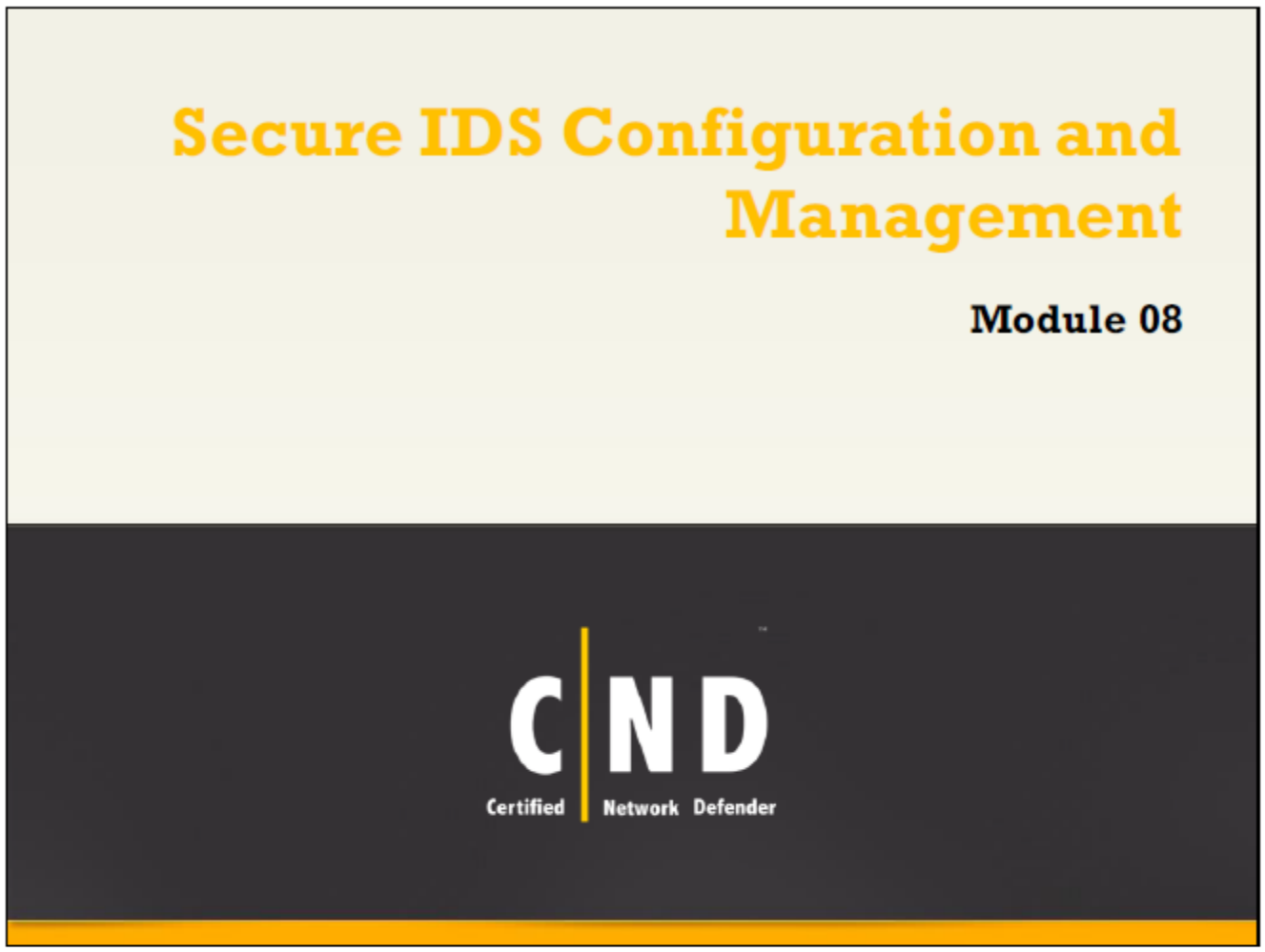
Secure IDS Configuration and Management

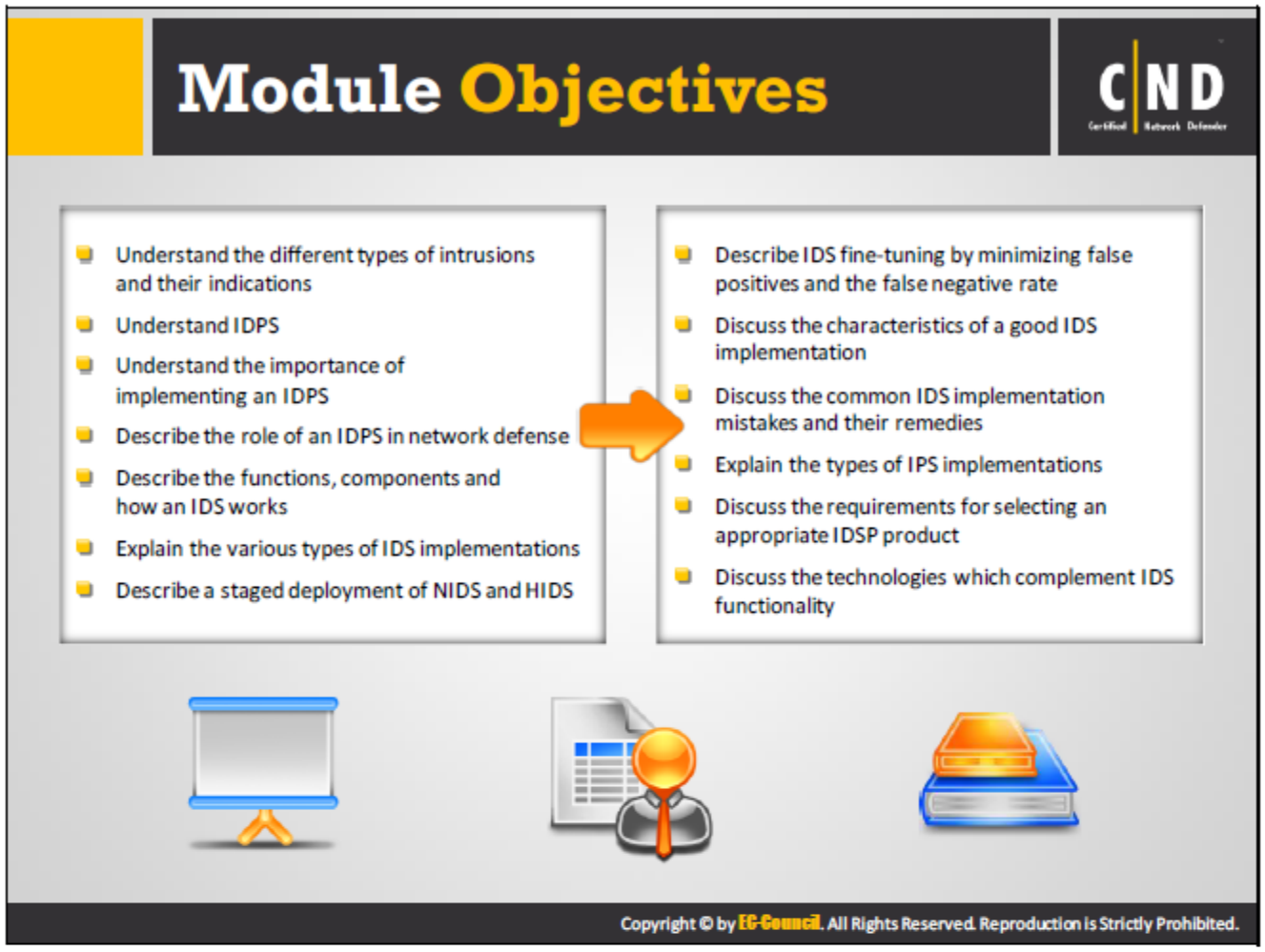
Module 08



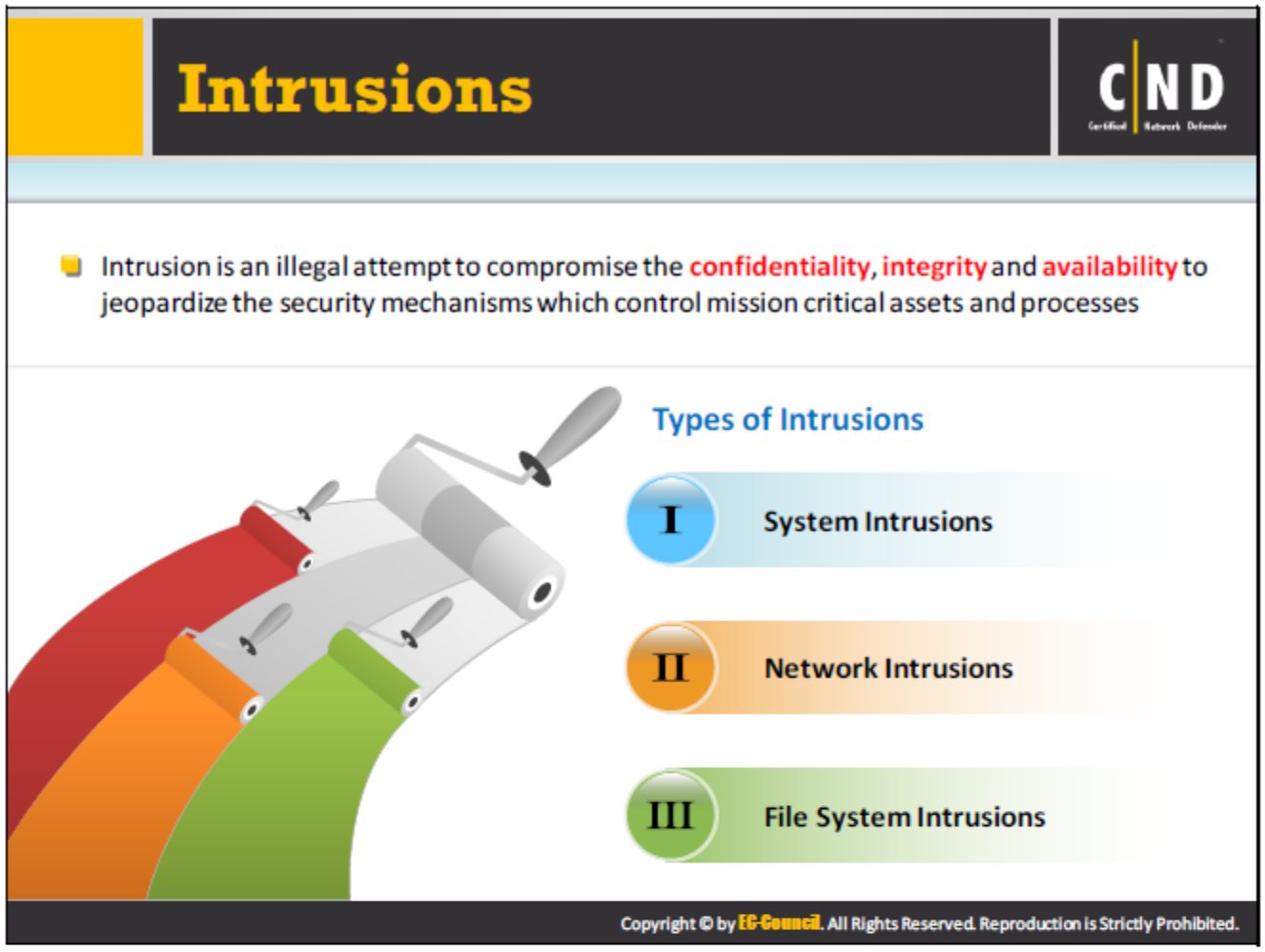
Certified Network Defender

Module 08: Secure IDS Configuration and Management

Exam 312-38



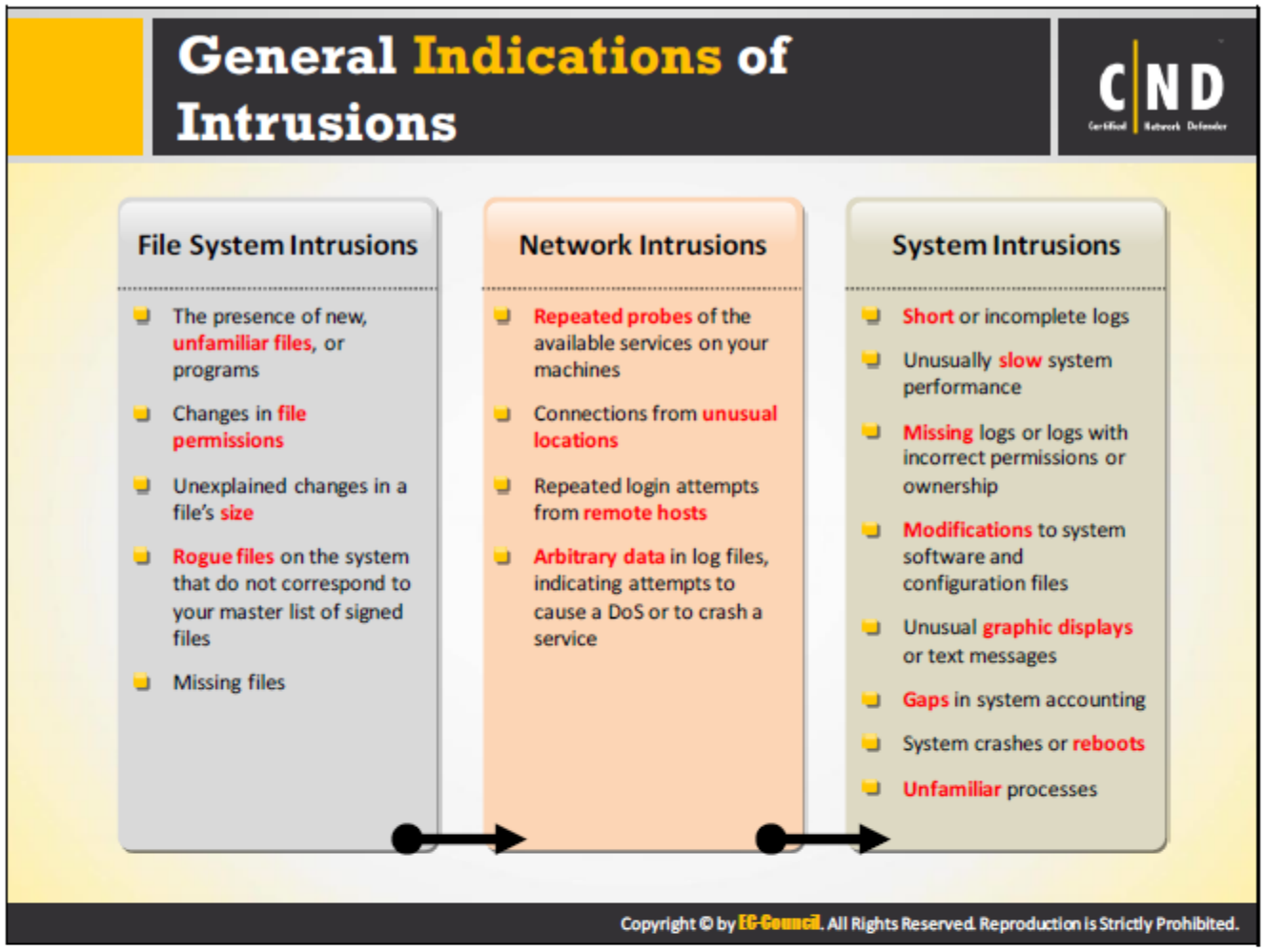
This module focuses on the configuration and deployment of IDS/IPS solutions in the network. The module starts with the basics of intrusion detection and prevention systems, how they work and the role they play in network defense. The module discusses the different types of IDS and IPS, their components, etc. The module also provides guidelines on the selection of an appropriate IDPS product and each of their deployment strategies.

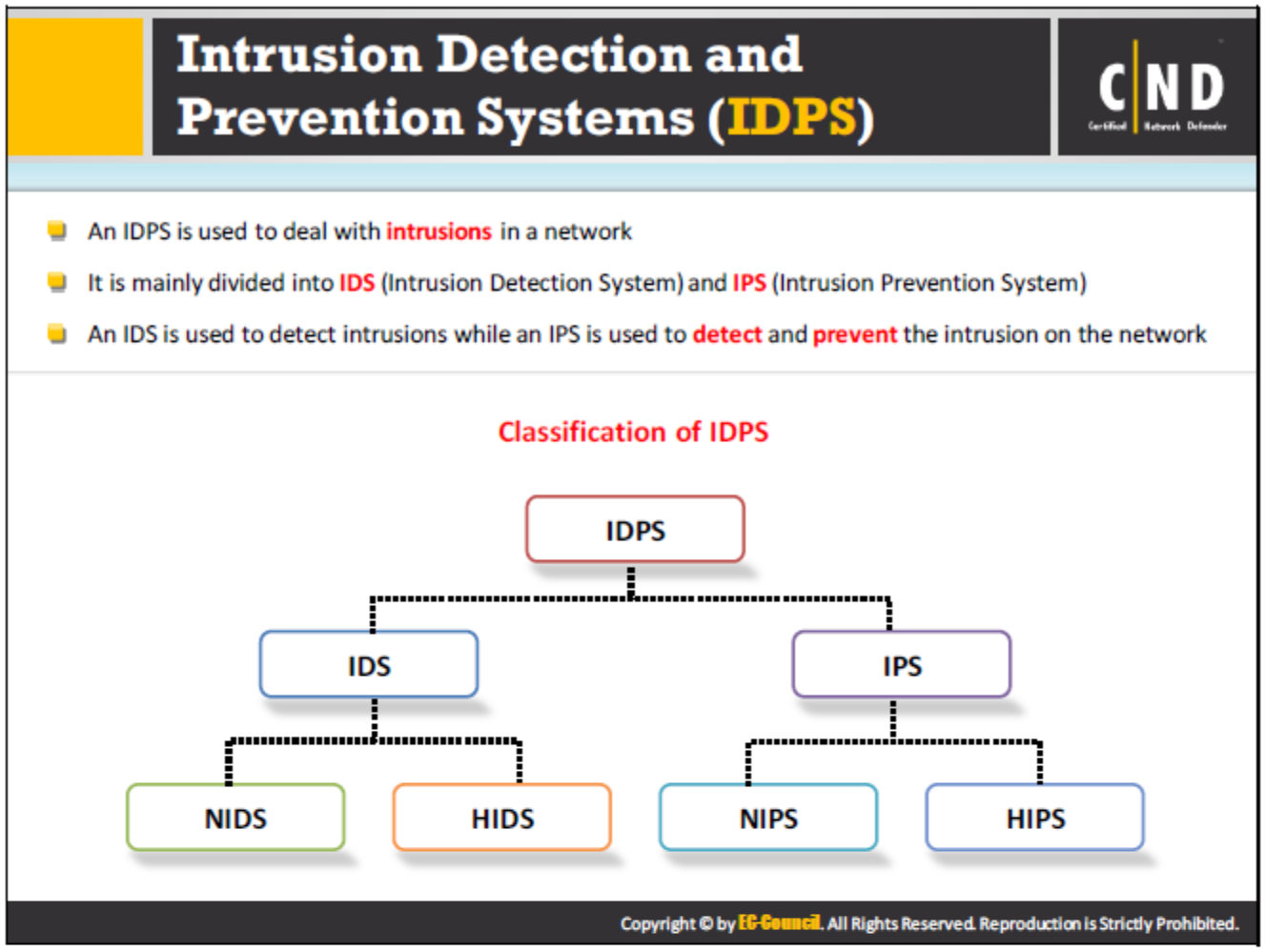


Intrusion is an Illegal attempt to compromise the confidentiality, integrity and availability or to jeopardize the security mechanisms of a computer system.

Intrusion is based on three types:

1. **System Intrusions:** System intrusions include the corruption and/or damage of the information stored in the system. An attacker exploits the system level vulnerabilities with the help of malware such as a Virus, Trojan, Worms, etc. to perform system level intrusions.
2. **Network Intrusions:** The attackers exploit network level vulnerabilities to perform network intrusions. It may include vulnerabilities which exist in the network infrastructure, configuration, protocol, etc. Attackers may perform various network level intrusions to compromise the target network. Some of the network level intrusions are ARP poisoning, Denial of Service, Spoofing, etc.
3. **File System Intrusions:** Vulnerabilities in the file system exist due to improper file handling or permissions. Attacks take advantage of file system level vulnerabilities to gain access to file systems. Attackers modify file permissions or content in the file.

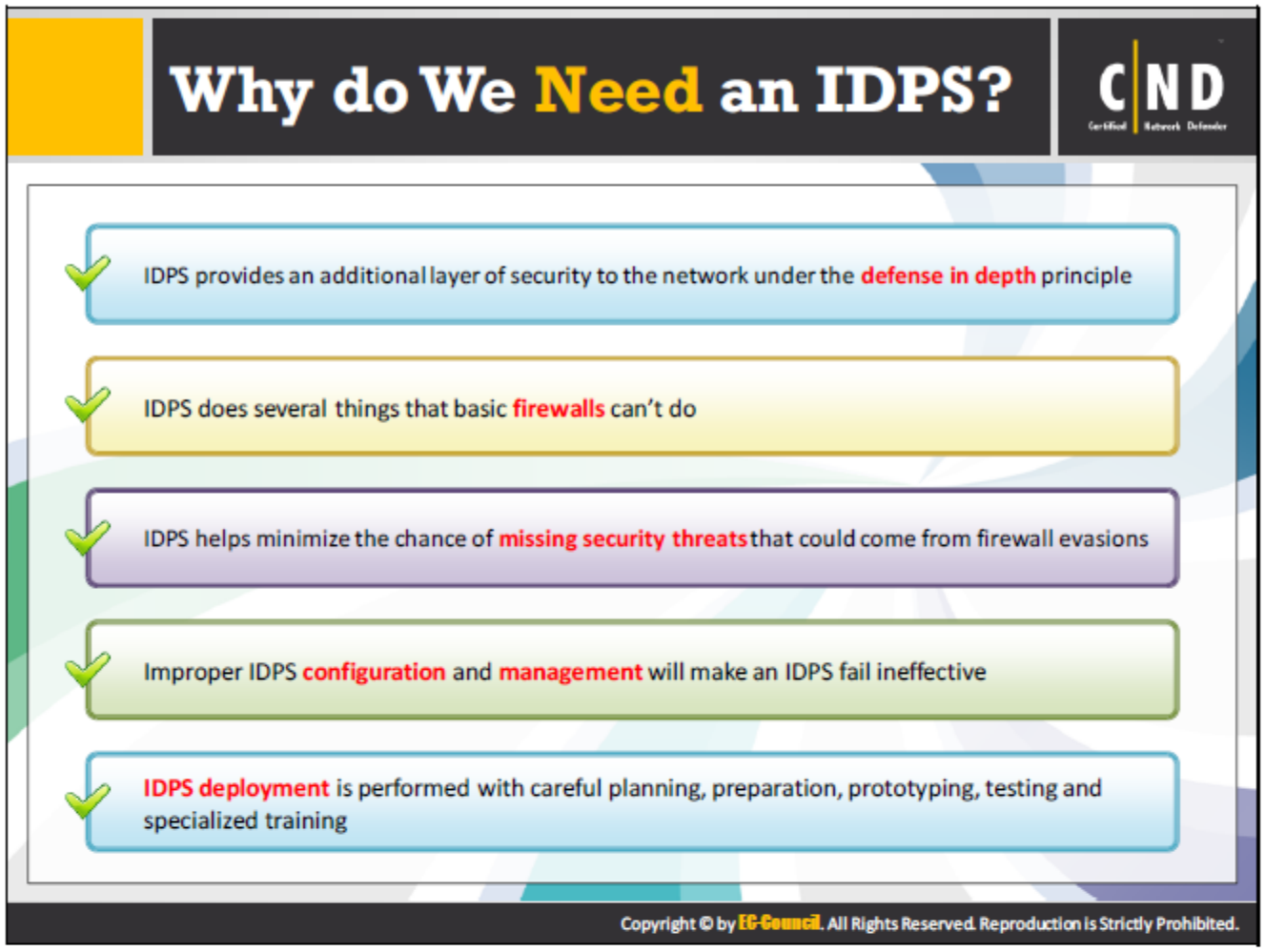




Intrusion detection and prevention systems (IDPS) are a network security appliance used to monitor the network for malicious activity. IDPS systems are categorized into Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) and are used for identifying, logging, blocking/stopping and reporting security incidents on the network. An IDPS also helps you locate weaknesses existing in security policies and assessing the network against possible threats. An IDPS is becoming an integral part of network security for most organizations.

Intrusion Prevention Systems (IPS) are considered extensions to Intrusion Detection Systems (IDS). Unlike IDS though, IPS is placed in-line and detects the incident as well as blocks it from getting into the network.

The IDS identifies and alerts the network administrator during an intrusion attempt. Besides these activities, an IDPS like IPS can detect and stop the intrusion attempts. IPS systems can also correct cyclic redundancy check (CRC) errors, defragment packet streams, TCP sequencing issues and manage the options in the transport and network layers.

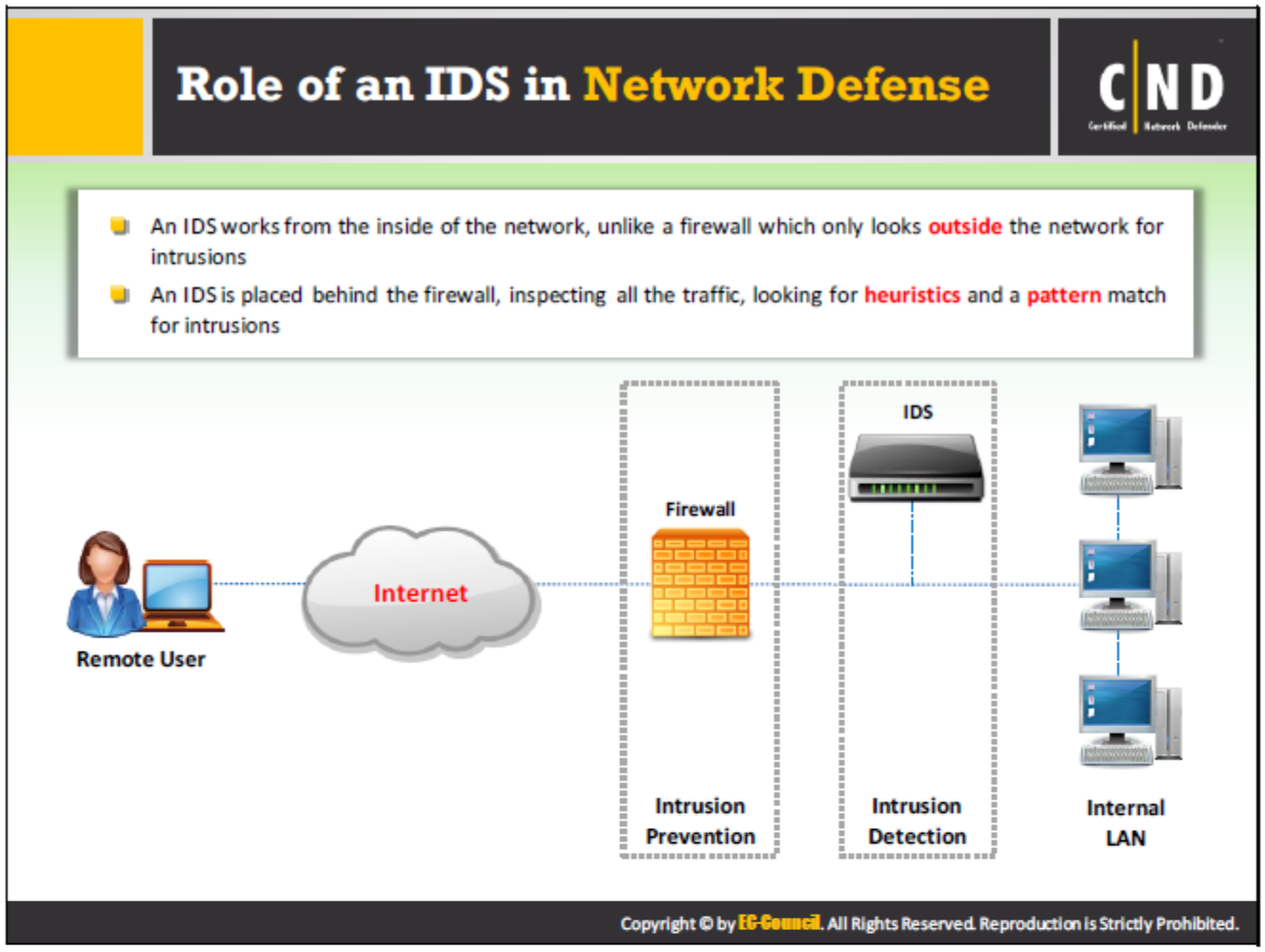


Relying solely on a firewall for network security can provide a false sense of security. The firewall is simply implemented in the IT security policy which allows or denies traffic based on the policy rules. It allows certain packets to pass through or denies access if it does not meet certain criteria specified in a rule. It does not check the content of legitimate traffic, allowed based on a rule set. The legitimate traffic may contain malicious content which is not evaluated during inspection by a firewall.

