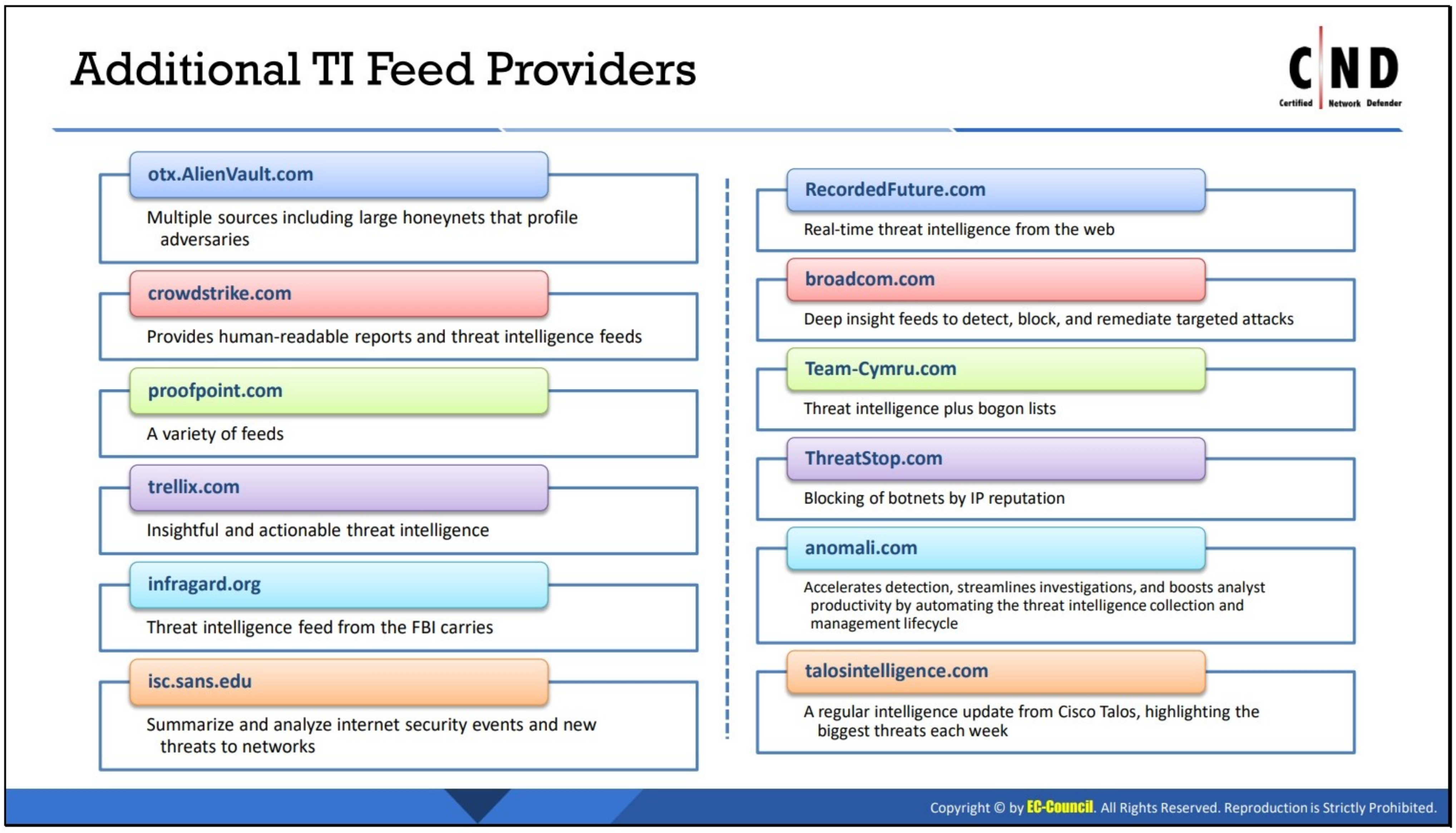
Source: https://www.fbi.gov/

FBI Cyber Crime is the lead US federal agency for investigating cyber-attacks. It enhances the Cyber Division’s investigative capacity to strengthen its focus on intrusions into government and private system networks. It provides news on the latest cases to Congress on cybercrime topics.

StopThinkConnect

Source: www.stopthinkconnect.org

StopThinkConnect is a global online safety awareness campaign that works under the leadership of the National Cyber Security Alliance (NCSA) of the US and the Anti-Phishing Working Group (APWG). It strives to make cybersecurity understandable by people.



Additional TI Feed Providers

otx.AlienVault.com
Multiple sources including large honeynets that profile adversaries

crowdstrike.com
Provides human-readable reports and threat intelligence feeds

proofpoint.com
A variety of feeds

trellix.com
Insightful and actionable threat intelligence

infragard.org
Threat intelligence feed from the FBI carries

isc.sans.edu
Summarize and analyze internet security events and new threats to networks

RecordedFuture.com
Real-time threat intelligence from the web

broadcom.com
Deep insight feeds to detect, block, and remediate targeted attacks

Team-Cymru.com
Threat intelligence plus bogon lists

ThreatStop.com
Blocking of botnets by IP reputation

anomali.com
Accelerates detection, streamlines investigations, and boosts analyst productivity by automating the threat intelligence collection and management lifecycle

talosintelligence.com
A regular intelligence update from Cisco Talos, highlighting the biggest threats each week

Additional TI Feed Providers

The following is an additional list of threat intelligence providers.

AlienVault.com

AlientVault Unified Security Management (USM) provides a complete defense solution to mid-market enterprises against the security threats through the following features:

- Unified, coordinated security monitoring
- Simple security event management and reporting
- Continuous threat intelligence
- Fast deployment
- Different security functions in a single console

CrowdStrike

CrowdStrike is an endpoint security and threat intelligence. It offers a comprehensive range of cybersecurity services. The features include-

- Endpoint protection
- Threat detection
- Incident response solutions

Trellix.com

Trellix.com provides advanced threat intelligence services for proactive cybersecurity defense. Its features include-

- Threat actor or Group attribution and TTP analysis.
- Threat Intelligence driven Risk assessments.
- Threat Intelligence analyst augmentation using multiple sources and tools.
- Malware analysis – Static or Dynamic limited reversing
- Malicious Infrastructure analysis

Infragard.org

Infragard is a public-private partnership in the United States dedicated to enhancing national cybersecurity through collaboration between the FBI and private sector organizations. Its features are-

- Information Sharing
- Threat Intelligence
- Critical Infrastructure Protection
- Incident Response support

Isc.sans.edu

ISC (Internet Storm Center) by SANS Institute is a leading cybersecurity resource offering real-time threat intelligence, incident handling, and valuable security insights to the global community. Its features are as follows:

- Threat Intelligence
- Incident Handling
- Security Awareness
- Monitoring & Analysis

Broadcom.com

Broadcom.com is a prominent provider of comprehensive cybersecurity solutions, empowering organizations with advanced threat protection and risk mitigation capabilities. Their features include-

- Comprehensive Threat Detection
- Endpoint Security
- Network Security
- IAM Management
- Security Analytics

Anomali.com

Anomali.com is known to be a leading provider of threat intelligence and detection solutions, empowering organizations to proactively defend against cyber threats. The features are-

- Threat Intelligence Feeds
- Threat Detection Analysis
- Integration with Security Tools
- Customizable alerts

EmergingThreats.net (Proofpoint.com)

Proofpoint provides protection and visibility for the greatest cybersecurity risk and compliance solutions to secure people on email, web, cloud, and social media. Its features include the following:

- **Threat protection** stops malware, credential phishing, etc.
- **Information protection** helps provide visibility to instances where sensitive data are exposed across email and cloud
- **User protection** protects people across personal webmail and browsing

RecordedFuture.com

Recorded Future Security Control Feeds provide organizations access to the quality indicators and context needed to automate action. Its key features include the operationalizing of trusted intelligence and the automatic detection and blocking of threats.

Team-Cymru.com

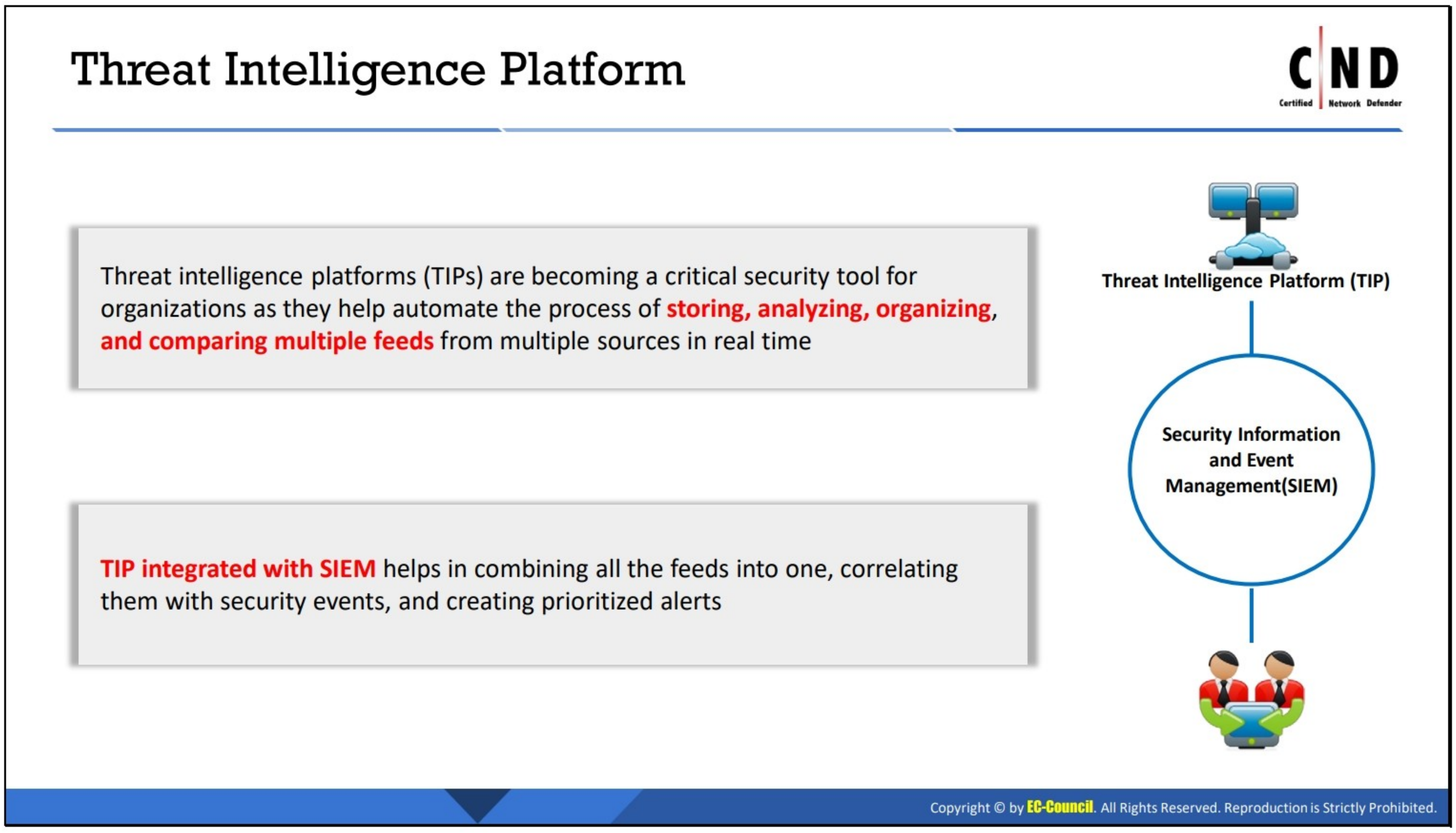
Team Cymru provides threat intelligence and insight for security vendors, network defenders, IR teams, and analysts. It has a query tool for direct access to more than 50 different threat categories.

ThreatStop.com

ThreatStop blocks malicious IP and DNS connections automatically to stop threats such as ransomware, phishing, and botnets. Its platform features threat intelligence collection, customized security policies, network device integrations, and advanced web-based reporting.

talosintelligence.com

A regular intelligence update from Cisco Talos, highlighting the biggest threats each week



Threat Intelligence Platform

Threat intelligence platforms (TIPs) are becoming a critical security tool for organizations as they help automate the process of **storing, analyzing, organizing, and comparing multiple feeds** from multiple sources in real time

TIP integrated with SIEM helps in combining all the feeds into one, correlating them with security events, and creating prioritized alerts

Threat Intelligence Platform (TIP)
Security Information and Event Management(SIEM)

Threat Intelligence Platform

Nowadays, the cybersecurity environment is facing common problems such as large amounts of data, shortage of skilled security analysts, and growingly adversarial attacks. To handle these problems, existing security systems use various tools that can manage the problems but are incapable of storing information in a centralized format. Thus, the task of storing, analyzing organizing, and comparing multiple feeds is rather tedious for systems with limited resources and time.

With large volumes of data, the exponential increase of complexity of threat vectors, and lack of threat intelligence analysts, organizations are choosing to implement threat intelligence platforms (TIPs) to facilitate the management of CTI. It can be installed as a software as a service (SaaS) or on the premises to gather and manage information about evolving threats and associated entities such as threat actors, IoCs, bulletins, and TTPs. It is becoming a critical security tool for organizations as it helps them automate the process of aggregating, correlating, and analyzing threat data from multiple sources in real time.

Its basic capabilities include data collection, data correlation, data enrichment, contextualization, data analysis, and data integration.

- **Data collection**

  CTI facilitates data collection by collecting and aggregating information in multiple data formats from multiple sources in a central location. Open source, government, trusted sharing communities (ISACs), etc. are examples of sources, whereas JavaScript Object Notation (JSON), XML, STIX/TAXII, PDF, .txt, etc. are examples of formats.

- **Data normalization and correlation**

  After collecting data from multiple sources, it is necessary to process data effectively to identify numerous indicators. Processing is performed in multiple steps, but its three main aspects are data normalization, data de-duplication, and data improvement. Data normalization refers to determining connected data across multiple inputs and sources; data de-duplication refers to deleting duplicate data; and data improvement refers to eliminating false positives, fake indicators, etc. Once the data are normalized, it is correlated and pivoted to identify actionable intelligence.

- **Data enrichment and contextualization**

  After correlating data, TIP should build enriched context around the threats. This can be performed automatically or using third-party analysis applications that provide as much information as possible related to the threat actor, their capabilities, and infrastructure.

- **Data analysis**

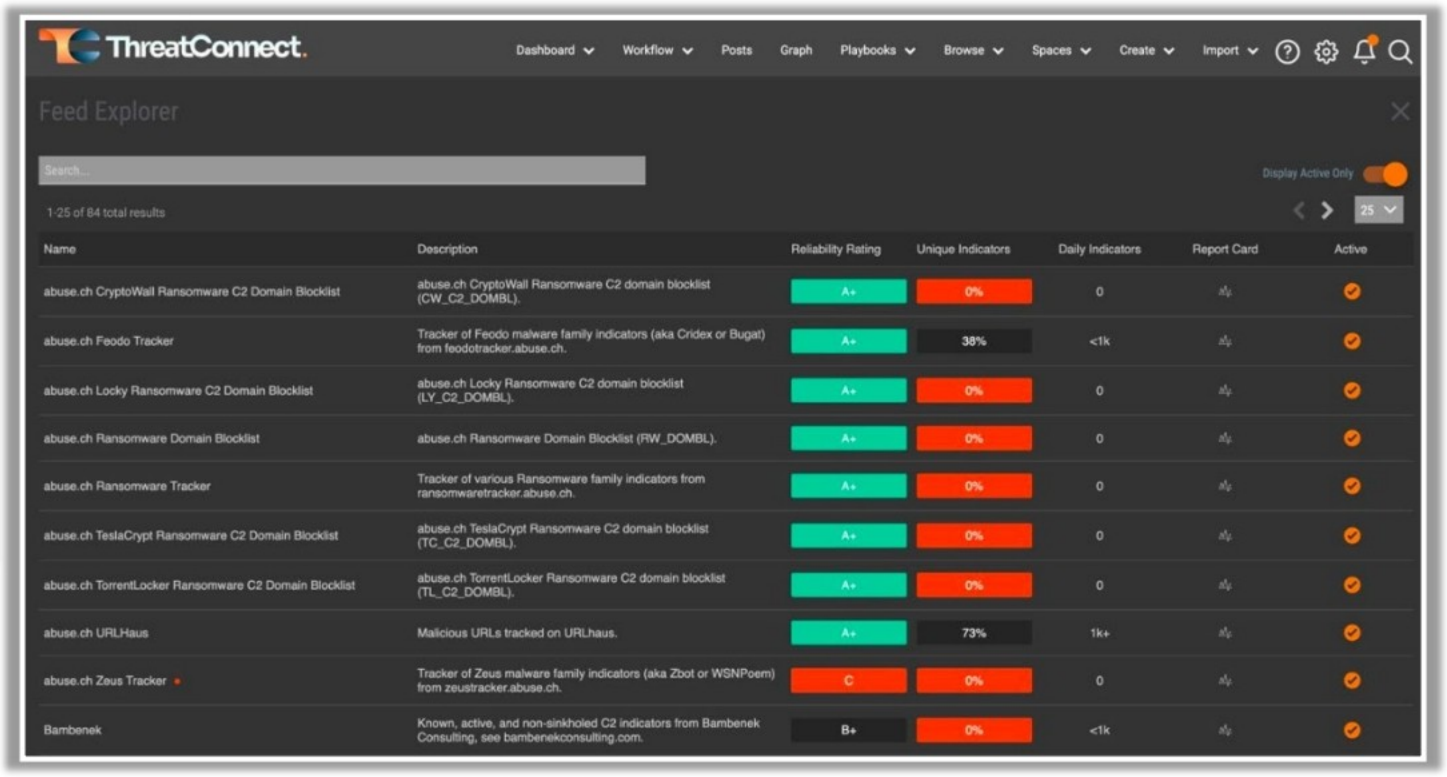
  TIP should analyze the content of threat indicators. Through analysis, it can investigate threats and suggest an investigation process. In addition, it can also determine the implication of threats on the organization.

- **Data integration**

  TIP should disseminate and integrate cleaned data to other existing security systems/tools/products used by an organization such as SIEM, firewalls, intrusion detection systems (IDSs) and intrusion prevention systems (IPSs), and ticketing systems.

Threat Intelligence Platform: TC Complete™

TC Complete™ is a security operations and analytics platform built on the ThreatConnect platform. It provides not only the ability to **orchestrate security functions**, but also the confidence that tasks and decisions are based on vetted, relevant threat intelligence.



1-25 of 84 total results

Name	Description	Reliability Rating	Unique Indicators	Daily Indicators	Report Card	Active
abuse.ch CryptoWall Ransomware C2 Domain Blocklist	abuse.ch CryptoWall Ransomware C2 domain blocklist (CW_C2_DOMBL).	A+	0%	0		✓
abuse.ch Feodo Tracker	Tracker of Feodo malware family indicators (aka Cridex or Bugat) from feodotracker.abuse.ch.	A+	38%	<1k		✓
abuse.ch Locky Ransomware C2 Domain Blocklist	abuse.ch Locky Ransomware C2 domain blocklist (LY_C2_DOMBL).	A+	0%	0		✓
abuse.ch Ransomware Domain Blocklist	abuse.ch Ransomware Domain Blocklist (RW_DOMBL).	A+	0%	0		✓
abuse.ch Ransomware Tracker	Tracker of various Ransomware family indicators from ransomwaretracker.abuse.ch.	A+	0%	0		✓
abuse.ch TeslaCrypt Ransomware C2 Domain Blocklist	abuse.ch TeslaCrypt Ransomware C2 domain blocklist (TC_C2_DOMBL).	A+	0%	0		✓
abuse.ch TorrentLocker Ransomware C2 Domain Blocklist	abuse.ch TorrentLocker Ransomware C2 domain blocklist (TL_C2_DOMBL).	A+	0%	0		✓
abuse.ch URLHaus	Malicious URLs tracked on URLhaus.	A+	73%	1k+		✓
abuse.ch Zeus Tracker ●	Tracker of Zeus malware family indicators (aka Zbot or WSNPoem) from zeustracker.abuse.ch.	C	0%	0		✓
Bambenek	Known, active, and non-sinkholed C2 indicators from Bambenek Consulting, see bambenekconsulting.com.	B+	0%	<1k		✓

Feed Explorer Dashboard of ThreatConnect

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

Threat Intelligence Platform: TC Complete™

Source: https://www.threatconnect.com

TC Complete™ is a security operations and analytics platform built on the ThreatConnect© platform. It provides not only the ability to orchestrate security functions but also the confidence that tasks and decisions are based on vetted, relevant threat intelligence.

It includes all the features of ThreatConnect©, such as indicator analytics, threat intelligence analysis, orchestration, and tasking, allowing for informed decision-making based on the power of the target organization's threat intelligence. This platform enables users to orchestrate security processes, analyze data, and proactively hunt threats in one central place.

TC Complete™ allows users to perform the following:

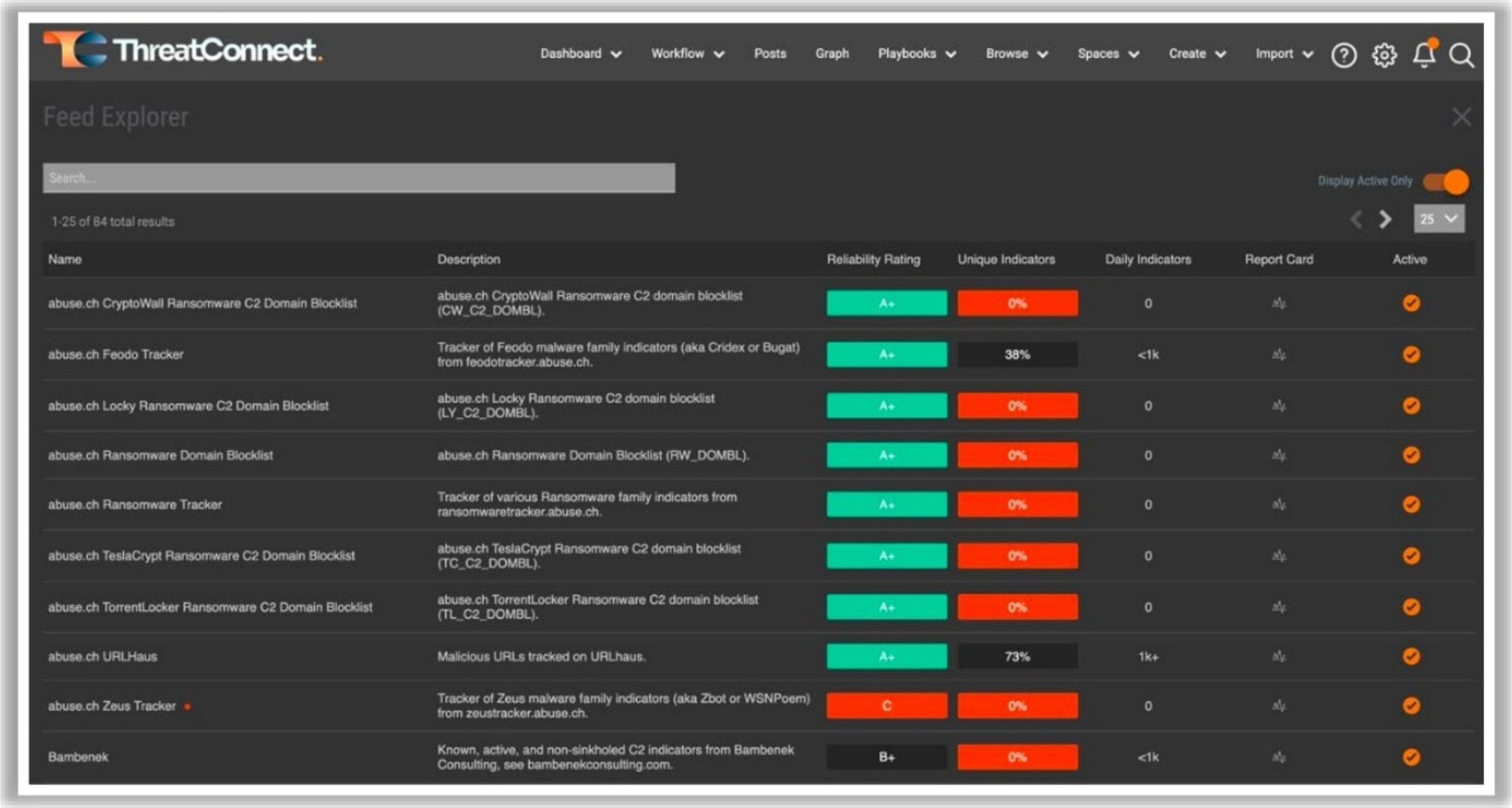
- Analyzing, hunting, creating, and acting on threat intelligence
- Studying what worked and what did not to continue improving defense mechanisms
- Configuring a ThreatConnect© instance with custom apps, playbooks, indicators, attributes, and import rules