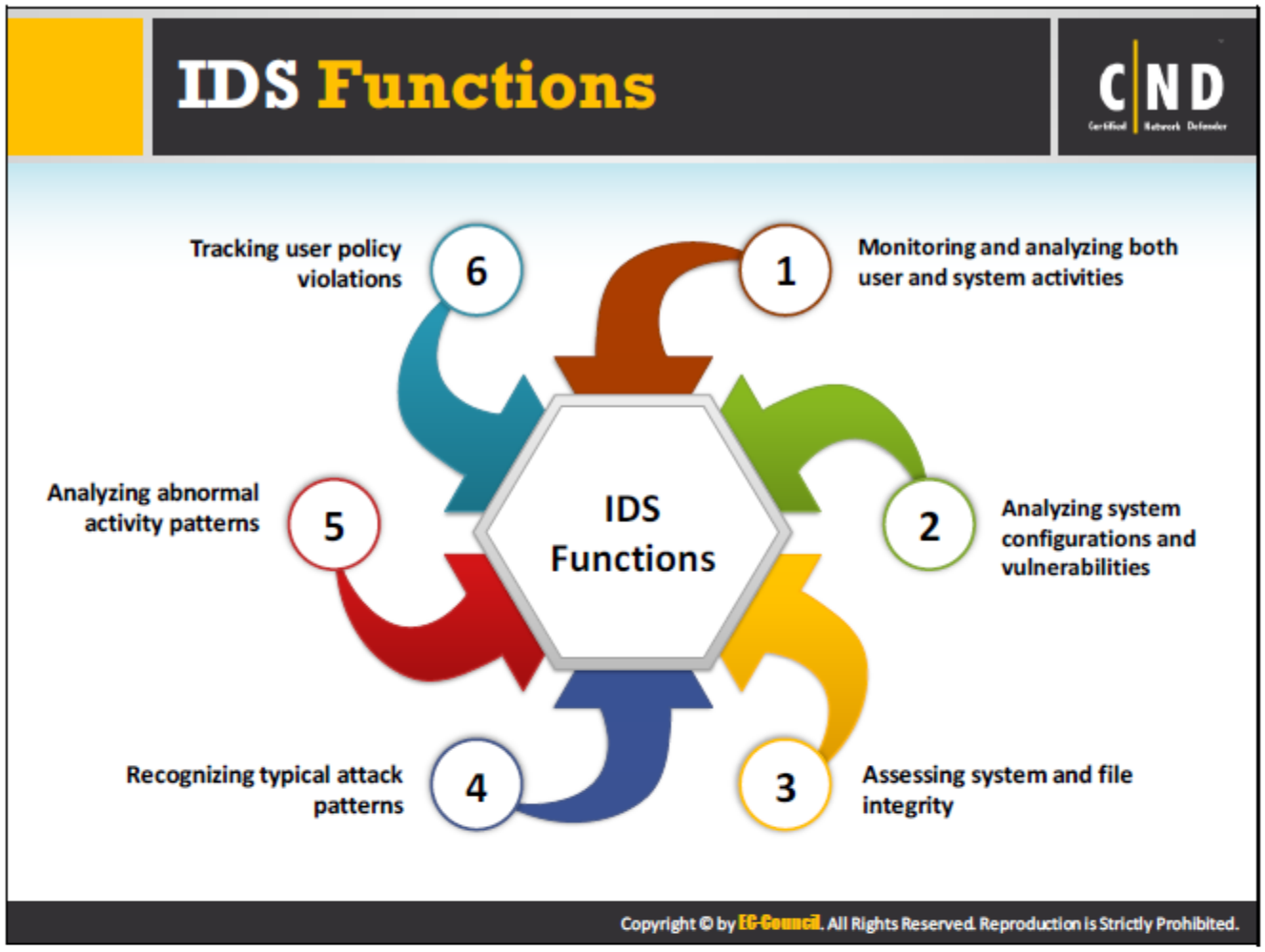
As an example, firewalls can be configured to pass traffic solely to port 80 of the Web server and to port 25 of the email server but it will not inspect the nature of the traffic flowing through either of these ports.

This is the reason for an IDPS and its applications. An IDPS application will inspect the legitimate traffic coming from firewall and conduct signature based analysis to identify malicious activity and raises an alarm to notify the administrators.

Intrusion detection and prevention systems (IDPS) are a proactive means of detecting and responding to threats from both inside and outside a network. It is an integral and necessary element of a complete network security infrastructure. An IDPS provides a complete level of supervision for a network, regardless of the action taken, in this way the information will always exist when attempting to determine the nature and source of a security incident.

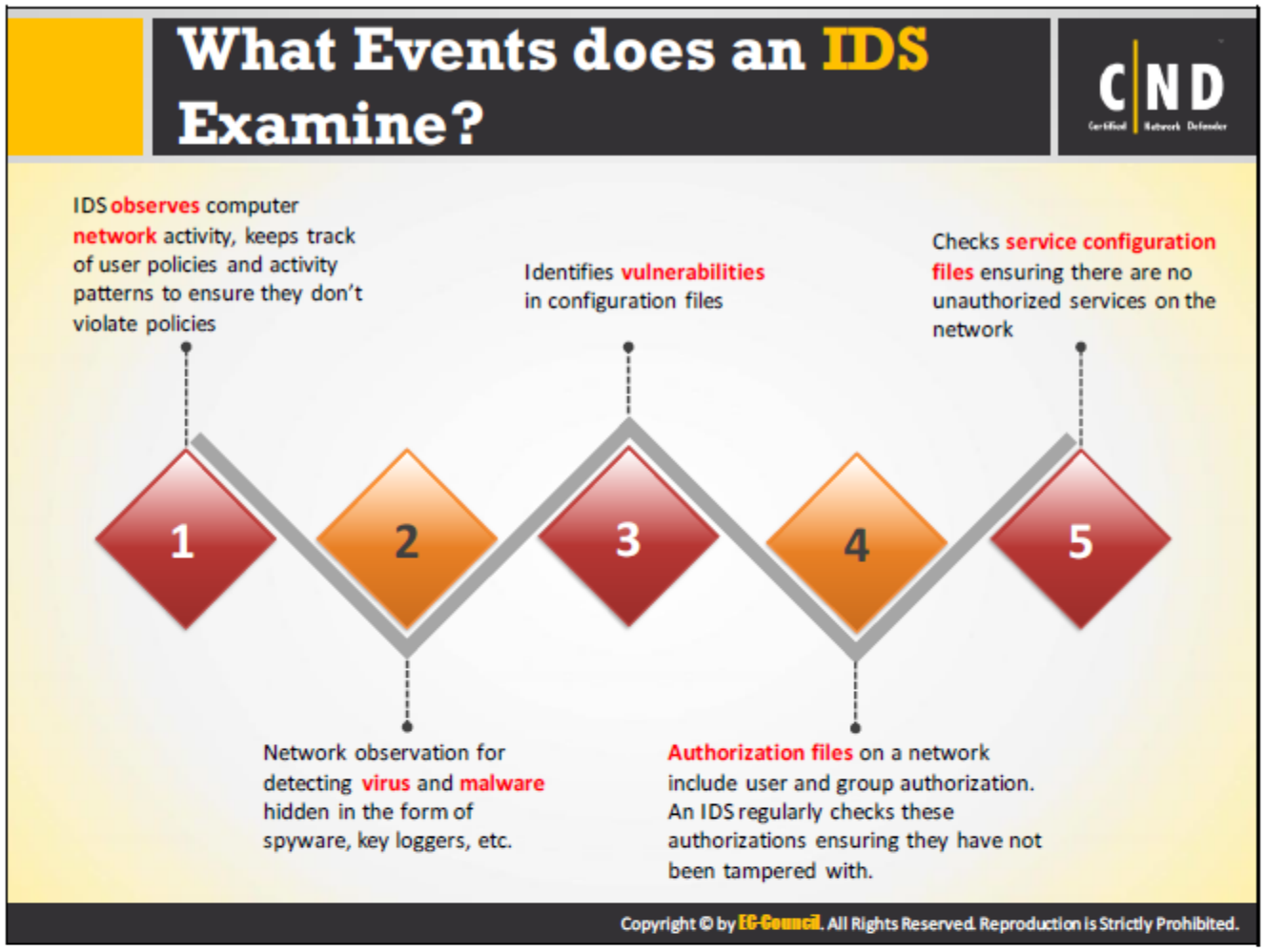


Though firewalls and IDPS applications are security services used to prevent a network from various types of attack, they are basically two different applications that tend to operate in tandem. They are functionally different from each other. IDPS is placed behind the firewall in the network. Firewalls use a filter for inbound/outbound traffic based on the rules configured. The purpose of a firewall is to control the traffic that should be allowed into a network based on static rules. IDPS applications are used to locate and stop malicious activities, mainly through signature based detection. An IDPS application monitors the filtered traffic coming from a firewall for malicious activity based on these signatures.



In addition to its core functionality of identifying and analyzing intrusions, an IDS can perform the following types of activities related to intrusion detection:

- **Records information about events**: Notes down every detail regarding the monitored events. The intrusion detection systems forward the recorded information to various other systems such as centralized logging servers, security information and event management (SIEM) and enterprise management systems.
- **Sending an alert**: The IDS sends an intrusion alert to the network security administrator through e-mails, pop up messages on the IDS user interface, etc.
- **Generating Reports**: The IDS generates reports providing insight into observed events or any suspicious event which has occurred.



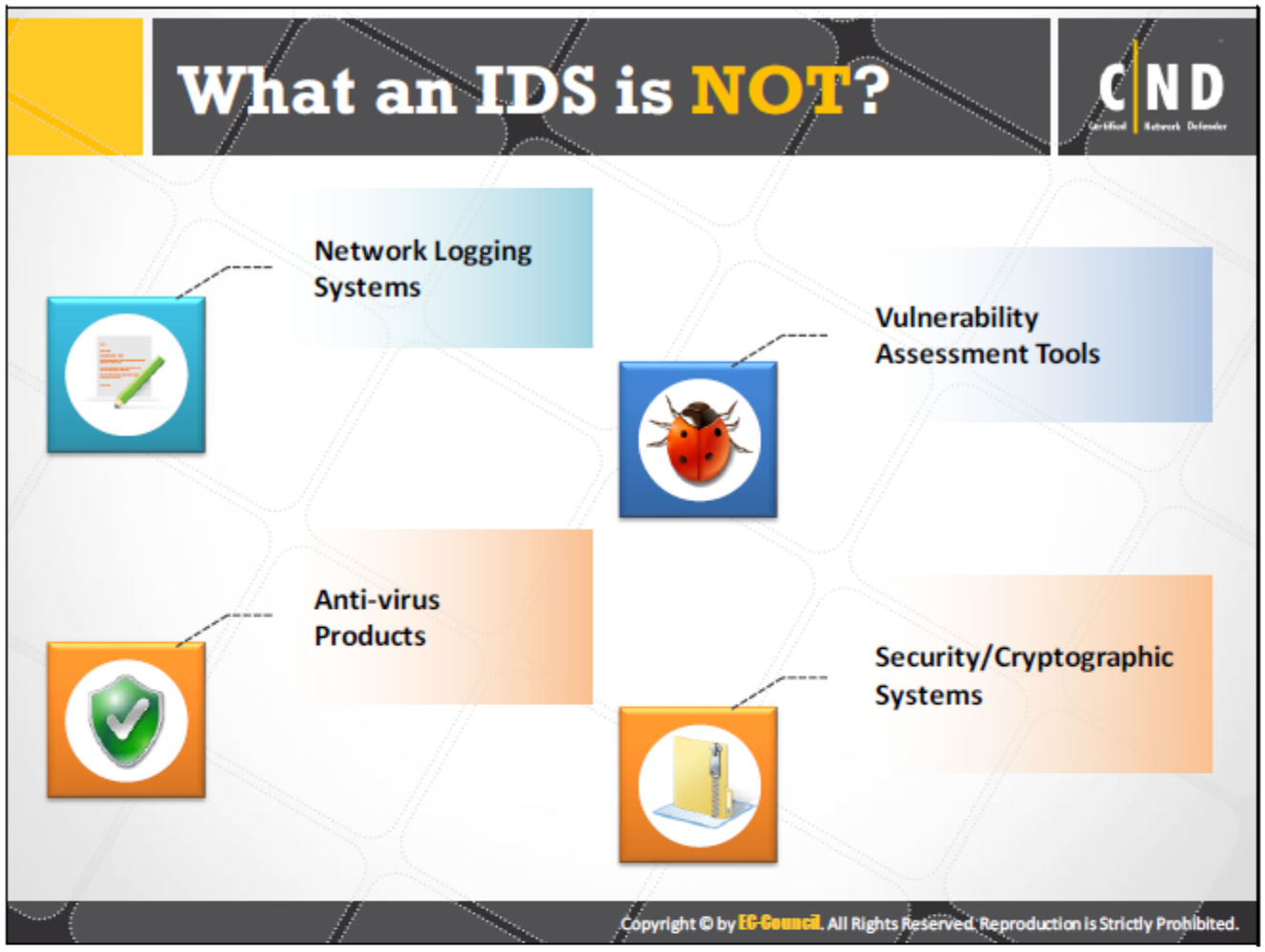
An IDS observes computer network activity, keeps track of user policies and activity patterns to ensure they do not violate policies. It also observes network traffic and components for detecting virus and malware hidden in the form of spyware, key loggers, etc.

An IDS works by gathering information about illicit attempts made to compromise security and verifies them. It also records the event data and an IT administrator will use this data to take future preventive measures and make improvements to network security.

An intrusion detection system works by examining certain events such as:

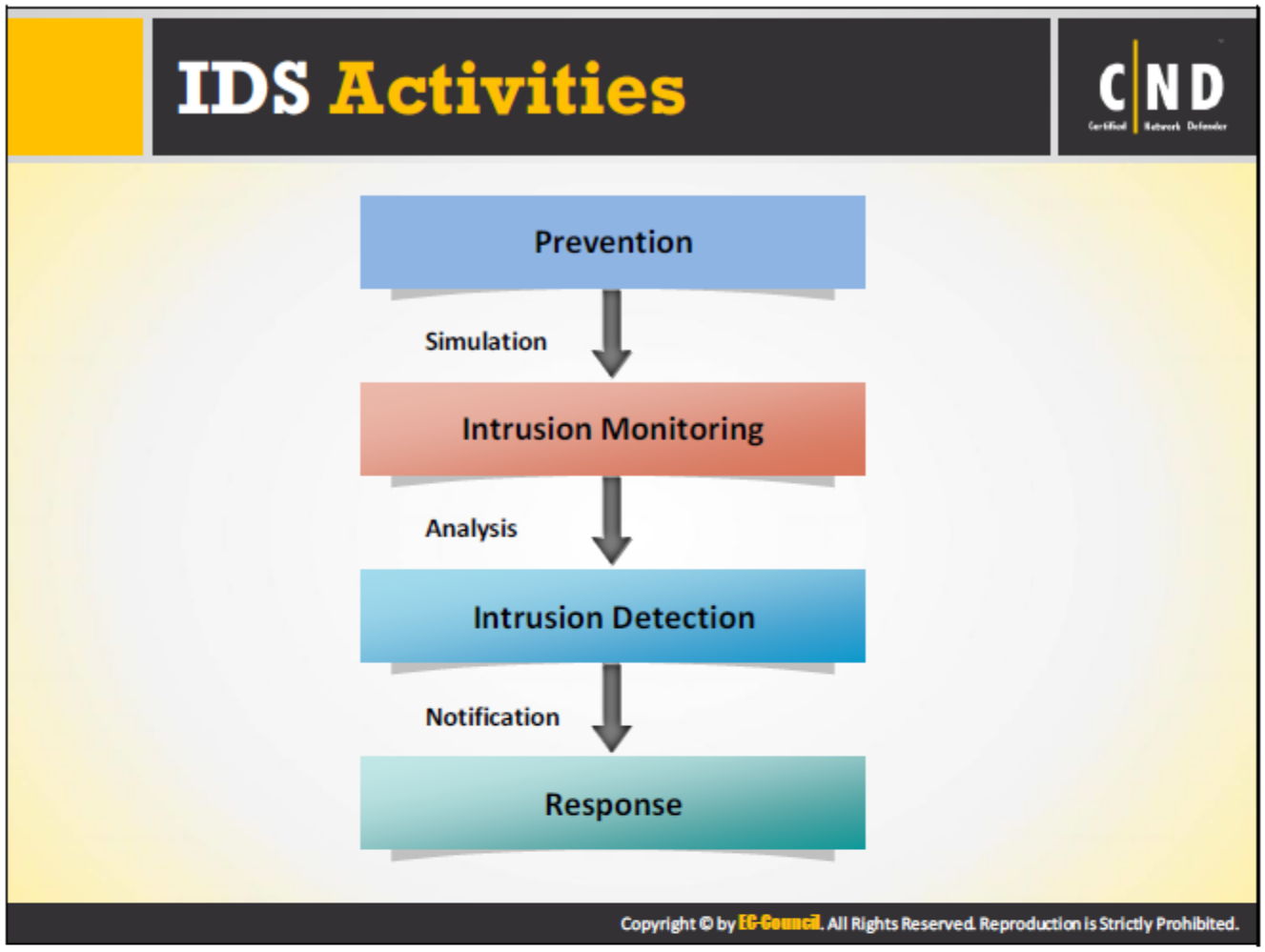
- **Observing Activity:** The IDS will track all the activities taking place within a network and keep track of user policies and activity patterns to detect any kind of attempts to violate these patterns.
- **Viruses:** An IDS is capable of detecting virus and malware hidden within a network system in the form of spyware, key logging, password theft, etc.
- **Vulnerabilities:** The IDS identifies vulnerabilities in the network configuration files and network components.
- **File Settings:** The IDS verifies user authorization and group authorization files on a network, and checks them for tampering.
- **Services:** Routinely checks configuration files for unauthorized services operating on the network.

- **Packet Sniffing:** These systems check for unauthorized network monitoring programs that can monitor and record user account activity data.
- **PC Check:** The IDS regularly checks PCs on the network for violations.



Contrary to popular belief and terminology employed in the literature on intrusion detection systems, not every security device falls into this category. In particular, the following security devices are not an IDS:

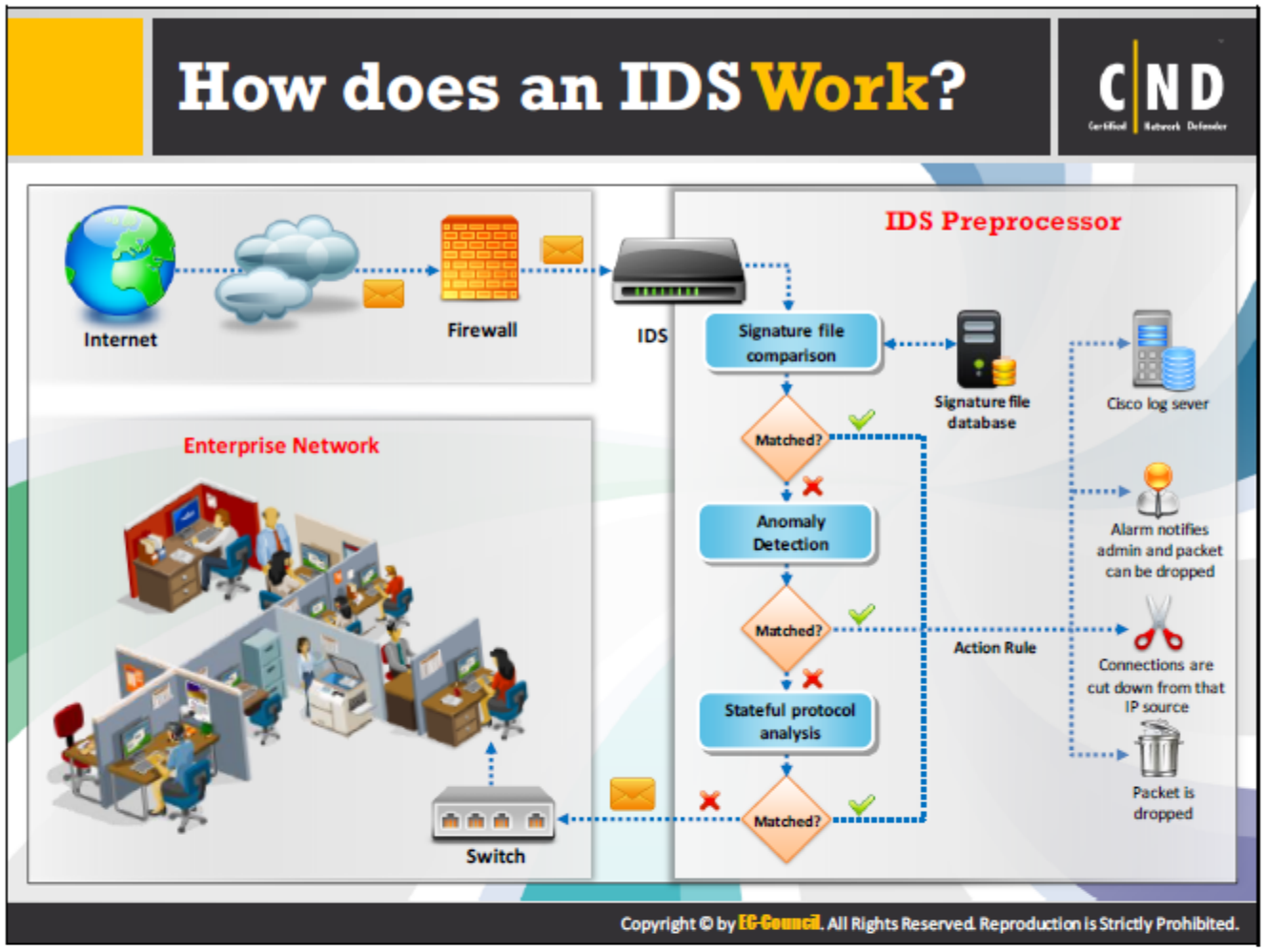
- **Network Logging Systems:** These devices are network traffic monitoring systems. They detect denial of service (DoS) vulnerabilities across a congested network.
- **Vulnerability Assessment Tools:** These devices check for bugs and flaws in operating systems and network services (security scanners).
- **Anti-virus Products:** These devices detect malicious software such as viruses, Trojan horses, worms, bacteria, logic bombs. When compared feature by feature, these devices are very similar to intrusion detection systems and often provide effective security breach detection.
- **Security/Cryptographic Systems:** These devices protect sensitive data from theft or alteration and user authentication. Examples include VPN, SSL, S/MIME, Kerberos, and Radius.



The main task of an intrusion detection system is detecting an intrusion attempt on a network and a notification about what occurred. Detecting hostile attacks depends on several types of actions including prevention, intrusion monitoring, intrusion detection and response. Intrusion prevention requires a well-selected combination of luring and tricking aimed at investigating threats. Diverting the intruder's attention from protected resources is another task. An IDS constantly monitors both the real system and a possible trap system and carefully examines data generated by intrusion detection systems for detection of possible attacks.

Once an IDS detects an intrusion it issues alerts notifying administrators. Once the intrusion is detected and notified, the administrators can execute certain countermeasures. It may include blocking functions, terminating sessions, backing up the systems, routing connections to a system trap, legal infrastructure, etc. An IDS is an element of the security policy.

An IDS alerts and logs are useful in forensic research of any incidents and installing appropriate patches to enable the detection of future attack attempts targeting specific people or resources.



In a network, the IDS's sensor monitors all packets transmitted to and from the network. The IDS detects network anomalies, attack patterns and the data containing viruses, malware and other harmful threats. An IDS scans the network traffic and components for anomalies or patterns that seem to be illicit. Then the IDS takes action against the threat and sends an alarm signal to the administrator, resets the TCP connection or drops the packet to prevent the threat signal from entering into the network.

An IDS should be implemented in combination with a firewall to offer better protection to the network. An IDS generally uses two techniques to detect any abnormalities in the traffic.

Signature/Pattern matching

It involves checking and comparing the network traffic for known attack patterns or signatures. Attacks are recognized by certain patterns in network traffic called signatures. An IDS is pre-installed with signatures for known attacks. These signatures are stored in a signature database. The IDS compares the traffic against these signatures to detect potential threats to the network and sends an alert, if a pattern match is found. The pattern/signature technique is highly efficient if and only if the database is up to date. The major disadvantage of this technique is if pattern matching fails to identify new attacks because there is no definite signature in the database.

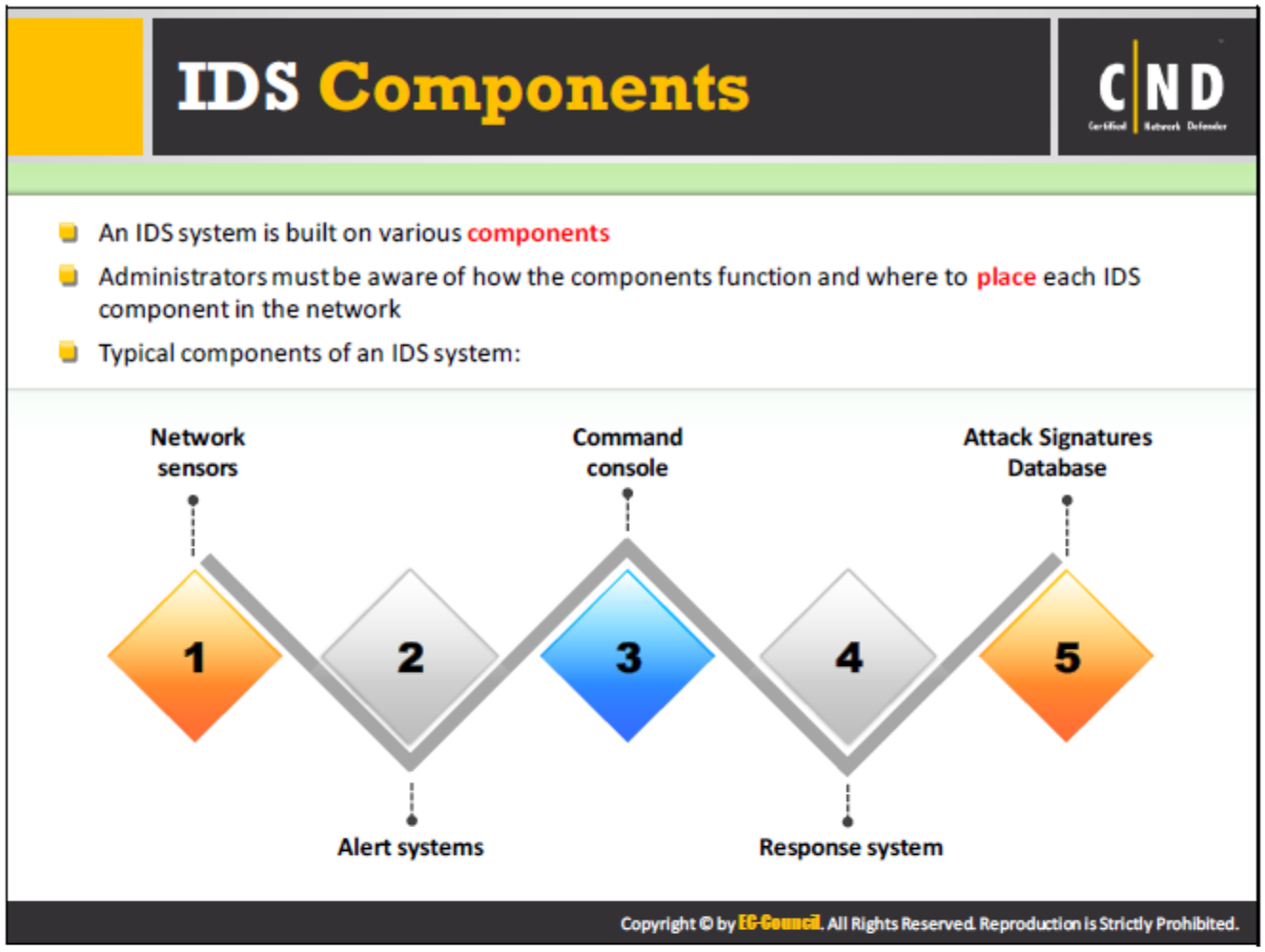
Statistical anomaly detection

Anomaly-based detection observes the network for abnormal usage patterns by determining the performance parameters for regular activities and monitoring for actions beyond the normal parameters. This method allows the administrators to detect new intrusions or attacks even without a known signature.

Stateful Protocol Analysis

Stateful Protocol Analysis is also known as deep packet inspection, which is a reliable and resource intensive approach in an IDS. The analysis defines the methods on how a particular protocol should work. It has the feature of determining the type of attack and responding to it respectively. For example, stateful protocol analysis can detect an unexpected generation of a sequence of repeated commands in the network. This also includes detecting variations in command length, command attributes and other anomalies.

The accuracy of a stateful protocol depends on the efficiency of the protocol models. Protocol models that already have a proprietary or are poorly defined, cannot have an accurate analysis. In large organizations, stateful protocol analysis requires a lot of resources to track and analyze the information. Attacks that do not violate the protocol characteristics go undetected by the stateful protocol analysis.



An IDS is comprised of different components. These components are used to collect information from a variety of systems and network sources, and then analyze the information for any abnormalities. Major components of an Intrusion Detection System include:

- **Network Sensors:** These agents analyze and report any suspicious activity.
- **Analyzer:** Analyzes the data collected by the sensors.
- **Alert Systems:** These systems trigger alerts when detecting malicious activity.
- **Command console:** It acts as an interface between the user and the intrusion detection system.
- **Response system:** An IDS uses this system to initiate countermeasures on detected activities.
- **Database of attack signatures or behaviors:** A list of previously detected signatures stored in a database that assist the IDS in intrusion detection.

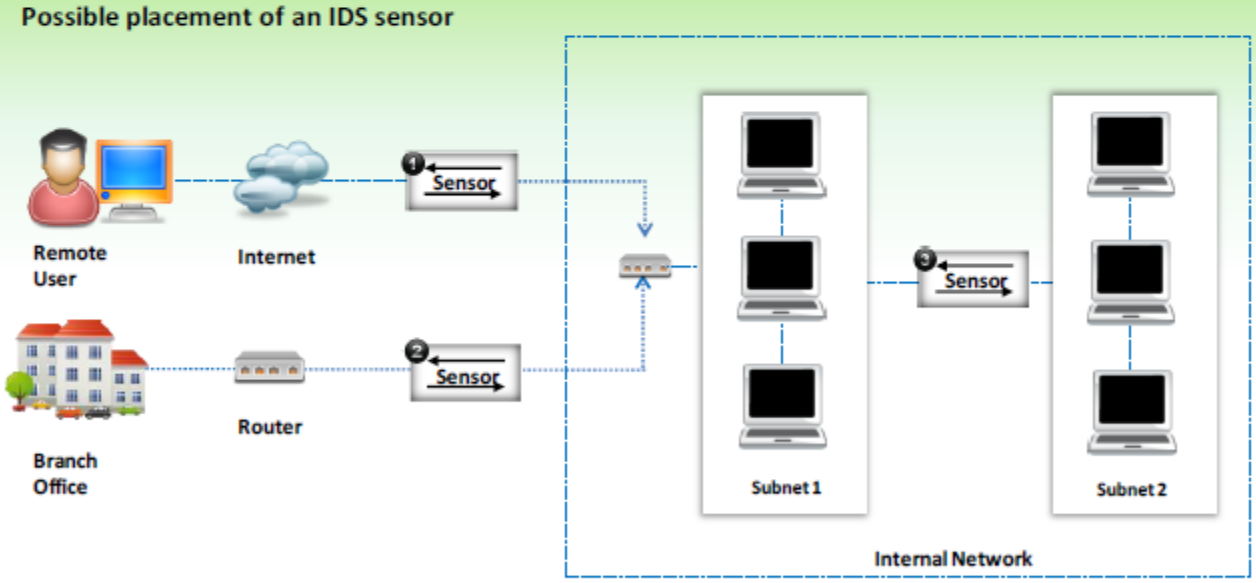
IDS Components: Network Sensors

- Network sensors are hardware and software components which monitor network traffic and trigger alarms if any abnormal activity is detected
- Placed and located at common entry points in a network such as:

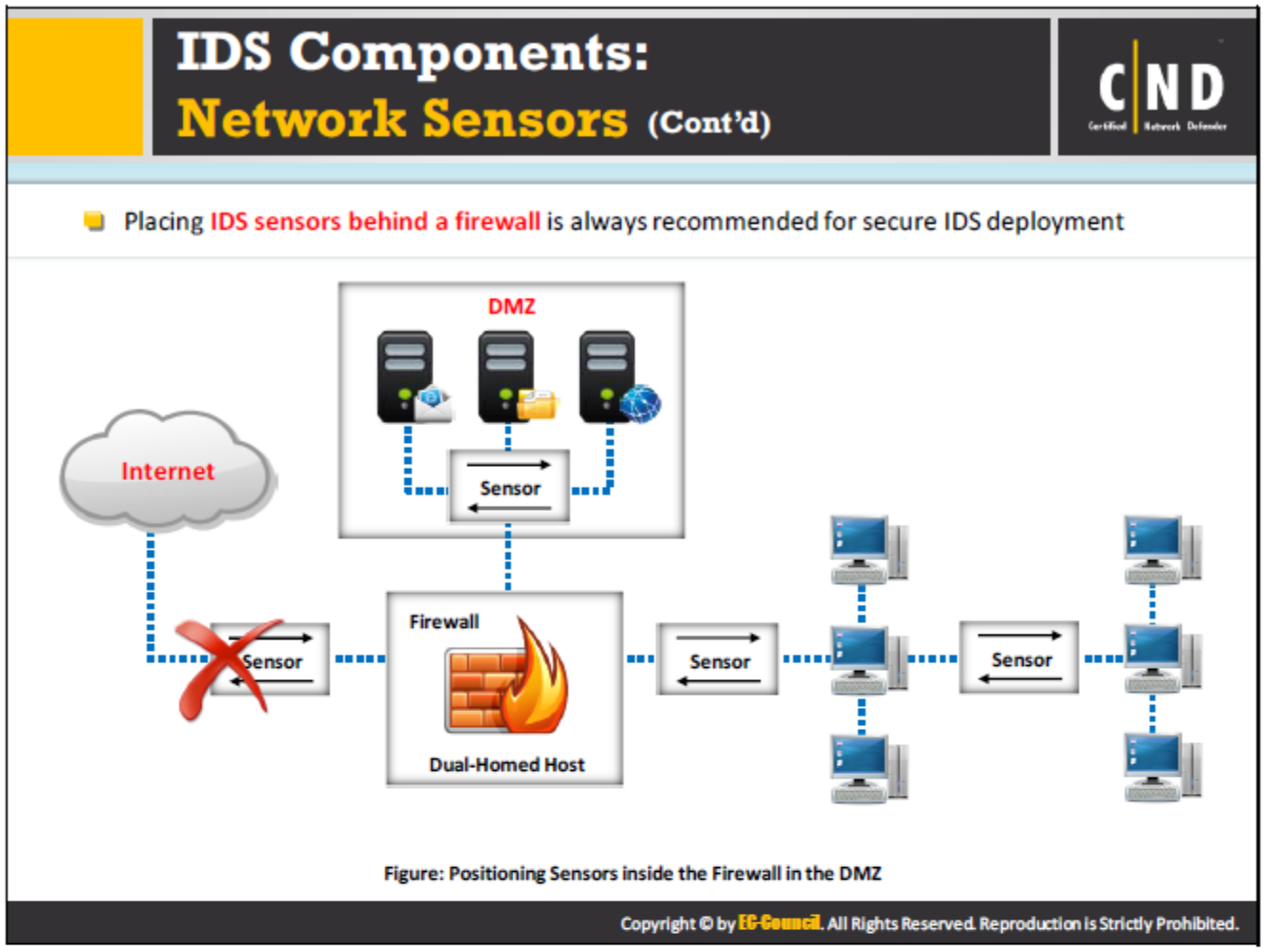
- Internet gateways
- In between LAN connections
- Remote access servers used to receive dial-up connections
- Virtual private network (VPN) devices
- Either side of Firewall

IDS Components: Network Sensors (Cont'd)

Possible placement of an IDS sensor



1. **Option 1:** Between a remote user and the internal network
2. **Option 2:** Between a branch office and the internal network
3. **Option 3:** Between one subnet and another subnet



A network sensor is a hardware and/or software device connected to the network and reports to the IDS. It is a primary data collection point for the IDS. Network sensors collect data from the data source and pass it to the alert systems.

The sensor integrates with the component responsible for data collection such as an event generator. Network sensors determine data collection based on the event generator policy which defines the filtering mode for event notification information.

The role of the sensor is to filter information and discard any irrelevant data obtained from the event set associated with the protected system, thereby detecting suspicious activities. Sensors check the traffic for malicious packets and trigger an alarm when they suspect a packet is malicious and then alert the IDS. If an IDS confirms the packet as malicious then the sensors generate an automatic response to block the traffic from the source of the attack.

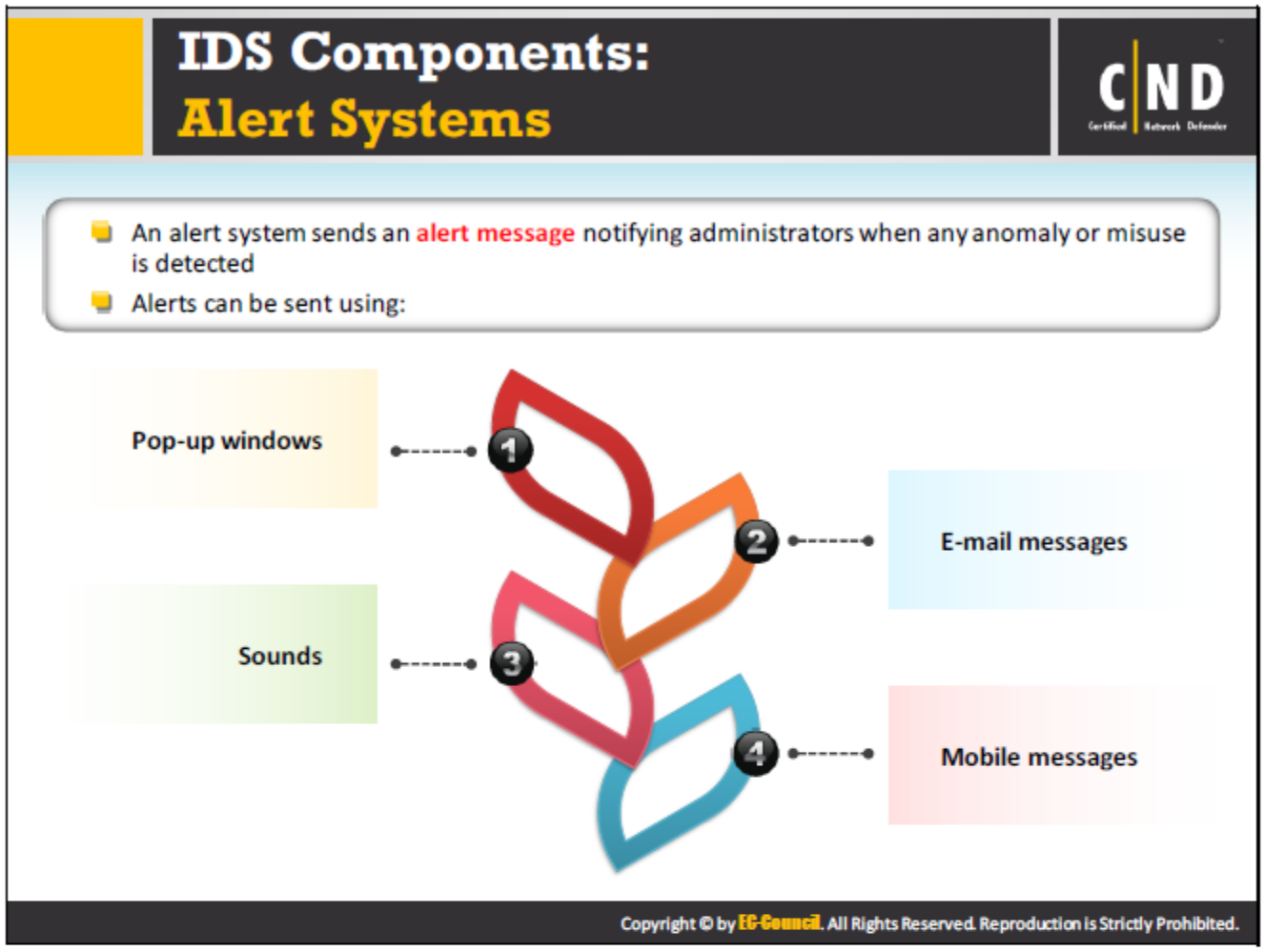
To detect network intrusions, administrators should place several network sensors at strategic locations on the network. The positioning of sensors will depend significantly on which kind of network resources you want to monitor for intrusion. Some organizations will want to use the IDS to monitor internal resources such as a sensitive collection of machines or a specific department or physical location. In that case, the most logical place for the IDS sensor will be on the choke point between those systems and the rest of the internal network. Some of the critical common-entry points to place sensors include:

- At Internet gateways.
- At connections between LAN connections.

- At remote access servers that receive dial-up connections from users.
- At virtual private network (VPN) devices that connect an internal LAN to an external LAN.
- Between subnets that are separated by switches.

If organizations are planning to monitor intrusions targeting internal servers, such as DNS servers or mail servers then they place a sensor inside the firewall on the segment that connects the firewall to the internal network. The logic behind this is that the firewall will prevent a vast majority of attacks aimed at the organization, and regular monitoring of firewall logs will identify them. The IDS on the internal segment will detect some of those attacks that manage to get through the firewall.

If a firewall is in place to protect the network then positioning sensors inside the firewall is more secure, then placing a sensor outside the firewall at a position exposed to the Internet. If it is placed outside the firewall, it can become the major focus for attacks. A more secure location to place a sensor is behind the firewall in the DMZ.



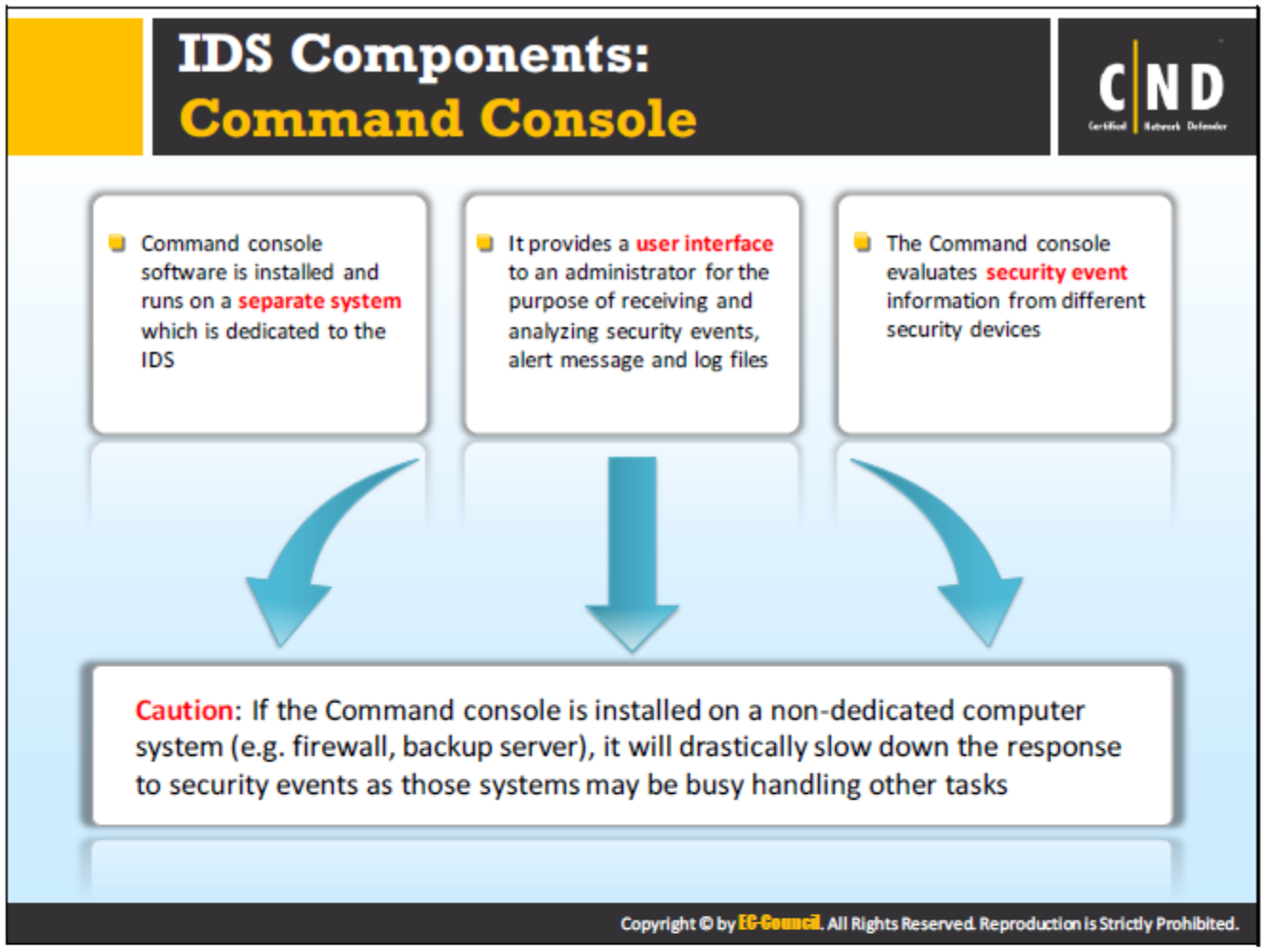
Alert Systems trigger an alert whenever sensors detect malicious activity in the network. The alert communicates to the IDS about the type of malicious activity and its source. The IDS uses triggers to respond to the alert and take countermeasures. An IDS can send alerts using:

- Pop-up windows
- E-mail messages
- Sounds
- Mobile messages

When a sensor triggers an alert, there are three possibilities:

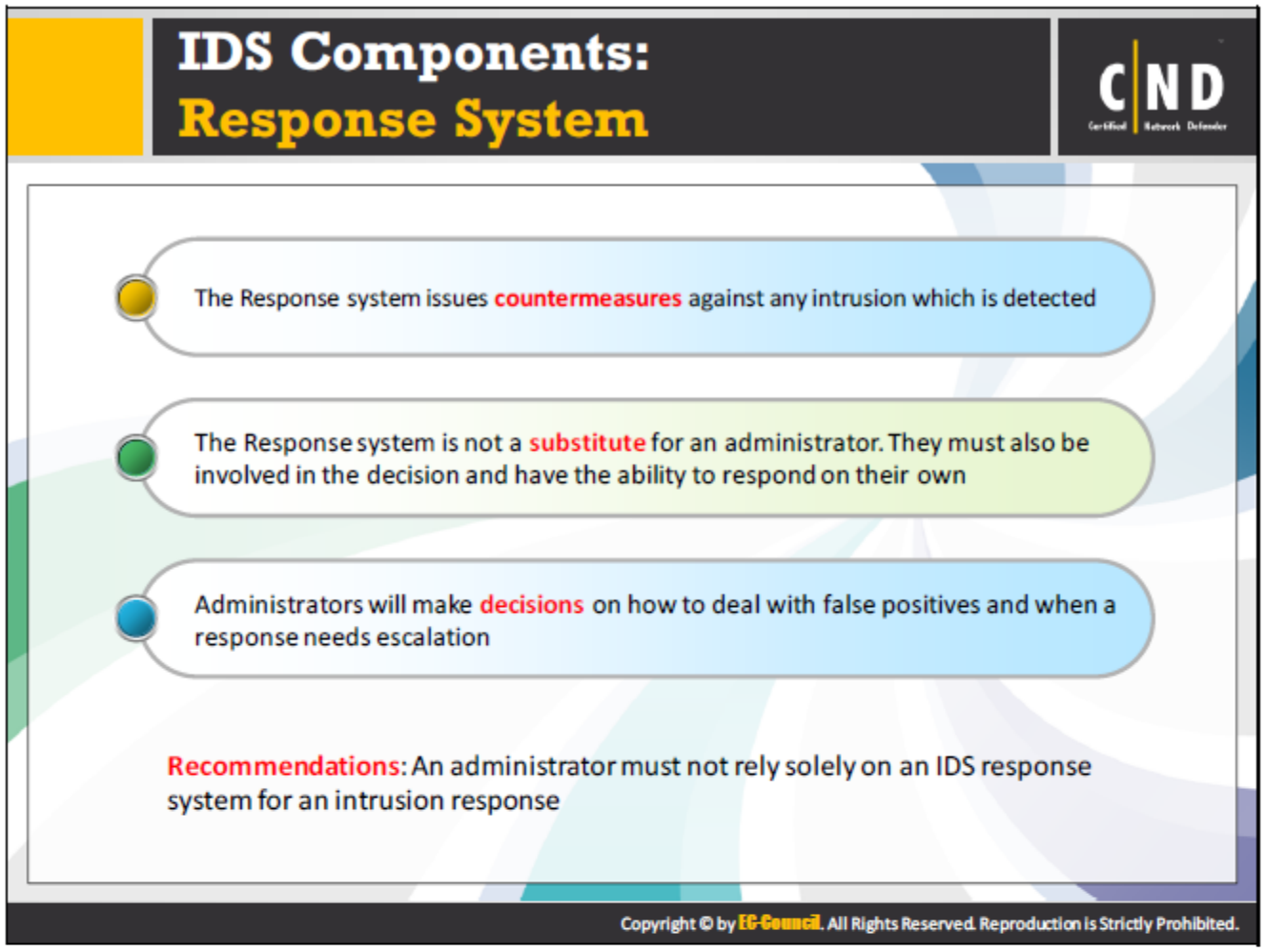
- The sensor has correctly identified a successful attack. This alert is most likely relevant, termed as a true positive.
- The sensor has correctly identified an attack, but the attack failed to meet its objectives. Such alerts are known as non-relevant positive or non-contextual.
- The sensor incorrectly identified an event as an attack. This alert represents incorrect information, termed as a false positive.

As more IDSs are developed, network security administrators must face the task of analyzing an increasing number of alerts resulting from the analysis of different event streams. In addition, IDSs are far from perfect and may produce both false positives and non-relevant positives.



The Command console is software that acts as an interface between a network administrator and the IDS. The IDS collects all the data from security devices and analyzes it using the command console. Administrators use the console to analyze alert messages triggered by the alert system and manage log files. The Command console allows administrators in large networks to process large volumes of activities and respond quickly.

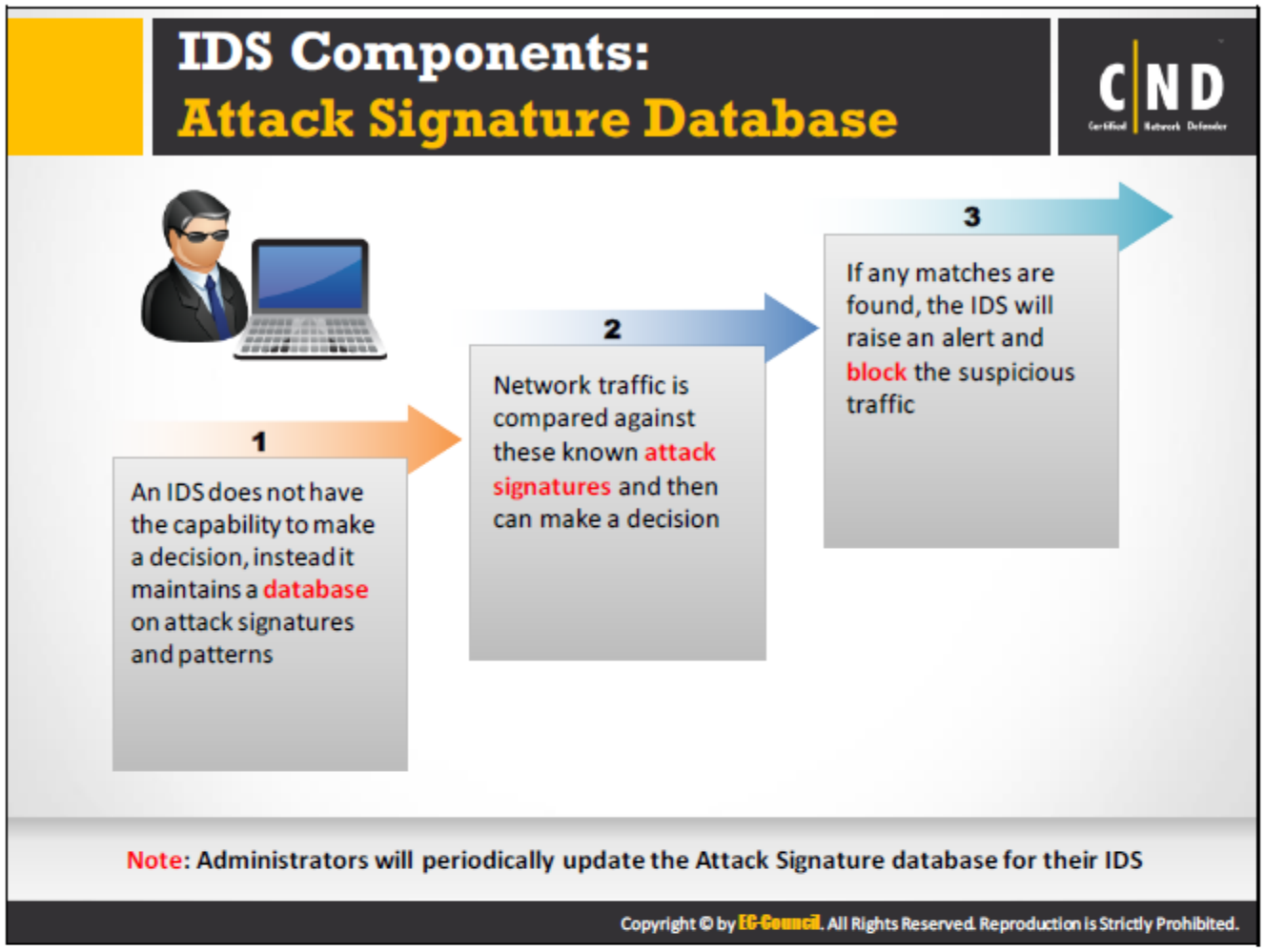
An IDS collects information from security devices placed throughout the network and sends it to the command console for evaluation. Installing a command console on the system for other purposes such as backing up files and firewall functions, will make it slow to respond to events which have occurred. Installing the command console on a dedicated system provides the benefit of a fast response.



A response system in an IDS is responsible for the countermeasures when an intrusion is detected. These countermeasures include logging out the user, disabling a user account, blocking the source address of the attacker, restarting a server or service, closing connections or ports, and resetting TCP sessions.