Benefits of TC Complete™

- **Improves visibility:** It explores who is attacking an organization and how through the following steps:
  - Aggregating and normalizing threat data from multiple sources
  - Viewing how often indicators are observed and how relevant they are

- Easily identifying platform ratings, team votes, and false-positive counts per indicator or incident

- **Maximizes efficiency:** TC Complete™ helps analysts do the following:
  - Creating automated, configurable playbooks in a single click without coding
  - Automating nearly any security operation or task such as sending alerts, enriching data, or assigning tasks to teams
- **Takes control:** It configures the platform based on organizational needs through the following steps:
  - Proactively hunting threats in the organization's network
  - Creating custom dashboards to view the data that are the most critical and useful for the organization's team
  - Customizing indicators, attributes, import rules, etc.
  - Creating private communities for secure, role-based collaboration

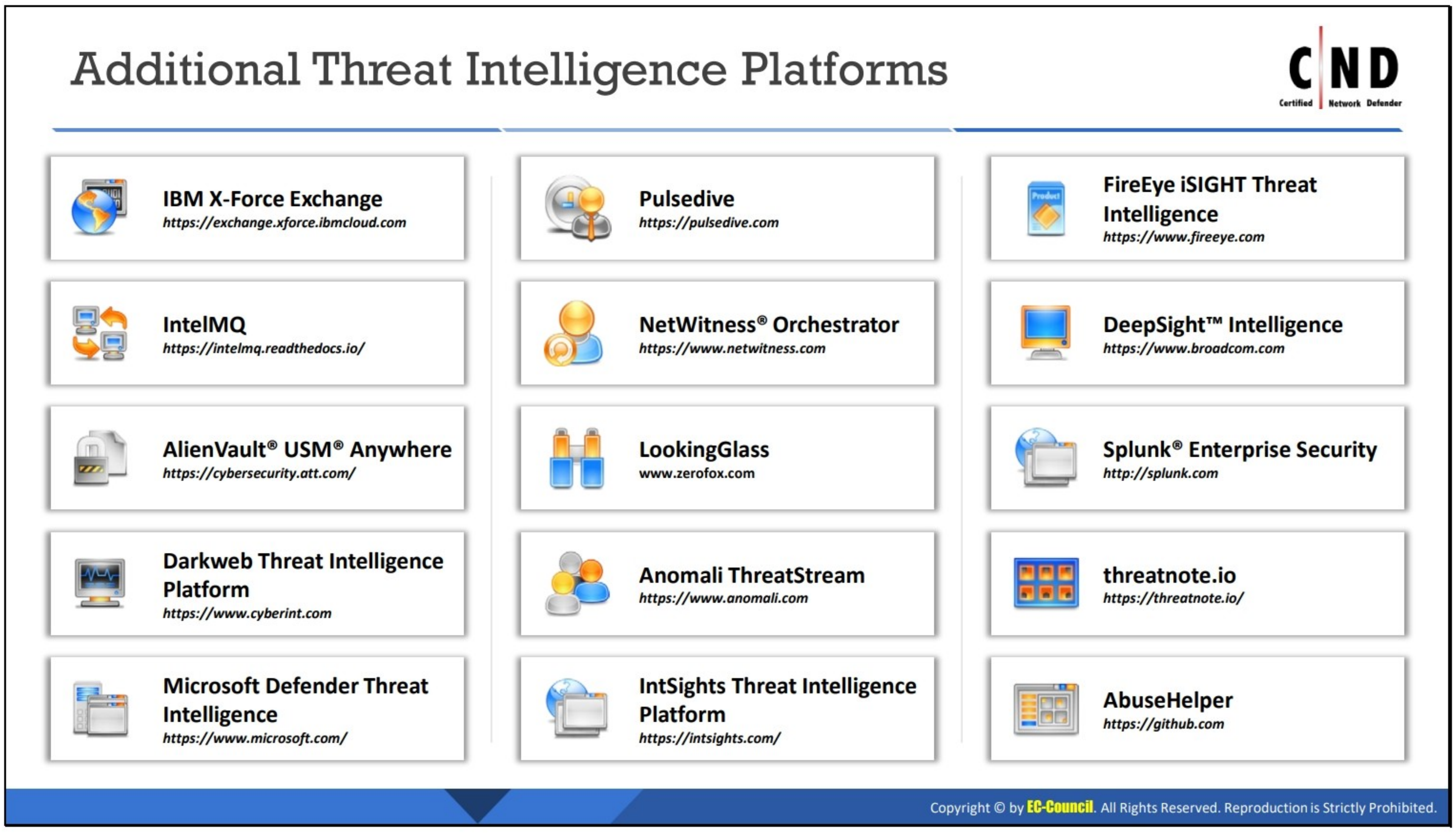


Feed Explorer

1-25 of 84 total results

Name	Description	Reliability Rating	Unique Indicators	Daily Indicators	Report Card	Active
abuse.ch CryptoWall Ransomware C2 Domain Blocklist	abuse.ch CryptoWall Ransomware C2 domain blocklist (CW_C2_DOMBL).	A+	0%	0		✓
abuse.ch Feodo Tracker	Tracker of Feodo malware family indicators (aka Cridex or Bugat) from feodotracker.abuse.ch.	A+	38%	<1k		✓
abuse.ch Locky Ransomware C2 Domain Blocklist	abuse.ch Locky Ransomware C2 domain blocklist (LY_C2_DOMBL).	A+	0%	0		✓
abuse.ch Ransomware Domain Blocklist	abuse.ch Ransomware Domain Blocklist (RW_DOMBL).	A+	0%	0		✓
abuse.ch Ransomware Tracker	Tracker of various Ransomware family indicators from ransomwaretracker.abuse.ch.	A+	0%	0		✓
abuse.ch TeslaCrypt Ransomware C2 Domain Blocklist	abuse.ch TeslaCrypt Ransomware C2 domain blocklist (TC_C2_DOMBL).	A+	0%	0		✓
abuse.ch TorrentLocker Ransomware C2 Domain Blocklist	abuse.ch TorrentLocker Ransomware C2 domain blocklist (TL_C2_DOMBL).	A+	0%	0		✓
abuse.ch URLHaus	Malicious URLs tracked on URLhaus.	A+	73%	1k+		✓
abuse.ch Zeus Tracker ●	Tracker of Zeus malware family indicators (aka Zbot or WSNPoem) from zeustracker.abuse.ch.	C	0%	0		✓
Bambenek	Known, active, and non-sinkholed C2 indicators from Bambenek Consulting, see bambenekconsulting.com.	B+	0%	<1k		✓

Figure 20.4: Screenshot of ThreatConnect© TC Complete™



Additional Threat Intelligence Platforms

- **IBM X-Force Exchange** *https://exchange.xforce.ibmcloud.com*
- **IntelMQ** *https://intelmq.readthedocs.io/*
- **AlienVault® USM® Anywhere** *https://cybersecurity.att.com/*
- **Darkweb Threat Intelligence Platform** *https://www.cyberint.com*
- **Microsoft Defender Threat Intelligence** *https://www.microsoft.com/*
- **Pulsedive** *https://pulsedive.com*
- **NetWitness® Orchestrator** *https://www.netwitness.com*
- **LookingGlass** *www.zerofox.com*
- **Anomali ThreatStream** *https://www.anomali.com*
- **IntSights Threat Intelligence Platform** *https://intsights.com/*
- **FireEye iSIGHT Threat Intelligence** *https://www.fireeye.com*
- **DeepSight™ Intelligence** *https://www.broadcom.com*
- **Splunk® Enterprise Security** *http://splunk.com*
- **threatnote.io** *https://threatnote.io/*
- **AbuseHelper** *https://github.com*

Additional Threat Intelligence Platforms

Listed below are some additional TIPs.

IBM X-Force Exchange

Source: https://www.ibm.com

IBM X-Force Exchange is a cloud-based TIP that allows the user to consume, share, and act on threat intelligence. It enables the user to rapidly research the latest global security threats, aggregate actionable intelligence, consult with experts, and collaborate with peers. It is supported by human- and machine-generated intelligence and leverages the scale of IBM X-Force to help users stay ahead of emerging threats.

Key Features of IBM X-Force Exchange

- Access to a wealth of threat intelligence data
- Collaborative platform for sharing threat intelligence
- Integrated solution to help suddenly stop threats
- Easy-to-use interface for organizing and annotating findings
- Monitor applicable indicators with watch lists
- Add third-party threat intelligence licenses to the platform
- Access to the latest actionable threat research

IntelMQ

Source: https://intelmq.readthedocs.io/

IntelMQ is a solution for IT security teams (CERTs, CSIRTs, abuse departments, etc.) for collecting and processing security feeds using a message queue protocol. It is a community-driven initiative called the Incident Handling Automation Project, which was conceptually designed by European CERTs/CSIRTs during several InfoSec events. Its main goal is to provide incident responders an easy method to collect and process threat intelligence, thereby improving the incident handling processes of CERTs.

IntelMQ's design was influenced by AbuseHelper; however, it was rewritten from scratch and aims at the following:

- Reduce the complexity of system administration.
- Reduce the complexity of writing new bots for new data feeds.
- Reduce the probability of events lost in all processes with persistence functionality (even system crashes).
- Use and improve the existing data harmonization ontology.
- Use the JSON format for all messages.
- Integrate with existing tools (AbuseHelper, Collective Intelligence Framework (CIF), etc.).
- Provide an easy way to store data into log collectors such as ElasticSearch, Splunk, and databases (including PostgreSQL).
- Provide an easy method to create custom blacklists.
- Provide easy communication with other systems via the HTTP RESTFUL application programming interface (API).

AlienVault® USM® Anywhere

Source: https://cybersecurity.att.com/

AlienVault® USM Anywhere™ provides centralized security monitoring for cloud, on-premises, and hybrid IT environments, including endpoints and cloud apps such as Office 365 and G Suite. With multiple essential security capabilities in one unified platform, USM Anywhere simplifies and accelerates threat detection, IR, and compliance management for resource-constrained IT security teams. It deploys rapidly to start detecting threats within minutes. Because it does not require the installation of any hardware appliance or maintenance in the data center, users can save significant time, resources, and money for an overall low total cost of ownership.

USM Anywhere uses virtual sensors that run on VMware and Microsoft Hyper-V to monitor on-premises physical and virtual IT infrastructure. In the cloud, lightweight cloud sensors natively monitor Amazon Web Services and Microsoft Azure Cloud. In addition, users can deploy AlienVault Agents on Windows and Linux endpoints. Security analysis and log storage are centralized in the AlienVault Secure Cloud, providing centralized security visibility for critical infrastructure.

USM Anywhere also receives a continuous stream of threat intelligence updates from the AlienVault Labs Security Research Team so that users always have access to the latest security intelligence. AlienVault Labs leverages data from the Open Threat Exchange® (OTX™)—the world's largest open threat community—to gain expansive intelligence on threats as they appear.

Pulsedive

Source: https://pulsedive.com

Pulsedive is a TIP that leverages OSINT threat feeds and user submissions to deliver actionable intelligence. It allows users to submit, search, correlate, and update IoCs; lists risk factors for why certain IoCs are high risk; and provides a high-level view of threats and threat activity.

LookingGlass

Source: www.zerofox.com

LookingGloass, each day, analyzes billions of pieces of raw intelligence from social media sites, mobile app stores, code shares, and forums. It provides you with the most comprehensive view of the threat.

FireEye iSIGHT Threat Intelligence

Source: https://www.fireeye.com

FireEye iSIGHT Threat Intelligence is a proactive, forward-looking means of qualifying threats poised to disrupt business based on the intents, tools, and tactics of the attacker. Its high-fidelity, comprehensive intelligence delivers visibility beyond the typical attack lifecycle, adding context and priority to global threats before, during, and after an attack. It helps mitigate risk, bolster IR, and enhance the organization's overall security ecosystem. It also enables the organization to predict an attack and refocus its attention on what matters most to the business.

DeepSight™ Intelligence

Source: https://www.symantec.com

DeepSight™ Intelligence is a cloud-hosted CTI platform that provides access to technical and adversary intelligence collected by Symantec through its endpoints and other security products and aggregated through its big data warehouse. The data are enriched, verified, and analyzed to provide attribution and to connect seemingly disparate indicators into campaigns with known actors and motivations behind them. It is powered by two newly released CTI services: Managed Adversary and Threat Intelligence and Directed Threat Research.

Splunk® Enterprise Security

Source: https://www.splunk.com

Splunk Enterprise Security (ES) gives security teams the insight to quickly detect and respond to internal and external attacks and simplify threat management to minimize risk. ES helps teams gain organization-wide visibility and security intelligence for continuous monitoring, IR, SOC operations, and providing executives a window into business risk.

Benefits of Splunk® ES

- **Continuously monitor**: It clearly visualizes the security posture with dashboards, key security indicators, static and dynamic thresholds, and trending threats.
- **Prioritize and act**: It optimizes, centralizes, and automates IR workflows with alerts, centralized logs, and predefined reports and correlations.
- **Conduct rapid investigations**: It uses ad-hoc search and correlations to detect malicious activities.
- **Handle multistep investigations**: It traces activities associated with compromised systems and applies the kill-chain methodology to view the attack lifecycle.

Threatnote.io

Source: *https://threatnote.io*

threat_note is a web application built by defense point security to provide security researchers the ability to add and retrieve indicators related to their research. It includes the ability to add IP addresses, domains, and threat actors, with more types to be added in the future. This app fills the gap between various solutions currently available as it is lightweight, is easy to install, and minimizes extraneous information that occasionally impedes the addition of information. To create a new indicator, the user only needs to supply the object itself.

Other applications built for storing indicators and research have some shortcomings that threat_note hopes to fix. The following are some common complaints with other apps:

- Difficult to install/configure/maintain
- Need to pay for added features (enterprise licenses)
- Excessive information

AbuseHelper

Source: https://github.com

AbuseHelper is an open-source framework for receiving and redistributing abuse feeds and threat intelligence.

Darkweb Threat Intelligence Platform

Source: https://www.cyberint.com

Darkweb Threat Intelligence Platform" is a specialized cybersecurity tool which is designed for monitoring and analyzing activities on the dark web, providing organizations with critical insights into potential threats and vulnerabilities.

Microsoft Defender Threat Intelligence

Source: https://www.microsoft.com/

Microsoft Defender Threat Intelligence is a cybersecurity service provided by Microsoft that is focused on advanced threat intelligence and protection. It is known for discovering the full scope of an attack. Understand an online adversary’s entire toolkit, prevent access by all their machines and known entities, and continuously block IP addresses or domains.

Netwitness Orchestrator

Source: https://www.netwitness.com

Netwitness Threat Intelligence provides services such as threat data aggregation, real-time threat detection, threat intelligence feeds and more. It also provides organizations with advanced threat intelligence and analysis capabilities.

Anomali ThreatStream

Source: https://www.anomali.com

Anomali Threat Stream specializes in information sharing as well as threat intelligence. It provides services like threat intelligence aggregation, customizable threat feeds, incident response support.

IntSights Threat Intelligence Platform

Source: https://intsights.com/

IntSights is a threat intelligence platform company. This company provides services like comprehensive threat data, real-time threat monitoring, automated threat analysis, etc. It also provides customizable dashboards to visualize and report threat intelligence data, risk management, etc.

DeepSight Intelligence

Source: https://www.broadcom.com

DeepSight Intelligence is a threat intelligence service provided by Broadcom. It offers services such as threat intelligence sharing, incident response support, attack analysis, vulnerability intelligence, customizable alerts, etc.

Threat Intelligence Professional Services

- In addition to providing TI feeds, threat intelligence providers offer the services of TI experts who help in obtaining **threat intelligence data**

Strengthen
Defenses w
Threat Inte

Webroot® Threat Intelligence for Cybersecurity

Integrated by leading security vendors worldwide, Webroot BrightCloud® Threat Intelligence Services help you give customers proactive protection against modern threats.

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

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

Threat Intelligence Professional Services

In addition to providing TI feeds, threat intelligence providers offer the services of threat intelligence experts who help in obtaining threat intelligence data.

The following are some examples.

Recorded Future

Source: https://www.recordedfuture.com

Recorded Future's technology collects and analyzes huge amounts of data to deliver relevant cyber threat insights in real time. Its key features include an intuitive web interface, a browser extension, expert analysis on requested topics relevant to the organization, third-party risk assessment, security control feeds, and a threat intelligence platform.

Webroot Threat Intelligence for Cybersecurity

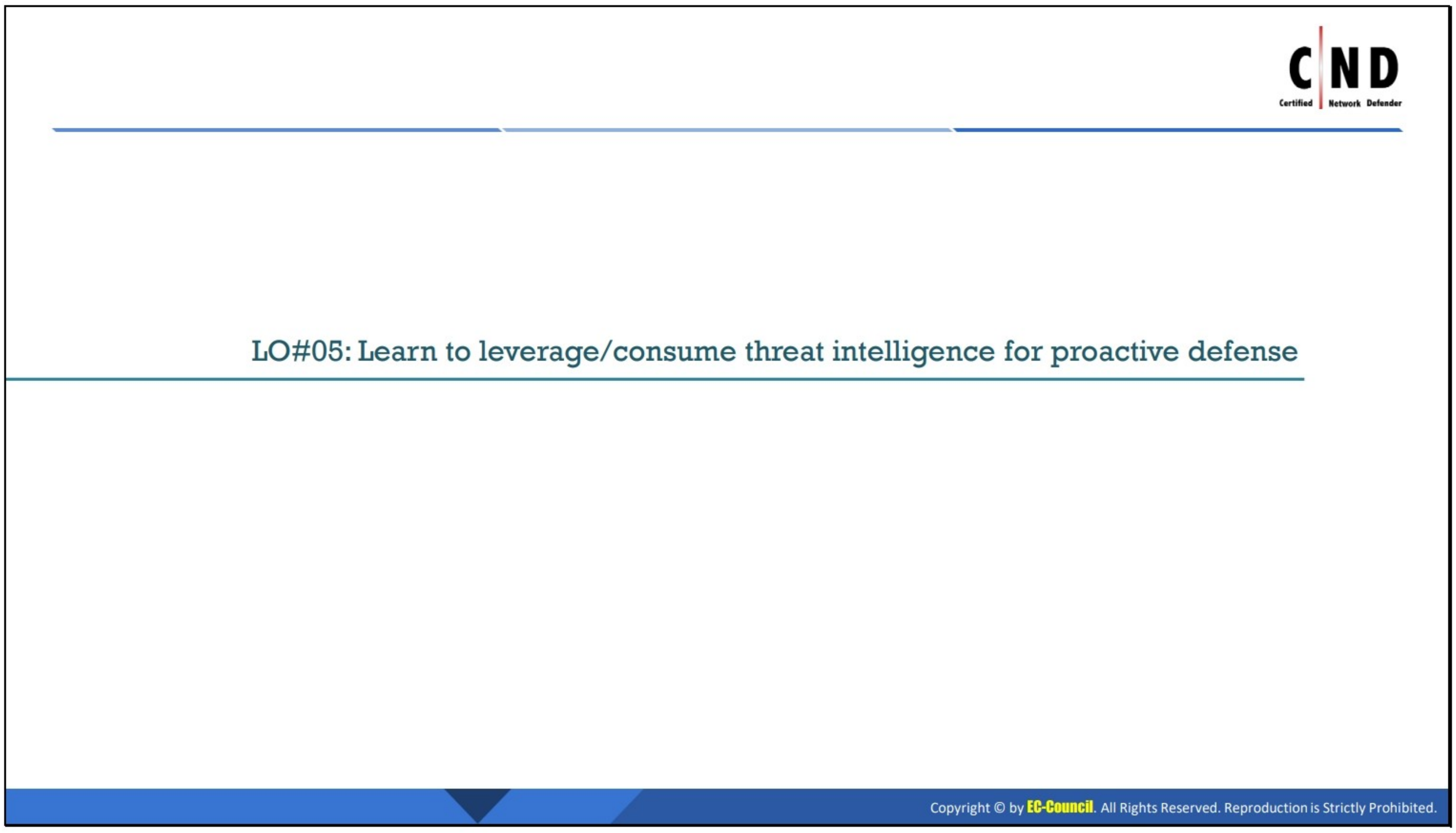
Source: https://www.webroot.com

Webroot BrightCloud Threat Intelligence Services offer proactive protection against modern threats. Its key features include an IP reputation service, web classification and reputation service, real-time anti-phishing service, streaming malware detection, and file reputation service.

Frontline Cyber Threat Management

Source: www.digitaldefense.com

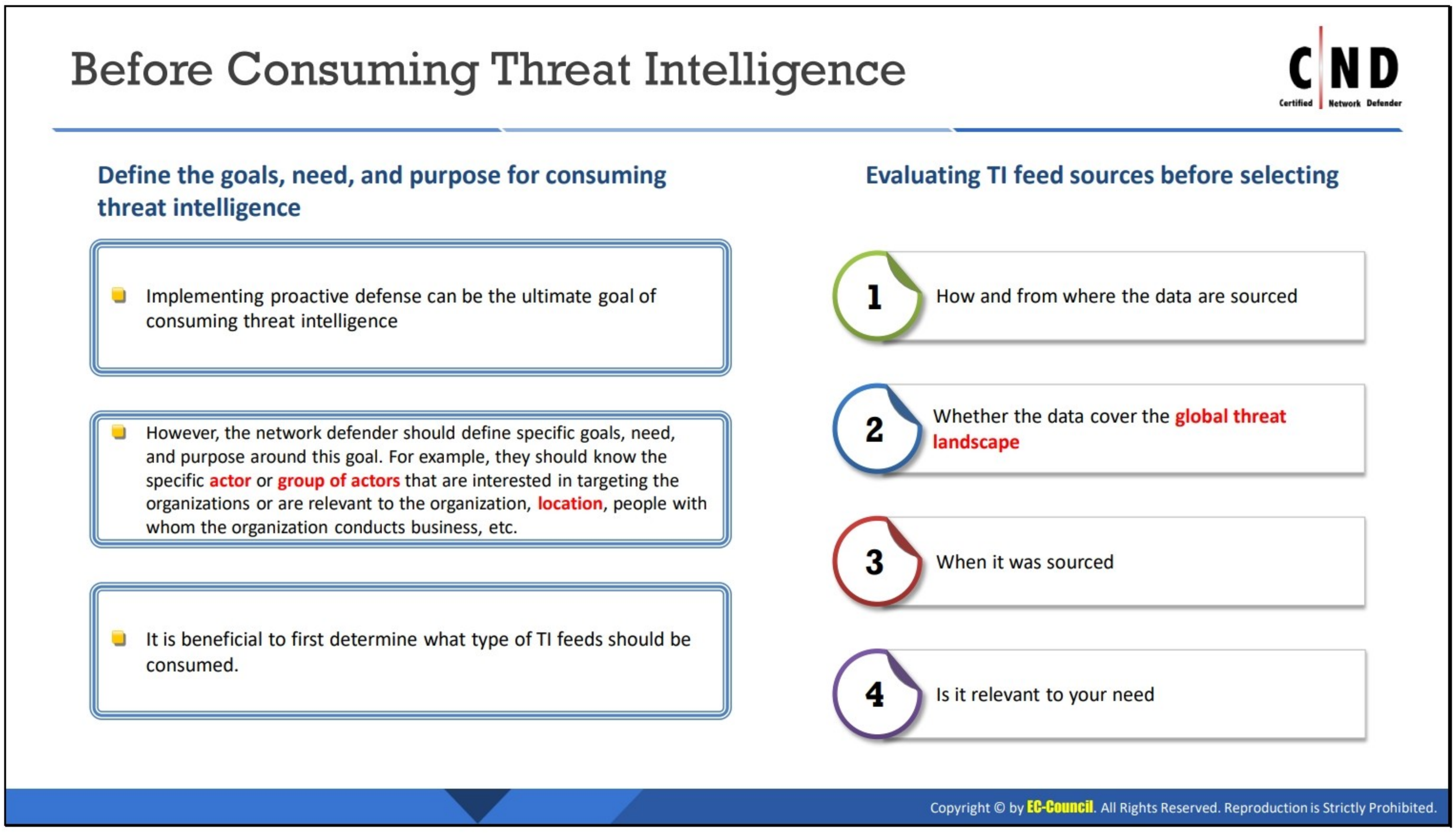
Frontline Cyber Threat Management (CTM) delivers expert threat intelligence to organizations seeking to evaluate the level of risk of cyber threats. Its key features include cyber threat risk report cards, cyber threat assessment, and cyber threat monitoring.



LO#05: Learn to leverage/consume threat intelligence for proactive defense

LO#05: Learn to Leverage/Consume Threat Intelligence for Proactive Defense

Using threat intelligence, network defenders make quick security decisions and change the security approach to proactive. A relevant and actionable TI feed helps network defenders defend their network and systems before an actual attack occurs. This section explains how to integrate TI feeds in security tools such as SIEMs.



Before Consuming Threat Intelligence

Define the goals, need, and purpose for consuming threat intelligence

- Implementing proactive defense can be the ultimate goal of consuming threat intelligence
- However, the network defender should define specific goals, need, and purpose around this goal. For example, they should know the specific **actor** or **group of actors** that are interested in targeting the organizations or are relevant to the organization, **location**, people with whom the organization conducts business, etc.
- It is beneficial to first determine what type of TI feeds should be consumed.

Evaluating TI feed sources before selecting

1. How and from where the data are sourced
2. Whether the data cover the **global threat landscape**
3. When it was sourced
4. Is it relevant to your need

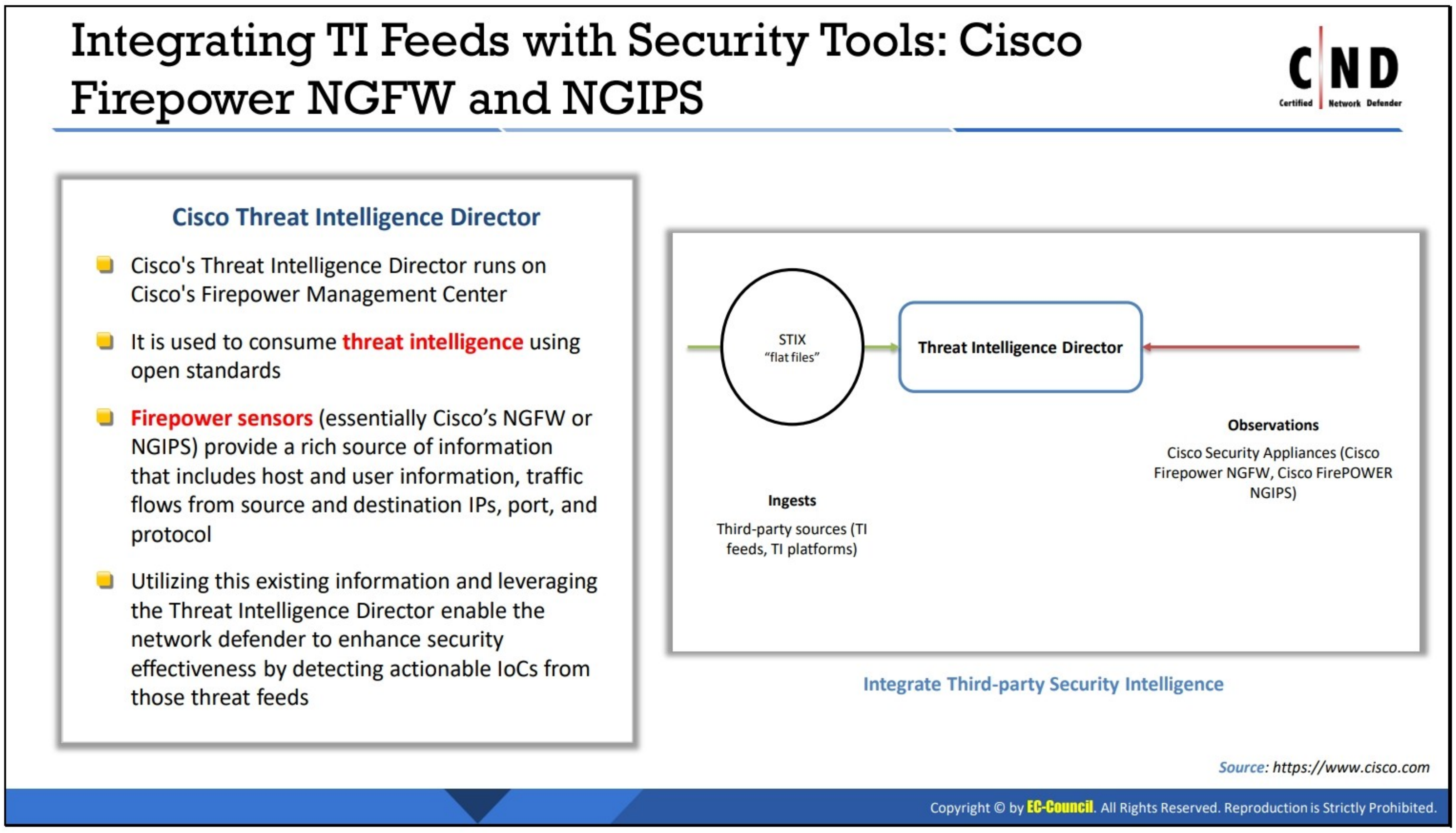
Before Consuming Threat Intelligence

Before consuming threat intelligence, a network defender should consider the following.

- **Define the goals, need, and purpose for consuming threat intelligence**
  - Implement proactive defense. This can be the goal of consuming threat intelligence.
  - Define specific goals, need, and purpose around the implementation of proactive defense.
  - Know the specific actor or group of actors that are interested in targeting the organization or are relevant to the organization, location, people with whom the organization conducts business, etc.
  - Assess the organization's capabilities and goals by asking following questions:
    - What does network infrastructure look like?
    - What is the current security posture and the availability of budget and resources to produce and apply threat intelligence?
- **Evaluating TI feed sources before selecting**

  Threat intelligence is classified into Internet (web reputation, IP reputation, anti-phishing), file (file reputation), and mobile (app reputation, mobile security) intelligence. Organizations integrate one or more of these types of threat intelligence based on their requirement. Before consuming threat intelligence, it is necessary to carefully evaluate the following:
  - How and from where the data are sourced

- Whether the data cover the global threat landscape
- Age of the data (when the data was sourced and how long the data took to process)
- Data efficacy (for false positives/negatives and correlation against other data)
- Relevance to specific needs (organization or geographic level)



Integrating TI Feeds with Security Tools: Cisco Firepower NGFW and NGIPS

Cisco Threat Intelligence Director

- Cisco's Threat Intelligence Director runs on Cisco's Firepower Management Center
- It is used to consume **threat intelligence** using open standards
- **Firepower sensors** (essentially Cisco's NGFW or NGIPS) provide a rich source of information that includes host and user information, traffic flows from source and destination IPs, port, and protocol
- Utilizing this existing information and leveraging the Threat Intelligence Director enable the network defender to enhance security effectiveness by detecting actionable IoCs from those threat feeds

STIX
"flat files"
Threat Intelligence Director
Observations
Cisco Security Appliances (Cisco Firepower NGFW, Cisco FirePOWER NGIPS)
Ingests
Third-party sources (TI feeds, TI platforms)

Integrate Third-party Security Intelligence

Source: https://www.cisco.com

Integrating TI Feeds with Security Tools: Cisco Firepower NGFW and NGIPS

Cisco's Threat Intelligence Director is used to ingest threat intelligence using open standards. It runs on Cisco's Firepower Management Center. The Firepower sensors (NGFW or NGIPS) provide information about the hosts, users, and traffic flows from source and destination IPs, port, and protocol.

By using this information and leveraging the Threat Intelligence Director, security can be increased by spotting the actionable indicators of compromise from threat feeds.

The Threat Intelligence Director has the following benefits:

- Detecting and blocking indicators and observables by using automated actions
- Reporting detection and incidents accurately
- Improved detection time and response time to threats on the network
- Providing a single integration point for all Structured Threat Information Expression (STIX)/Trusted Automated Exchange of Indicator Information (TAXII) and flat file intelligence sources

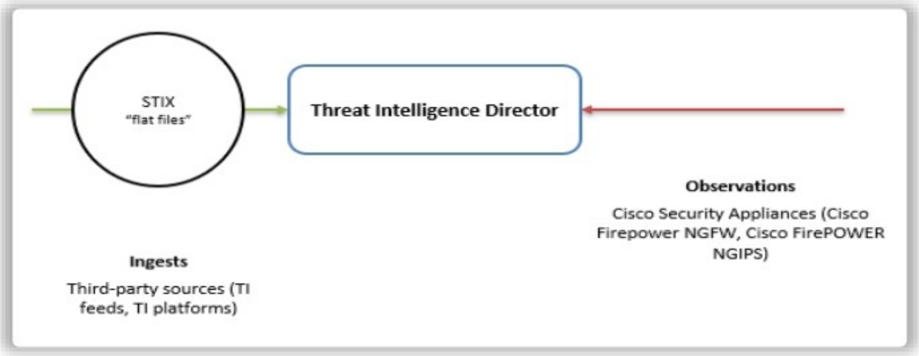
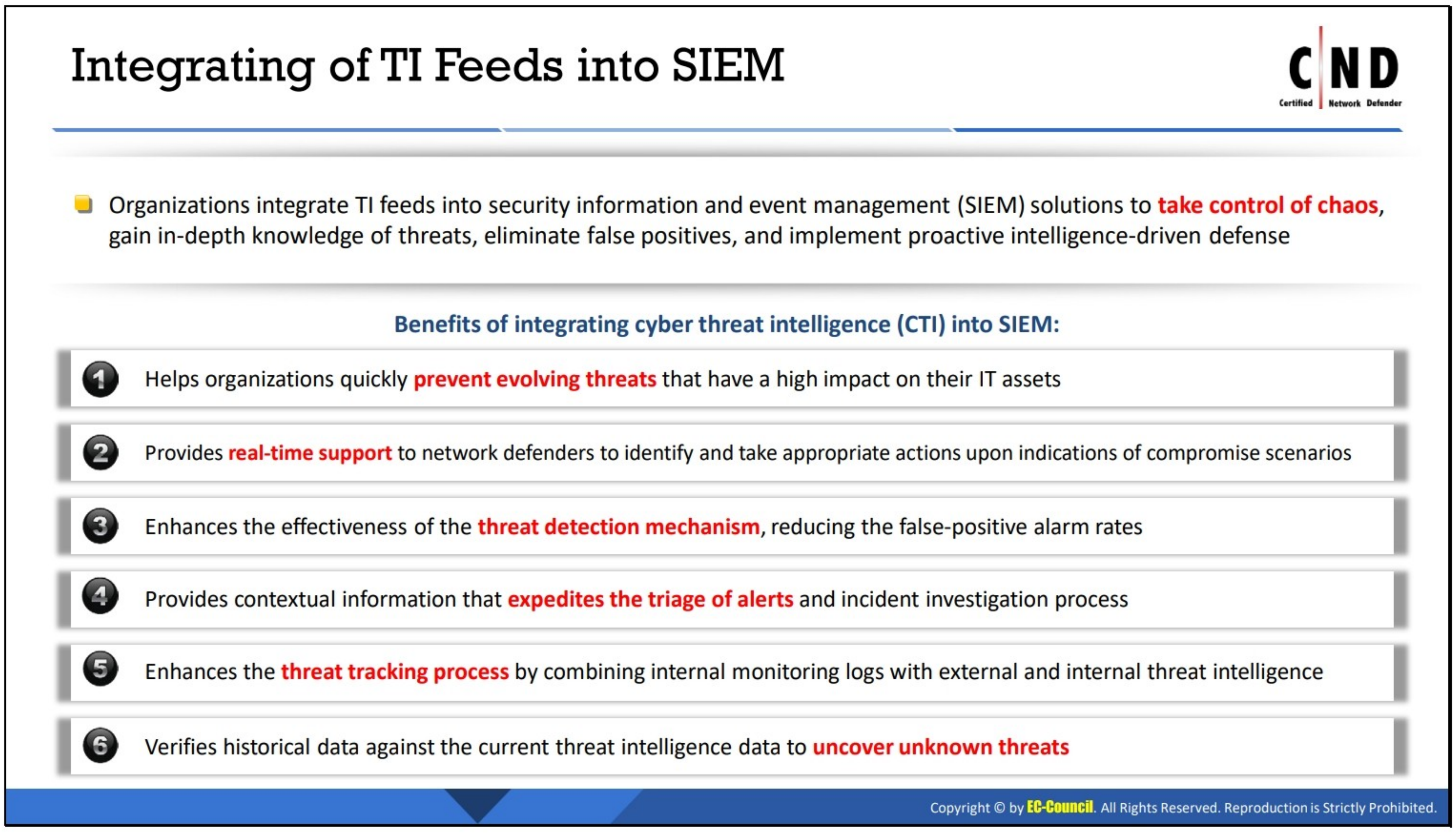

STIX
"flat files"
Threat Intelligence Director
Observations
Cisco Security Appliances (Cisco Firepower NGFW, Cisco FirePOWER NGIPS)
Ingests
Third-party sources (TI feeds, TI platforms)

Figure 20.5: Integration of third-party security intelligence in

Cisco Threat Intelligence Director



Integrating of TI Feeds into SIEM

- Organizations integrate TI feeds into security information and event management (SIEM) solutions to **take control of chaos**, gain in-depth knowledge of threats, eliminate false positives, and implement proactive intelligence-driven defense

Benefits of integrating cyber threat intelligence (CTI) into SIEM:

1. Helps organizations quickly **prevent evolving threats** that have a high impact on their IT assets
2. Provides **real-time support** to network defenders to identify and take appropriate actions upon indications of compromise scenarios
3. Enhances the effectiveness of the **threat detection mechanism**, reducing the false-positive alarm rates
4. Provides contextual information that **expedites the triage of alerts** and incident investigation process
5. Enhances the **threat tracking process** by combining internal monitoring logs with external and internal threat intelligence
6. Verifies historical data against the current threat intelligence data to **uncover unknown threats**

Integrating of TI Feeds into SIEM

Organizations integrate TI feeds into SIEM to take control of chaos, gain in-depth knowledge of threats, eliminate false positives, and implement proactive intelligence-driven defense.

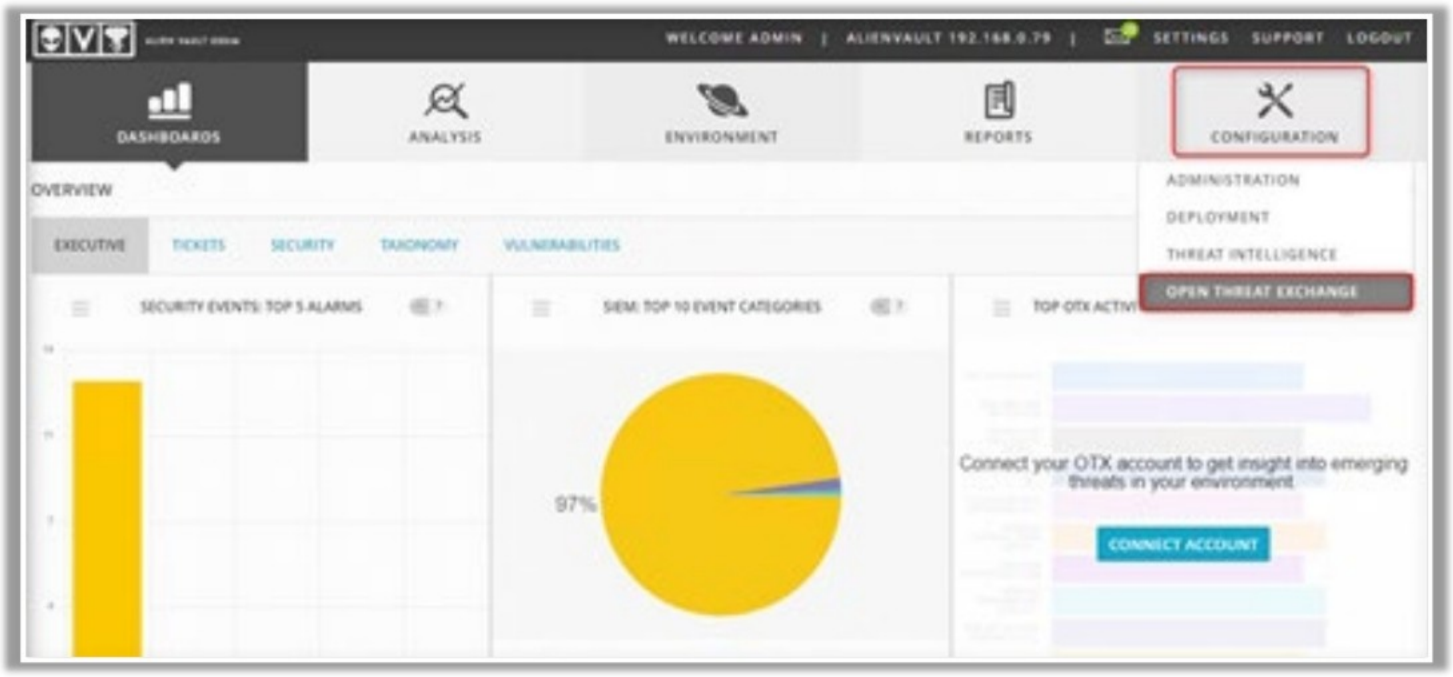
Listed below are the benefits of integrating TI feeds into SIEM:

- Integration of CTI into SIEM helps organizations quickly prevent evolving threats that have a high impact on their IT assets.
- CTI provides real-time support to identify threats and take appropriate actions upon indications of compromise scenarios.
- Threat data feeds integrated with SIEM enhance the effectiveness of the threat detection mechanism, reducing the false-positive alarm rates.
- CTI provides SIEM with the capability of providing real-time alerts of upcoming threats along with a complete understanding of the threats and their TTPs.
- High-quality threat intelligence feeds provide contextual information that expedites the triage of alerts and incident investigation process.
- CTI enhances the threat-tracking process by combining internal monitoring logs with external and internal threat intelligence.
- CTI provides SIEM with the capability to verify historical data against the current threat intelligence data to uncover unknown threats.
- CTI integrated with SIEM helps organizations use contextual information such as IoCs to prioritize incidents, retain historical threat data along with related indicators and past incidents, and generate threat profiles.

- CTI is used to find the scope of an incident by relating local observations to threat data feeds to identify all the compromised IT resources and traces of an attack.
- CTI helps analysts mitigate advanced threats by collaborating in response and protection mechanisms without analyzing huge volumes of log data.
- CTI allows proactive analysis by pivoting outside the threat information and known IoCs to add context and intelligence to evolving threats.
- CTI integrated with SIEM adds context and relationship to the identified indicators that enable organizations to understand the nature of threats and the level of risk they pose to their IT assets and to provide an effective response.

Integrating of TI Feeds with SIEM: OSSIM

- **AlienVault Labs Threat Intelligence** drives the USM platform's threat assessment capabilities by identifying the latest threats, resulting in the broadest view of threat vectors, attacker techniques, and effective defenses



Connect your OTX account to get insight into emerging threats in your environment

Integrating of TI Feeds with SIEM: OSSIM

AlienVault Labs Threat Intelligence drives the Unified Security Management (USM) platform's threat assessment capabilities by identifying the latest threats, resulting in the broadest view of threat vectors, attack techniques, and effective defenses.

The Open Threat Exchange (OTX) provides users the ability to collaborate, research, and receive alerts on emerging and evolving threats. The latest TI feeds are updated in the Open Source SIEM (OSSIM) for enhanced security monitoring.

The following rules of OSSIM are updated.

Correlation directives: An extensive library of pre-defined rules to convert raw events into specific, actionable threat information by linking events from across the network

Network IDS signatures: Detects the latest malicious traffic on the network

Host IDS signatures: Identifies the latest threats targeting critical systems

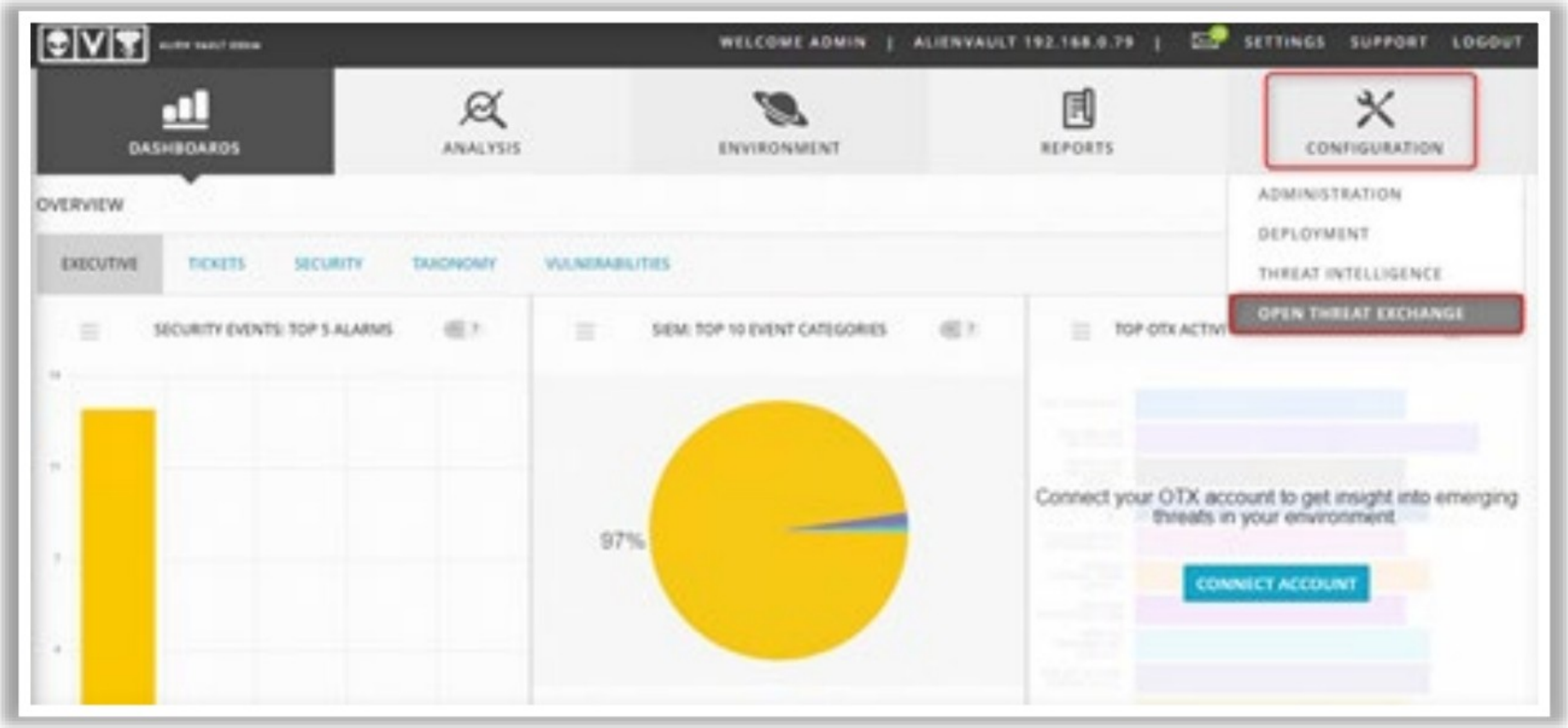
Asset discovery signatures: Detects the latest operating systems, applications, and device information

Vulnerability assessment signatures: Vulnerability signatures of systems

Reporting modules: Views of critical data about the environment

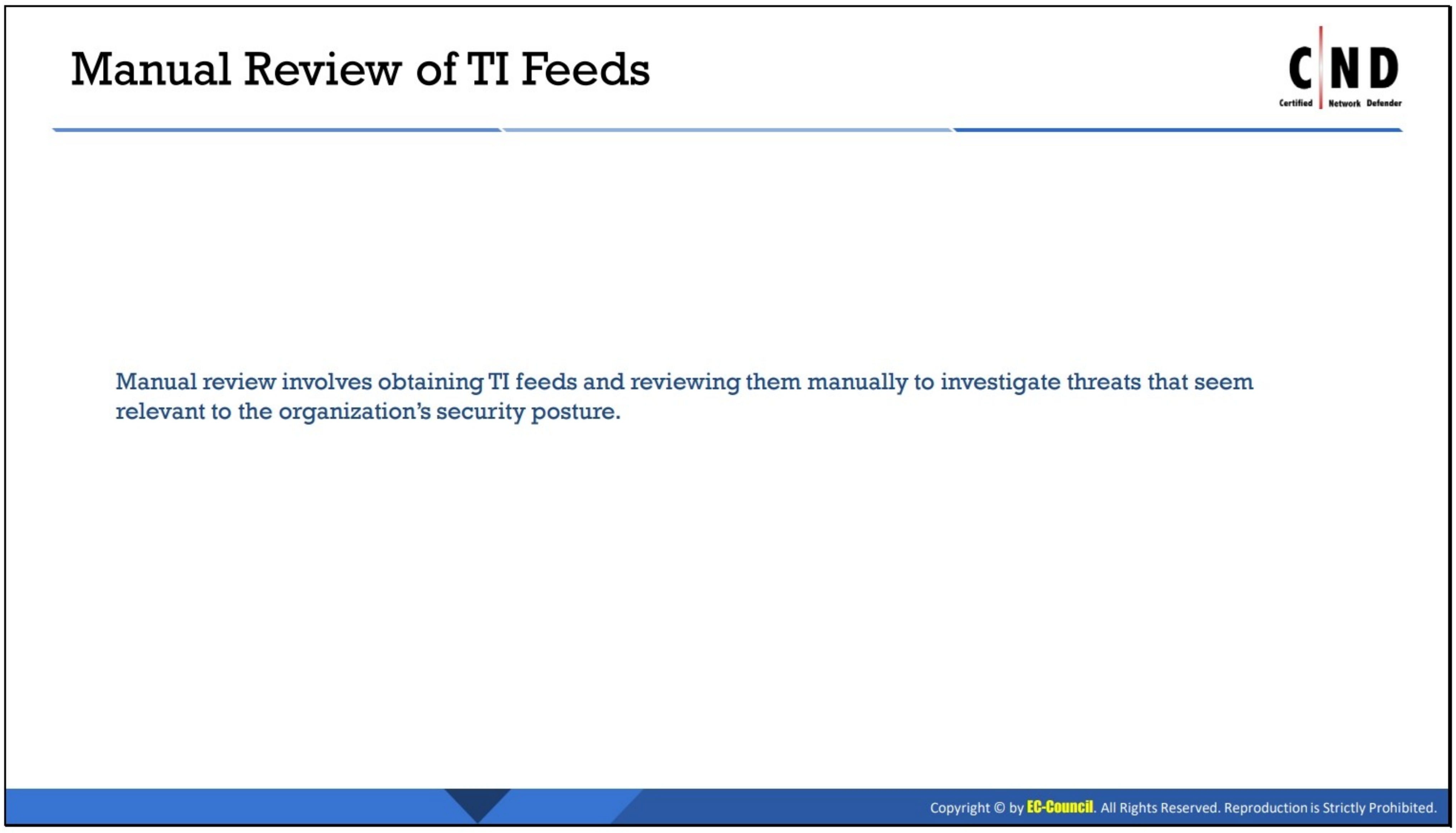
Dynamic IR templates: Customized guidance on how to respond to each alert