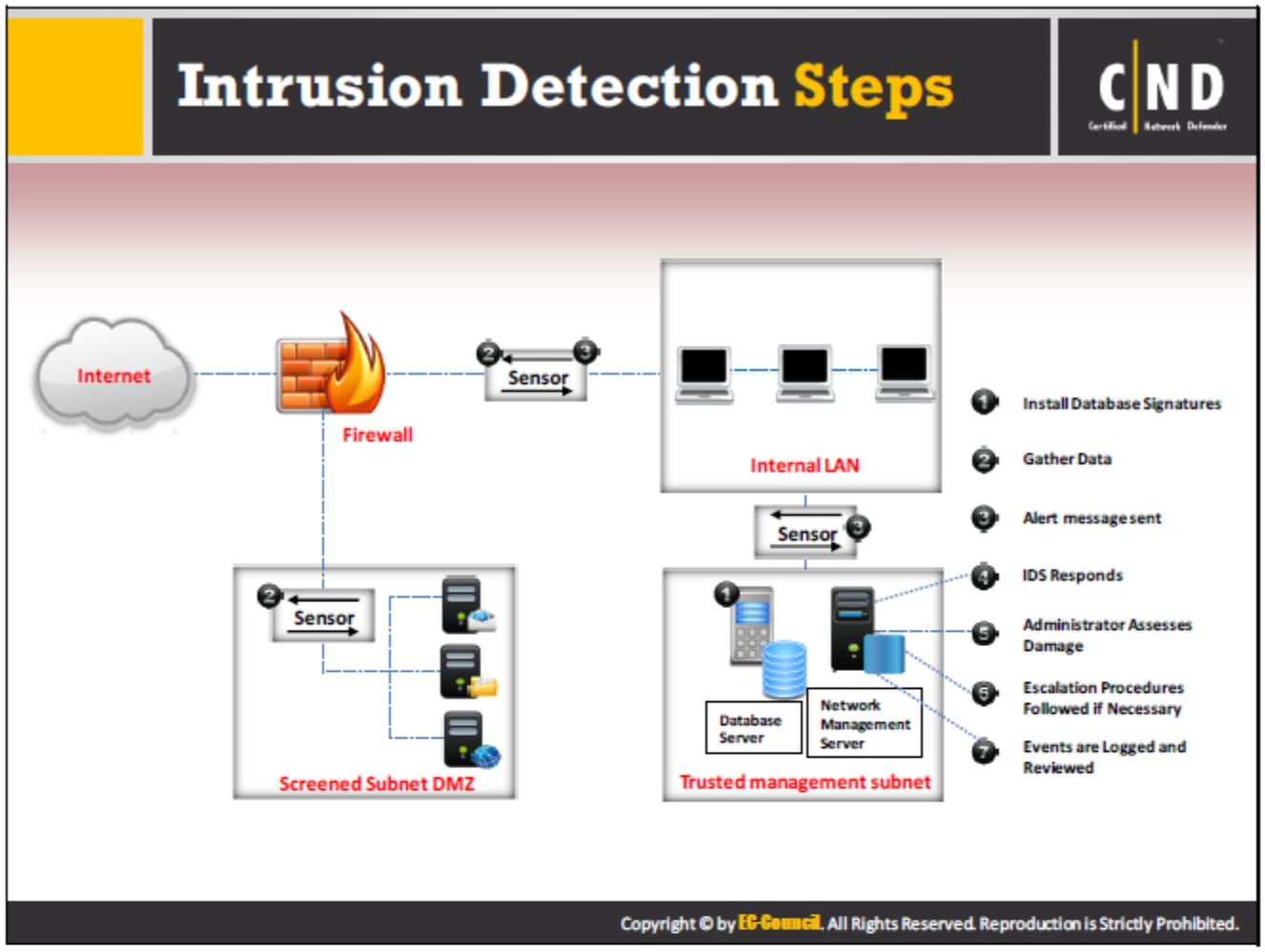
Administrators can set up an IDS to allow the response system to take actions against intrusions or they can respond on their own. In the case of false positives, administrators need to respond to allow this traffic into the network without blocking it. Using the response system, administrators can also define the level of counter action an IDS must take to respond to the situation, depending on the severity of the intrusion.

An IDS has the advantage of providing real-time corrective action in response to an attack. They automatically take action in response to a detected intrusion. The exact action differs per product and depends on the severity and type of attack detected. A common active response is increasing the sensitivity level of the IDS to collect additional information about the attack and the attacker. Another possible active response is making changes to the configuration of systems or network devices such as routers and firewalls to stop the intrusion and block the attacker. Administrators are responsible for determining the appropriate responses and ensuring that those responses are carried out.



Network administrators should exercise their own judgment when evaluating security alerts because an IDS does not have the ability to make these kinds of decisions. However, an IDS can use a list of previously detected signatures, which are stored in the attack signature database, to detect suspicious activity. The IDS compares the signature of packets in the network traffic with the database of known attack signatures. The IDS blocks the traffic if a packet matches a stored signature in the database. Administrators should always keep the database updated to detect new types of attacks.

The IDS uses normal traffic logs to match against currently running network traffic to find suspicious activity. If an IDS finds unusual traffic activity, it determines the traffic as suspicious activity and blocks it before it enters the network.



An IDS operates in different ways depending on the purpose of the configuration. There is a generalized process for intrusion detection. The steps involved in the process include:

Install Database Signatures

The first step of intrusion detection occurs before any packets are detected on the network. Network administrators install the database of signatures or user profiles along with the IDS software and hardware. This database helps the IDS compare traffic passing through the network.

Gather Data

The IDS gathers all the data passing through the network using network sensors. The sensors monitor all the packets allowed through the firewall and pass it to the next line of sensors. If it identifies malicious packets, the sensor sends alert messages to the IDS.

Alert Message Sent

The IDS compares all the packets entering the network with signatures stored in the database. An alert message is transmitted when a packet matches an attack signature or deviates from normal network use. The alert message goes to the IDS command console, where the network administrator can evaluate it.

IDS Responds

When the command console receives an alert message, it notifies the administrator of the alert through a pop-up window, and/or email message depending on how it is configured for alerts. However, if the administrator configured it to respond automatically, the IDS responds to the alert and takes a counter action such as dropping the packet, restarting the network traffic and more.

Administrator Assesses the Damage

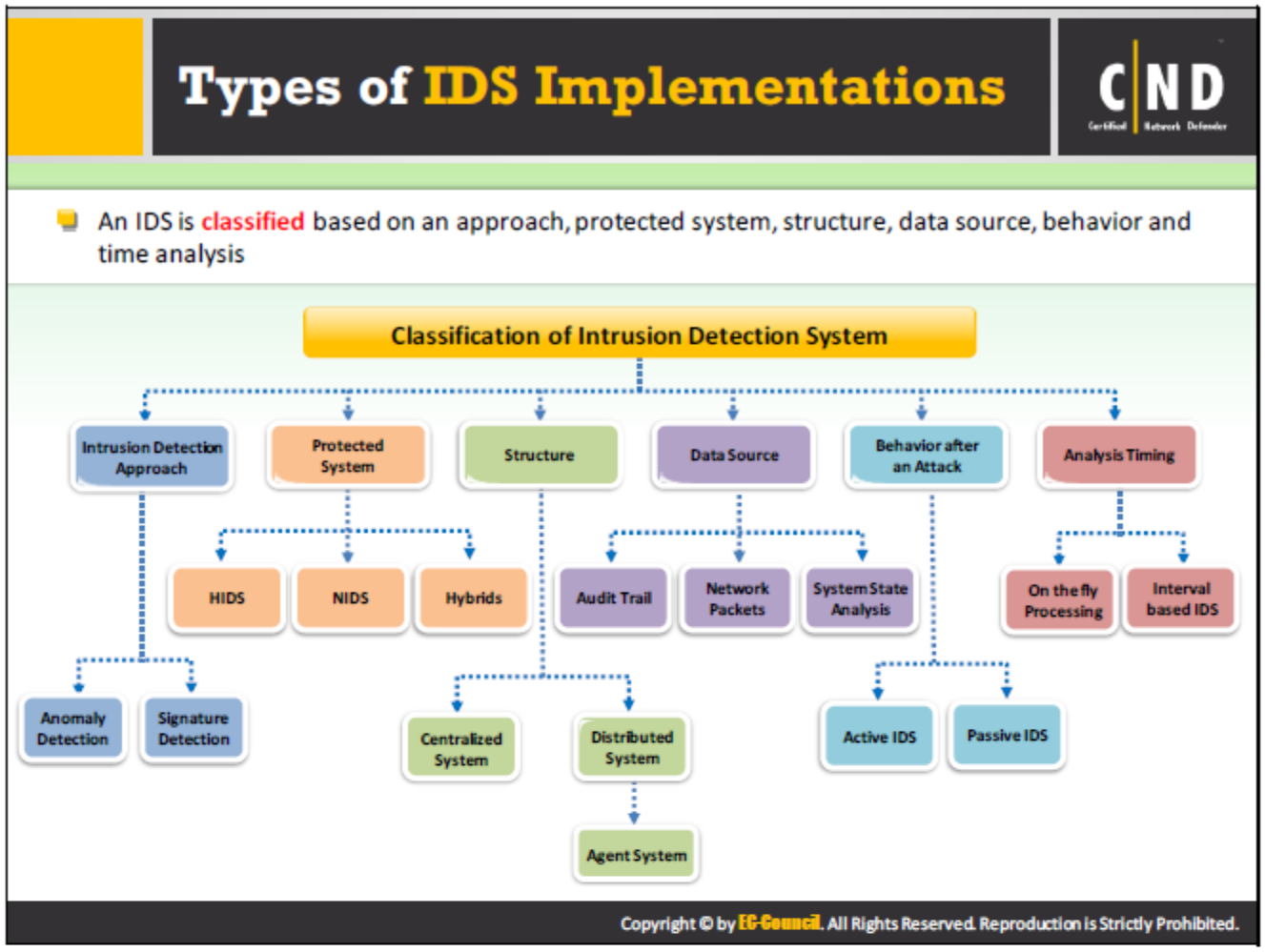
The network administrator has to monitor the IDS alerts and determine whether to take any countermeasures or not. The IDS sends alerts depending on the database information and these alerts can include false positives. Administrators need to update the signature database to eliminate the false positives alarms.

Escalation Procedures (if Necessary)

Escalation procedures are a set of actions written in the security policy and followed if the IDS detects a true positive (attack). These procedures vary depending on the severity of the incident.

Events are Logged and Reviewed

Administrators should maintain a log of any intrusion events detected and review them to decide on what countermeasures should be used for future events. These logs can assist administrators in updating the database of attack signatures with new events and to detect future attacks.



Generally, an IDS uses anomaly based detection and signature based detection methods to detect intrusions. Depending on the source of data an IDS uses or what it protects or other factors, they are classified as shown in following figure. This categorization depends on the information gathered from a single host or a network segment, in terms of behavior, based on continuous or periodic feed of information, and the data source.

Approach-based IDS

Signature-Based Detection

- Known as **misuse detection**
- **Monitors** patterns of data packets in the network and compares them to pre-configured network attack patterns, known as signatures
- This method uses string comparison operations to compare **ongoing activity**, such as a packet or a log entry, against a list of signatures

Advantages

- It detects attacks with minimal false alarms
- It can **quickly** identify the use of a specific tool or technique
- It assists administrators to quickly track any potential **security issues** and initiate incident handling procedures

Disadvantages

- This approach only detects **known threats**, the database must be updated with new attack signatures constantly
- It utilizes tightly defined signatures which prevent them from detecting **common variants** of the attacks

Examples of signatures are

- A telnet attempt with a username of 'root', which is a violation of the corporate security policy
- An operating system log entry with a status code of 645 indicates the host auditing system is disabled

Approach-based IDS (Cont'd)

Anomaly-based Detection

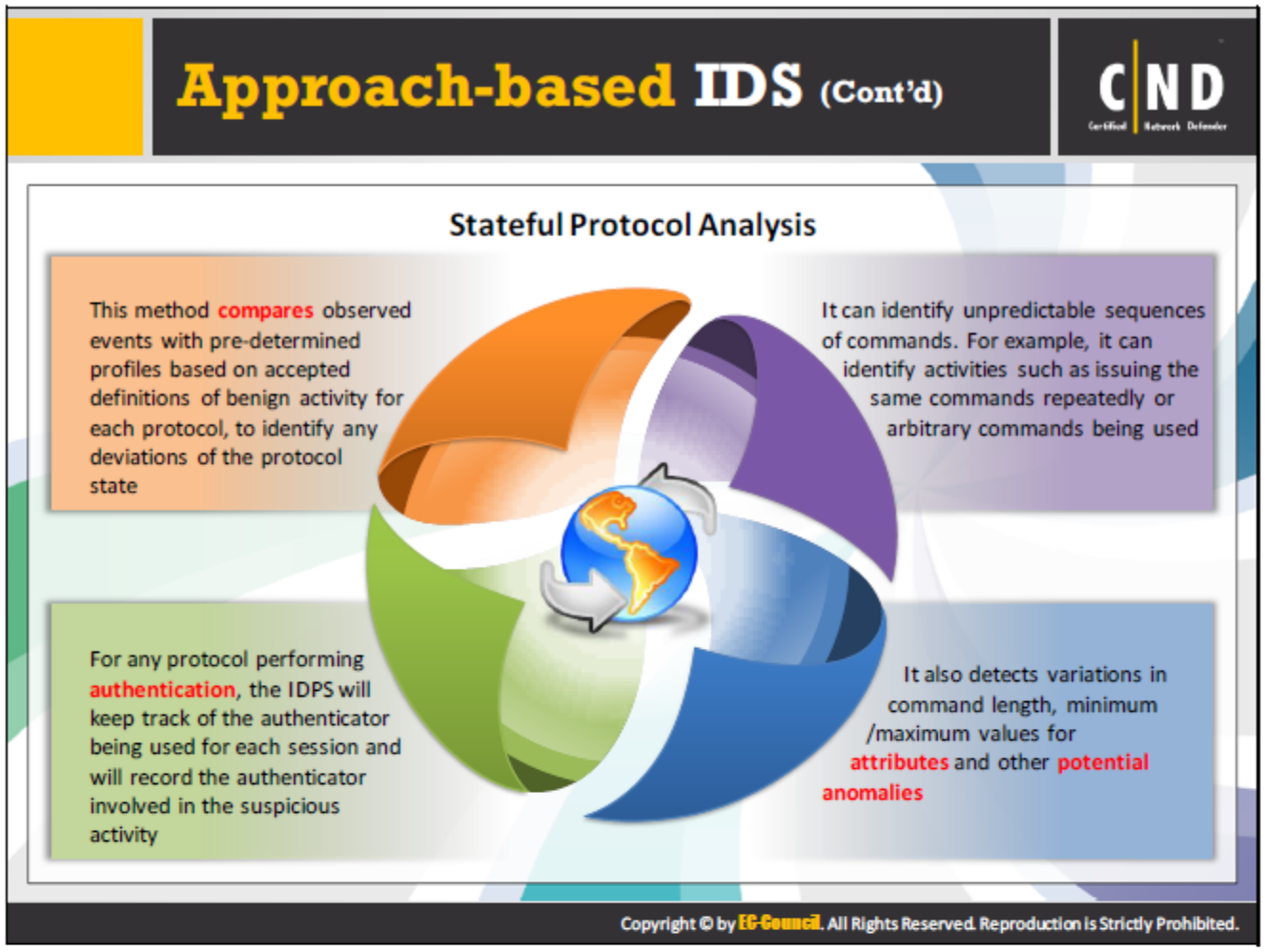
- In this approach, alarms for **anomalous** activities are generated by evaluating network patterns such as what sort of bandwidth is used, what protocols are used, what ports and which devices are connected to each other
- An IDS monitors the typical activity for a particular time interval and then builds the **statistics** for the network traffic
- An example: Anomaly-based IDS monitors activities for normal Internet bandwidth usage, failed logon attempts, processor utilization levels, etc.

Advantages

- An Anomaly based IDS identifies **abnormal** behavior in the network and detects the symptoms for attacks without any clear details
- Information acquired by anomaly detectors is further used to define the signatures for **misuse detectors**

Disadvantages

- The rate of generating **false alarms** is high, due to unpredictable behaviors for users and networks
- The need to create an **extensive set of system events** in order to characterize normal behavior patterns



Signature-Based Detection

A signature is a pre-defined pattern in the traffic on a network. Normal traffic signatures denote normal traffic behavior. However, attack signatures are malicious and are harmful to the network. These patterns are unique and the attacker uses these patterns to get in to the network.

Anomaly-Based Detection

The Anomaly-based detection process depends on observing and comparing the observed events with the normal behavior and then detects the deviation from it. The comparison provides an understanding of significant deviations in the events. The normal activity of an event depends on factors such as users, hosts, network connections and/or applications. These factors are considered only after examining a particular activity for a period of time.

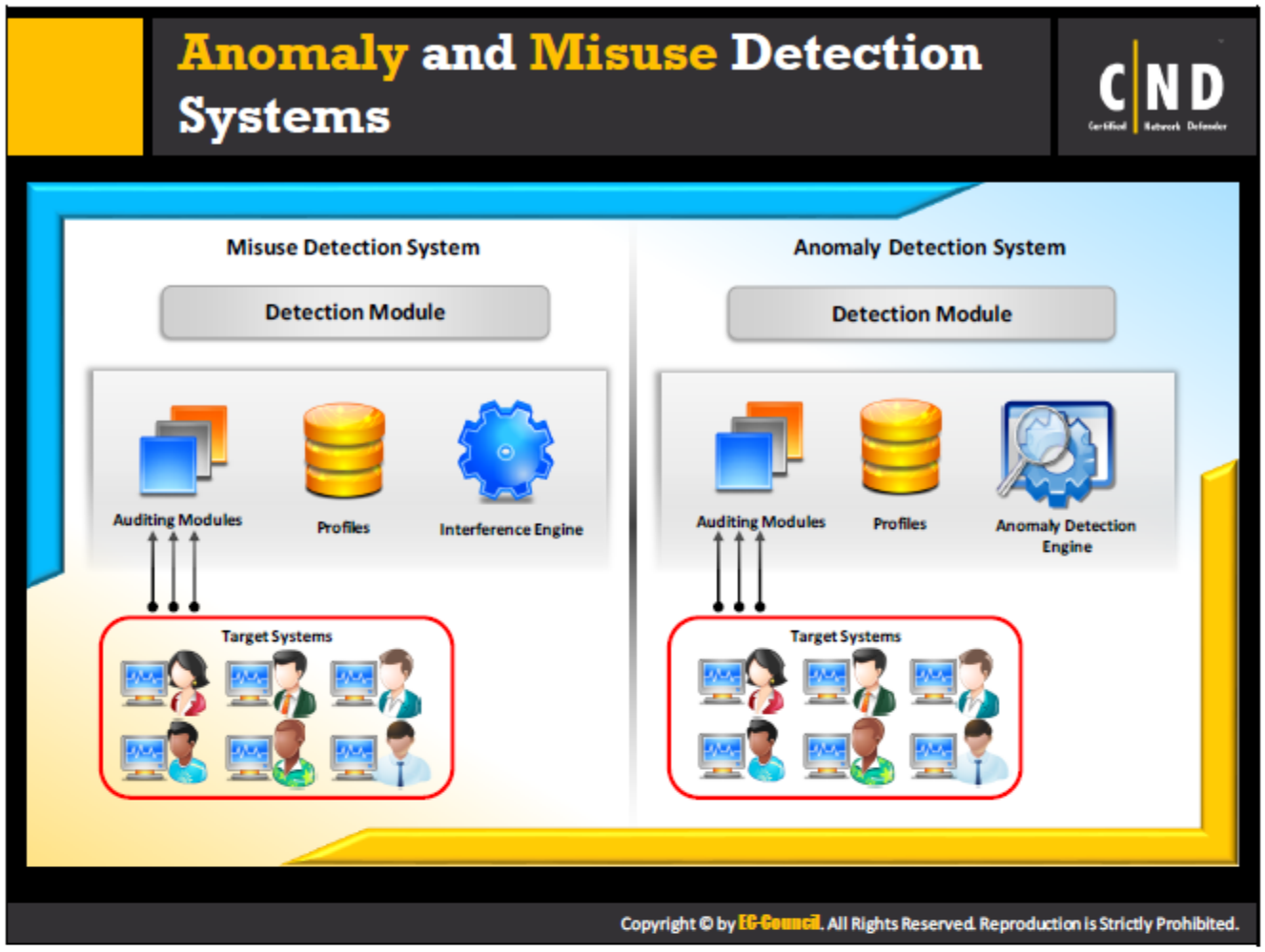
The normal behavior of traffic is based on various behavioral attributes. For example, normal email activity, reasonable failed attempts, processor usage. Any activity that does not match with normal behavior can be treated as an attack. For example, numerous emails coming from a single sender, a high number of failed login attempts can indicate suspicious behavior. Unlike signature-based detection, anomaly based detection can detect previously unknown attacks.

Stateful Protocol Analysis

Network communication uses various types of protocols to exchange information on different layers. These protocols define the accepted behavior. Stateful Protocol Analysis based IDS

detect the suspicious activity by analyzing the deviation for specific protocol traffic from its normal behavior. With this analysis, an IDS can analyze the network, transport and application layer protocols and traffic against their normal behavior.

There are certain IDSs that can specify the suitable activities for each class of users in accordance with the authenticator information.



Anomaly detection system

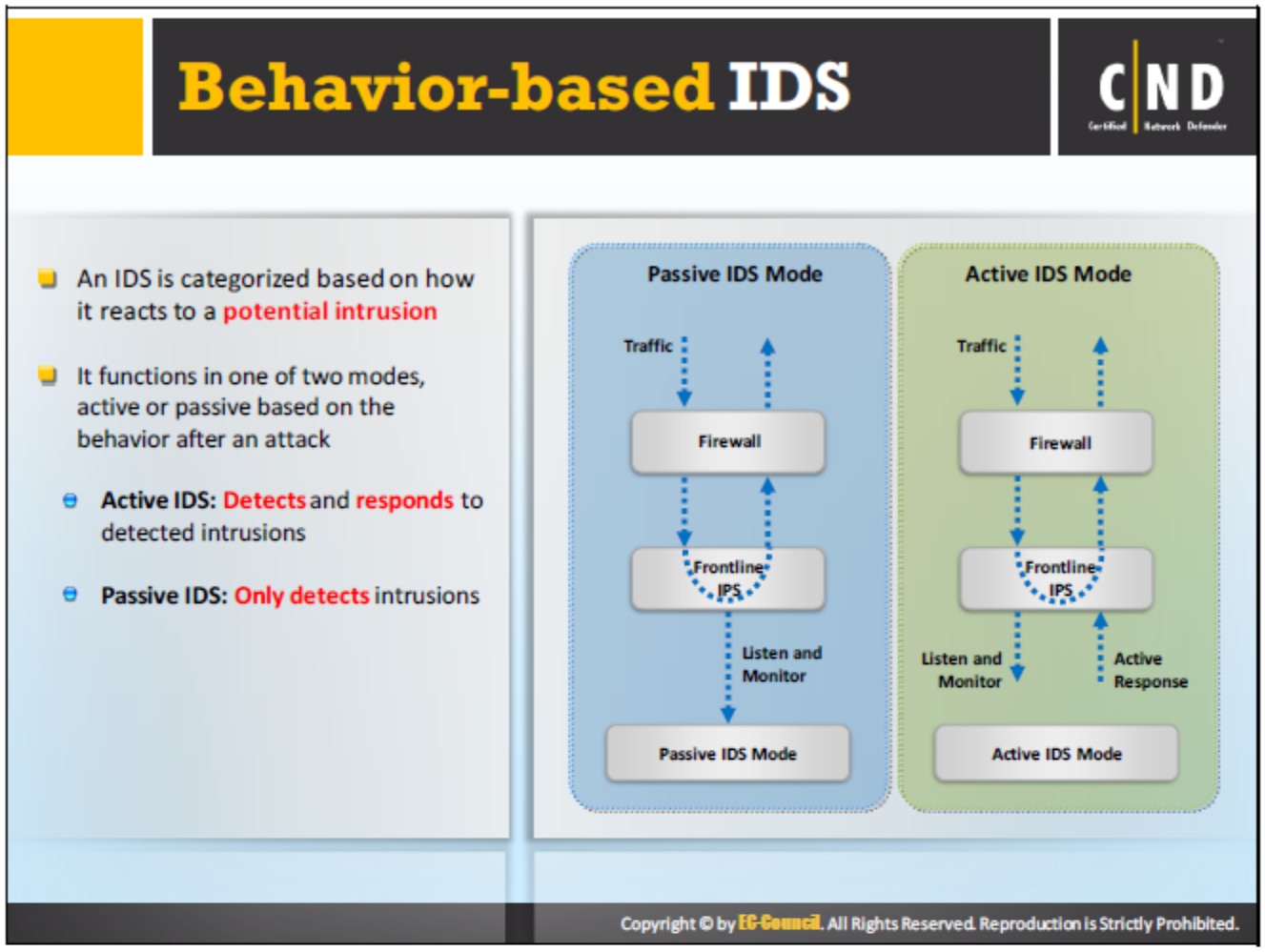
An anomaly detection system involves detecting intrusions on the network. It uses algorithms to detect discrepancies occurring in a network or system. It categorizes an intrusion as either normal or anomalous. Anomaly intrusion is a two-step process where, the first step involves gathering information of how data flows and the second step is, working on that data flow in real time. Detecting if the data is normal or not. By implementing this process, anomaly intrusion detection protects the target systems and networks that can prove vulnerable against malicious activities. You can detect anomalies in the system through artificial intelligence, neural networks, data mining, statistical method, etc.

- **Advantages:**
  - It detects and identifies probes in network hardware. Providing early warnings about attacks.
  - It has the ability to detect a wide range of attacks in the network.
- **Disadvantages:**
  - If a legitimate network behavior is not part of the designed model, the system will detect it as anomalous. This increases the number of false positive alerts in the system.
  - Network traffic varies and deployment of the same model throughout can lead to a failure in detecting known attacks.

Misuse detection system

In a Misuse detection system, first the abnormal behavior system is defined and then the normal behavior. A Misuse detection system has a static approach in detecting attacks. The Misuse detection system works differently to the anomaly detection system. The Misuse detection system has a low rate of false positive, as the rules are pre-defined. Misuse detection systems use methods like rule based languages, state transition analysis, expert system, etc.

- **Advantages:**
  - More accurate detection than an Anomaly detection system.
  - Has fewer false alarms.
- **Disadvantage:**
  - Unable to detect new attacks due to pre-defined rules.