Data source plugins: Monitoring footprint by integrating data from legacy security devices and applications



Connect your OTX account to get insight into emerging threats in your environment

Figure 20.6: Screenshot of AlienVault OSSIM

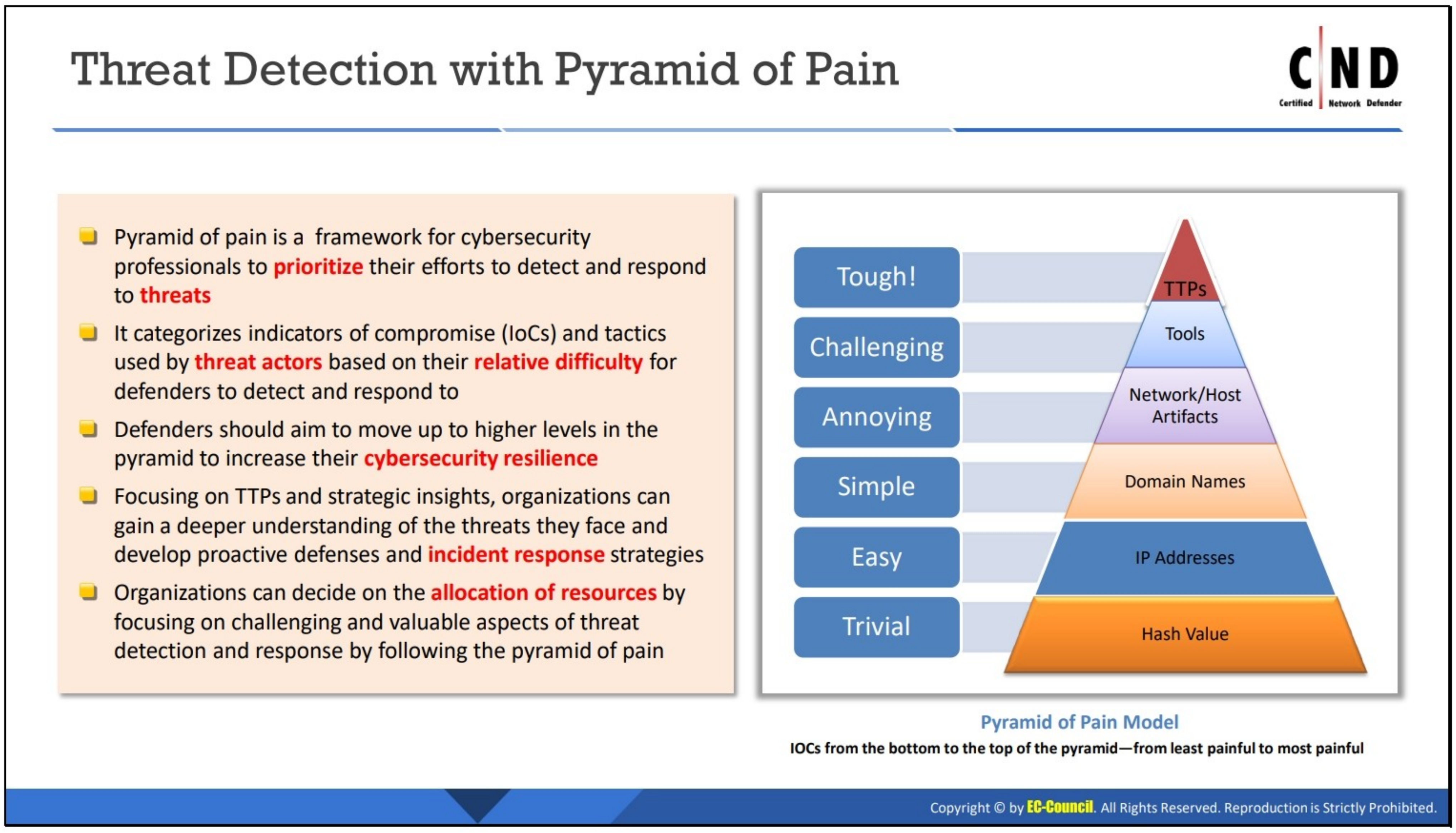


Manual Review of TI Feeds

Manual review involves obtaining TI feeds and reviewing them manually to investigate threats that seem relevant to the organization's security posture.

Manual Review of TI Feeds

Manual review involves obtaining TI feeds and reviewing them manually to investigate threats that seem relevant to the organization's security posture.



Threat Detection with Pyramid of Pain

- Pyramid of pain is a framework for cybersecurity professionals to **prioritize** their efforts to detect and respond to **threats**
- It categorizes indicators of compromise (IoCs) and tactics used by **threat actors** based on their **relative difficulty** for defenders to detect and respond to
- Defenders should aim to move up to higher levels in the pyramid to increase their **cybersecurity resilience**
- Focusing on TTPs and strategic insights, organizations can gain a deeper understanding of the threats they face and develop proactive defenses and **incident response** strategies
- Organizations can decide on the **allocation of resources** by focusing on challenging and valuable aspects of threat detection and response by following the pyramid of pain

Pyramid of Pain Model

IOCs from the bottom to the top of the pyramid—from least painful to most painful

Threat Detection with Pyramid of Pain

The Pyramid of Pain is a framework that enables security teams to prioritize indicators of compromise (IoCs) for identifying security threats. It demonstrates the relationship between different types of IoCs and the impact they have on attackers when denied. Additionally, it represents the level of difficulty organizations face when utilizing each IOC as a threat intelligence piece for defense. The more challenging an IOC is to utilize, the more effective it is against threat actors. The Pyramid of Pain categorizes IoCs and tactics used by threat actors based on the relative difficulty for defenders to detect and respond to them. Defenders should strive to move up the pyramid to higher levels to enhance their cybersecurity resilience. By focusing on tactics, techniques, and procedures (TTPs) and strategic insights, organizations can gain a deeper understanding of the threats they face and develop proactive defense and incident response strategies. This framework also allows organizations to allocate resources effectively by prioritizing the most challenging and valuable aspects of threat detection and response. The Pyramid of Pain arranges six IoCs in ascending order, with each indicator being used to detect attacker activities. The higher the placement of IoCs on the pyramid, the more costly it becomes for threat actors to perform attacks.

The indicators that make up the pyramid are,

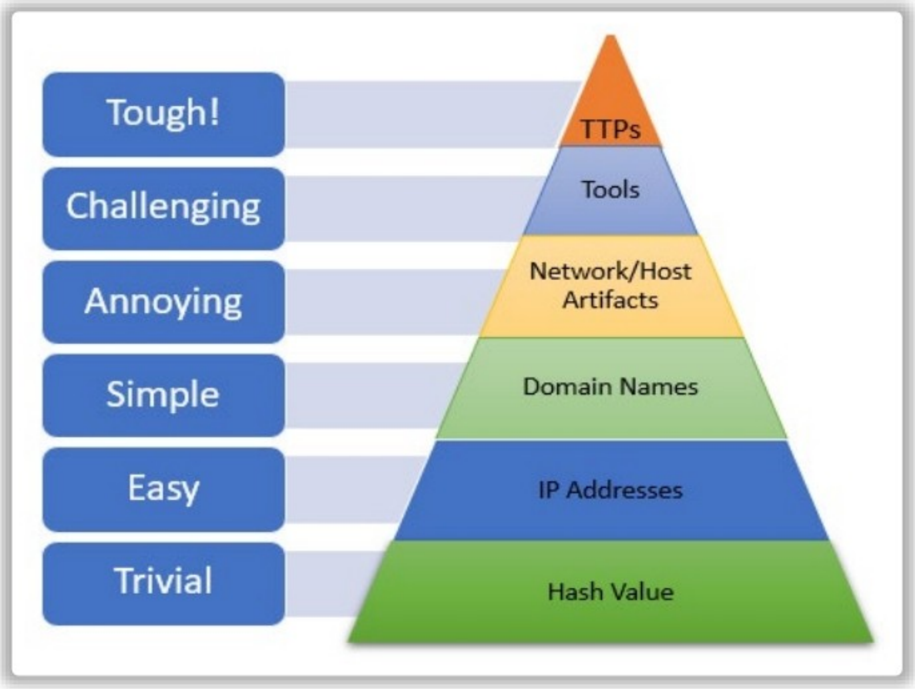


Figure 20.7: Pyramid of Pain Model

- **Hash Values**: Hashes such as SHA1 and MD5 correspond to suspicious or malicious files and are used to provide unique references to specific sample malware or files involved in an intrusion. The alteration of hash values can be easily done by metamorphic or polymorphic techniques. This IOC is likely the least advantageous, as threat actors can effortlessly bypass defense measures by altering hash values. Concentrating on hash values holds little significance for an attacker.

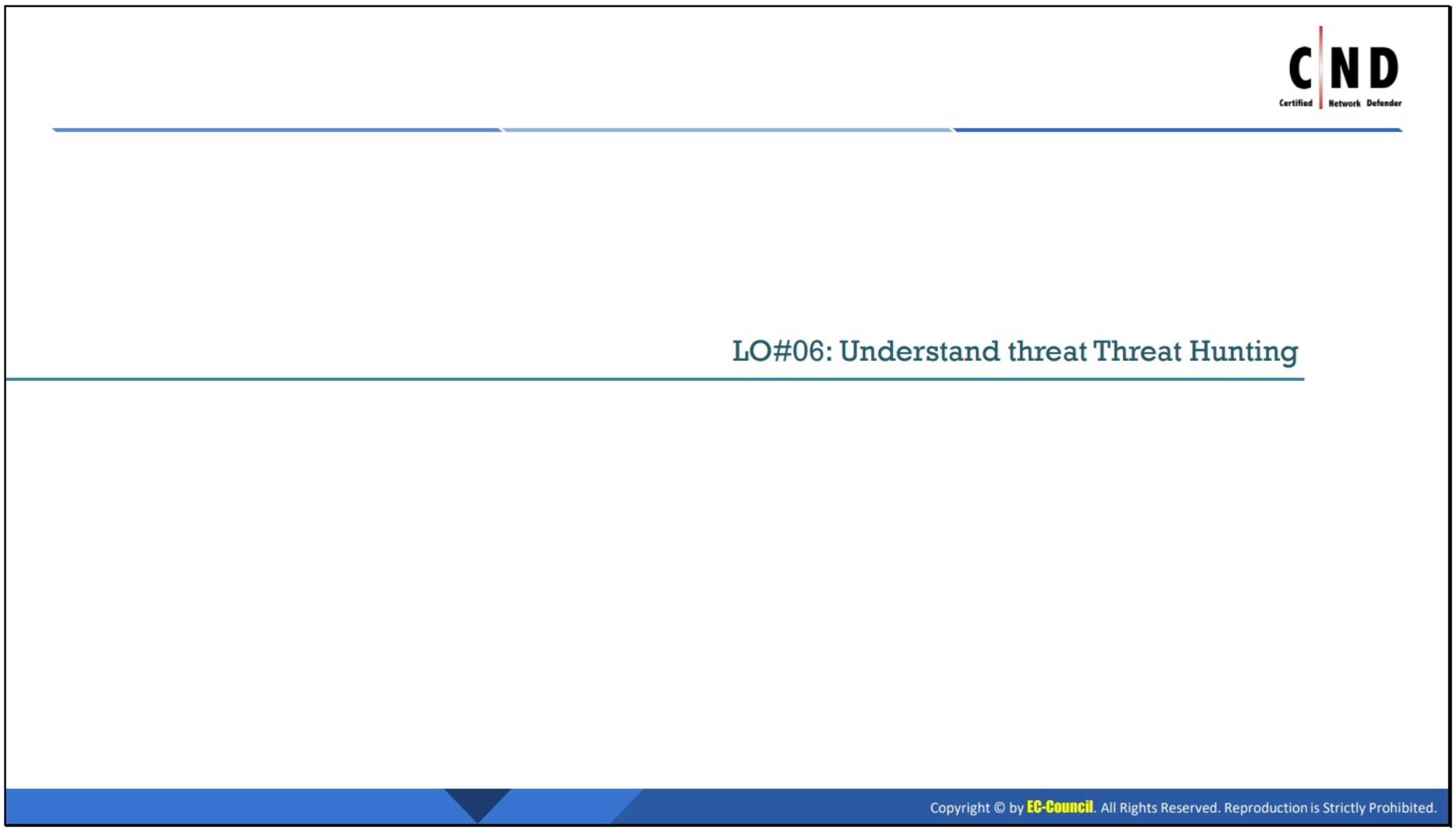
- **IP addresses**: If IP addresses are denied, the attacker can recover quickly and easily perform an attack. VPNs and anonymous proxies can be employed to alter IP addresses as required, and the attackers can easily bypass this obstacle.

- **Domain names**: Domain names are a bit more difficult to change than IP addresses. If the attacker is denied the use of domains, they use Dynamic domain name system services and domain-generated algorithms to edit domain names.

- **Network/host artifacts**: These are indicators arising from attackers' actions affecting one or more of your host systems. Attackers get annoyed when the indicators are detected at this level. The attackers must work on how this indicator was detected and the way the security team is responding. The artefacts can be command and control information, files and directories, registry objects, and URL patterns. Rejecting these artefacts causes pain for the attacker.

- **Tools**: As the security team gets good at detecting artefacts of their tools, the attacker must find different tools or create a new tool for the same purpose. It will be challenging for the attackers as they must research the existing tool or create a new tool, they must figure out how it works.

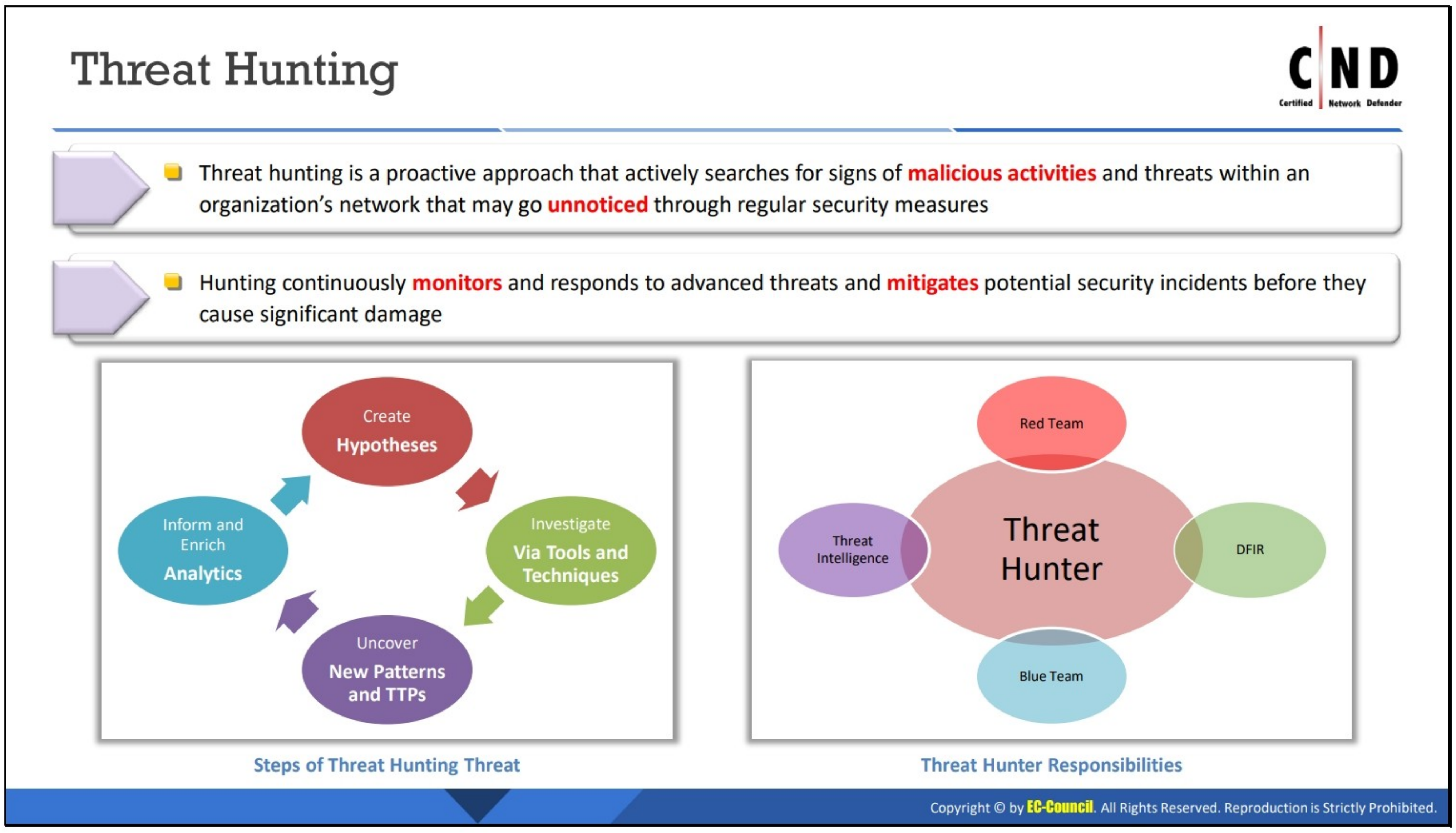
- **Tactics, Techniques, and Procedures (TTPs)**: Lastly, at the highest level are the TTPs. When you detect and respond at this level, you are directly countering attackers' behaviors, rather than targeting their tools. Defending at this level creates substantial obstacles for attackers and diminishes their prospects of executing their attacks successfully.



LO#06: Understand threat Threat Hunting

LO#06: Understand Threat Hunting

This section covers the foundational building blocks of threat hunting, explores a maturity model, and highlights the strategic integration of AI/ML in threat hunting and intelligence. Gain insights into leveraging advanced technologies for effective threat detection, response, and phishing detection, scontributing to a resilient cybersecurity framework.



Threat Hunting

CND Certified Network Defender

- Threat hunting is a proactive approach that actively searches for signs of **malicious activities** and threats within an organization's network that may go **unnoticed** through regular security measures
- Hunting continuously **monitors** and responds to advanced threats and **mitigates** potential security incidents before they cause significant damage

Create **Hypotheses**

Investigate **Via Tools and Techniques**

Uncover **New Patterns and TTPs**

Inform and Enrich **Analytics**

Steps of Threat Hunting Threat

Threat Hunter

Red Team

DFIR

Blue Team

Threat Intelligence

Threat Hunter Responsibilities

Threat Hunting

Threat actors have the ability to remain undetected within a network for months. Once they gain access, they can quietly gather data, search for sensitive information, or obtain login credentials to move throughout the network. If an organization lacks detection capabilities, they are unable to stop the advanced persistent threats that exist within their network. This is why threat hunting isimportant.

Threat hunting involves conducting thorough investigations to uncover any malicious actors that have evaded the organization's initial endpoint security defenses. It is a proactive approach that actively looks for signs of malicious activity and threats that may be missed by regular security measures.It does not rely on signatures, as it is a proactive approach. By continuously monitoring and responding to advanced threats, threat hunting can prevent significant damage by mitigating potential security incidents. The findings from threat hunting can be used directly in the incident response process upon the detection of malicious activity, or can be used to improve security monitoring and develop new detection methods.

Steps of Threat Hunting

The step-by-step process for threat hunting is as follows:

- **Create Hypothesis:** Create a hypothesis about the activities that go on in an organization. It involves creating attack models and the strategies a threat might use, identifying aspects already addressed by automated alerting systems, and devising a hunting investigation to uncover additional potential threats or activities.
- **Investigate using tools and techniques:** A threat hunter explores hypotheses by conducting investigations using a range of tools and techniques. Efficient tools will

combine raw and linked data analysis methods such as machine learning to merge diverse cybersecurity datasets.

- **Uncover new attack patterns and TTPs:** Investigating threats using tools and techniques uncover new patterns of behavior that are malicious and TTP. This step represents the definitive success criteria for a hunting operation.
- **Inform and enrich analytics:** Effective hunts form the foundation for informing and enriching automated analytics. After identifying a successful technique for uncovering threats, automate it to allow the team to concentrate on the next investigation. Insights gained from hunts can also be utilized to enhance existing detection mechanisms.

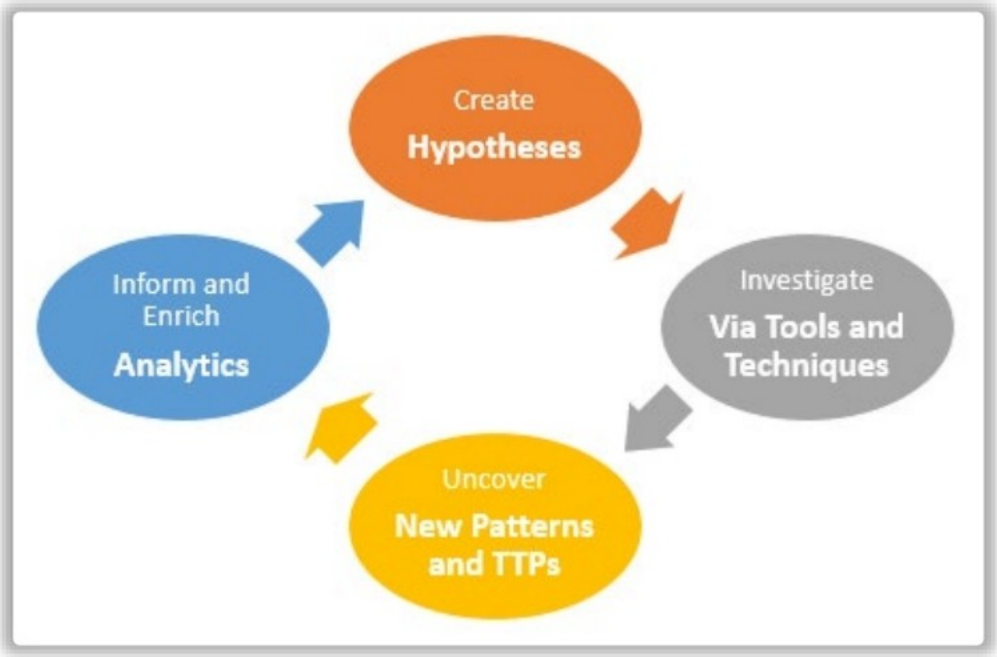


Figure 20.8: Step-by-step Process for Threat Hunting

Threat Hunter Responsibilities

The responsibilities of a threat hunter are as follows:

- Hunting for insider threats/outsider attackers.
- Proactively hunting for known adversaries.
- Searching for hidden threats to prevent the attack from happening.
- Executing the incident response plan.

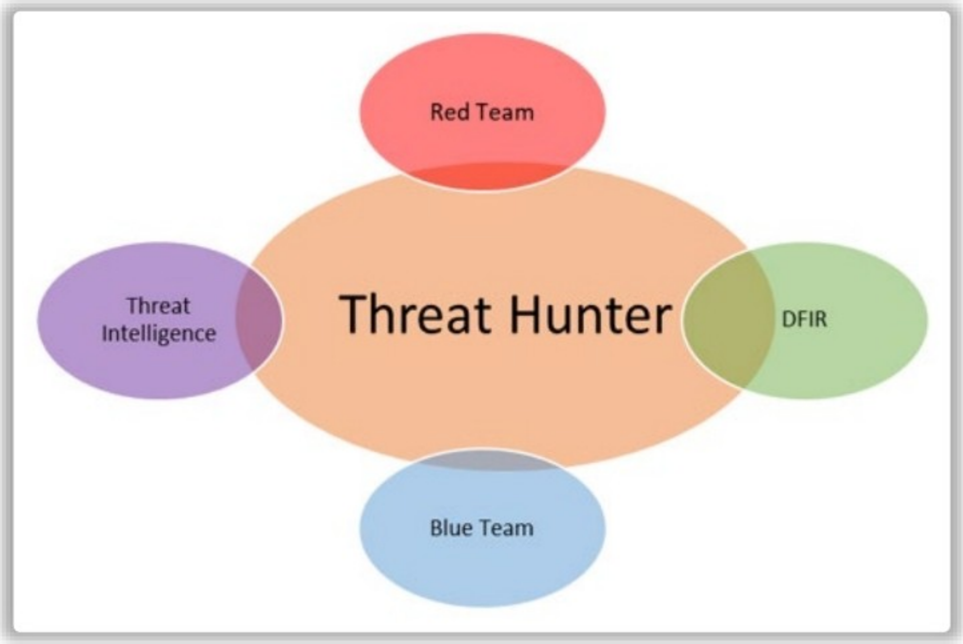
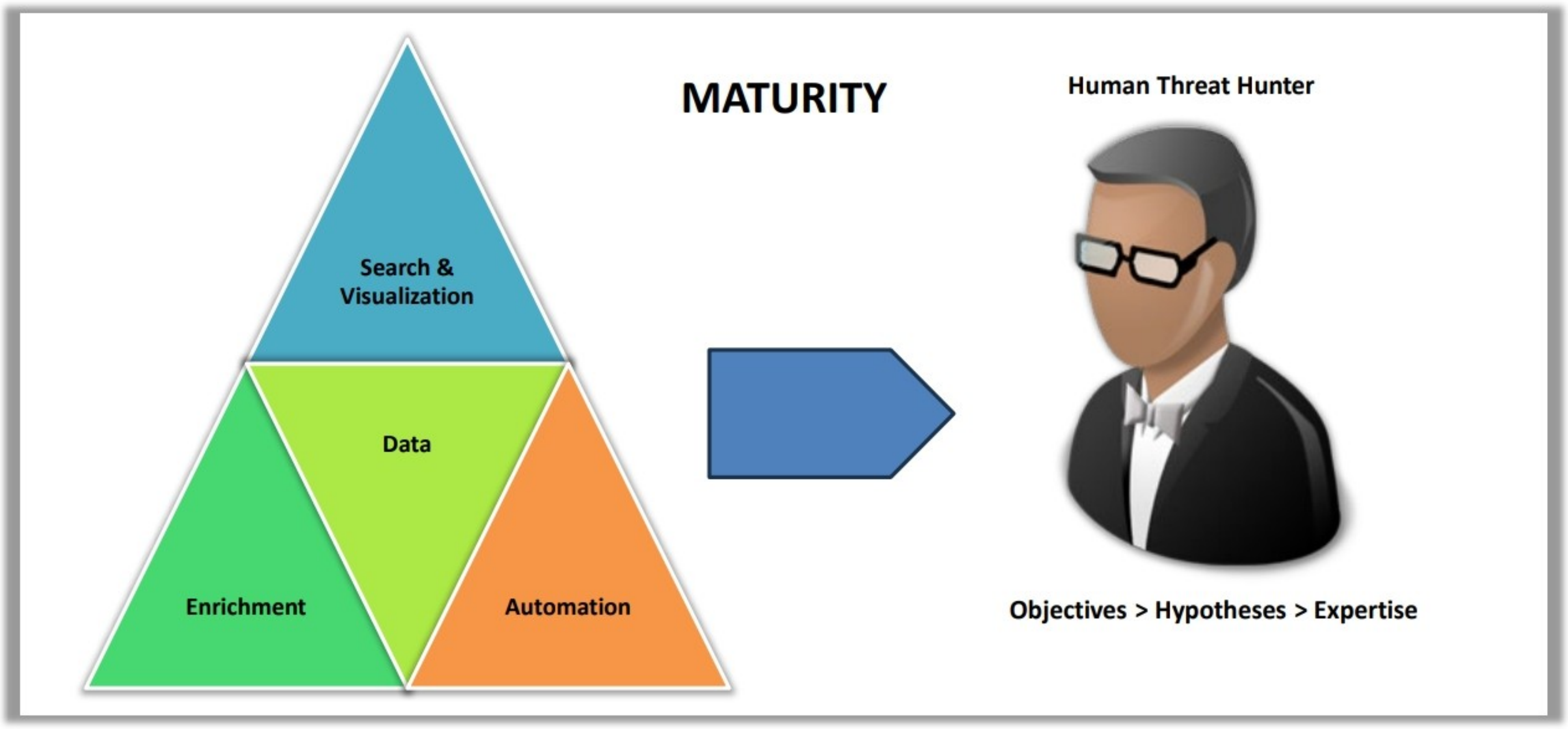


Figure 20.9: Threat Hunter Responsibilities

Threat Hunting Building Blocks



Threat Hunting Building Blocks

Organizations must understand that the threat hunting process is distinct from both preventing adversaries from breaching their environment and addressing vulnerabilities in their network. To effectively conduct threat hunting, they need to invest in the necessary security infrastructure and exercise proper use of threat hunting tools and practices. The primary focus for organizations engaging in threat hunting should be searching for data availability and effectively sorting through that data.

The following are the building blocks for threat hunting:

- **Automation:** Security teams use automation to avoid starting their threat hunting process from the beginning every time they hunt an adversary.
- **Enrichment:** For effective data analysis, the organizations have to ensure the data is enriched with its contextual information.
- **Visualization:** Additionally, organizations should use data visualization to identify links between different data sets.
- **Threat Hunters:** Hunters possess a natural curiosity, a deep passion, and a knack for skillfully using different tools. They have varied background and are passionate for uncovering threats that can complement the overall effort.

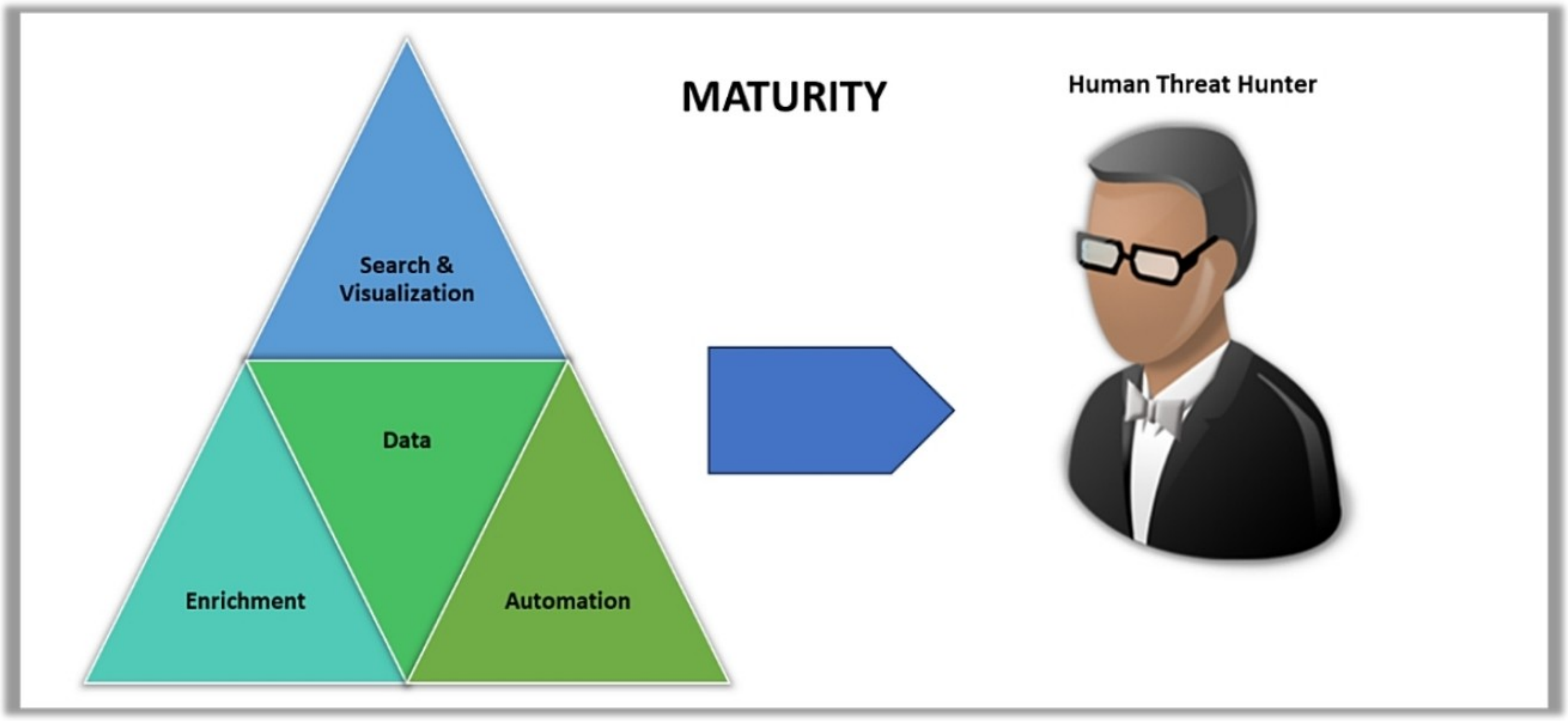
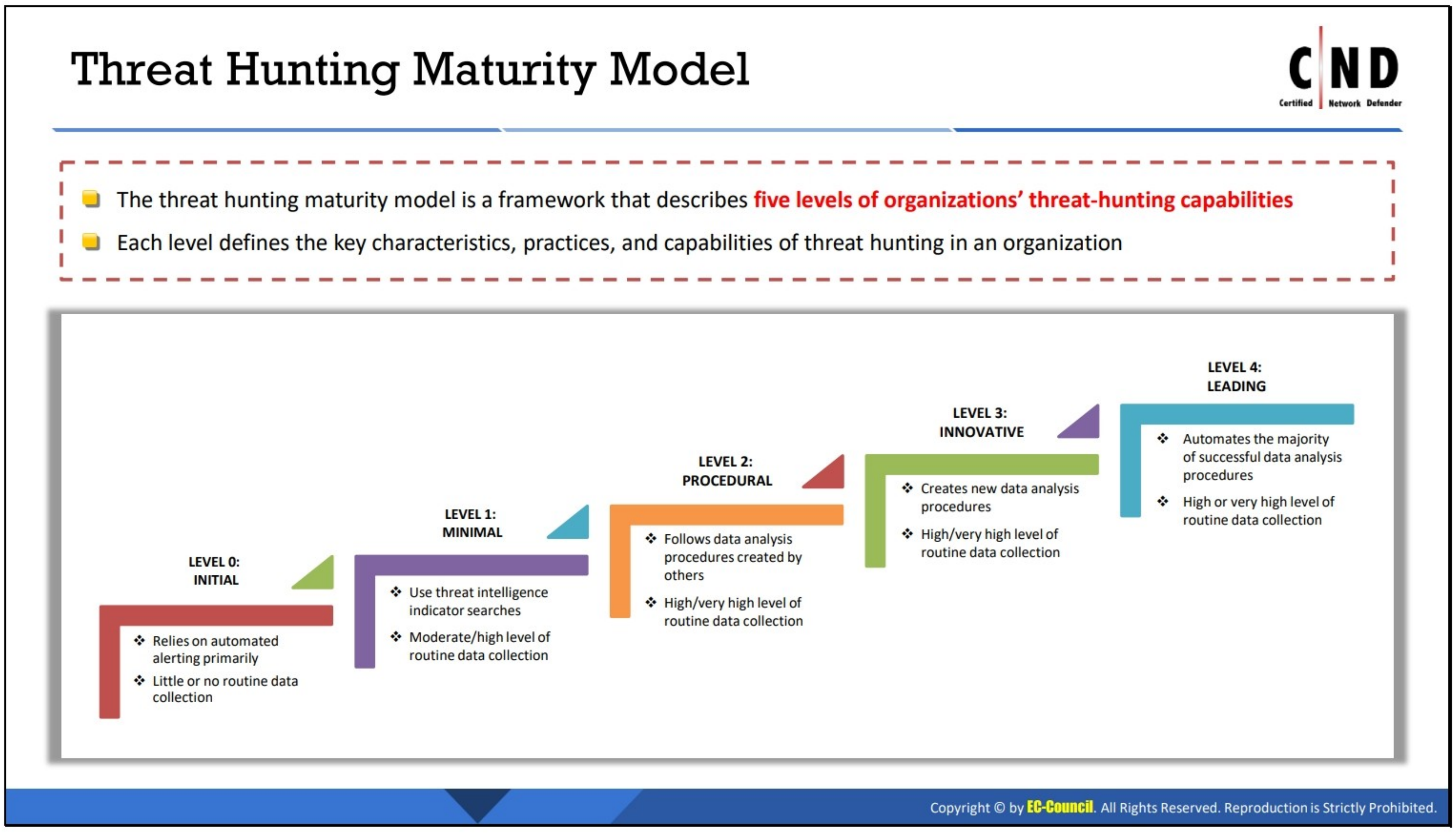


Figure 20.10: Building Blocks of Threat Hunting Maturity



Threat Hunting Maturity Model

- The threat hunting maturity model is a framework that describes **five levels of organizations' threat-hunting capabilities**
- Each level defines the key characteristics, practices, and capabilities of threat hunting in an organization

LEVEL 0: INITIAL
- Relies on automated alerting primarily
- Little or no routine data collection

LEVEL 1: MINIMAL
- Use threat intelligence indicator searches
- Moderate/high level of routine data collection

LEVEL 2: PROCEDURAL
- Follows data analysis procedures created by others
- High/very high level of routine data collection

LEVEL 3: INNOVATIVE
- Creates new data analysis procedures
- High/very high level of routine data collection

LEVEL 4: LEADING
- Automates the majority of successful data analysis procedures
- High or very high level of routine data collection

Threat Hunting Maturity Model

The threat hunting maturity model assesses an organization's ability to conduct effective cyber hunting and respond to threats. A higher level on the hunting maturity model (HMM) indicates greater capability, with HMM0 being the least capable and HMM4 representing the highest level of efficiency. The threat hunting model analyzes the following criteria:

- Data collection
- Hypotheses creation
- Tools and techniques for hypothesis testing
- Analytics automation

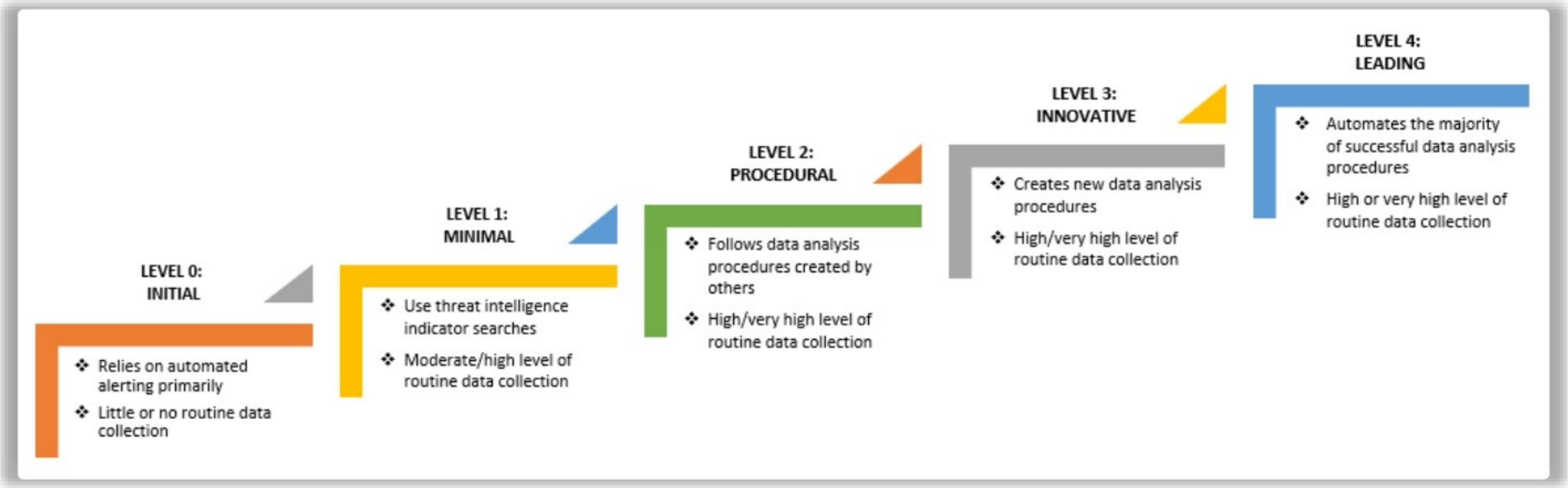

LEVEL 0: INITIAL
Relies on automated alerting primarily
Little or no routine data collection
LEVEL 1: MINIMAL
Use threat intelligence indicator searches
Moderate/high level of routine data collection
LEVEL 2: PROCEDURAL
Follows data analysis procedures created by others
High/very high level of routine data collection
LEVEL 3: INNOVATIVE
Creates new data analysis procedures
High/very high level of routine data collection
LEVEL 4: LEADING
Automates the majority of successful data analysis procedures
High or very high level of routine data collection

Figure 20.11: Levels in Threat Hunting Maturity Model

Levels in Threat Hunting Maturity Model

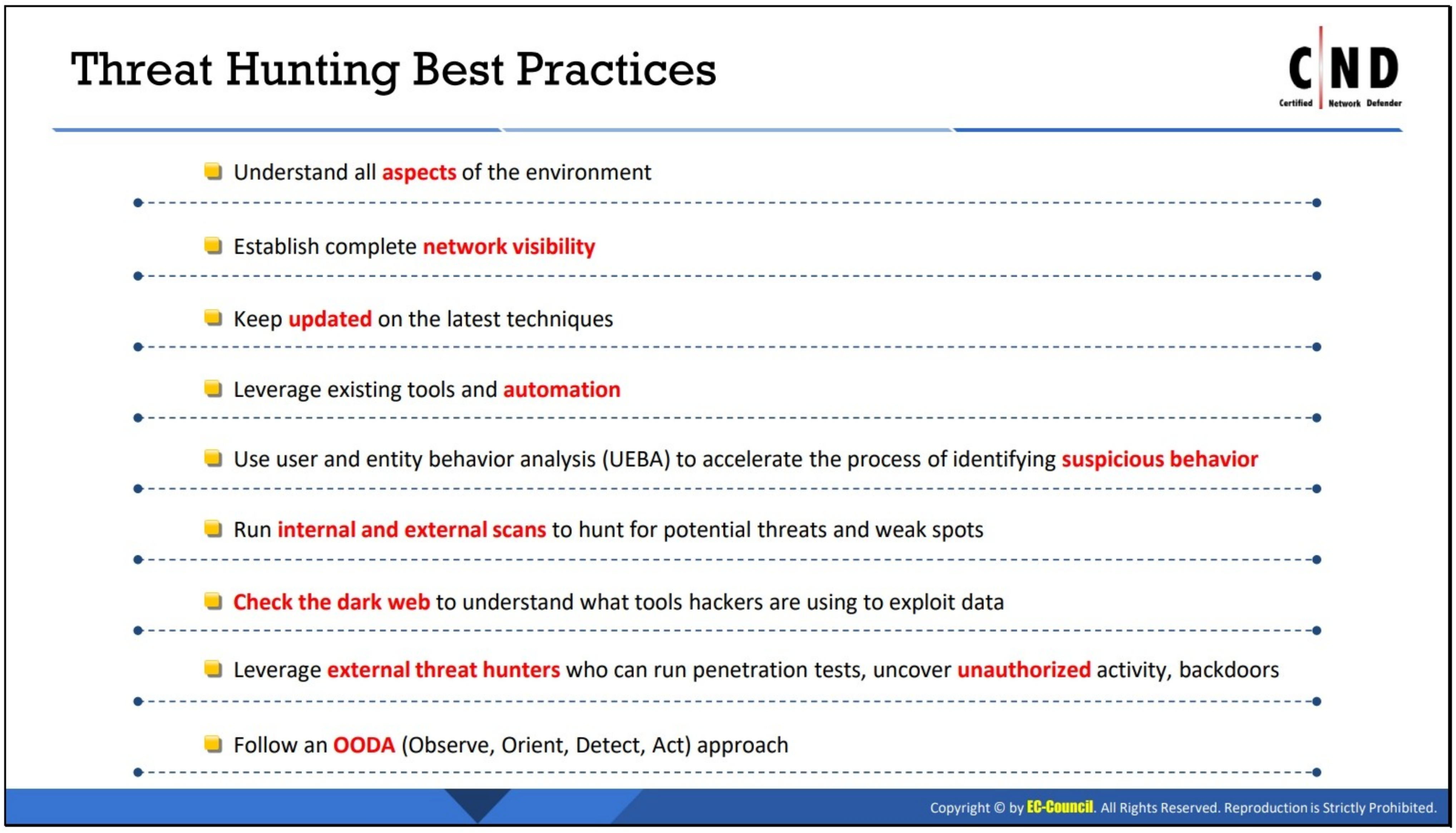
Level 0 (initial level of threat hunting maturity model): At this level, organizations do not collect data from their systems. Organizations at the HMM0 level typically rely on threat intelligence indicators and feeds from open-source services. These indicators mainly consist of data from the lower levels of the Pyramid of Pain, which includes easily changeable and less reusable information such as domains, hashes, URLs, and IP addresses. HMM0 organizations often lack substantial threat intelligence capability.

Level 1 (minimal level of threat hunting maturity model): At this level, organizations primarily rely on automated alerting to direct their incident response efforts. At this stage, there is an improvement in the visibility of the environment, primarily attributed to the collection of a variety of logs. Despite being limited, some form of threat hunting takes place. At the minimal level of the threat hunting framework, organizations strive to enhance their threat intelligence capabilities by incorporating a threat intelligence platform that enriches the individually generated indicators of compromise (IoCs).

Level 2 (procedural level of threat hunting maturity model): This is the most organizations prefer the procedural level of threat hunting maturity model. At this level, organizations use analytical and hunting processes created by others. Organizations typically collect large amounts of data from across the organization as their methods depend on least-frequency analysis.

Level 3 (innovative level of threat hunting maturity model): Organizations typically maintain at least a few threat hunters who possess a comprehensive understanding of various data analysis techniques and can utilize them to identify malicious behavior. These organizations develop and release hunting methods unlike depending on third-party procedures. Analytical capabilities can span from elementary statistics to more complex subjects such as linked data analysis, data visualization, or machine learning. These level organizations are more effective in identifying and combating adversary activity.

Level 4 (leading level of threat hunting maturity model): At the leading level, most threat hunting methods are operationalized and transformed into automatic detection. Organizations can stop and detect adversary activity. Because of the extensive automation in place, hunting teams can dedicate their efforts to the ongoing enhancement of their hunting methodologies, leading to continuous development.