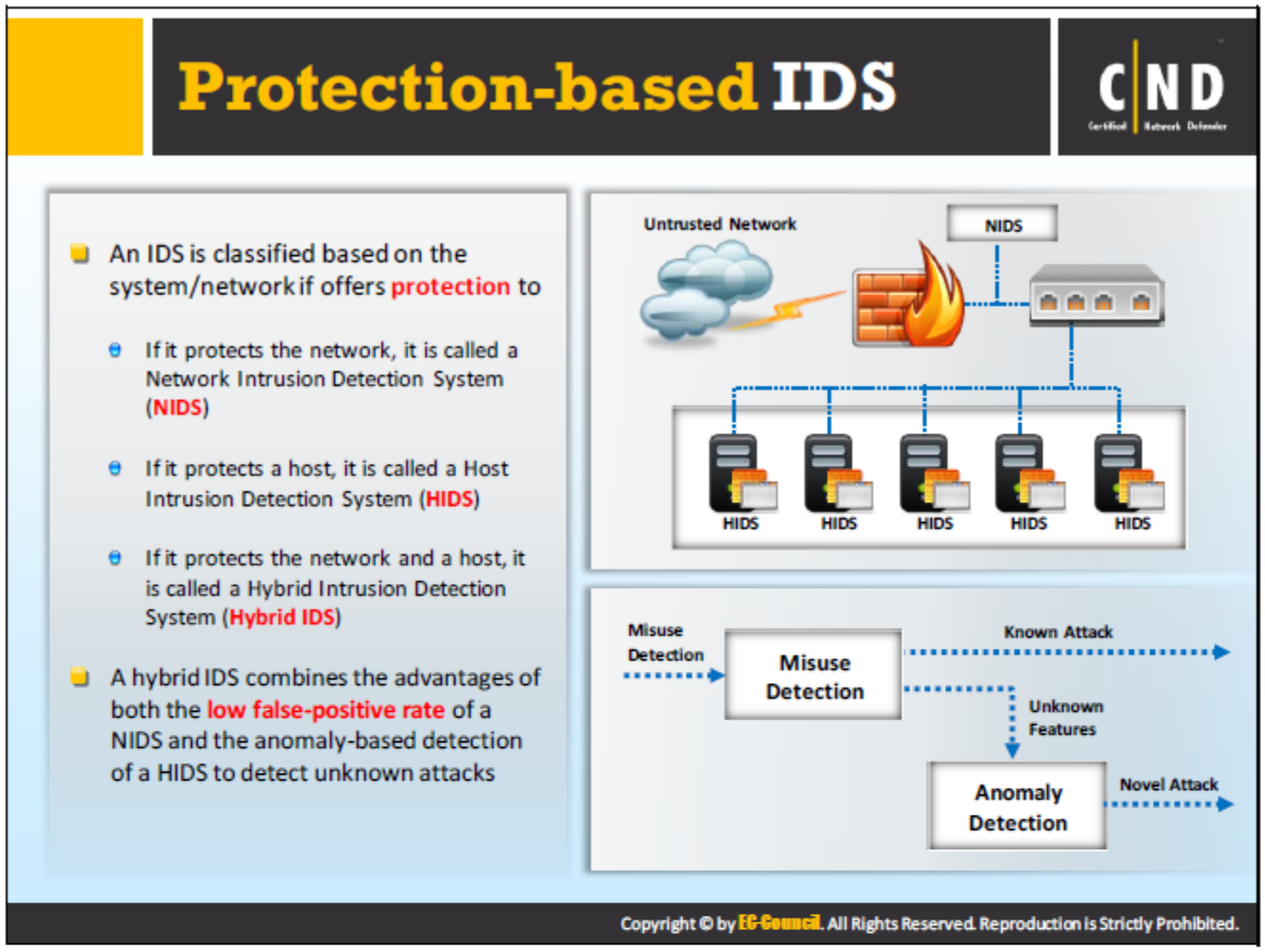
Behavior-based intrusion detection techniques assume an intrusion can be detected by observing a deviation from normal or expected behavior of the system or users. The model of normal or valid behavior is extracted from reference information collected by various means. The intrusion detection system later compares this model with current activity. When a deviation is observed, an alarm is generated. In terms of behavior, intrusion detection systems (IDS) are classified into two types: active and passive.

Active IDS

An Active intrusion detection system (IDS) is configured to automatically block suspected attacks without any intervention from the administrator. This type of an IDS has the advantage of providing real-time corrective action in response to an attack. An active IDS automatically takes action in response to a detected intrusion. The exact action differs per product and depends on the severity and type of the attack.

Passive IDS

A Passive intrusion detection system (IDS) is configured only to monitor and analyze network traffic activity, alert the administrator of any potential vulnerabilities and attacks. This type of IDS is not capable of performing any protective or corrective functions on its own. It merely logs the intrusion and notifies an administrator, through email or pop-ups. A system administrator or someone else will have to respond to the alarm, take appropriate action to halt the attack and possibly identify the intruder.



An IDS can be classified based on the device or network to which it offers protection. There are mainly three types of IDS technologies under this category which includes Network Intrusion Detection Systems (NIDS), Host Intrusion Detection Systems (HIDS) and Hybrid Intrusion Detection Systems (Hybrid IDS).

Network Intrusion Detection System (NIDS)

A NIDS is used to observe the traffic for any specific segment or device and recognize the occurrence of any suspicious activity in the network and application protocols. The NIDS is typically placed at boundaries between networks, behind network perimeter firewalls, routers, VPN, remote access servers and wireless networks.

Host Intrusion Detection Systems (HIDS)

A HIDS is installed on a specific host and is used to monitor, detect and analyze events occurring on that host. It monitors activities related to network traffic, logs, process, application, file access and modification on the host. The HIDSs is normally deployed on servers containing very sensitive information and publicly accessible servers.

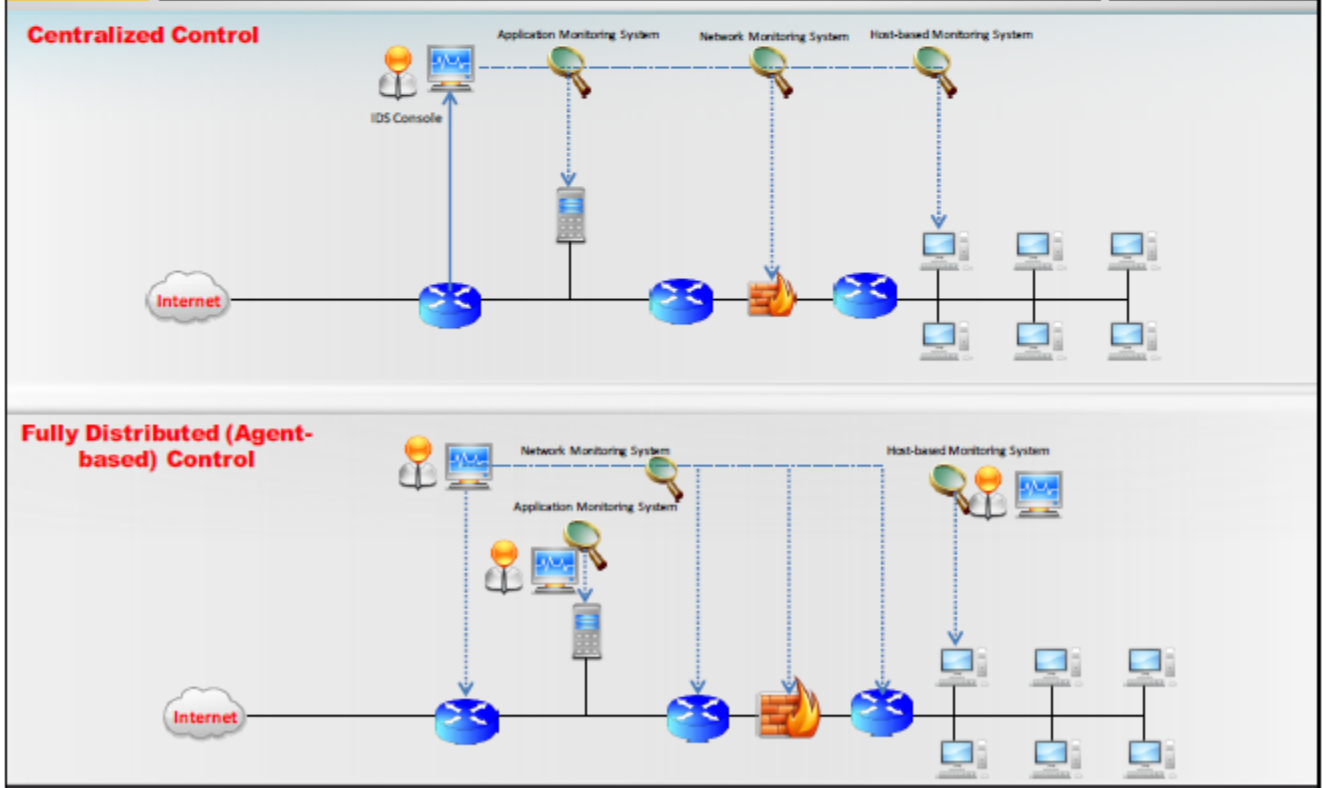
Hybrid Intrusion Detection Systems (Hybrid IDS)

A hybrid IDS is a combination of both HIDS and NIDS. It has its agent installed on almost every host in the network. It has the ability to work online with encrypted networks and storing data on a single host.

Structure-based IDS

1. An IDS is also classified as a Centralized IDS or a Distributed IDS, this classification is based on the structure of the IDS
2. In a centralized IDS, all data is shipped to a central location for analysis, independent of the number of hosts which are monitored
3. In a distributed IDS, several IDS are deployed over a large network and each IDS communicates with each other for traffic analysis

Structure-based IDS (Cont'd)



Depending on the structure, traditional IDSs can be categorized into two types:

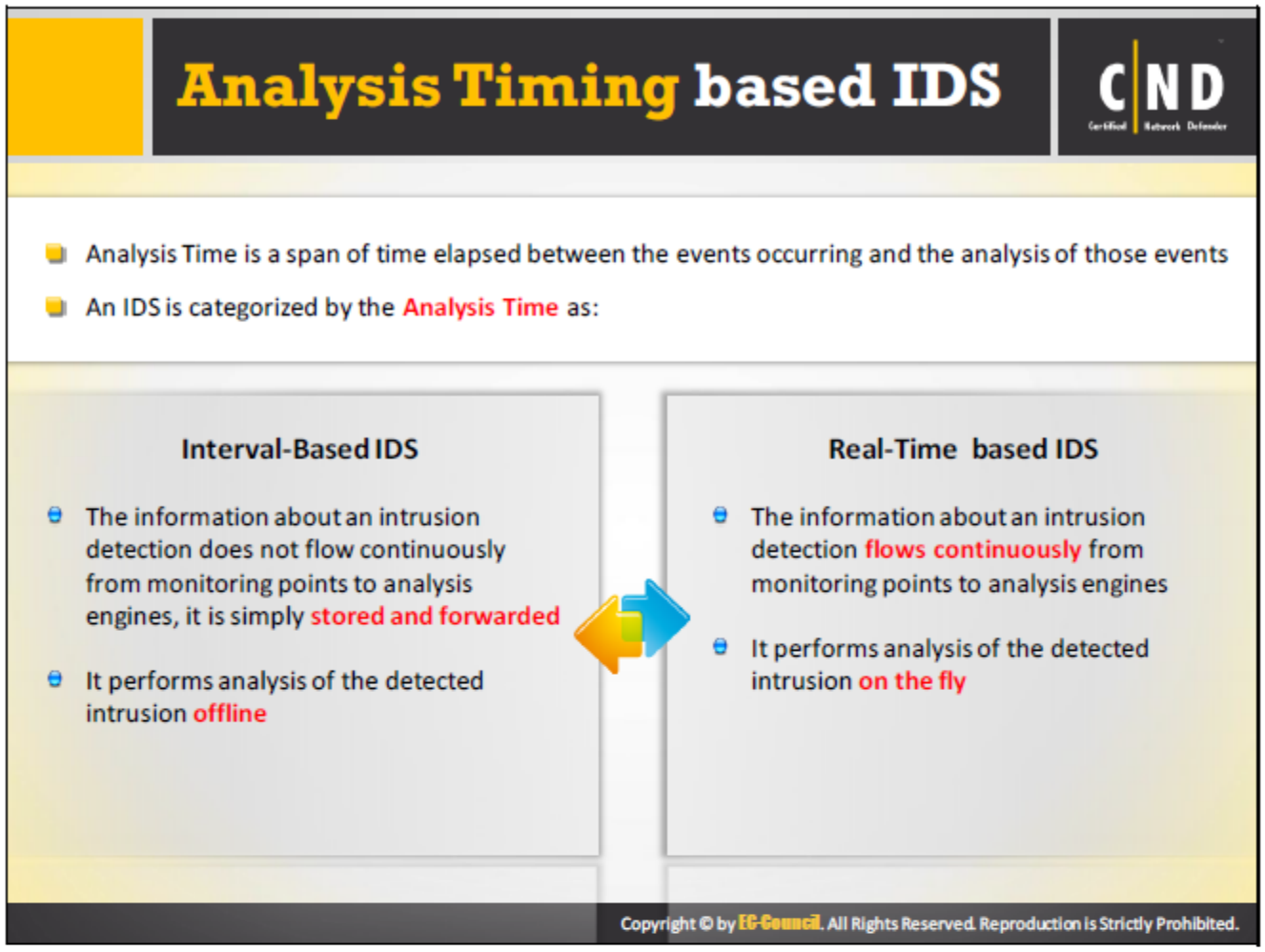
Distributed structure of an IDS

A Distributed Intrusion Detection System (dIDS) consists of multiple intrusion detection systems (IDS) over a large network. These systems communicate with each other, or with a central server that facilitates an advanced network of monitoring, incident analysis, and instant attack data. By having these cooperative agents distributed across a network, network operators can get a broader view of what is occurring on their network as a whole.

A dIDS also allows a company to efficiently manage its incident analysis resources by centralizing its attack records and by giving the analyst a way to spot new trends, patterns and identify threats to the network across multiple network segments.

Centralized structure of IDS

In centralized system, the data is gathered from different sites to a central site, central coordinator analyzes the data for checking the different intrusion. This type of IDS is designed for centralized systems. In a centralized IDS, data analysis is performed in a fixed number of locations, independent of how many hosts are being monitored. The centralized structure of an IDS can be harmed in a high-speed network as a result.



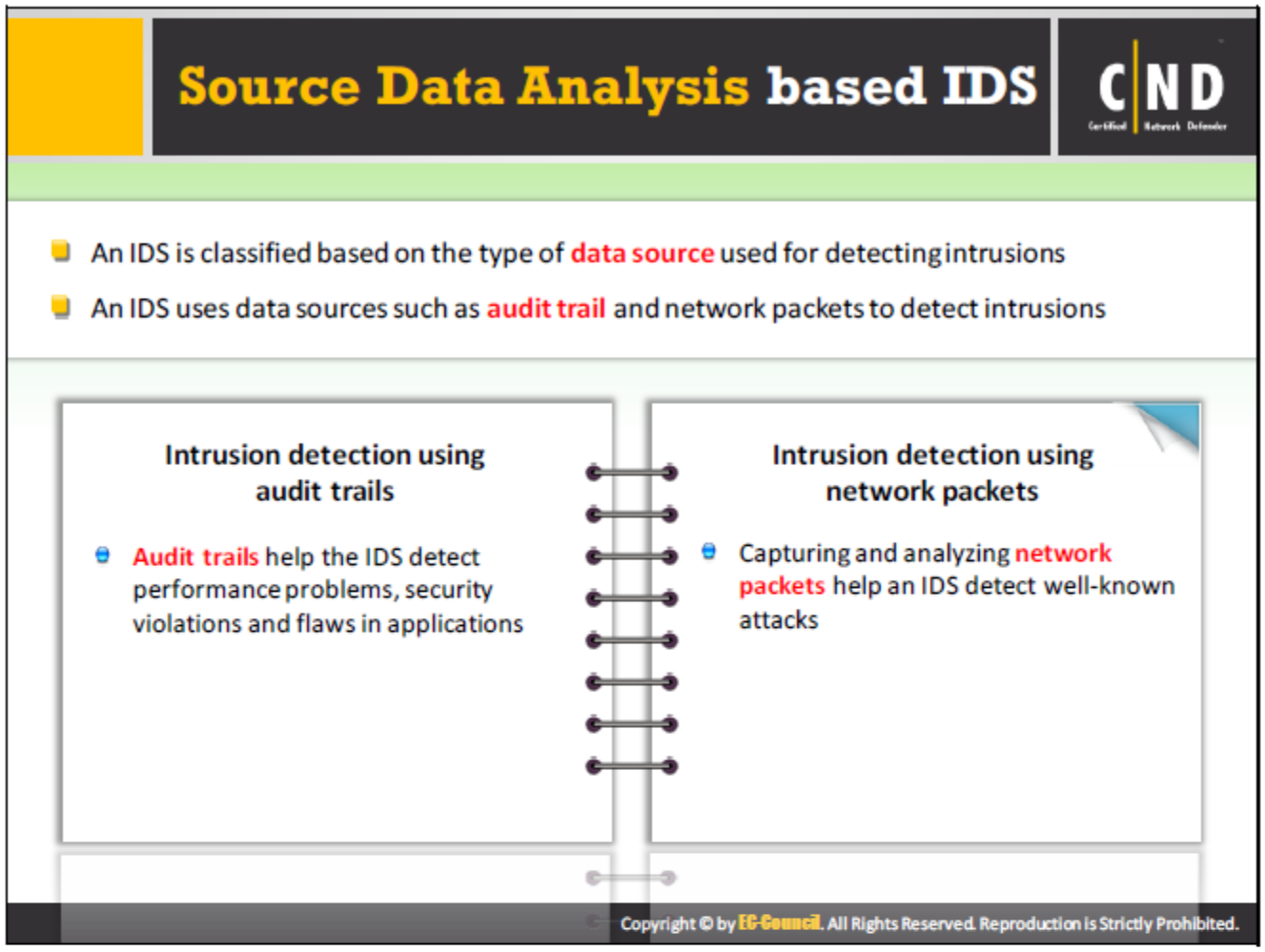
Analysis timing refers to the elapsed time between the occurrence of events and analysis of those events. Based on analysis timing, an IDS can be classified into two distinct types: Interval-Based IDS and Real-Time based IDS.

Interval-Based IDS

Interval based or offline analysis refers to the storage of the intrusion related information for further analysis. This type of IDS checks the status and content of log files at predefined intervals. The information flow from monitoring points to the analysis engine is not continuous. Information is handled in a fashion similar to "store and forward" communication schemes. Interval-based IDSs are prohibited from performing active responses. Batch mode is common in early IDS implementations because their capabilities did not support real time data acquisition and analysis.

Real-Time based IDS

Real-Time based IDS are designed for on the fly processing and are the most common approach for a network based IDS. They operate on a continuous information feed. Real-Time based IDS gathers and monitors information from network traffic streams regularly. Detection is performed by this type yields results quick enough to allow the IDS to take action affecting the progress of the detected attack. The IDS can conduct online verification of the events with the help of on-the-fly processing, and respond to them simultaneously. An IDS using this type of processing requires more RAM and a large hard drive because of the high data storage required to trace all of the network packets online.



Depending on the data source, an intrusion detection can be categorized into two types: Intrusion detection using audit trails and Intrusion detection using network packets.

Intrusion detection using audit trails:

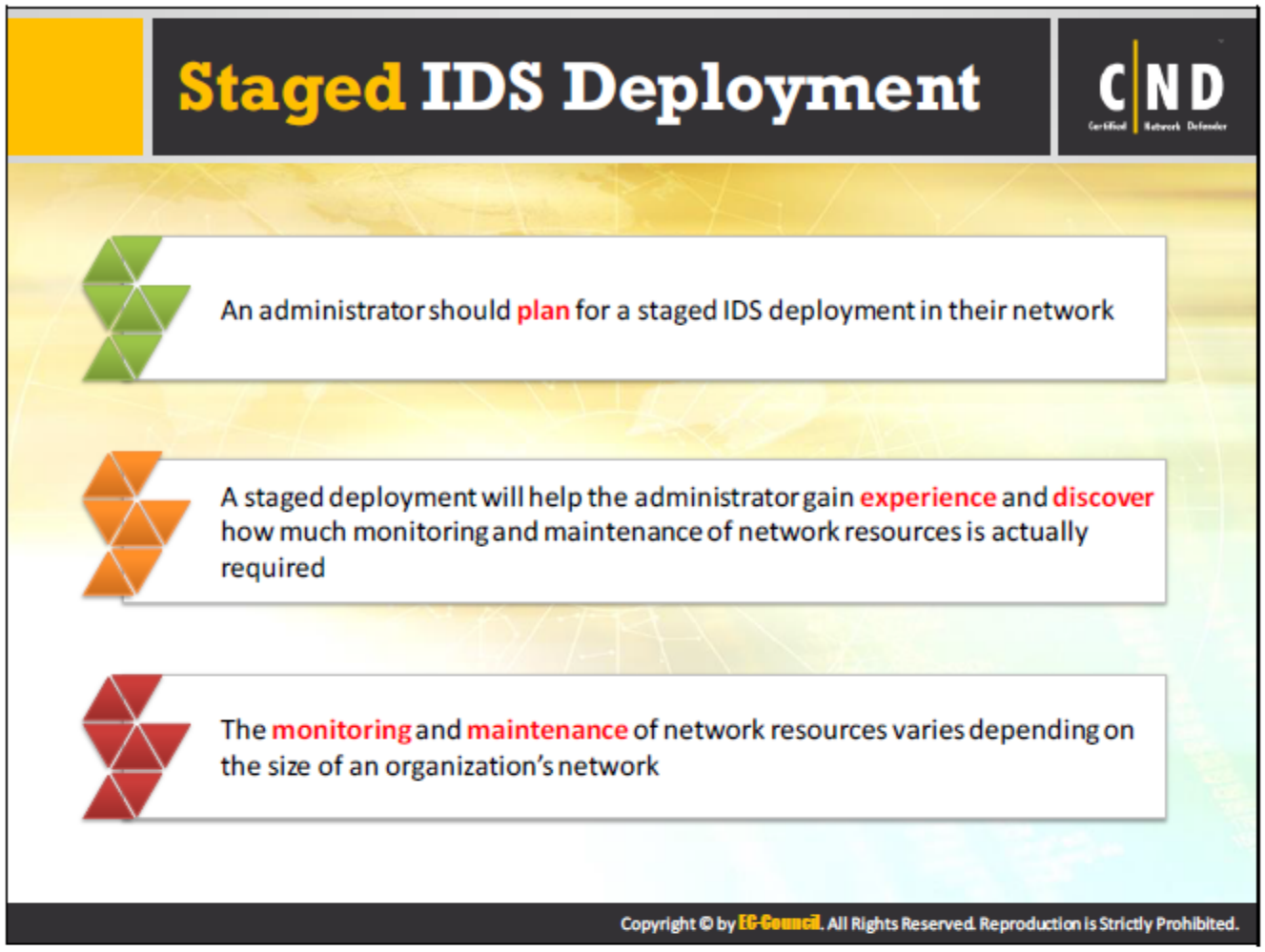
Audit trail is a set of records that provide documentary evidence of a system's activity by the system and application processes and user activity of systems and applications. Audit trails help the IDS in detecting performance problems, security violations, and flaws in applications. Administrators should avoid storage of audit trail reports in a single file to avoid intruders from accessing the audit reports and making changes.

- Audit systems are used to:
  - Watch file access
  - Monitor system calls
  - Record commands run by user
  - Record security events
  - Search for events
  - Run summary reports
- The reasons for performing audit trails are as follows:
  - Identifying the signs of an attack using event analysis.

- Identifying recurring intrusion events.
- Identifying system vulnerabilities.
- To develop access and user signatures.
- To define network traffic rules for anomaly detection-based IDSs.
- Provides a form of defense for a basic user against intrusions.

Intrusion detection using network packets:

A network packet is a unit of data transmitted over a network for communication. It contains control information in a header and user data. The header of the packet contains the address of the packet's source, destination and the payload is the body of the packet storing the original content. The header and the payload of a packet can contain malicious content sent by attackers. Capturing these packets before they enter their final destination is an efficient way to detect such attacks.



Before effectively deploying an IDS, administrators have to understand their network infrastructure and organizational security policies. The organization should consider a staged deployment of an IDS. The initial deployment of an IDS requires high maintenance. Then the organization can think of implementing an IDS at the next stage. The staged deployment helps the organization discover exactly where they need security for the IDS. Implementing an IDS across the organization's network is advisable when they are able to handle the IDS alerts from different sensors placed at various places. The staged deployment provides administrators enough time to think and get used to the new technology. This staged approach is beneficial to those evaluating and investigating IDS alerts and IDS logs.

Deploying Network-based IDS

An effective deployment of NIDS requires a lot of attention concerning the network topology of the organization

An administrator is required to consider IDS deployment options and all the advantages/disadvantages associated with each location

Consider all possible options when placing a network-based IDS

Deploying Network-based IDS (Cont'd)

Location 1

Place an IDS sensor behind each external firewall and in the network DMZ

Advantages:
- Monitors attacks originating from the outside world
- Highlights the inability of the firewall and its policies to defend against attacks
- It can see attacks which target the web or FTP servers located in the DMZ
- Monitors outgoing traffic results from a compromised server

Location 2

Place an IDS sensor outside an external firewall

Advantages:
- Ability to identify the number and types of attack originating from the Internet to the network

Location 3

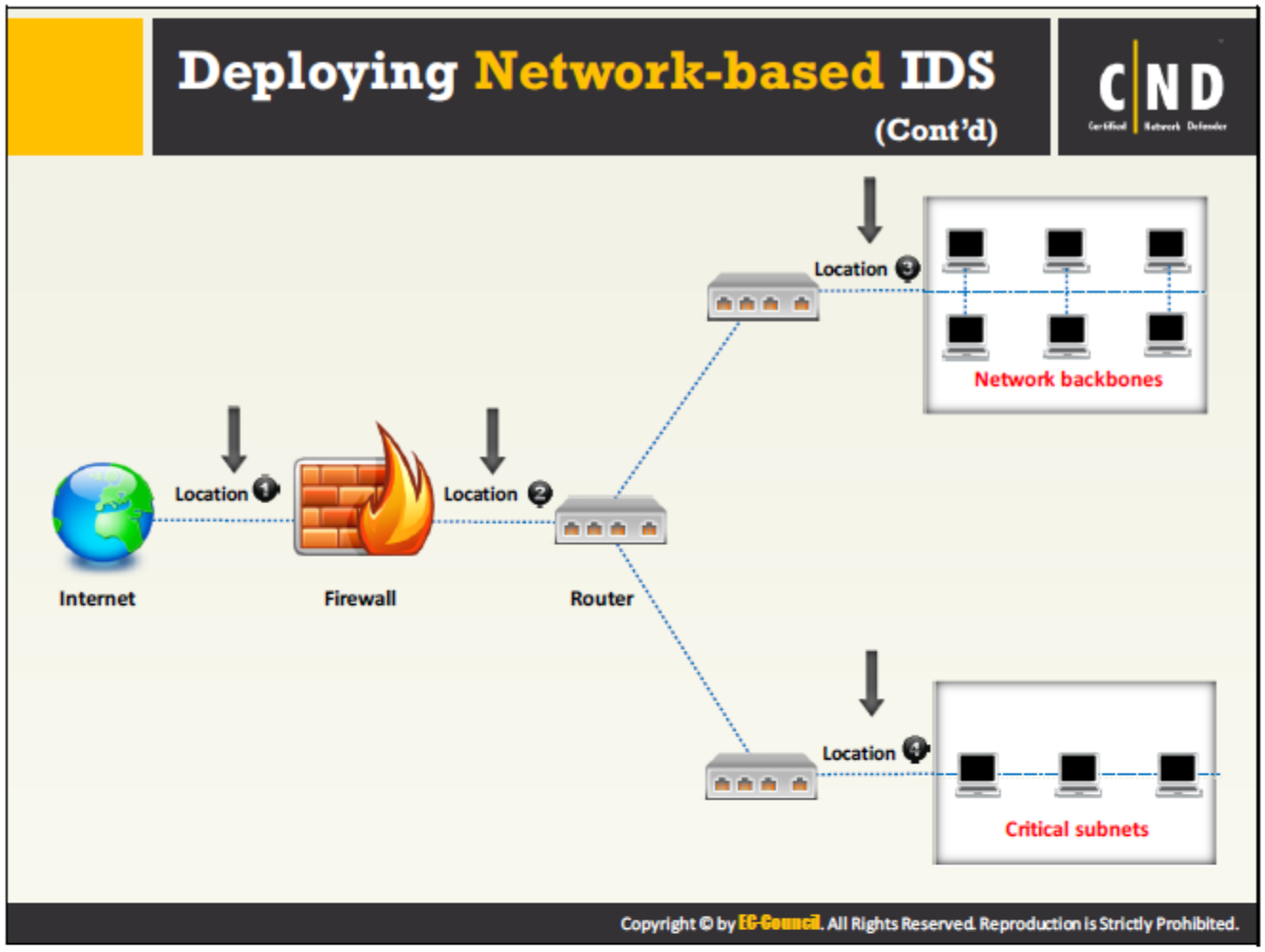
Place an IDS sensor on major network backbones

Advantages:
- Monitors and inspects large amounts of traffic, increasing the chance for attack detection
- Detects unauthorized attempts from outside the organization

Location 4

Place an IDS sensor on critical subnets

Advantages:
- Detects attacks on critical systems and resources
- Focuses on specific critical systems and resources



As a NIDS protects multiple hosts from a single location, the administrator can also consider customizing the NIDS to provide security for the entire network. The administrator should consider deploying an IDS management console before adding its sensors.