Threat Hunting Best Practices

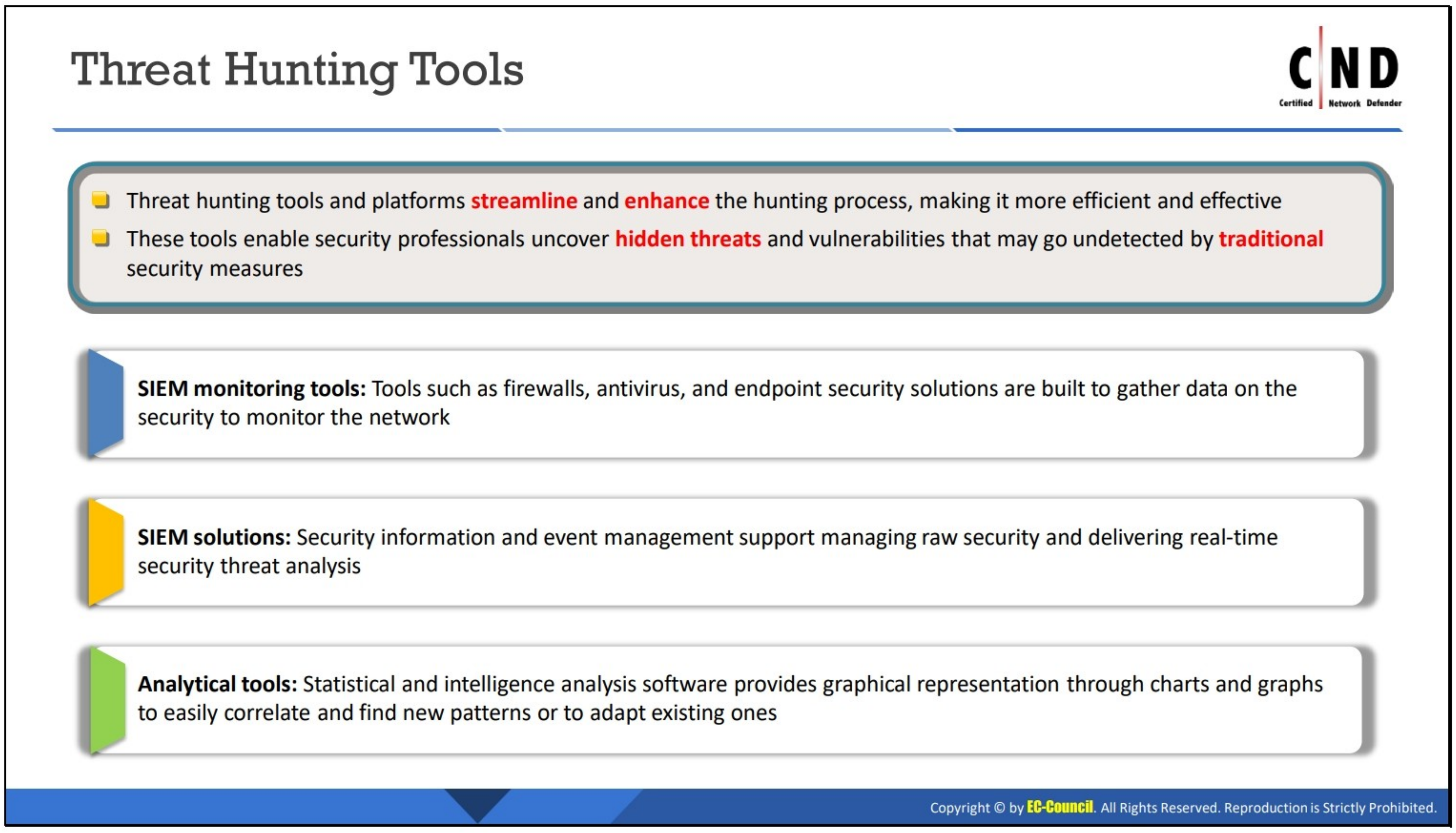
- Understand all **aspects** of the environment
- Establish complete **network visibility**
- Keep **updated** on the latest techniques
- Leverage existing tools and **automation**
- Use user and entity behavior analysis (UEBA) to accelerate the process of identifying **suspicious behavior**
- Run **internal and external scans** to hunt for potential threats and weak spots
- **Check the dark web** to understand what tools hackers are using to exploit data
- Leverage **external threat hunters** who can run penetration tests, uncover **unauthorized** activity, backdoors
- Follow an **OODA** (Observe, Orient, Detect, Act) approach

Threat Hunting Best Practices

The best practices to perform effective threat hunting are as follows:

- **Understand all aspects of the environment:** Comprehend all aspects of the environment to identify anomalies. These aspects include communication flows, user rights, and architecture. Contemporary threat hunting must uncover zero-day exploits, or attacks that transcend security boundaries, such as amalgamating account compromise with injection attacks or network breaches.
- **Establish complete network visibility:** Be aware of the organization's networks and understand the techniques of cyberattacks to repel them effectively using network monitoring and network security solutions.
- **Keeping updated on the latest techniques:** Understand the emerging techniques and continuously improve your approach toward techniques.
- **Leverage existing tools and automation:** Gain access to all the tools and processes that are in use. Use the data sets and technologies. Use the automated analytics tools that can save from manual labor. For example, use machine learning algorithms that can process more data speedily.
- **Use UEBA (User and Entity Behavior Analysis) to accelerate the process of identifying suspicious behavior**: Use user and entity behavior analysis (UEBA) solutions to keep an eye on how users, apps, and other network entities behave, examine how they interact with information and systems to spot unusual activity.

- **Run internal and external scan to hunt for potential threats and weak spots**: Run internal and external scans to know if operating systems are out of data or if devices are patched.
- **Leveraging external threat hunters who can run penetration tests, uncover unauthorized activity, and backdoors:** Organizations can benefit from external threat hunters' significant cybersecurity knowledge as this knowledge can allow to detect unauthorized activity, backdoors and trojans, and perform regular penetration tests, validate network integrity and the overall cybersecurity posture, monitor the attack surface and flag suspicious activity.
- **Checking the dark web to know what tools the hackers use to exploit data**: Regularly, monitor the dark web to check what is out there on the internet and what may be abused.
- **Follow an OODA (Observe, Orient, Detect, Act) approach:** Observe the current situations to understand their context, detect the possible threats or opportunities, and then take the relevant action against it.



Threat Hunting Tools

- Threat hunting tools and platforms **streamline** and **enhance** the hunting process, making it more efficient and effective
- These tools enable security professionals uncover **hidden threats** and vulnerabilities that may go undetected by **traditional** security measures

SIEM monitoring tools: Tools such as firewalls, antivirus, and endpoint security solutions are built to gather data on the security to monitor the network

SIEM solutions: Security information and event management support managing raw security and delivering real-time security threat analysis

Analytical tools: Statistical and intelligence analysis software provides graphical representation through charts and graphs to easily correlate and find new patterns or to adapt existing ones

Threat Hunting Tools

The types of tools that can be used in threat hunting are as follows:

- **Security Monitoring Tools**

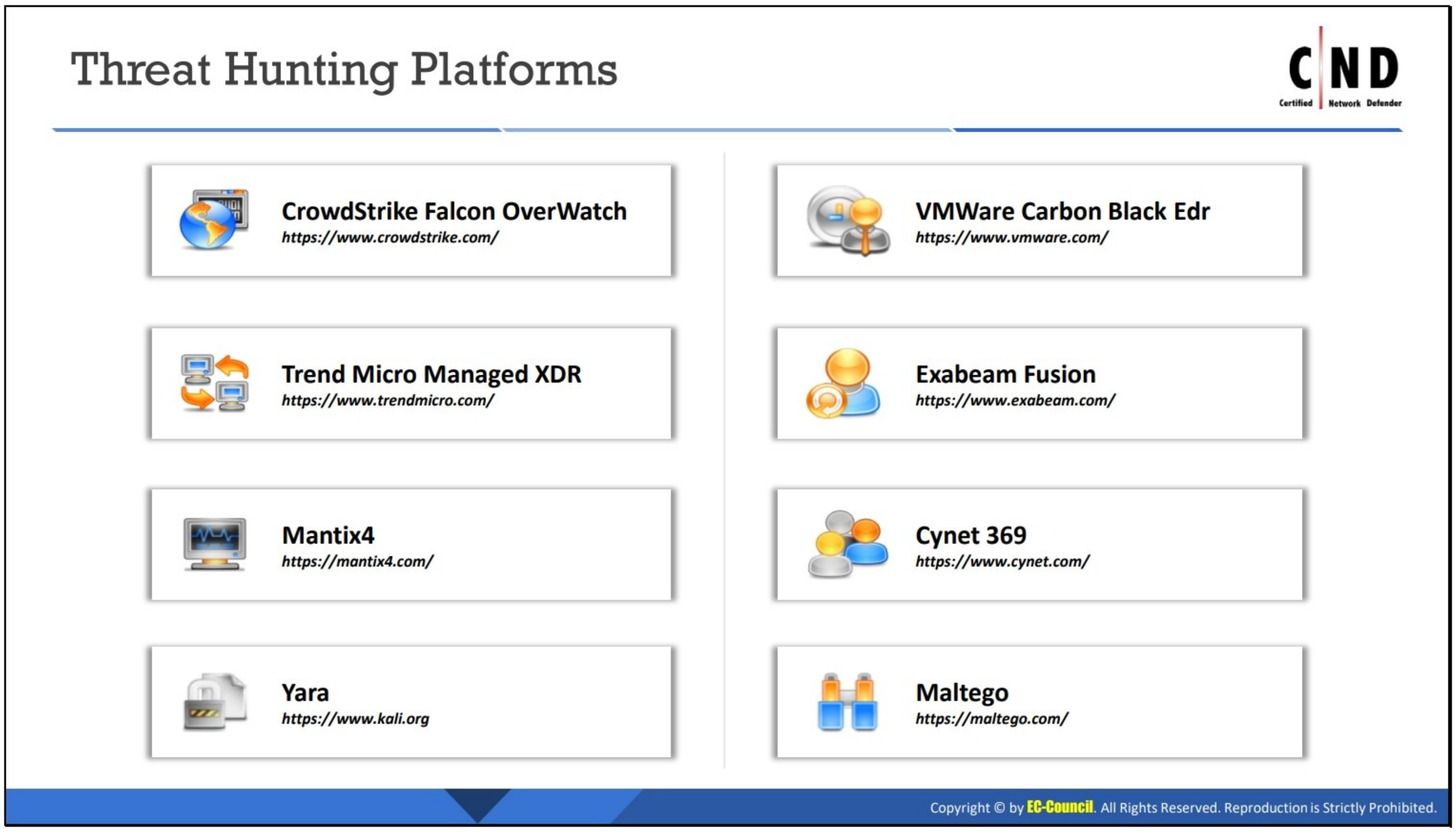
  Security monitoring tools involves collecting and analyzing the gathered information to identify any unusual behavior or changes in the administrator settings. Tools such as firewalls, antivirus and endpoint security solutions gather security data and allows monitoring the network. For example, the security monitoring tools that can used in threat hunting are SolarWinds, Nagios, Wireshark, etc.

- **SIEM Solutions**

  Security information and event management solutions enable monitoring all the activities across the network in real-time to detect any threats that could disrupt the normal functioning of the organization. For example, the SIEM Solutions that can be used in threat hunting are Security QRadar SIEM, Splunk, IBM QRadar SIEM, etc.

- **Analytics Tools**

  Use the statistical and intelligence analysis software (analytics tools) that provide a visual report through interactive charts and graphs. These help to easy correlating entities and detecting threat patterns. For example, use the analytics-driven tools such as YARA.



Threat Hunting Platforms

CND Certified Network Defender

CrowdStrike Falcon OverWatch
https://www.crowdstrike.com/

VMWare Carbon Black Edr
https://www.vmware.com/

Trend Micro Managed XDR
https://www.trendmicro.com/

Exabeam Fusion
https://www.exabeam.com/

Mantix4
https://mantix4.com/

Cynet 369
https://www.cynet.com/

Yara
https://www.kali.org

Maltego
https://maltego.com/

Threat Hunting Platforms

The threat hunting platforms are as follows:

CrowdStrike Falcon OverWatch

Source: www.crowdstrike.com

CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence on evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities—all through a single, lightweight agent. With CrowdStrike, customers benefit from superior protection, better performance, reduced complexity, and immediate time-to-value.

Trend Micro Managed XDR

Source: www.trendmicro.com

Trend Micro Managed XDR offers 24/7 analysis and monitoring. Email, endpoint, server, cloud, workload, and network sources are correlated for stronger detection and greater insight into targeted attack source and spread. It maximizes security effectiveness through a cross-layered detection and response service.

Mantix4

Source: www.mantix4.com

Mantix4's Cyber Threat Hunting Platform, originally developed by a team of defense intelligence, cybersecurity, and military experts, improves the cybersecurity team's hunt by enabling proactive defense against cyber threats. The Mantix4 platform meshes critical human intuition and analysis with advanced machine learning to analyze proactively and persistently, hunt, disrupt and neutralize the most dangerous cyber threats.

VMWare Carbon Black EDR

Source: www.vmware.com

VMware Carbon Black EDR is an incident response and threat hunting solution designed for Security Operations Center teams with offline environments or on-premises requirements. Carbon Black EDR continuously records and stores endpoint activity data so security professionals can hunt threats in real-time and visualize the complete attack kill chain, using the VMware Carbon Black Cloud's aggregated threat intelligence.

Exabeam Fusion

Source: www.exabeam.com

Exabeam Fusion represents cloud-native SIEM and New-Scale SIEM. It unites the combined capabilities of all Exabeam products such as cloud-native data storage, rapid data ingestion, hyper-quick query performance, powerful behavioral analytics, and automation that change the way analysts do their jobs.

Cynet 369

Source: www.cynet.com

Cynet 369 Threat Hunting enables you to scan endpoints on demand, according to known IoCs. As opposed to continuous file scanning that Cynet 360 performs on the host, that targets running processes, Threat Hunting can be used to discover files that have been saved on the host, even if not opened by the user.

YARA

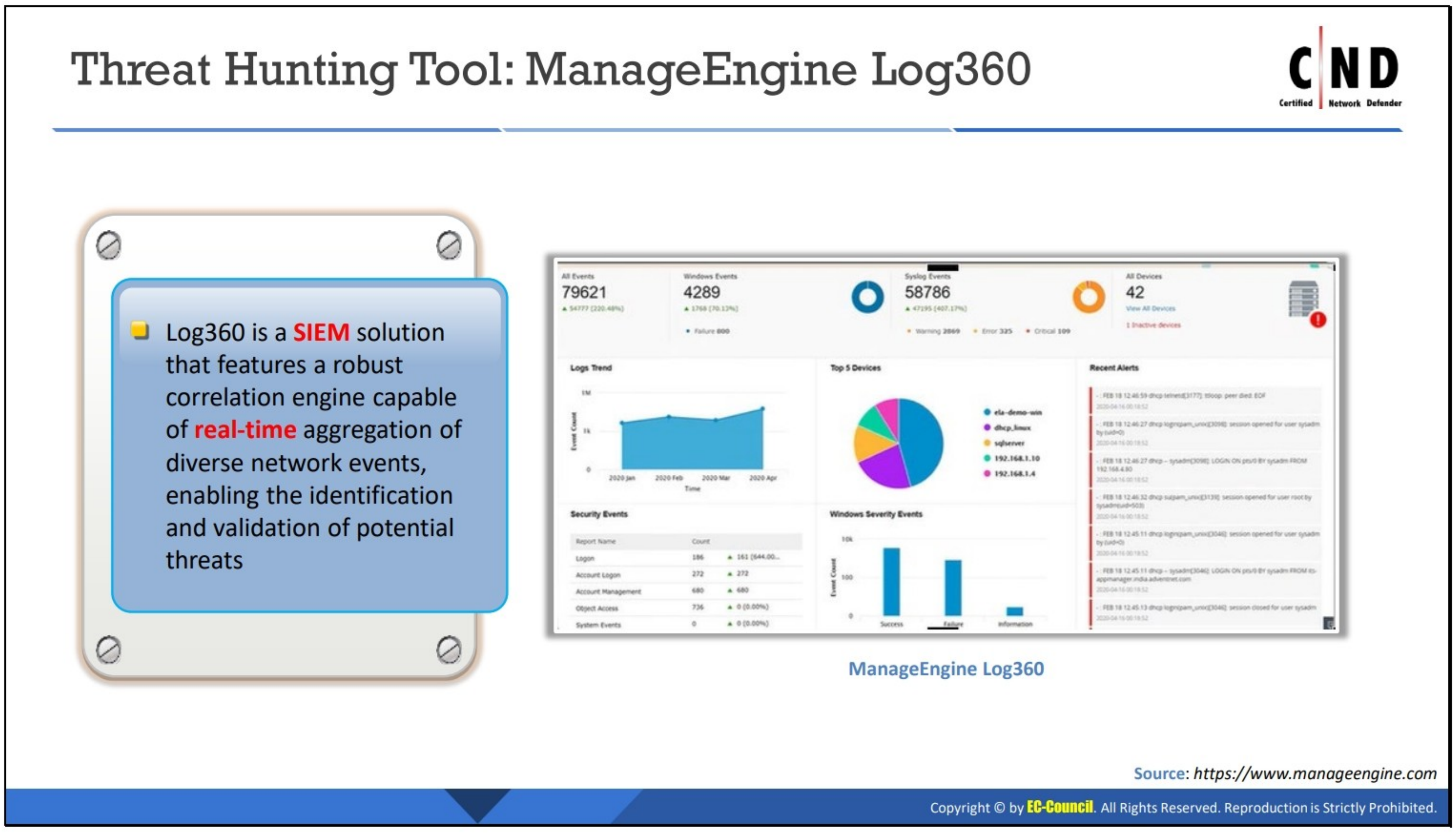
Source: *www.www.kali.org*

YARA is a tool aimed at helping malware researchers to identify and classify malware samples. With YARA. It is possible to create descriptions of malware families based on textual or binary patterns contained in samples of those families.

Maltego

Source: *www.maltego.com*

Fight fraud, abuse and insider threat with Maltego, and forget about in-house maintenance, development and deprecation risk.



Threat Hunting Tool: ManageEngine Log360

- Log360 is a **SIEM** solution that features a robust correlation engine capable of **real-time** aggregation of diverse network events, enabling the identification and validation of potential threats

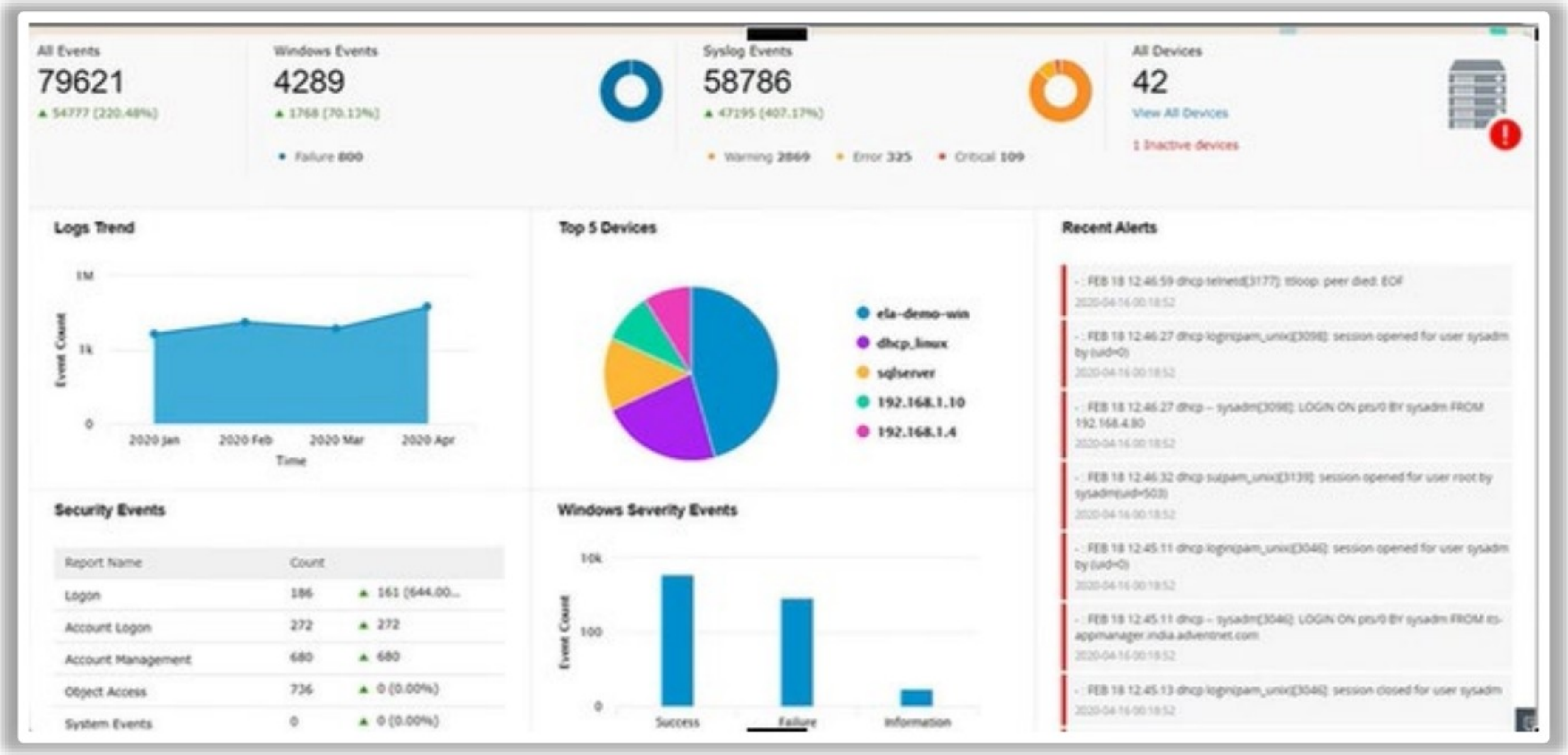
ManageEngine Log360

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

Threat Hunting Tool: ManageEngine Log360

Source: *www.managengine.com*

MangeEngine Log360 helps find malicious actors and potential hidden attacks that have slipped through initial security defenses by leveraging advanced threat analytics. It provides a high-speed, flexible, and easy-to-use search tool that lets you build queries in SQL to search through your entire log bucket in seconds. Later, it will notify when threat patterns repeat in a network.



All Events 79621 ▲ 54777 (220.48%)

Windows Events 4289 ▲ 1768 (70.13%) • Failure 800

Syslog Events 58786 ▲ 47195 (407.17%) • Warning 2869 • Error 325 • Critical 109

All Devices 42 View All Devices 1 Inactive devices

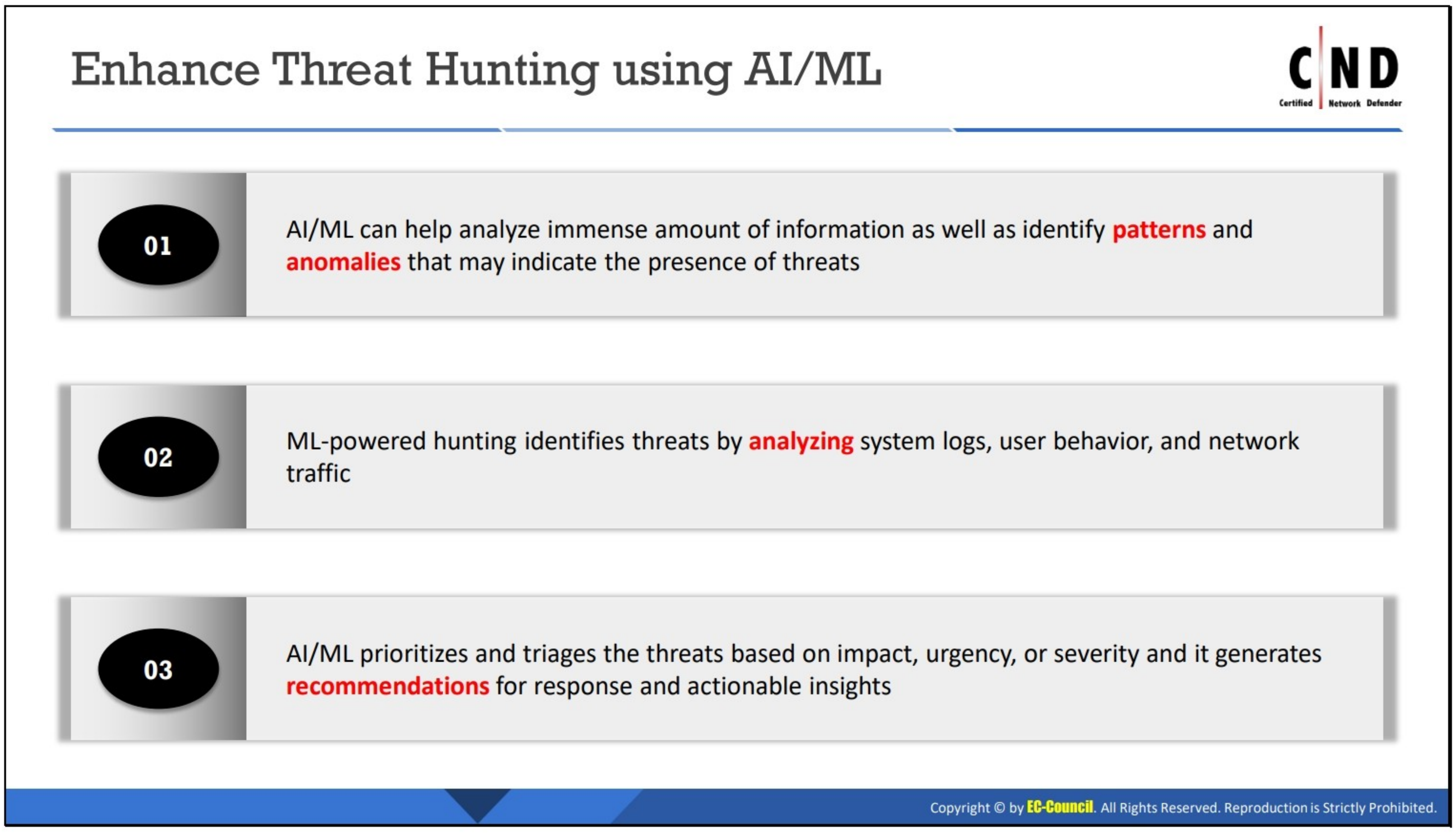
Security Events

Report Name	Count	
Logon	186	▲ 161 (644.00...
Account Logon	272	▲ 272
Account Management	680	▲ 680
Object Access	736	▲ 0 (0.00%)
System Events	0	▲ 0 (0.00%)

Recent Alerts

```
- : FEB 18 12:46:59 dhcp telnetd[3177]: ttloop: peer died: EOF
2020-04-16 00:18:52
- : FEB 18 12:46:27 dhcp login(pam_unix)[3098]: session opened for user sysadm by (uid=0)
2020-04-16 00:18:52
- : FEB 18 12:46:27 dhcp -- sysadm[3098]: LOGIN ON pts/0 BY sysadm FROM 192.168.4.80
2020-04-16 00:18:52
- : FEB 18 12:46:32 dhcp su(pam_unix)[3139]: session opened for user root by sysadm(uid=503)
2020-04-16 00:18:52
- : FEB 18 12:45:11 dhcp login(pam_unix)[3046]: session opened for user sysadm by (uid=0)
2020-04-16 00:18:52
- : FEB 18 12:45:11 dhcp -- sysadm[3046]: LOGIN ON pts/0 BY sysadm FROM its-appmanager.india.adventnet.com
2020-04-16 00:18:52
- : FEB 18 12:45:13 dhcp login(pam_unix)[3046]: session closed for user sysadm
2020-04-16 00:18:52
```

Figure 20.12: Threat Hunting using ManageEngine Log360



Enhance Threat Hunting using AI/ML

01 AI/ML can help analyze immense amount of information as well as identify **patterns** and **anomalies** that may indicate the presence of threats

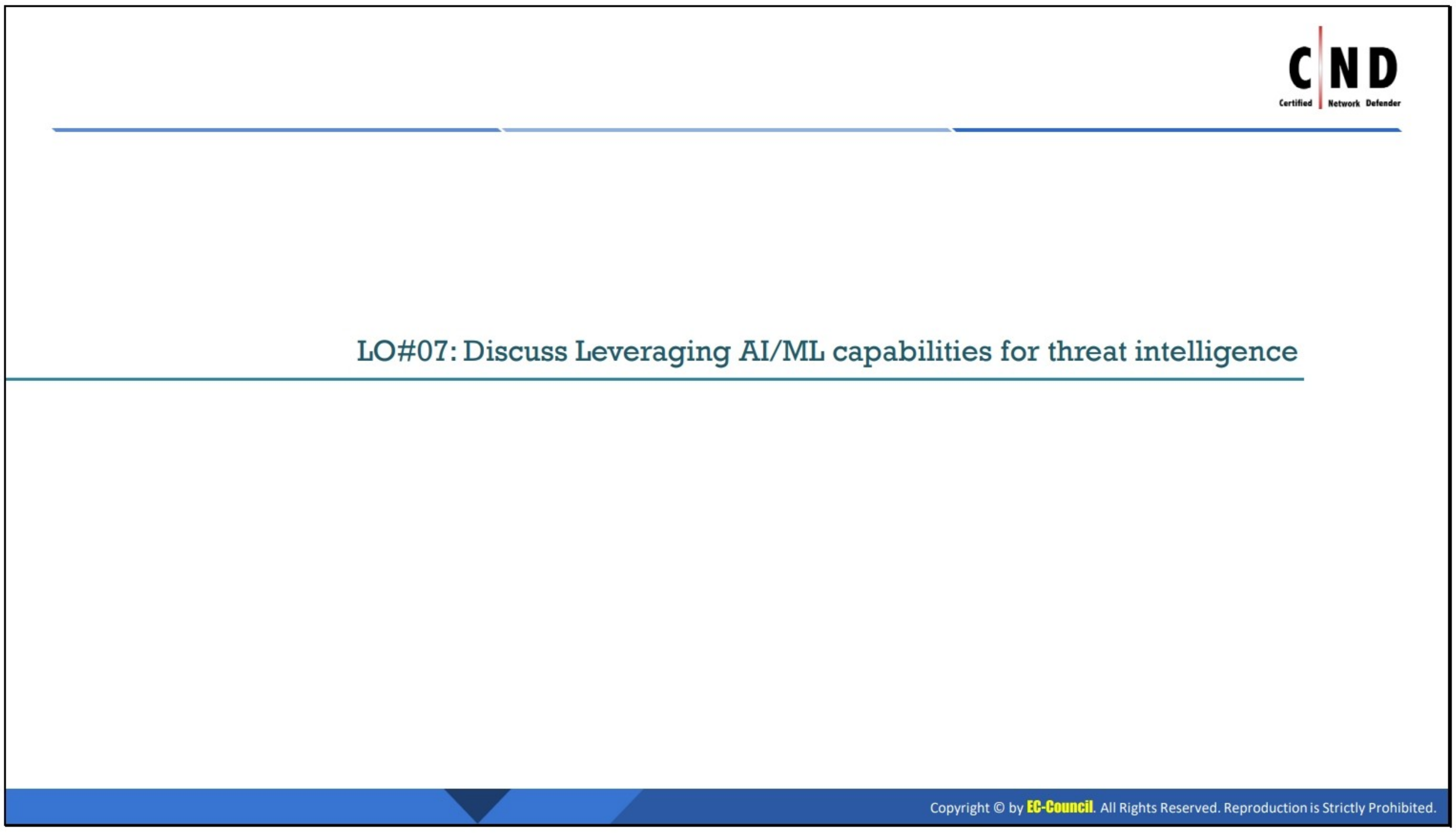
02 ML-powered hunting identifies threats by **analyzing** system logs, user behavior, and network traffic

03 AI/ML prioritizes and triages the threats based on impact, urgency, or severity and it generates **recommendations** for response and actionable insights

Enhance Threat Hunting using AI/ML

The methods to enhance threat hunting using AI/ML are as follows:

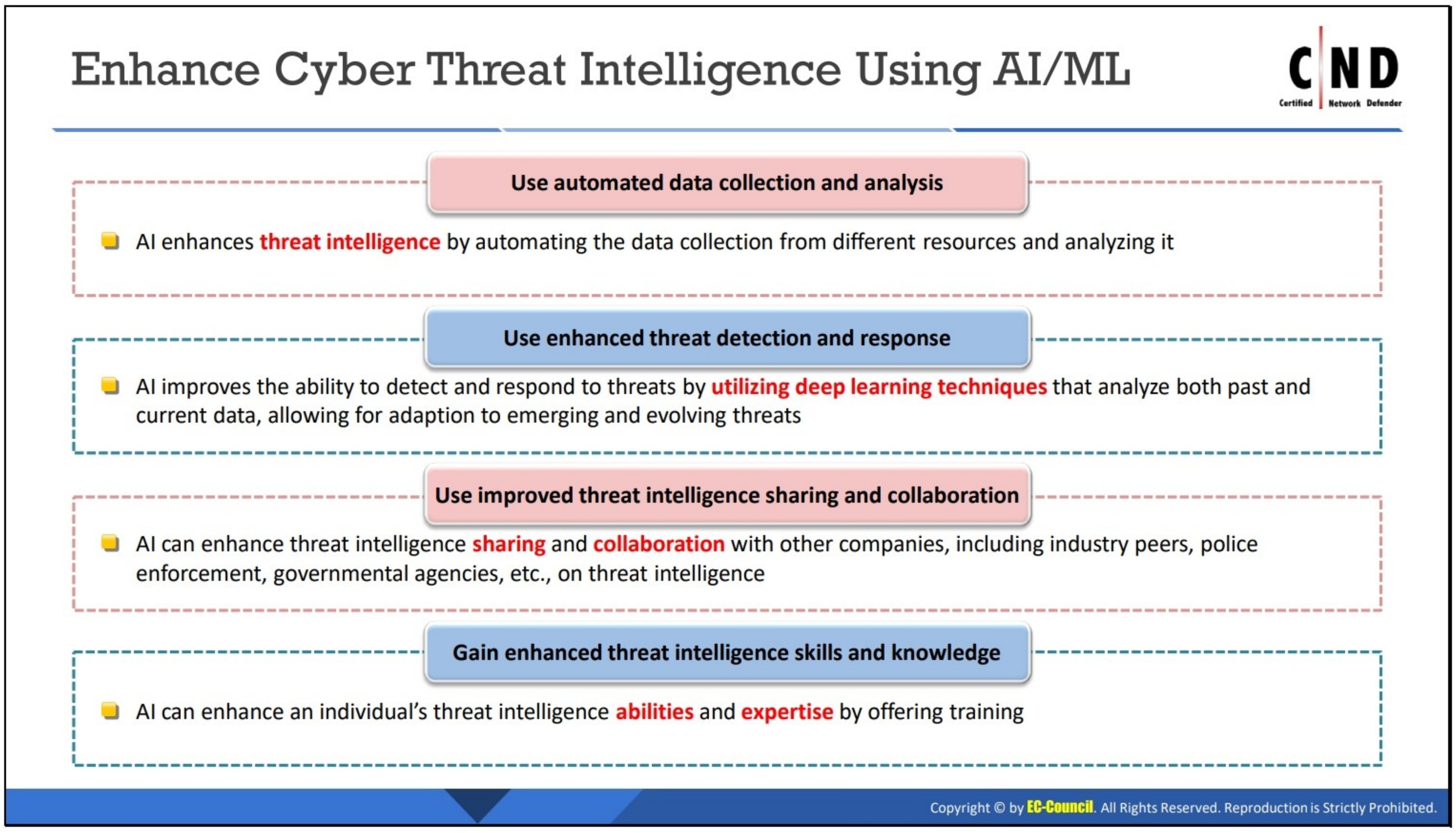
- AI and ML, through techniques such as anomaly detection, pattern recognition, natural language processing, and behavioral analysis, can assist in automating and optimizing the threat identification and analysis procedures.
- By using ML techniques, find and categorize malicious activities, events, or IoCs that differ from usual behavior. They can also extract and correlate pertinent data from a variety of sources, including threat intelligence feeds, logs, user behaviors, traffic, and alerts.
- Automate threat hunting using AI and ML to produce meaningful insights and response suggestions by prioritizing and triaging threats according to their severity, impact, or urgency.



LO#07: Discuss Leveraging AI/ML capabilities for threat intelligence

LO#07: Discuss Leveraging AI/ML Capabilities for Threat Intelligence

In the dynamic landscape of cybersecurity, the integration of Artificial Intelligence (AI) and Machine Learning (ML) has become pivotal in fortifying threat intelligence practices. This section explores the transformative impact of AI/ML capabilities on threat intelligence, highlighting their role in enrichment of IoCs, phishing detection and application of AI to threat intelligence.



Enhance Cyber Threat Intelligence Using AI/ML

Use automated data collection and analysis

- AI enhances **threat intelligence** by automating the data collection from different resources and analyzing it

Use enhanced threat detection and response

- AI improves the ability to detect and respond to threats by **utilizing deep learning techniques** that analyze both past and current data, allowing for adaption to emerging and evolving threats

Use improved threat intelligence sharing and collaboration

- AI can enhance threat intelligence **sharing** and **collaboration** with other companies, including industry peers, police enforcement, governmental agencies, etc., on threat intelligence

Gain enhanced threat intelligence skills and knowledge

- AI can enhance an individual's threat intelligence **abilities** and **expertise** by offering training

Enhance Cyber Threat Intelligence Using AI/ML

Use the below capabilities of AI/ML to enhance an organization's cyber threat intelligence.

- **Use Automated Data Collection and Analysis**

  AI can enhance data collection and analysis by automating it. Collect and analyze a lot of data from a variety of sources, including network logs, security alerts, open-source intelligence, etc. AI also can extract pertinent IoCs such as IP addresses, domain names, hashes, etc., by removing unimportant data. This can save time and resources, and provide actionable insights.

- **Use Enhanced Threat Detection and Response**

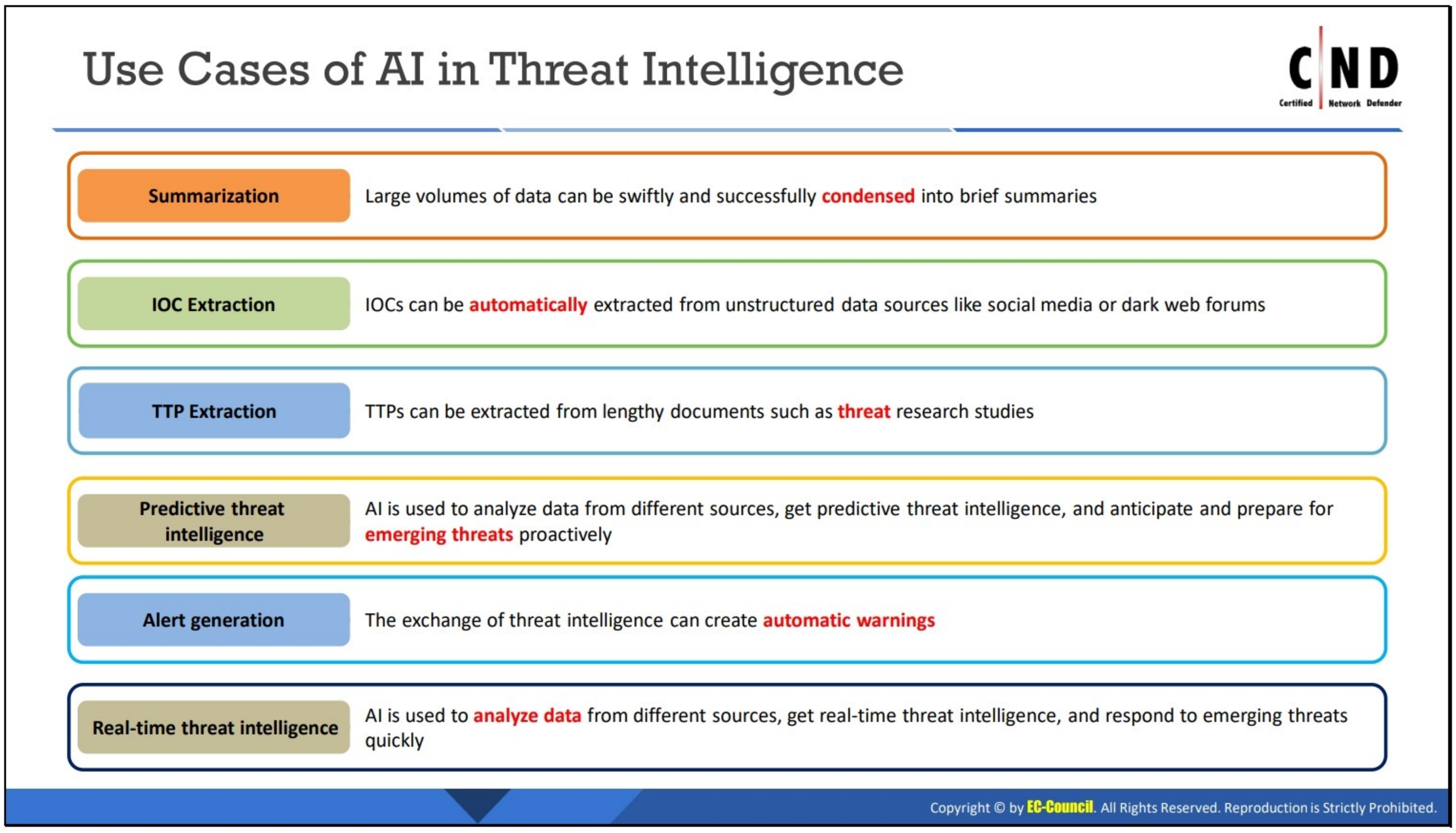
  AI can enhance threat detection and response by employing machine learning and deep learning techniques that learn from past and current data and adapt to new and developing threats. AI can assist in prioritizing the most critical dangers and offer suggestions and instructions on how to neutralize them.

- **Use Improved Threat Intelligence Sharing and Collaboration**

  AI can enhance threat intelligence sharing and collaboration with other companies, including industry peers, police enforcement, governmental agencies, etc., on threat intelligence. By cross-referencing and validating the threat intelligence data with other sources and databases, AI can also aid in its enrichment and validation.

- **Gain Enhanced Threat Intelligence Skills and Knowledge**

  AI can assist in improving threat intelligence abilities and expertise by offering training and educational tools like courses, tutorials, webinars, podcasts, etc. By giving feedback and ideas on how to enhance threat intelligence processes and practices, AI may also help to learn from own and other people's experiences.



Use Cases of AI in Threat Intelligence

Summarization	Large volumes of data can be swiftly and successfully **condensed** into brief summaries
IOC Extraction	IOCs can be **automatically** extracted from unstructured data sources like social media or dark web forums
TTP Extraction	TTPs can be extracted from lengthy documents such as **threat** research studies
Predictive threat intelligence	AI is used to analyze data from different sources, get predictive threat intelligence, and anticipate and prepare for **emerging threats** proactively
Alert generation	The exchange of threat intelligence can create **automatic warnings**
Real-time threat intelligence	AI is used to **analyze data** from different sources, get real-time threat intelligence, and respond to emerging threats quickly

Use Cases of AI in Threat Intelligence

The use cases of AI in threat intelligence are as follows:

- **Summarization**

  Large volumes of data can be swiftly and successfully condensed into summaries using natural language processing (NLP) models, with LLMs serving as a notable example. This makes it simpler for security analysts to take in and comprehend threat information and transform it into useful insight.

- **IOC Extraction**

  IOCs can be automatically extracted by AI-driven solutions from unstructured data sources like social media or dark web forums, which helps speed up the identification of possible threats.

- **TTP Extraction**

  TTPs can be extracted from lengthy documents like threat research studies, which enables enterprises to better comprehend and protect against certain adversary behaviors.

- **Predictive Intelligence**

  Organizations may proactively adjust their security posture by using artificial intelligence models to assess past threat data and forecast future trends.

- **Alert Generation**

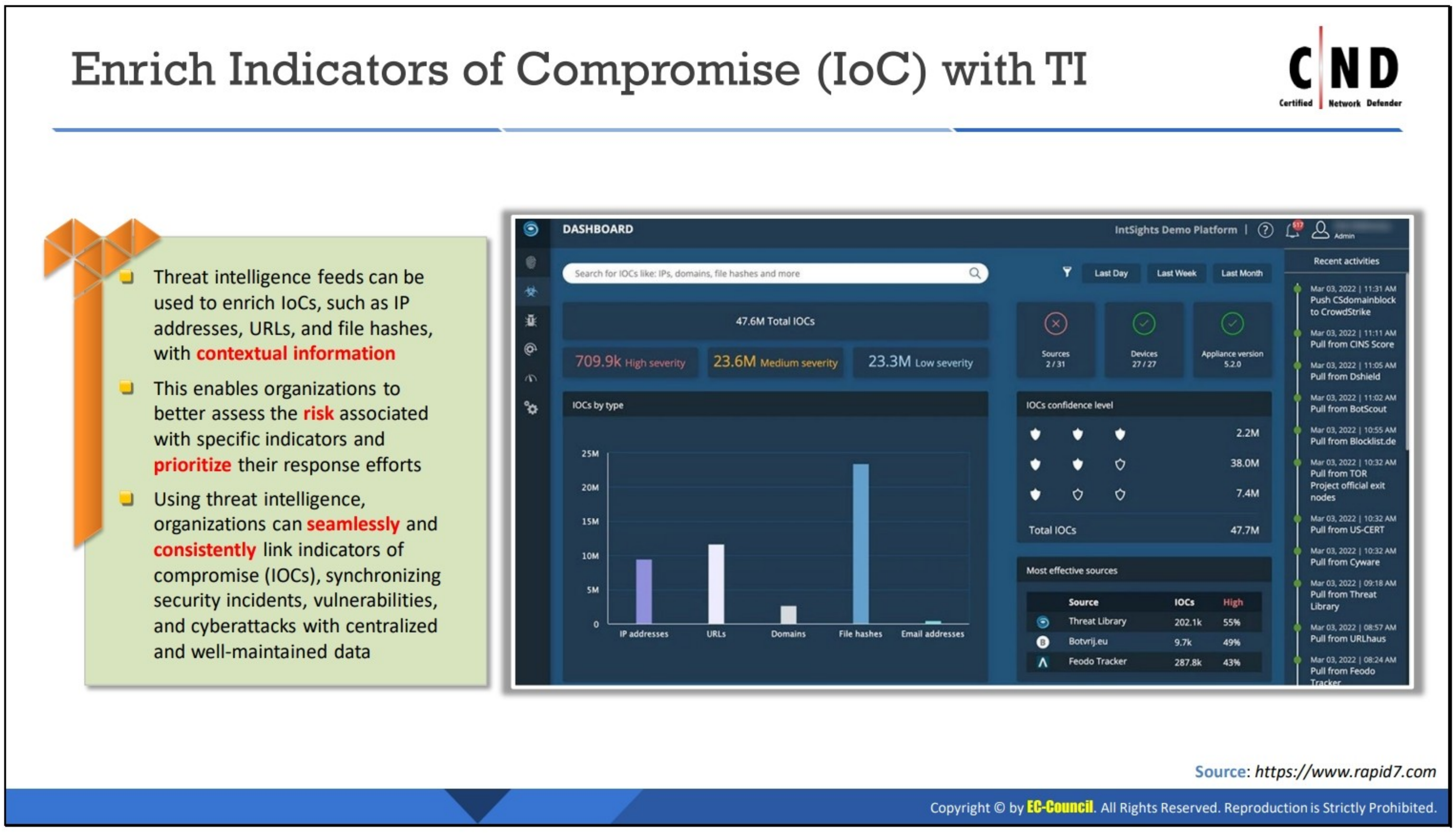
The exchange of threat intelligence and the communication of risk for security teams may be streamlined by LLMs, which can automatically create warnings or reports depending on risks discovered.

- **Enhanced Decision Making**

  Insights and suggestions from AI models can help firms better prioritize and distribute resources by enhancing decision-making linked to cyber threat intelligence.

- **Real-time Threat Intelligence**

  AI is used to analyze data from different sources, get real-time threat intelligence, and respond to emerging threats quickly.



Enrich Indicators of Compromise (IoC) with TI

- Threat intelligence feeds can be used to enrich IoCs, such as IP addresses, URLs, and file hashes, with **contextual information**
- This enables organizations to better assess the **risk** associated with specific indicators and **prioritize** their response efforts
- Using threat intelligence, organizations can **seamlessly** and **consistently** link indicators of compromise (IOCs), synchronizing security incidents, vulnerabilities, and cyberattacks with centralized and well-maintained data

DASHBOARD
IntSights Demo Platform | Admin
Search for IOCs like: IPs, domains, file hashes and more
Last Day | Last Week | Last Month
47.6M Total IOCs
709.9k High severity | 23.6M Medium severity | 23.3M Low severity
Sources 2 / 31 | Devices 27 / 27 | Appliance version 5.2.0

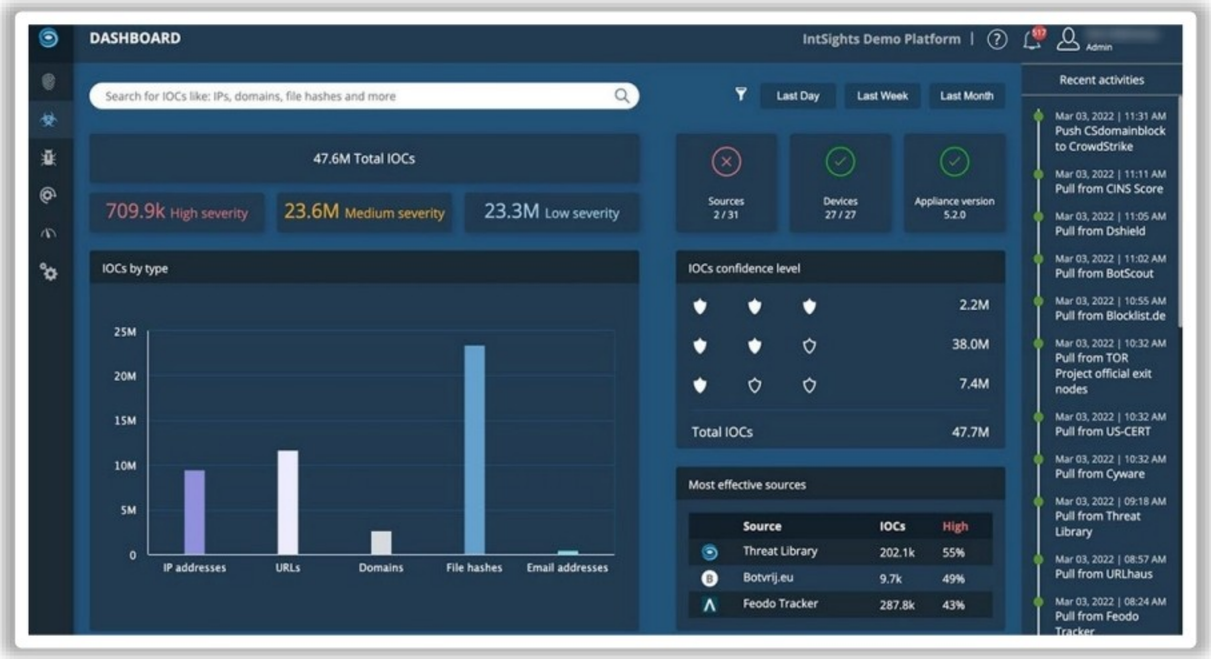
Source: *https://www.rapid7.com*

Enrich Indicators of Compromise (IoCs) with TI

Use the threat intelligence feeds to enhance the IoCs in the organization, such as IP address, domain names, file hashes etc. This makes the organization more accurately evaluate potential risks and allows it to prioritize the risk based on the level of impact on critical resources of the organization to respond efficiently.