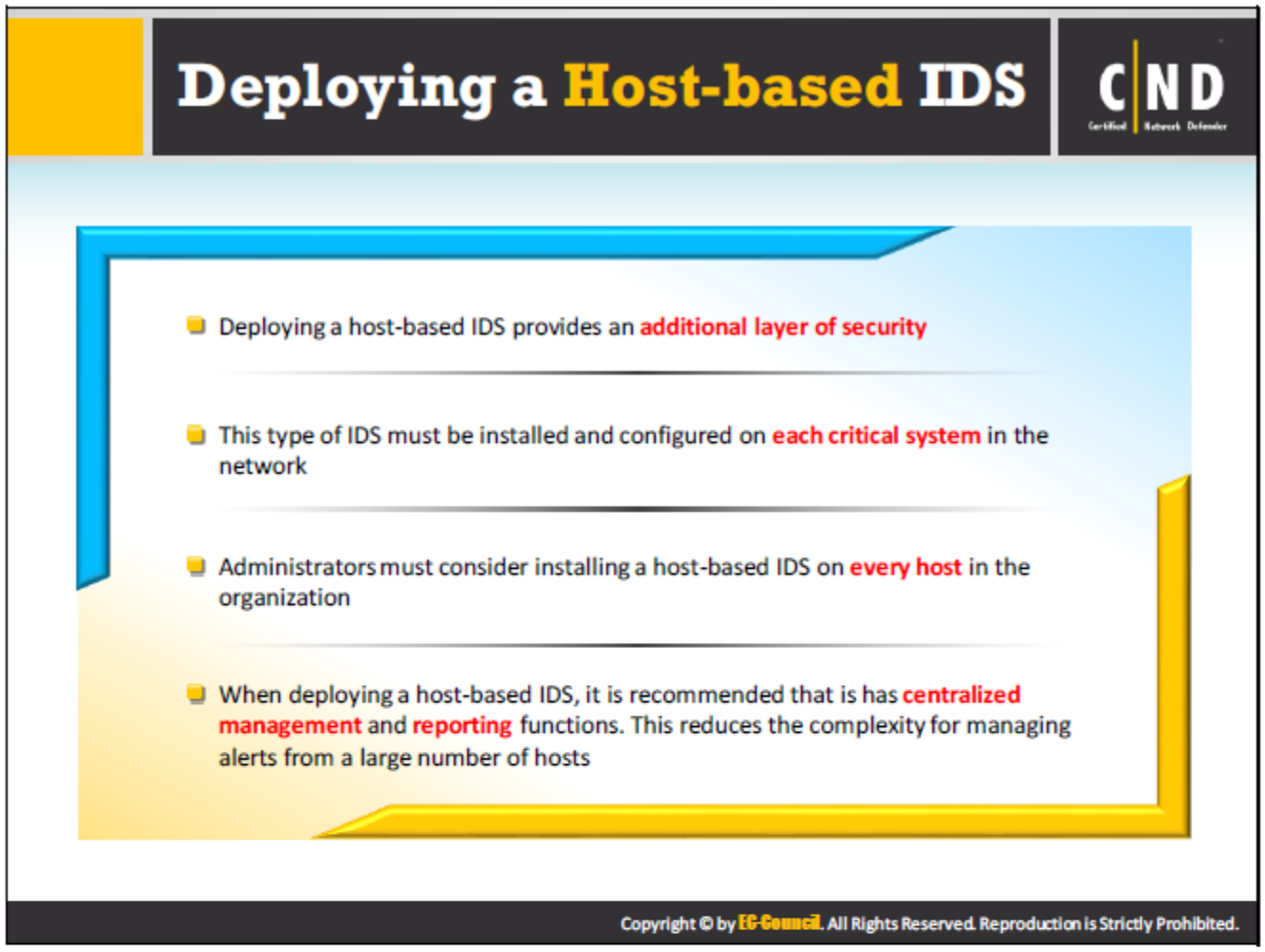
Administrators need to incrementally deploy IDS sensors throughout the network. Administrators must consider various factors such as the difference in traffic, logging, reporting, and alerts received when they deploy a new sensor for an IDS.

Different options for the deployment of sensors in the network include:

- **Location 1:** The sensor is placed outside the organizational network and perimeter firewall. The sensor placed at this location can detect inbound attacks. They are also configured to detect outbound attacks. The sensors are configured to detect the least sensitive attacks to avoid false alarms. These sensors are configured to only log the attack attempts, instead of sending alerts out for them.
- **Location 2:** This location is ideal for securing the perimeter network as well as identifying those attacks that bypass the external firewall. The NIDS sensor secures web, FTP and other servers located on the perimeter of the network. The NIDS sensors detect attacks with low to moderate impact in order to avoid the chances of generating false alarms. The sensors placed here also have the ability to monitor for outbound attacks.
- **Location 3:** The sensor placed at this location is used to secure the internal network of the organization. It detects the attack that bypasses the internal firewall. Sensors at this

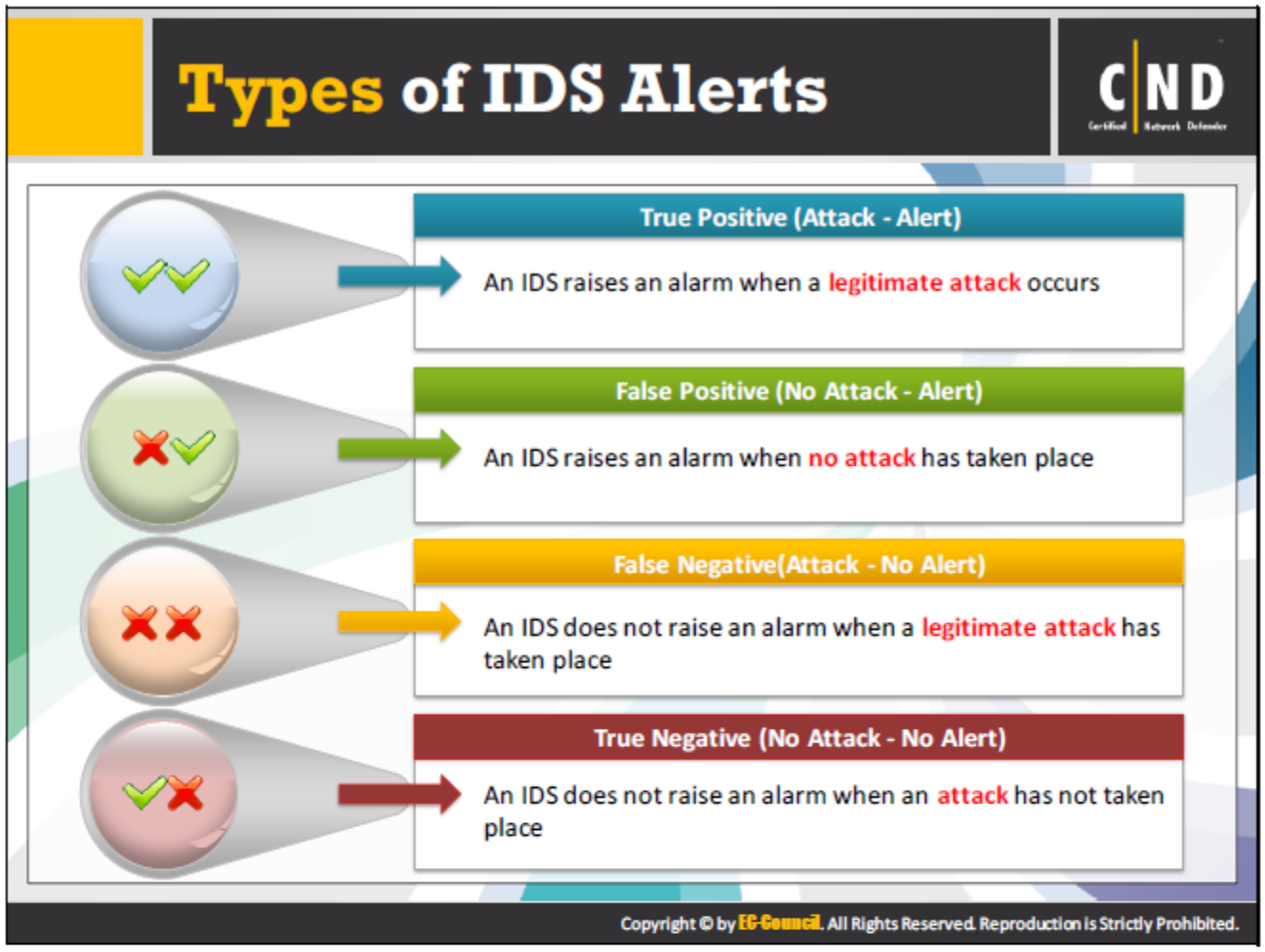
location are capable of detecting both inbound and outbound attacks. These sensors are configured to detect medium to high impact level attacks.

- **Location 4:** The sensors at this location are used to protect sensitive hosts in the network. It may include critical servers. These sensors are capable of detecting both inbound and outbound attacks. These sensors are configured to detect high impact level attacks.



Host-based IDS deployment is done with a proper plan and care, as deploying these types of IDS on a large scale environment have the potential to generate numerous false alarms. It is quite difficult to manage such a huge amount of false alarms. Initial deployment of a HIDS is done on critical servers only. Administrators must consider implementing an IDS management console before adding additional hosts.

If an administrator comfortably manages the HIDS on critical servers at the initial stage, then and only then can they consider deploying the HIDS on all remaining hosts in the network. This allows an administrator to provide security at the individual host level. However, deploying HIDS on every host on the network is quite expensive and requires additional software and maintenance especially in those cases of a wide-scale HIDS deployment.



An IDS generates four types of alerts which include: True Positive, False Positive, False Negative and True Negative.

True Positive (Attack - Alert)

A true positive is a condition occurring when an event triggers an alarm and causes the IDS to react as if a real attack is in progress. The event may be an actual attack, in which case an attacker is actually making an attempt to compromise the network, or it may be a drill, in which case security personnel are using hacker tools to conduct tests of a network segment.

False Positive (No attack - Alert)

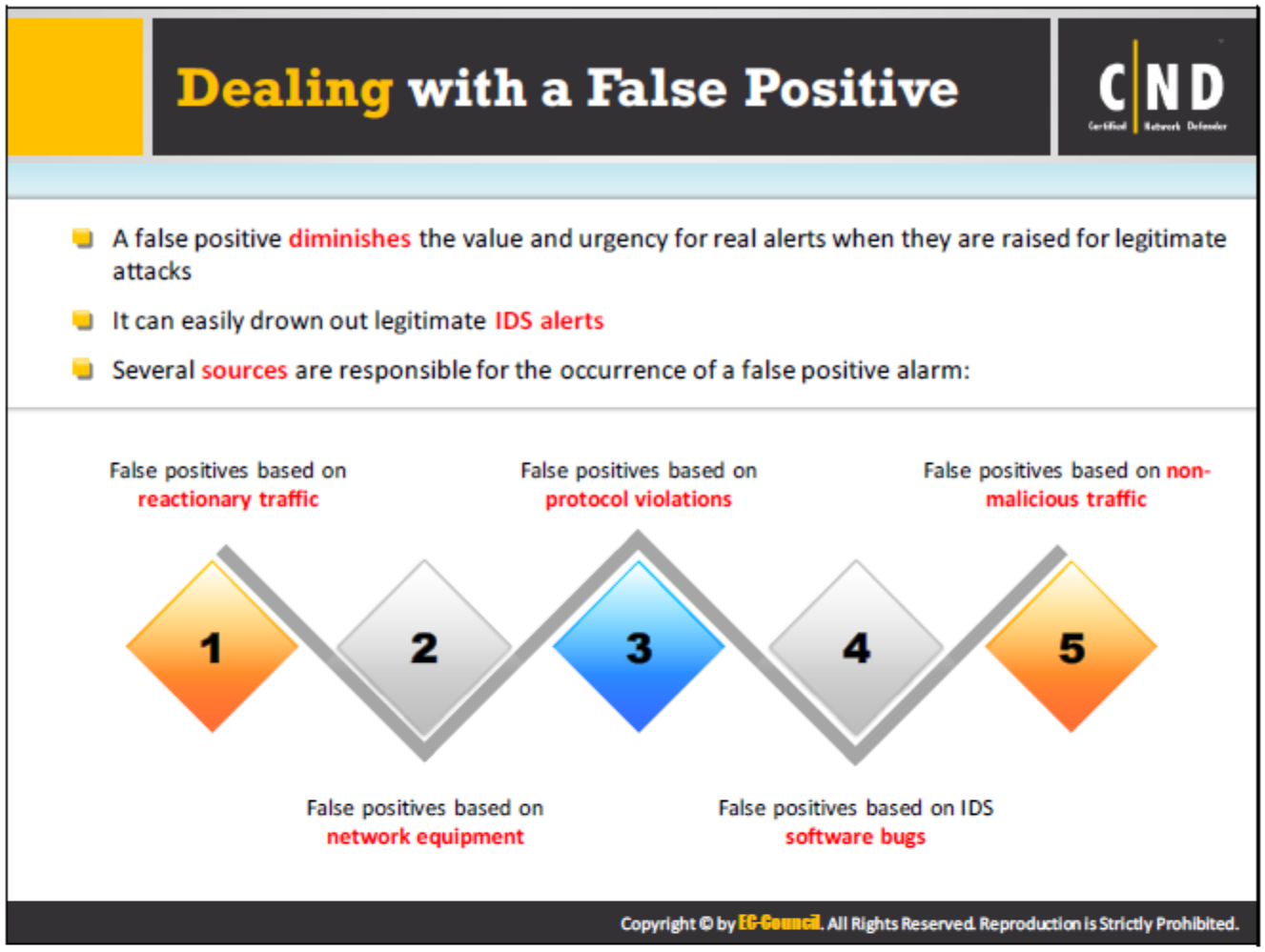
A false positive occurs if an event triggers an alarm when no actual attack is in progress. A false positive occurs when an IDS treats normal system activity as an attack. False positives tend to make users insensitive to alarms and reduce their reactions to actual intrusion events. While testing the configuration of an IDS, administrators use false positives to determine if the IDS can distinguish between false positives and real attacks or not.

False Negative (Attack - No Alert)

A false negative is a condition occurring when an IDS fails to react to an actual attack event. This is the most dangerous failure, since the purpose of an IDS is to detect and respond to attacks.

True Negative (No attack - No Alert)

A true negative is a condition occurring when an IDS identifies an activity as acceptable behavior and the activity is actually acceptable. A true negative is successfully ignoring acceptable behavior. It is not harmful as the IDS is performing as expected.



In a false positive alarm an IDS raises an alarm on a non-malicious event. As false positive alarm triggers during unjustified alerts, they cause more chaos in the organization. They nullify the urgency and the value of the real alerts, leading to ignoring the actual alarm situation.

- Causes of a False positive alarm:

  1. **A network traffic false alarm:** A network traffic false alarm triggers when a non-malicious traffic event occurs. A great example of this would be: an IDS triggers an alarm when the packets do not reach the destination, due to network device failure.
  2. **A network device alarm:** An IDS triggers a network device alarm when the device generates unknown or odd packets. E.g. load balancer
  3. **An Alarm caused by an incorrect software script:** If poorly written software generates odd or unknown packets, an IDS will trigger a false positive alarm.
  4. **Alarms caused by an IDS bug:** A software bug in an IDS will raise an alarm for no reason.

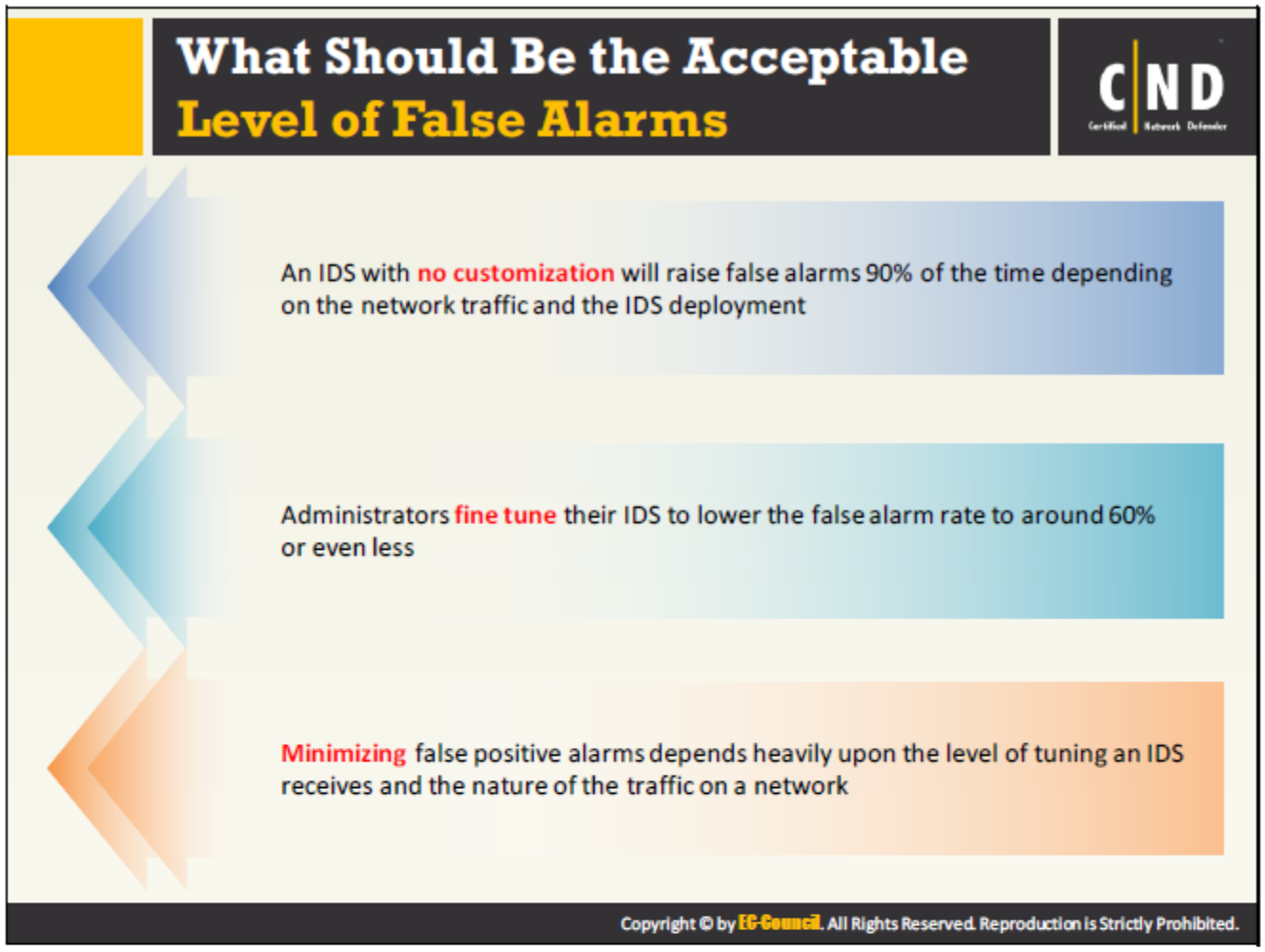
- Reducing false positive alarms:

  To reduce false positive alarms it is important to understand the weakness of the device. Implementing effective countermeasures can help reduce the occurrences of false positive alarms.

  1. **Differentiating Alerts:** Administrators distinguish the important priority alerts against the less important ones. One of the methods used, is to verify the alerts with an alert

triggered earlier. For example, a specific signature triggering an alert at regular intervals can be termed as an important alert. For future reference, the administrator can maintain logs of these alerts. They can also classify the alerts based on their behavior. For instance, classification is done based of normal behavior, intrusion behavior and suspicious behavior occurring in the network.

2. **Aggregating the Alerts:** A single intrusion can create multiple alerts with generic features. Aggregating the alerts helps to reduce the alert volume belonging to the same attack. These aggregators create sub-aggregators which simplify the process of alert aggregation.

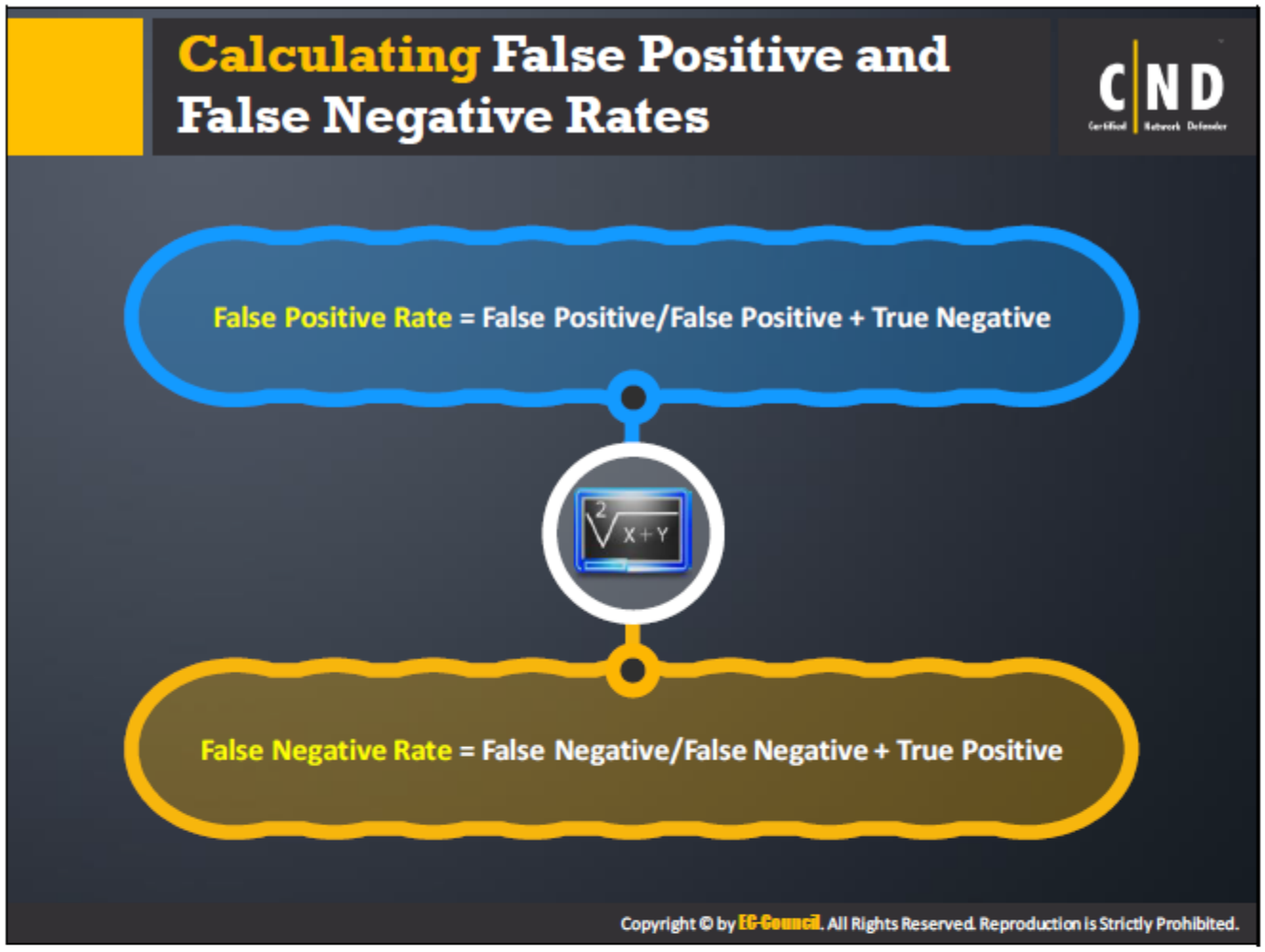


If the number of intrusions in a network is low, compared to the network usage, the rate of false alarms will be high. It is important to keep the false positive rate as minimal as possible. At times an IDS will ignore half of the network traffic, tuning is not the only option. An effective implementation of an IDS inspects both the incoming and outgoing traffic for anomalies. Based on the organization's network tolerance towards false positives, administrators can set up a threshold level for the IDS.

The amount of false alarms depends on two phases:

1. The detection phase: To bring false alarms down to acceptable levels, administrators enhance the configuration of the IDS and change the detection approach methods. The higher the detection rate and accuracy, the lower the amount of false alarms will be. Techniques like data mining and data clustering reduce the amount of false alarms.
2. The alert processing phase: Alert processing studies the cause of false alarms, recognizes the high amount and uses case scenarios to subsequently provide a coherent response to the alarm. Alert processing techniques like statistical filtering and fuzzy alert aggregation help identify the sequences for false alarms, filters and later discards them from the system.

Based on the organization's network tolerance, administrators can reduce false alarms by raising the threshold level of the IDS. The threshold level depends on two statistics called sensitivity and specificity of the IDS. Sensitivity displays a graph on the legitimacy of alerts detected by the IDS. Specificity filters the accuracy of the alerts detected in the IDS.



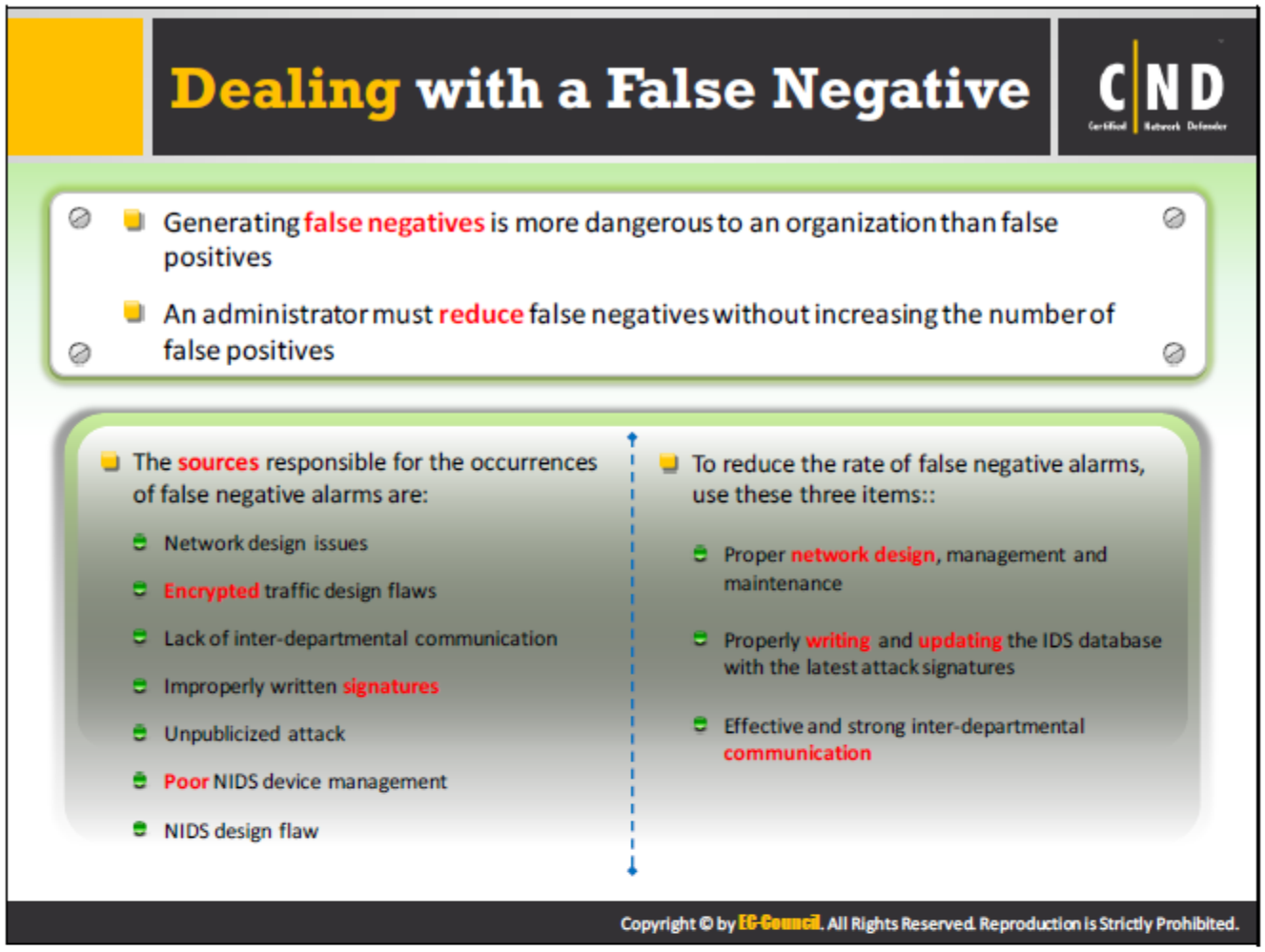
The false positive and false negative rates for a specific IDS are calculated with a certain formula. This formula will help calculate the rate of each for your IDS solution and by fine tuning the IDS, will reduce both of these rates.