Threat hunting also allows the organization to correlate the IoCs to comprehensively understand and synchronize various incidents, and vulnerabilities to eliminate them. This approach makes the data resources centralized and will have a clear view of the network.

Threat hunting mechanism brings in the ability to structure the IoCs to make the defense system robust and instantly implement preventive measures to safeguard the assets by blocking indicators on the firewall and EDR.



DASHBOARD

IntSights Demo Platform | Admin

Search for IOCs like: IPs, domains, file hashes and more

Last Day | Last Week | Last Month

47.6M Total IOCs

709.9k High severity | 23.6M Medium severity | 23.3M Low severity

Sources 2 / 31 | Devices 27 / 27 | Appliance version 5.2.0

IOCs by type

IOCs confidence level

●●●	2.2M
●●○	38.0M
●○○	7.4M
Total IOCs	47.7M

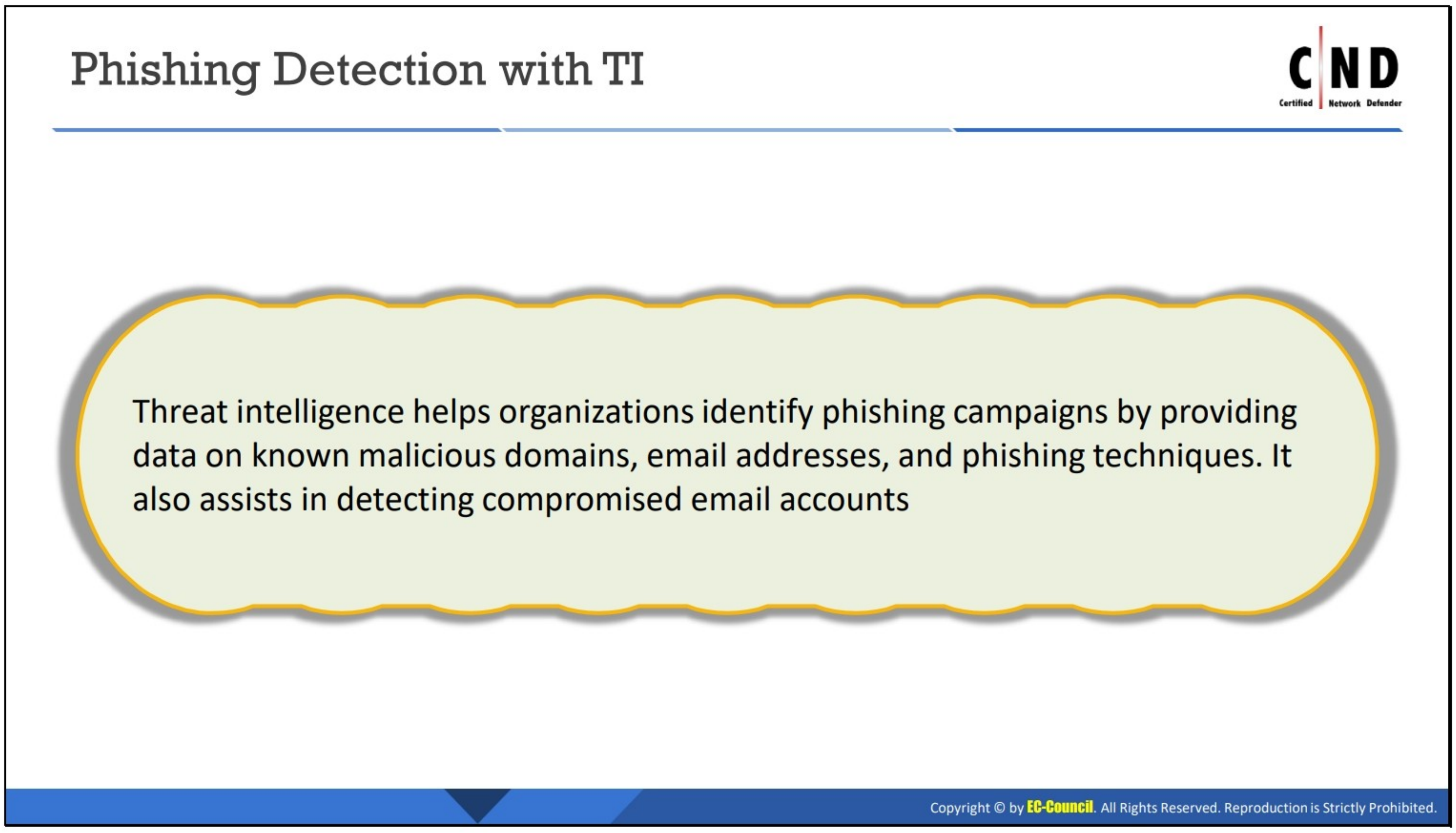
Most effective sources

Source	IOCs	High
Threat Library	202.1k	55%
Botvrij.eu	9.7k	49%
Feodo Tracker	287.8k	43%

Recent activities

- Mar 03, 2022 \| 11:31 AM Push CSdomainblock to CrowdStrike
- Mar 03, 2022 \| 11:11 AM Pull from CINS Score
- Mar 03, 2022 \| 11:05 AM Pull from Dshield
- Mar 03, 2022 \| 11:02 AM Pull from BotScout
- Mar 03, 2022 \| 10:55 AM Pull from Blocklist.de
- Mar 03, 2022 \| 10:32 AM Pull from TOR Project official exit nodes
- Mar 03, 2022 \| 10:32 AM Pull from US-CERT
- Mar 03, 2022 \| 10:32 AM Pull from Cyware
- Mar 03, 2022 \| 09:18 AM Pull from Threat Library
- Mar 03, 2022 \| 08:57 AM Pull from URLhaus
- Mar 03, 2022 \| 08:24 AM Pull from Feodo Tracker

Figure 20.13: Rapid7’s IntSights Demo Platform’s Dashboard



Phishing Detection with TI

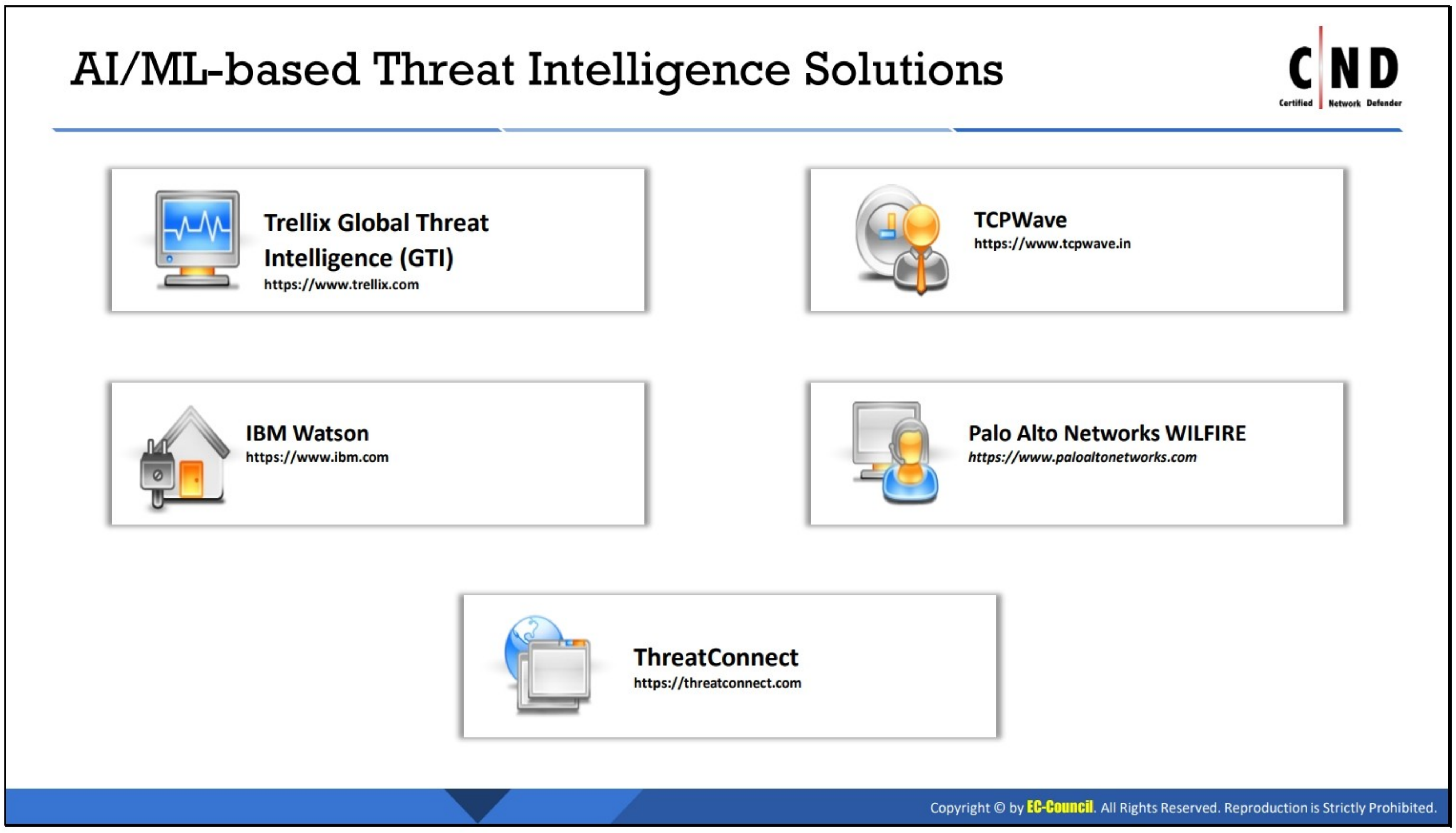
Threat intelligence helps organizations identify phishing campaigns by providing data on known malicious domains, email addresses, and phishing techniques. It also assists in detecting compromised email accounts

Phishing Detection with TI

Threat intelligence helps organizations identify phishing campaigns by providing data on known malicious domains, email addresses, and phishing techniques. It also assists in detecting compromised email accounts.

The approaches in which phishing attacks can be detected using threat Intelligence are as follows:

- **Use automated processes:** Use threat intelligence tools to automate processes and free up team members from manual efforts for finding phishing threats.
- **Use proactive preventive tools:** Use proactive preventive approach for phishing threats by utilizing threat intelligence software tools.
- **Use AI analyses:** Use AI tools to utilize artificial intelligence to get detailed analyses of phishing threats.



AI/ML-based Threat Intelligence Solutions

Trellix Global Threat Intelligence (GTI)
https://www.trellix.com

TCPWave
https://www.tcpwave.in

IBM Watson
https://www.ibm.com

Palo Alto Networks WILFIRE
https://www.paloaltonetworks.com

ThreatConnect
https://threatconnect.com

AI/ML-based Threat Intelligence Solutions

Trellix Global Threat Intelligence (GTI)

Source: https://www.trellix.com

Global Threat Intelligence (GTI) is a comprehensive, real-time, cloud-based reputation service, fully integrated into Trellix products that protects organizations and their users from both known and emerging cyber threats, regardless of the source of those threats or where they propagate.

IBM Watson

Source: https://www.ibm.com

IBM Watson for cybersecurity offers an advanced type of artificial intelligence, leveraging various forms of AI, including machine learning algorithms and deep learning networks, that get stronger and smarter over time.

TCPWave

Source: https://www.tcpwave.in

TCPWave, utilizing AI-driven threat intelligence analysis, constantly scans real-time threat intelligence feeds, identifying potential dangers as they surface. Using deep learning algorithms, TCPWave's system efficiently differentiates between benign and malicious activities, allowing organizations to act pre-emptively. This default-built anomaly-detection process not only enhances the real-time response to impending threats but also fosters a resilient cybersecurity posture for modern organizations.

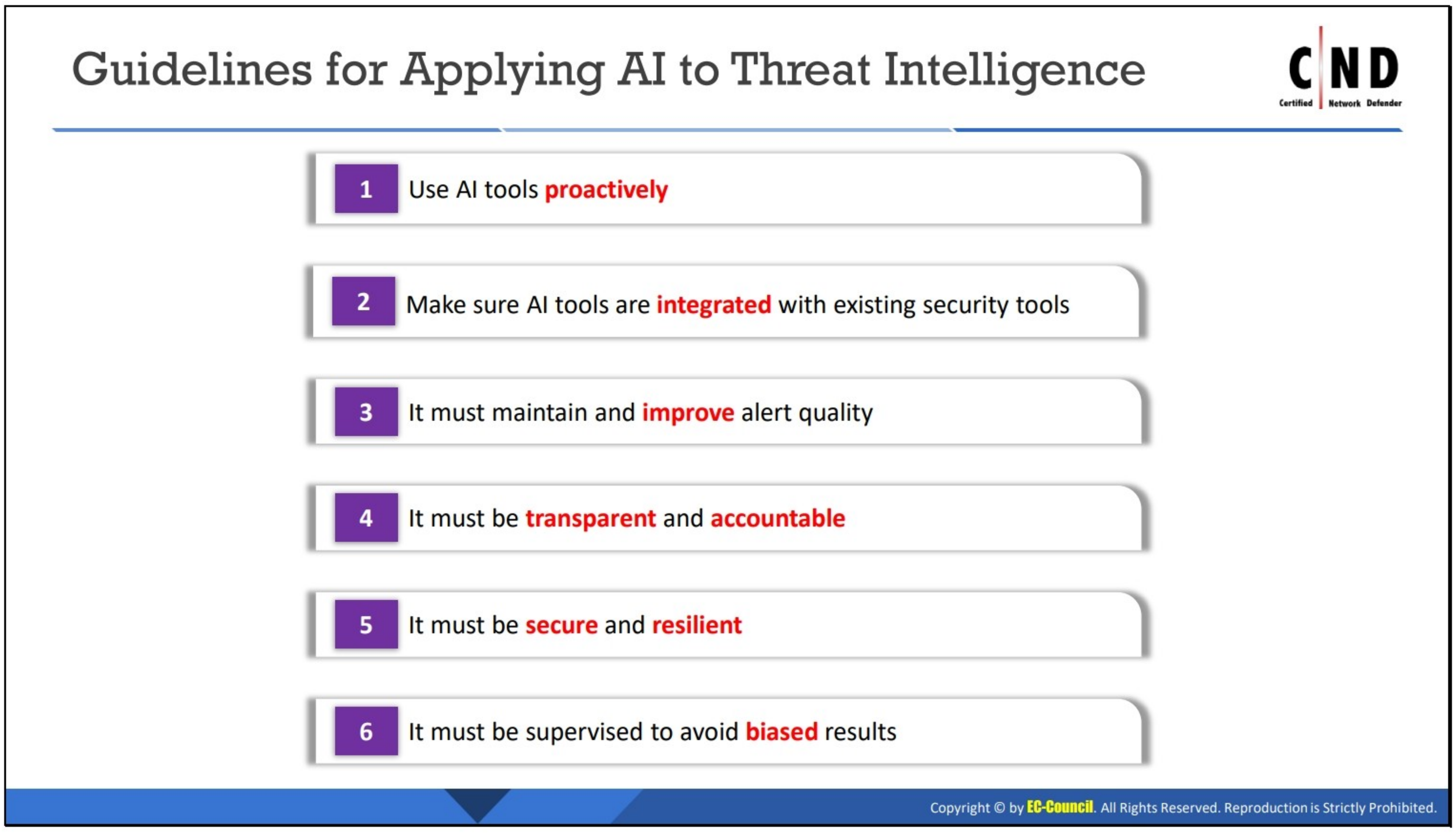
Palo Alto Networks WILFIRE

Source: https://www.paloaltonetworks.com
Palo Alto Networks WILFIRE ensures the files are safe by automatically preventing unknown malware variants and recieve protections 60X faster with the industry's largest threat intelligence and malware prevention engine.

ThreatConnect

Source: https://threatconnect.com

ThreatConnect TIP is a single platform that centralizes the aggregation and management of all the threat data that is relevant to the security program. It normalizes data, enriches it with additional context, and automates manual threat intelligence-related security processes, providing a full view of the current threat landscape. The ThreatConnect TIP informs the security center operations (SOC) team about known cyber threats, such as malware. Threat intelligence software also allows the cybersecurity team to identify, investigate, and respond to threats efficiently and accurately.



Guidelines for Applying AI to Threat Intelligence

1. Use AI tools **proactively**
2. Make sure AI tools are **integrated** with existing security tools
3. It must maintain and **improve** alert quality
4. It must be **transparent** and **accountable**
5. It must be **secure** and **resilient**
6. It must be supervised to avoid **biased** results

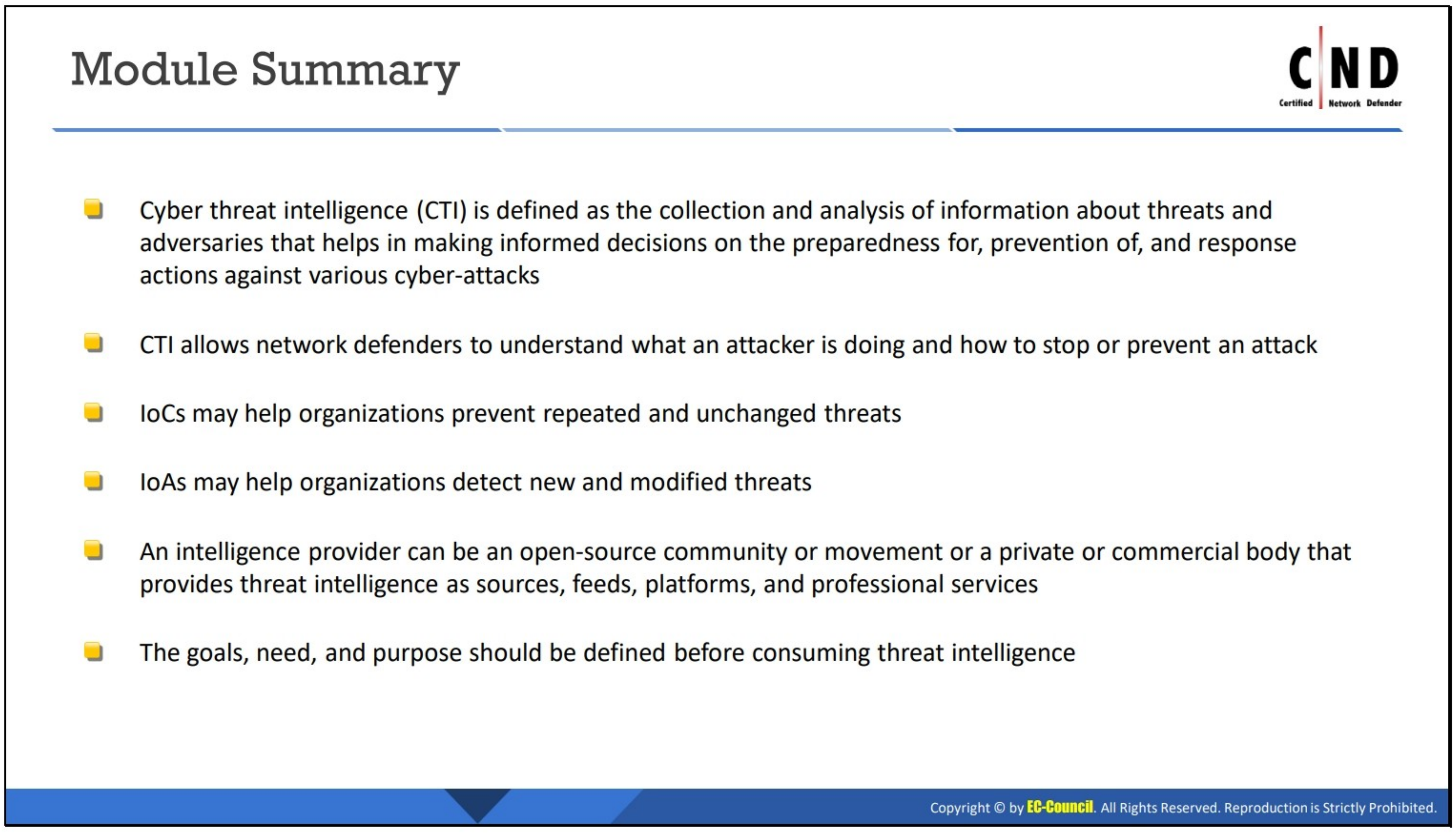
Guidelines for Applying AI to Threat Intelligence

The following are some of the guidelines to effectively apply AI to enhance threat intelligence

- **Use AI tools Proactively:** Threat intelligence acts as a guide to identify vulnerabilities and exploits in the environment. Threat intelligence supports categorizing risky behaviors and events, guiding early detection and better response. It is especially helpful when included in automated response processes because it aids in attack flow prediction and countermeasure prescription. Another way to make sure you identify and respond to attacks as quickly as possible is through automated response.
  - The threat vectors are acknowledged by the deployment of security tools.
  - It is determined to restrict access controls and permissions to prevent previously known attacks.
  - Security updates that need to be patched and applied to vulnerable systems.
- **Make sure AI tools are integrated with existing security tools:** Threat intelligence works best when integrated with other security technologies because it is less effective when used alone. Automated security systems should incorporate threat intelligence, and users should use it to improve the ability of tools to recognize suspicious and malicious activities and events.
- With the use of proactive alerting, prioritizing, and the addition of contextual data for alerts that support investigation, threat intelligence is frequently combined and integrated with SIEM. Threat intelligence data can also be used for many other security systems, including web application firewalls (WAF), next-generation firewalls (NGFW), and endpoint security solutions.

- **It must maintain and improve alert quality:** It occurs when security teams are overwhelmed by the volume or poor quality of warnings, making it impossible for them to review and respond to every alarm. Security analysts frequently end up rejecting signals when there are too many false positives or when they need significant inquiry to understand by comparing data in the alert with threat intelligence feeds and databases, AI aids in the categorization and prioritization of alerts as well as the elimination of false positives. This can prevent alert fatigue and guarantee that security teams never miss crucial notifications, ensuring that higher-priority issues are resolved first.
- **It must be transparent and accountable:** Transparency is the ability to understand information about AI systems and know what data is generated by AI rather than the data that is generated by humans.

  Accountability is determined as a shared responsibility between the vendors and creators to use AI for a certain purpose and those who have developed AI in the environment are accountable.
- **It must be secure and resilient:** In an organization, the security of the physical assets, technologies and sensitive information should be prioritized. This can be assured by implementing the CIA triad (confidentiality, integrity, and availability) based on the organization's priority level. Resilience in AI is defined as the tolerance that tools can take to withstand unforeseen disasters and cyberattacks that could bring organizations potentially down and the time taken to recover from them.
- **It must be supervised to avoid biased results:** Artificial intelligence models may reflect biases in the results that are generated. This data cannot be considered for vital analytical operations. This can be mitigated by improving diversity, mitigating diversity deficits, and using supervised learning algorithms and general awareness tools.



Module Summary

- Cyber threat intelligence (CTI) is defined as the collection and analysis of information about threats and adversaries that helps in making informed decisions on the preparedness for, prevention of, and response actions against various cyber-attacks
- CTI allows network defenders to understand what an attacker is doing and how to stop or prevent an attack
- IoCs may help organizations prevent repeated and unchanged threats
- IoAs may help organizations detect new and modified threats
- An intelligence provider can be an open-source community or movement or a private or commercial body that provides threat intelligence as sources, feeds, platforms, and professional services
- The goals, need, and purpose should be defined before consuming threat intelligence

Module Summary

This module focused on threat predictions with cyber threat intelligence (CTI). The module discussed the role of CTI in network defense, types of threat intelligence, and indicators of compromise (IoCs) and indicators of attack (IoAs). The following are the key points discussed in this module:

- CTI is defined as the collection and analysis of information about threats and adversaries that helps in making informed decisions on the preparedness for, prevention of, and response actions against various cyber-attacks.
- CTI allows network defenders to understand what an attacker is doing and how to stop or prevent an attack.
- IoCs may help organizations prevent repeated and unchanged threats.
- IoAs may help organizations detect new and modified threats.
- An intelligence provider can be an open-source community or movement or a private or commercial body that provides threat intelligence as sources, feeds, platforms, and professional services.
- The goals, need, and purpose should be defined before consuming threat intelligence.

This page is intentionally left blank.