False Positive Rate

- False Positive rate = False Positive/(False Positive + True Negative).

False Negative Rate

- False Negative rate = False Negative/(False Negative + True Positive).



A false negative is a more complex issue than a false positive. In a false negative, the intrusion detection system does not detect the legitimate attacks on the network.

Some of the causes behind generating False Negative alarms are:

- **Network setup issue**: Network flaws involving improper port spanning on switches and network traffic imbalance. Failure of NIDS devices to detect incoming and outgoing network traffic due to multiple entry points is one of the causes of a false negative alert. Improper configuration of an IDS will also raise a false negative alert.
- **Encrypted Traffic design flaws**: An IDS is not capable of detecting intrusions when encapsulated in encrypted traffic, it is not possible to match encrypted traffic to signatures. It is advisable to place an IDS behind a VPN termination with SSL encryption.
- **Misleading signatures:** If the signatures are not correctly written it can mislead in determining the attacks. Vendors cannot create signatures of those attacks which they are not aware. Occasionally even the tools are incapable of determining the legitimate signatures.

Dealing with False Negative alarms:

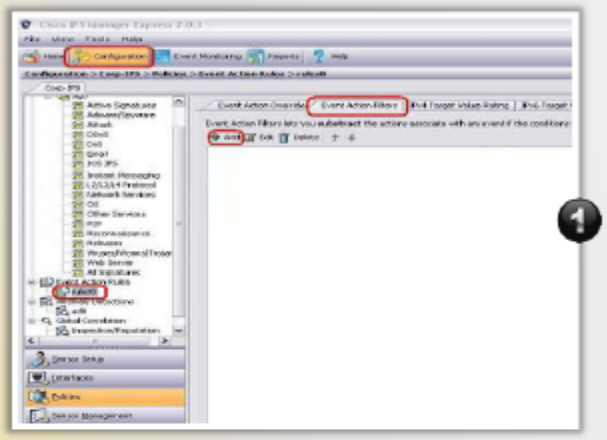
To reduce false negative alerts, it is important to understand them and implementation issues of the device. The effective ways to deal with false negative alerts are listed below:

- **Appropriate Network Design:** The primary requirement for minimizing a false negative alert is to set up a proper network design. The network design should be parallel to the security policies of the organization.
- **Proper placement of an IDS:** The proper placement of an IDS is behind the firewall. This will raise the alerts against port scans, automated scans and denial of service attacks. The IDS should also be configured to detect illegitimate signatures.
- **Network Analysis:** Active network analysis and monitoring will minimize the false negative alert. For this, administrators can utilize various network analysis tools or utilities. The IDS should also be configured to nullify false negative alerts from triggering the rules set on it.
- **Inclusion of additional data:** False alerts can be reduced by including additional data about the network in the security event. The additional information includes information about the organization's assets, users, networks and network device sources. Inclusion of this additional data can be through automated or manual processes.

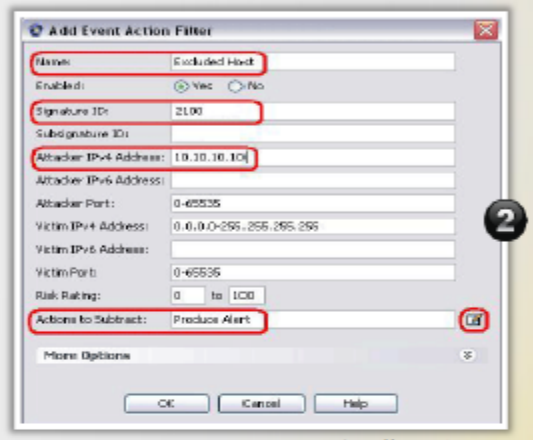
Excluding False Positive Alerts using Cisco Secure IPS

- Exclude signatures from or to a specific host or network address from generating false alarms
- An IPS will not generate an alarm or log records when an excluded signature triggers
- Steps to exclude a specific host (source IP address) from generating a specific signature alarm:

- Go to Configuration → Corp-IPS → Policies → Event Action Rules > rules0, and click the Event Action Filters tab and click Add



- Type the filter name, signature ID, attacker's IPv4 address, and action to subtract in the appropriate fields, and then click OK

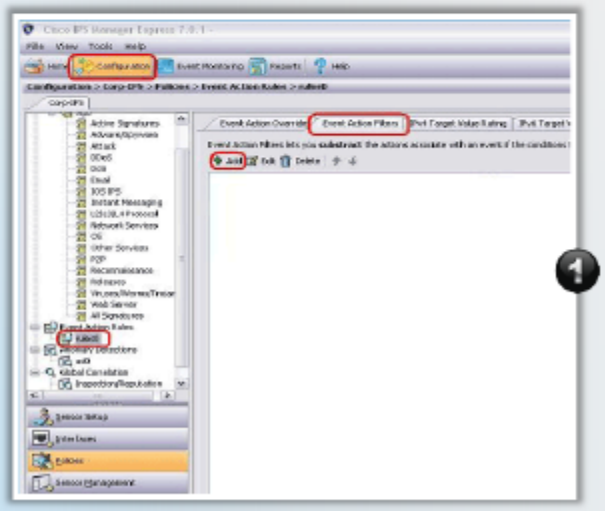


http://www.cisco.com

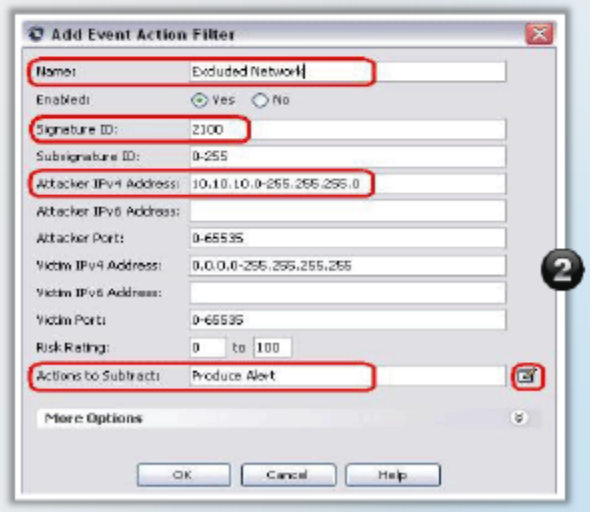
Excluding False Positive Alerts using Cisco Secure IPS(Cont'd)

- Steps to exclude a network from generating a specific signature alarm:

- Go to Event Action Filters tab and click Add



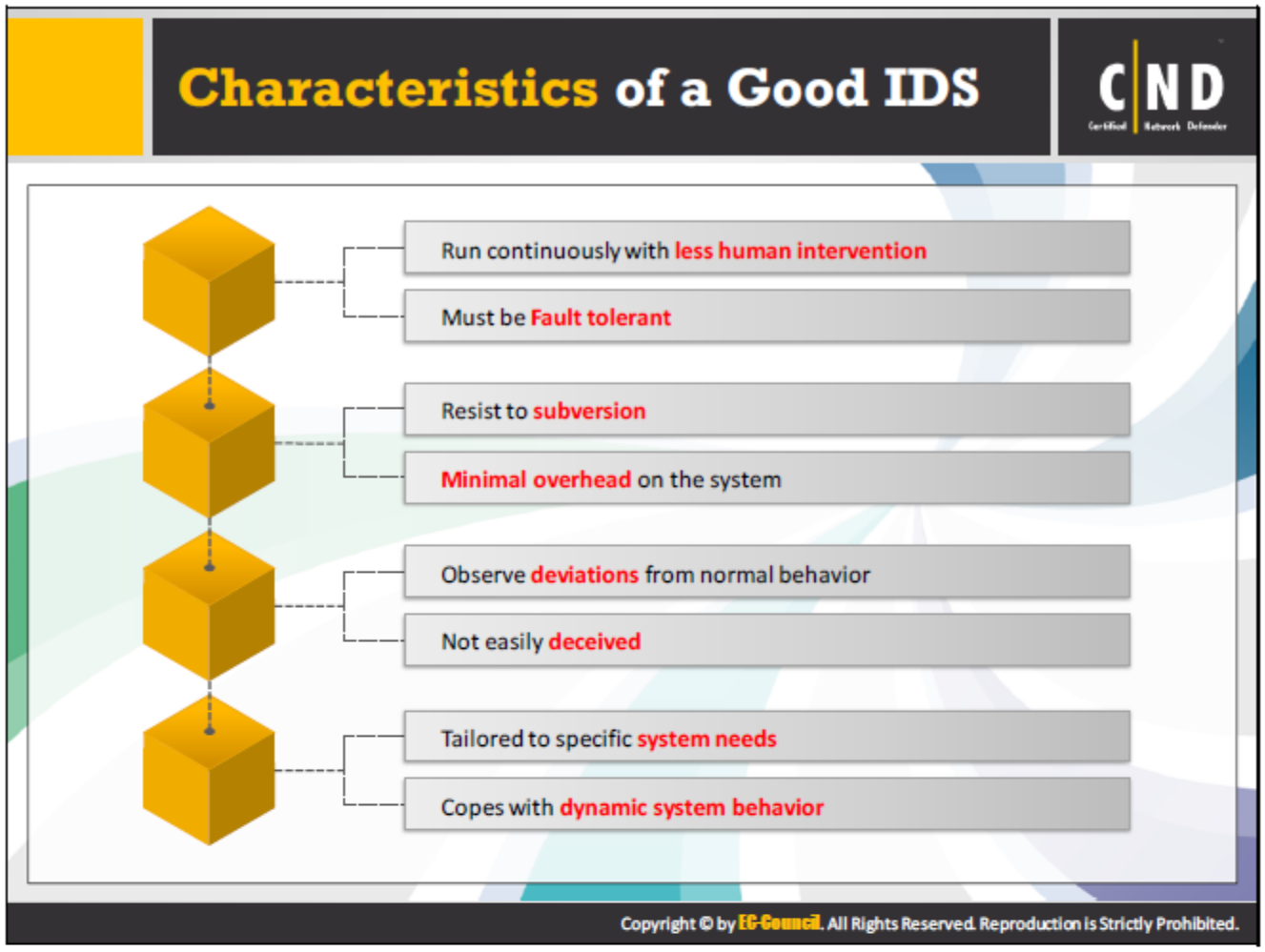
- Type the filter name, signature ID, network address with subnet mask, and action to subtract in the appropriate fields, and then click OK



http://www.cisco.com

Cisco Secure IPS provides the capability to exclude a specific signature from or to a specific host or network address. Excluded signatures do not generate alarm icons or log records when they are triggered from the hosts or networks that are specifically excluded through this mechanism. For example, a network management station might perform network discovery by running ping sweeps, which trigger the ICMP Network Sweep with Echo signature (signature ID 2100). If you exclude the signature, you do not have to analyze the alarm and delete it every time the network discovery process runs.

Source: *http://www.cisco.com*

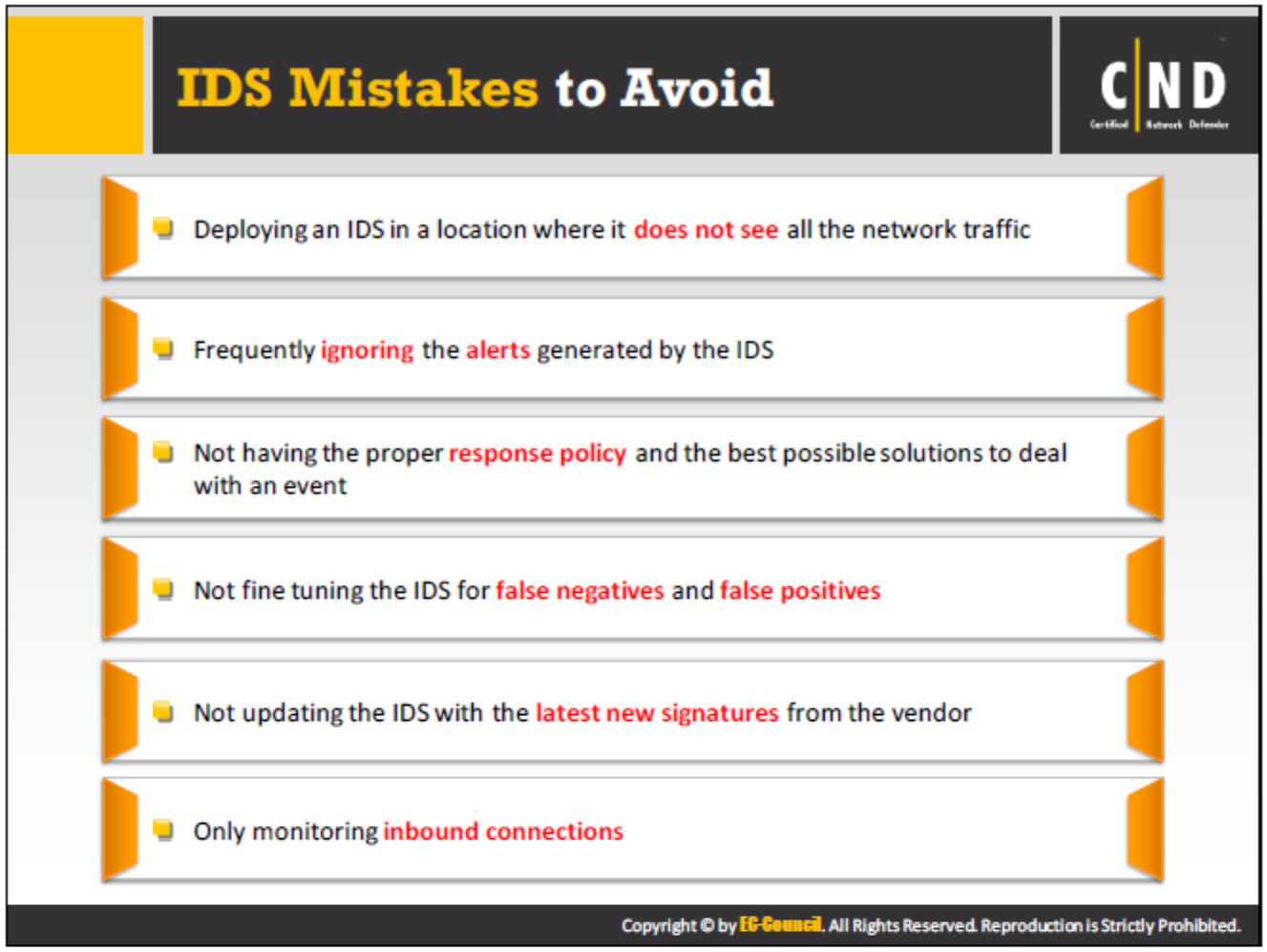


An ideal IDS should have the following characteristics:

- Organizations should have an IDS that can run without or with minimal human intervention. The configuration of the system monitors and detects all suspicious activities on the host system. However, administrators should have all the privileges in auditing and monitoring for this to work.
- Even if the host system fails or crashes the IDS will still function reliably. It is advisable to configure the IDS so it is fault tolerant and does not require a reconfiguration or reboot every time the host system fails. Also, it should be capable of monitoring itself to avoid any damage.
- An IDS should have the features for halting and blocking attacks. These attacks can occur from any application or software. This also involves alerting the administrator through online, mobile or email notification. The method of notification depends on the configuration set up by the administrator.
- By having the feature for information gathering, an IDS helps an administrator detect the type of attack, source of the attack and the effects the attack caused in the network. Gathering evidence for a cyber-forensic investigation is one of the required characteristics of an IDS.
- In large organizations, an IDS is built with a fail-safe feature to help hide itself in the network. This feature helps create a fake network to attract intruders to as well as for

analyzing the possibilities of different types of attacks. It also helps vulnerability analysis of the network.

- An IDS detects changes in the files of the system or network. The file checker feature in an IDS notifies the administrator if the intruder made any sort of alteration to the files. An IDS reports every activity which has occurred on the network and this aids an administrator when analyzing vulnerabilities and rectifying them.
- When recursive changes occur in the network, an IDS should be adaptable to these changes. This also includes adapting different defense mechanisms for every different system in the network.
- The configuration of an IDS is such, that it does not cause overhead in the network or system.

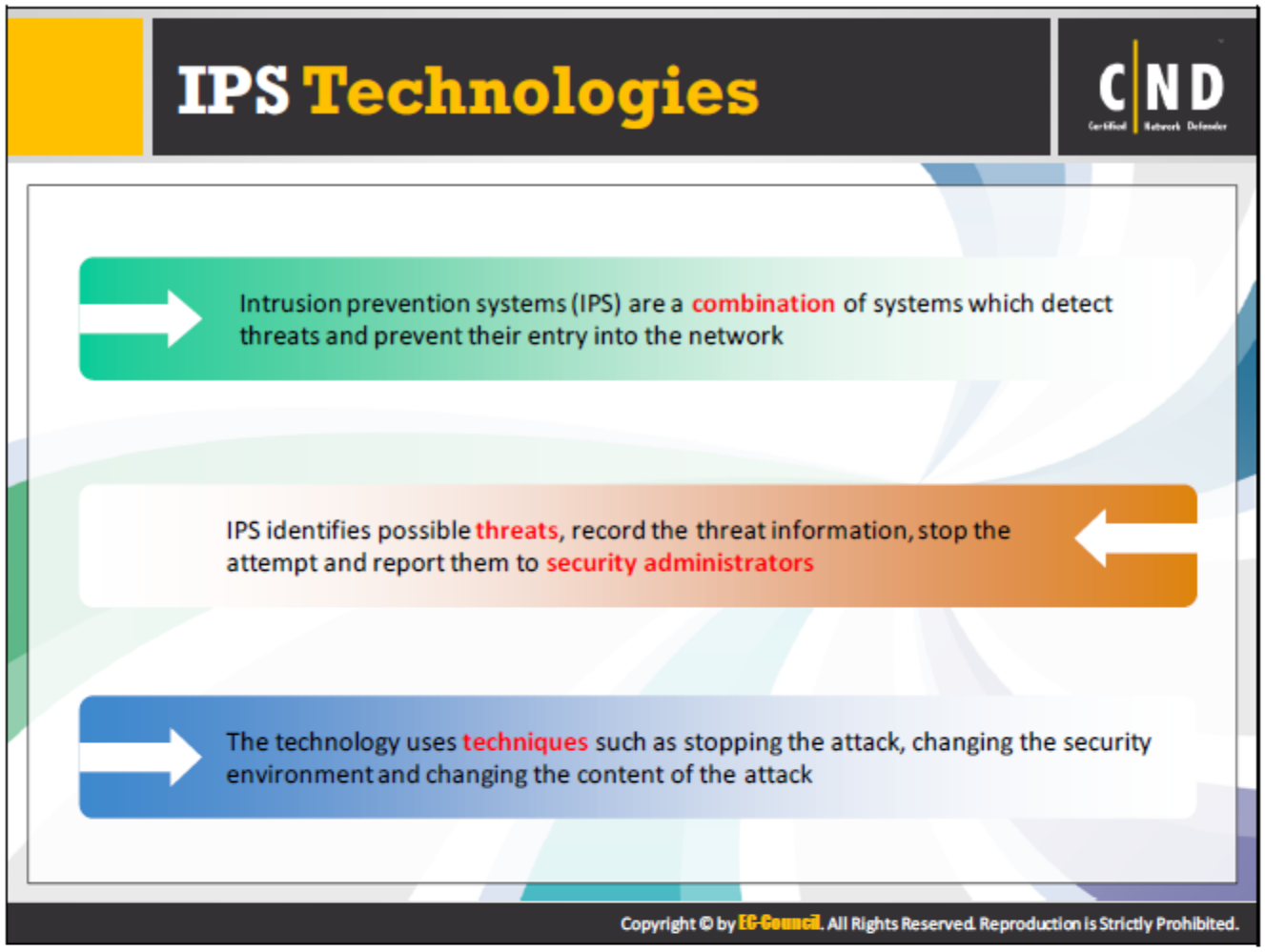


Below are the mistakes and the work arounds to avoid mistakes while deploying the IDS in the network:

- Do not deploy an IDS if the infrastructure planning is not efficient. An improper or incomplete network infrastructure will not help the functioning of an IDS. If the tuning of the IDS does not follow the network infrastructure, it has the potential to disable the network by flooding it with alerts.
- After the deployment of an IDS, the organization sets its level to the highest sensitivity enabling the IDS to detect a large number of attacks. However, this also includes a rise in the number of false positives. An IDS generates a large number of false positive alerts per day, which could cause the administrator to miss an actual alert. In the long run, ignoring these alerts can be harmful for network security.
- Detecting an intrusion is not enough. Organizations should also design a response policy that administrators implement in response to an incident which has occurred. This response policy should answer the following questions: What is the normal event and what is the malicious event? What is the response for every event generating an alert? The person reviewing the alerts should be aware of this action plan.
- An infrastructure which has established a NIDS without IPsec network protocols, makes the network more vulnerable to intrusions. A NIDS listens to all the traffic that it senses and then compares the legitimacy of the traffic. If it encounters encrypted traffic, it can

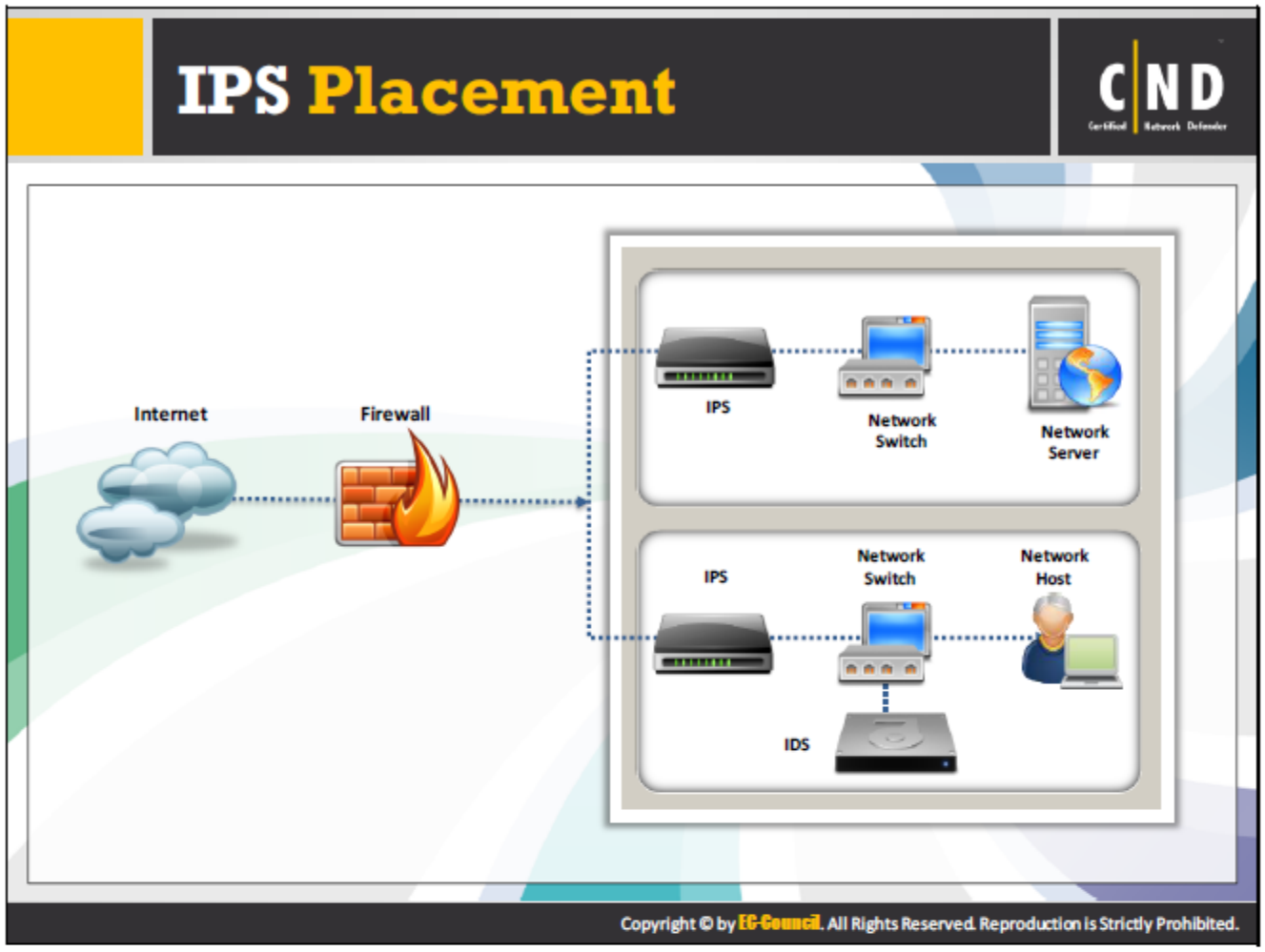
only perform packet level analysis as the application layer contents are inaccessible. This increases the vulnerability of the network.

- Many organizations prefer securing and monitoring only the inbound traffic and ignore the outbound traffic. It is important to place the IDS sensors throughout the organization. If the setup is cost effective, the organization should place the sensors near the choke points on the network. This will help monitor outbound as well as internal host network traffic.
- Do not deploy IDS sensors on a single NIC or on multiple data links. This will lead to an IDS sensor sending the data on the same interface on which it is sensing. This leads to possible attacks as the interface reports all the data to the centralized database. If an attacker gets access to this infrastructure, they can disable the IDS, preventing further alerts. The attacker can also intercept the data on the interface and alter it. This issue can be resolved by connecting the interface to a dedicated monitoring network.



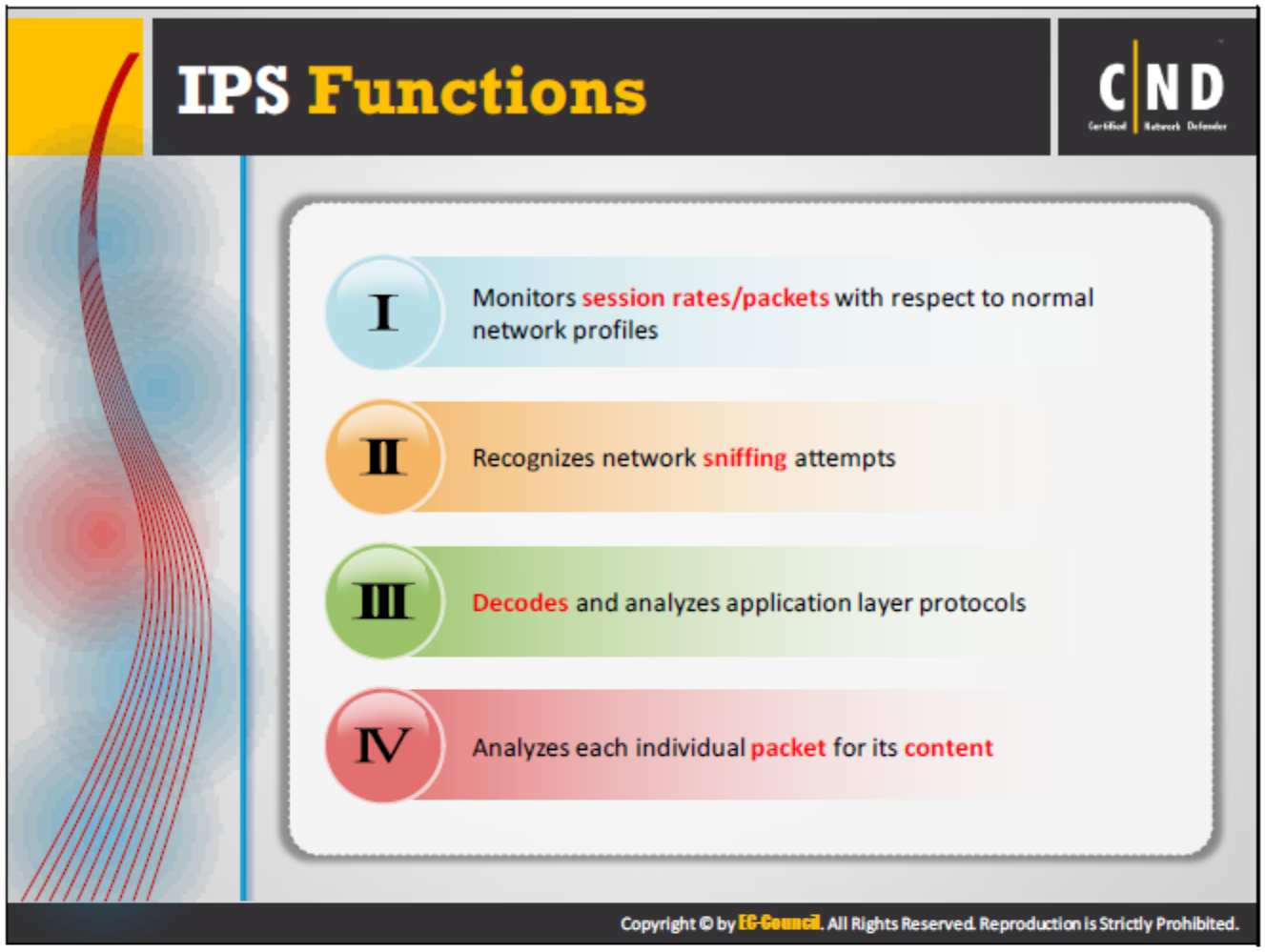
An Intrusion Prevention System (IPS) is a network security technology which has the capability of detecting an intrusion in the network. In addition, it also has the capability of blocking or stopping the detected intrusions. Therefore, sometimes it is called an inline firewall. It is considered an extension of an IDS. The main function of an IPS is to detect, log, attempt to block, and report malicious activity on the network. It provides a layer of analysis for the network. It works and is configured efficiently, otherwise deploying an IPS can degrade network performance. An IPS also uses the same techniques for intrusion detection as an IDS uses.

The combination of an IDS and an IPS enhances network security by identifying real-time threats and preventing them.



Unlike an IDS, IPSs are placed in-line in the communication path between the source and destination and generally sit directly behind the firewall. An IPS works from inside the firewall and monitors for internal attacks as well as attacks penetrating the firewall. It will inspect the network traffic for attacks before the firewall filters the attacks, thereby serving as an early warning system and alerting when threats are found. An internal IPS configuration consumes more time to investigate and the IDS reports to detect the attacks can fail and/or succeed as the normal network generates many alerts.

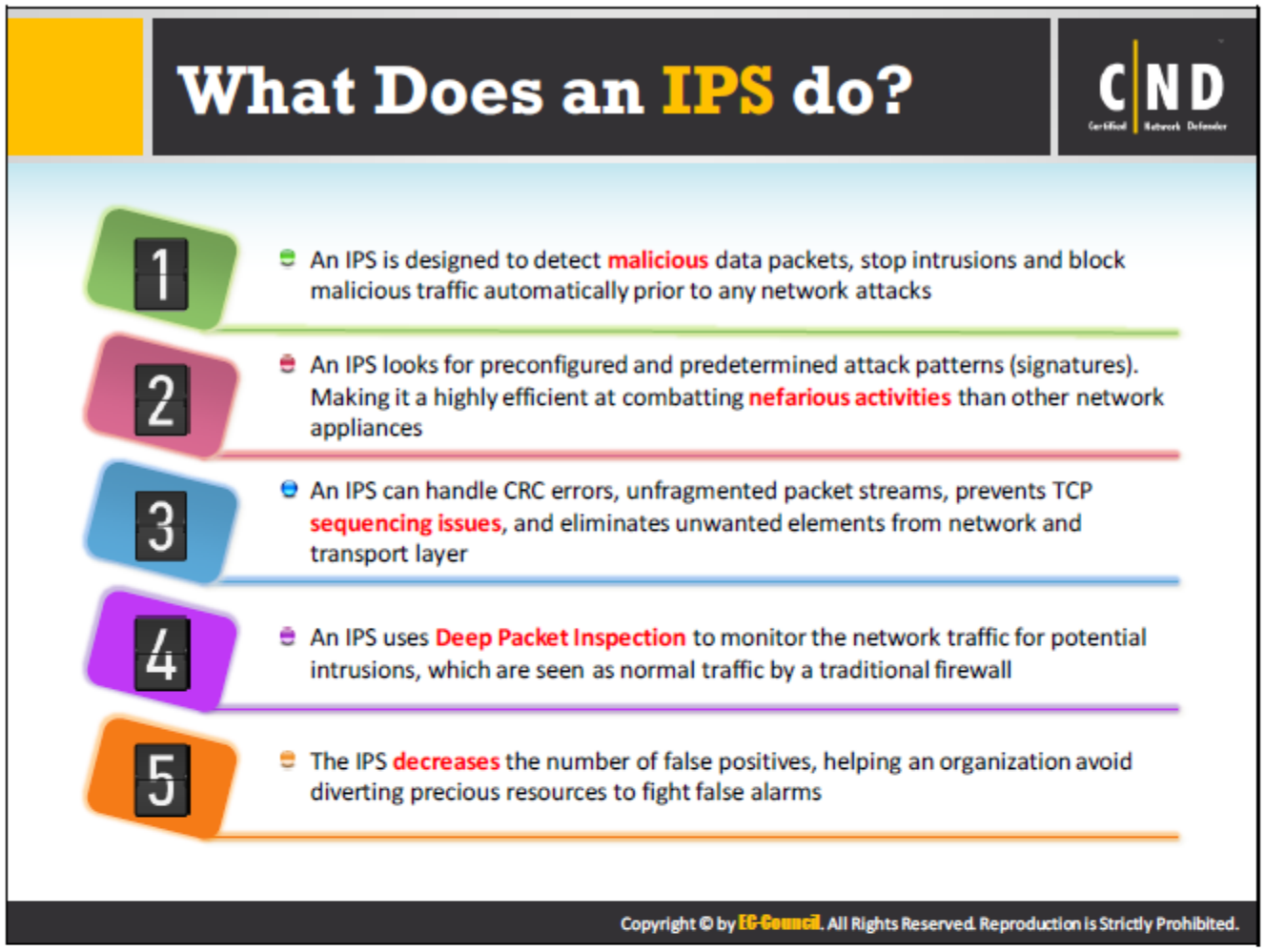
There are major drawbacks with placing an IPS on the outside of the firewall. It results in a number of false positives making it difficult to manage and sniff out the real issues. Frame reassembly is also an issue, since your IPS must be powerful enough to handle the reassembly of packets before it can inspect them.



An IPS detects as well as actively prevents any detected intrusions and even blocks traffic from improper IP addresses. An IPS recognizes network-sniffing attempts that try to steal data packets from the network. It decodes and analyzes application layer protocols.

Major functions of an IPS are:

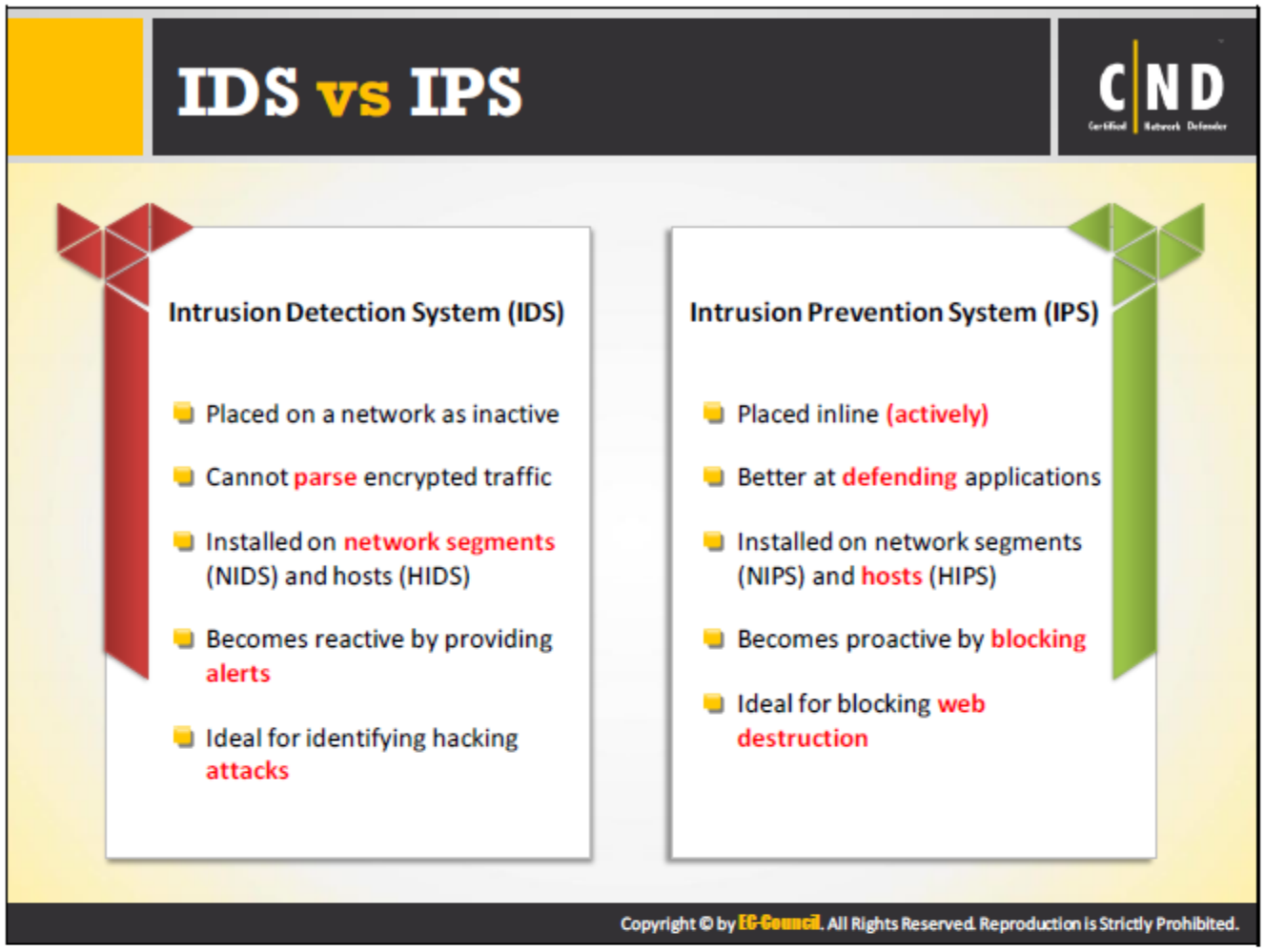
- **Identify malicious activity:** Detects malicious activity, notifies by raising an alarm.
- **Log information:** Creates logs on a regular basis with the all the information about the activities performed on the network.
- **Attempts to block/stop and report:** Blocks the malicious activity by itself and reports the activity to the administrator.



An IPS performs the same functions as a firewall, but with firewalls most of the rules are to allow the traffic. In an IPS, most of the rules are to deny the traffic.

Advantages of an IPS

- Quickly blocks known threats.
- Detects, stops and blocks network attacks automatically.
- Decreases false positives and helps organizations avoid diverting their network resources to fight false alarms.
- Corrects CRC errors, defragment of packet streams, TCP sequencing issues, etc.
- Uses deep packet inspection to monitor network traffic for potential intrusions which usually would be seen as normal traffic by a traditional firewall.
- Looks for preconfigured and predetermined attack patterns (signatures), making it more efficient than other network appliances to combat nefarious activities.



Intrusion Detection System (IDS)

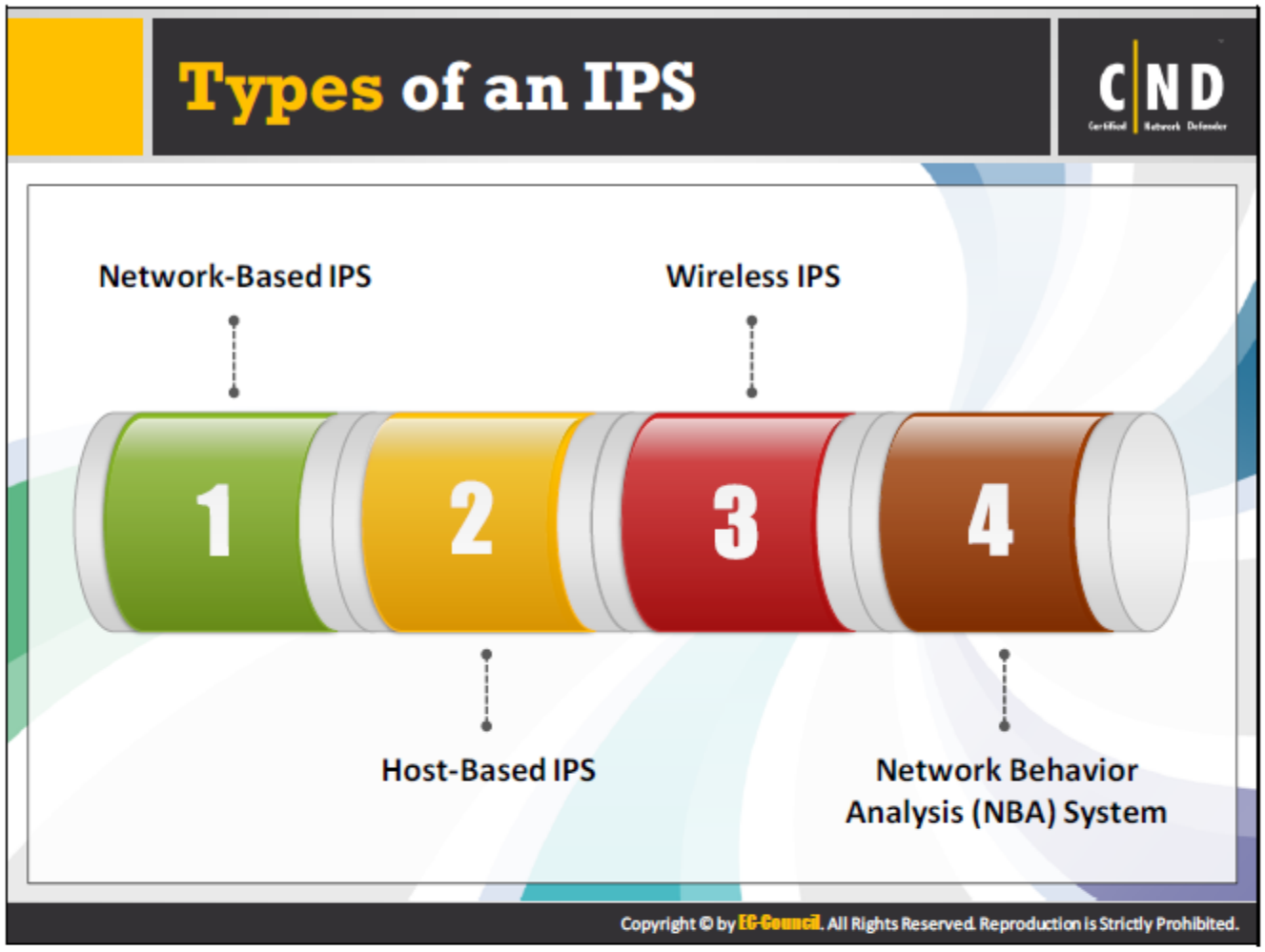
The IDS senses malicious activity on the network and alerts the administrator. Functions of an IDS are:

- Installed on both a network segment and host systems.
- Monitoring network traffic and detects signs of intrusions.
- Alerts the network administrator concerning potential intrusions.
- Issues include false positives and false negatives.
- Requires continuous monitoring and frequent signature updates.
- Uses encrypted traffic to prevent data intrusions.

Intrusion Prevention System (IPS)

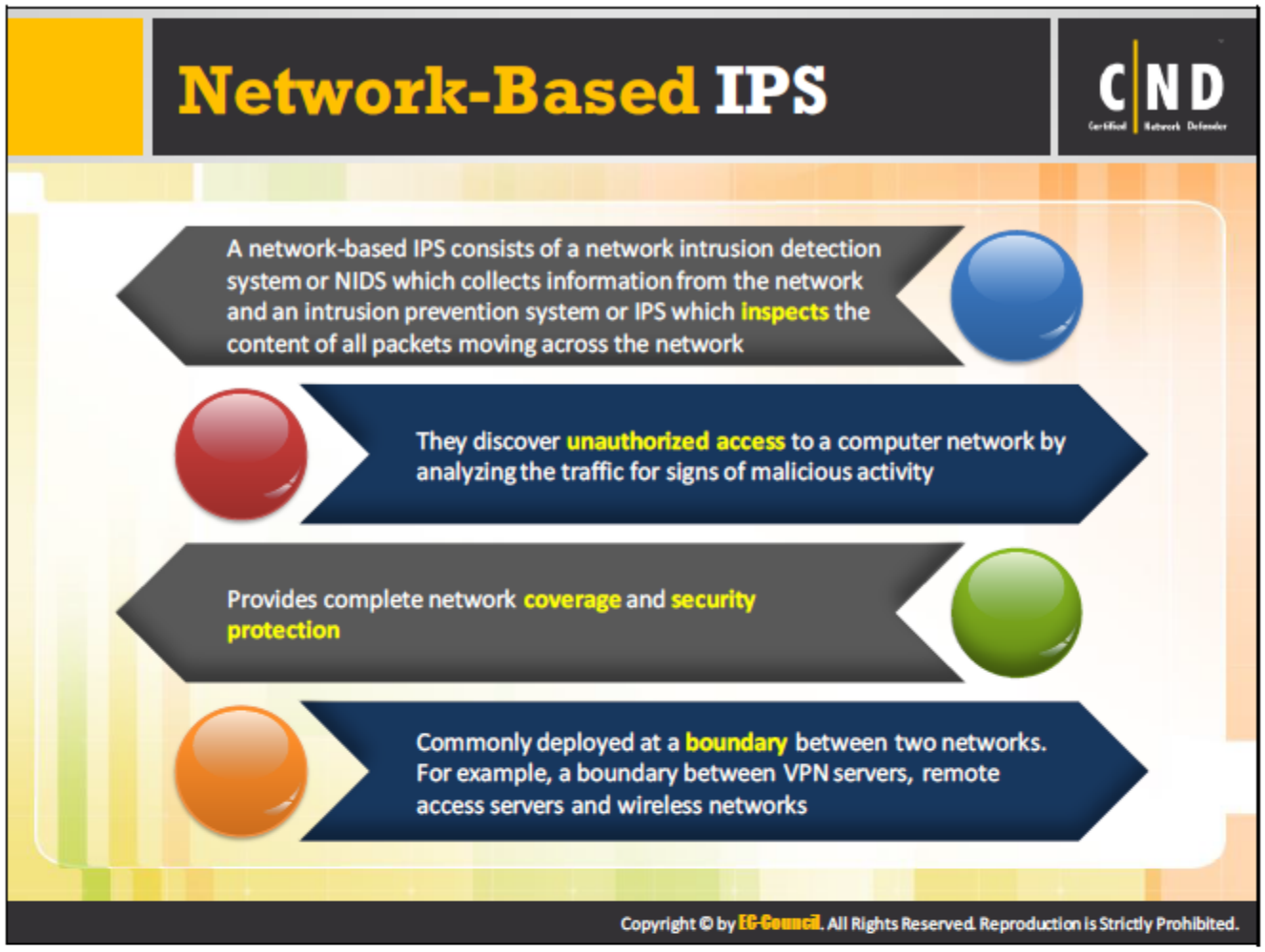
The IPS not only senses the malicious activity on the network, but also tries to give a proactive response to the attack.

- Installed on both a host and network segments.
- Monitors network traffic, detects intrusions and tries to prevent them.
- Automatically takes action to protect the network from the attacks.
- Reduces the emergency in the implementation of security patches.
- Continuous monitoring is not required.



Intrusion prevention systems are categorized into four different types:

- **Network-based Intrusion Prevention System (NIPS):** Monitors network traffic for suspicious behavior.
- **Wireless Intrusion Prevention Systems (WIPS):** Monitors wireless network traffic for suspicious behavior.
- **National Behavior Analysis (NBA):** Monitors traffic deviating from normal traffic.
- **Host-based Intrusion Prevention System (HIPS):** Monitors events on a host for suspicious behavior.



A network-based IPS is comprised of a network intrusion detection system (NIDS) and an intrusion prevention system (IPS) that monitors a network and analyzes the network traffic, packet content and application protocol activity. It helps detect signs of possible incidents on the network and protects the network from suspicious activities such as viruses, malware, denial of service (DoS) attacks, and buffer overflows. It detects threats and responds to them by either stopping it or reporting it. It uses detection software known as an agent to detect statistical and protocol anomalies by transmitting data to the network server in order to prevent these types of intrusions. It sends alerts about the attack or the threats to the proper personnel and helps resolve them before they can corrupt and destroy the network.

As a drawback, it sends alerts to conditions that are not threatening. To avoid these problems, it needs to be reconfigured by altering or reducing the security control signaling these conditions as incidents. This can be set based on network administrator policies.

Network-Based IPS: Security Capabilities

- A network-based IPS provides **security capabilities** which are classified into four categories

Information gathering capabilities are limited and include the host network activity along with:

- The identification of **hosts** by creating a list in the network in accordance with the IP address or MAC address
- The identification of the **operating systems** and versions of all systems on the network, using a passive fingerprinting technique to uncover user vulnerabilities
- The identification of **applications** by verifying the ports used and monitoring certain characteristics of application communications
- The identification of **network characteristics** such as the number of hops between two devices, which is useful when detecting changes in the network configuration

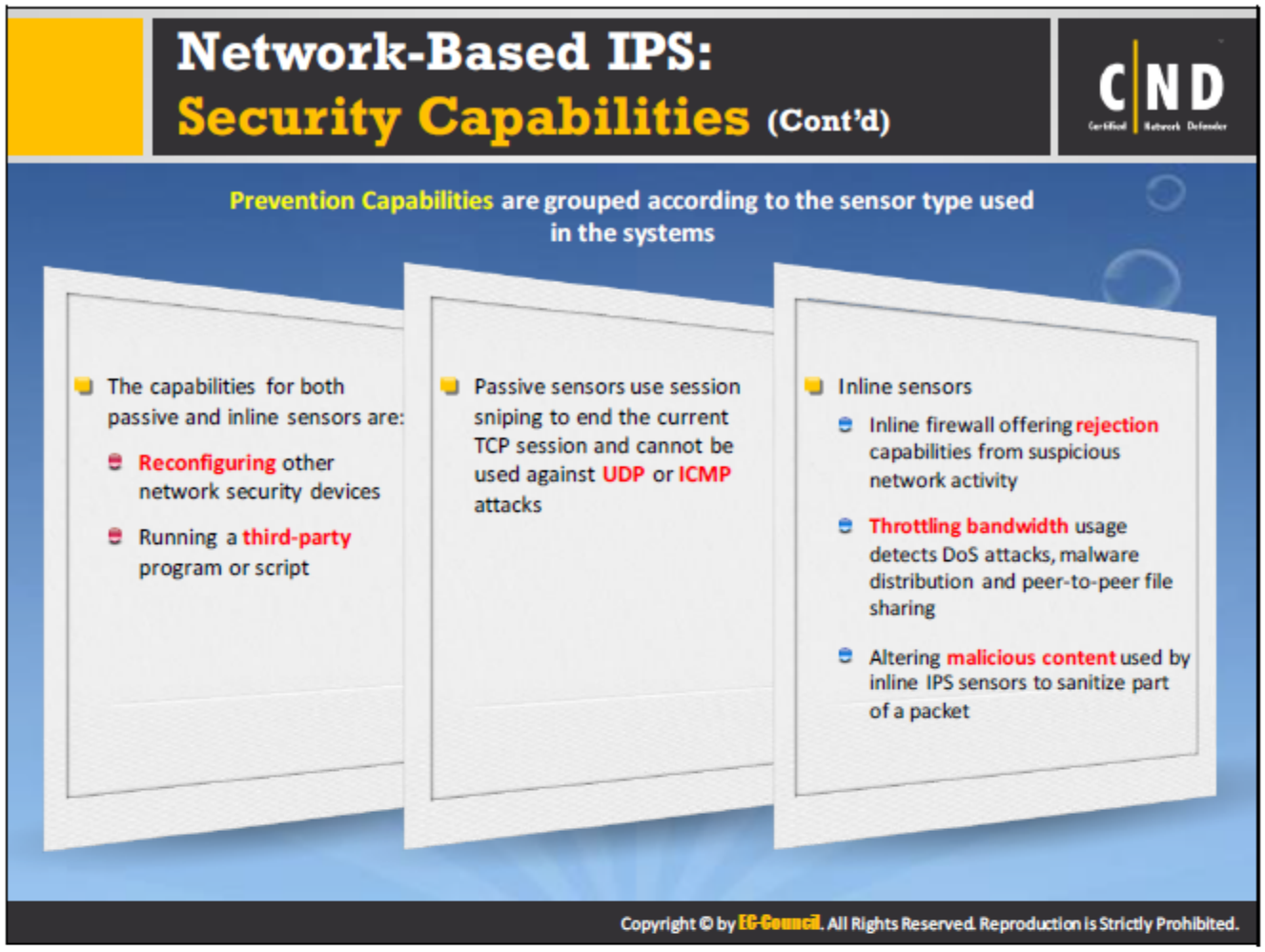
Network-Based IPS: Security Capabilities (Cont'd)

Detection Capabilities include the evaluation of:

- **Detecting the accuracy ranges** between the high rates for false positives and false negatives
- **Tuning and customization** is required to improve the detection capability
- **Technology limitations** include:
  - **Analysis of encrypted** network traffic
  - Handling **high traffic** loads
  - Preventing an IPS bypass
- Types of **events** that are detected include:
  - **Application** layer reconnaissance and attacks
  - **Transport** layer reconnaissance and attacks
  - **Network** layer reconnaissance and attacks
  - Unexpected **application** services
  - Policy violations

Logging Capabilities

- Storing **log data** for detected events
- Confirming the validity of alerts (False positives and false negatives)
- Investigating incidents
- Correlating events with other logging sources



The network-based IPS offers many security related capabilities including information gathering, monitoring, logging, detection and prevention of attacks. There are also certain network-based IPS products that offer security information and event management (SIEM) capabilities.

Information Gathering Capabilities

The network-based IPS has the ability to gather information on certain hosts and its network activities. Examples of information gathering capabilities are as follows:

- **Identifying Hosts**: An IPS sensor creates a list of hosts arranged according to the IP address or MAC address on the organization's network. The list identifies the new hosts on the network.
- **Identifying Operating Systems**: Using various techniques, an IPS sensor identifies the organization's host OSs and OS versions.
- **Identifying Applications**: An IPS sensor identifies the application versions in use by monitoring the characteristics of the application communication and tracking the ports that are used. It identifies potential vulnerable applications and unauthorized use of applications.
- **Identifying Network Characteristics**: IDPS sensors generally gather network details such as number of hops between two devices, network traffic, configuration of network devices and hosts in network.

Like an IDS, a network based IPS also features detection capabilities which use signature-based detection, anomaly-based detection and stateful protocol analysis techniques.

The types of events commonly detected by a network-based IDPS sensor include:

- Application layer reconnaissance and attacks
- Transport layer reconnaissance and attacks
- Network layer reconnaissance and attacks
- Unexpected application services
- Policy violations

Detection Accuracy

To increase the accuracy and the scope of detection, newer technologies use a combination of detection methods. The different network-based IDPSs analyze the network activity using a different method. This is very similar to how different types of web servers understand the same kind of web requests in different ways. This enables the sensor to enhance their detection capability and accuracy. Organizations should implement network-based IDPSs to deal with evasion issues.

Tuning and Customization

The network-based IPSs need extensive tuning and customization in order to improve the accuracy in their detection. Some examples of the tuning and customization capabilities include setting thresholds for port scans, authentication attempts, etc.

Technology limitations include:

- Analyzing the encrypted traffic
- Managing heavy load traffic
- Attack resistance against themselves

Logging Capabilities

The network-based IPS is able to log the detected events. These logs are useful when investigating incidents, checking the validity of the alerts, etc.

The various prevention capabilities provided by a Network-based IDPS is:

- **Passive Only**
  - Ending the Current TCP Session

    Passive sensors send TCP reset packets to both endpoints in an attempt to end the existing TCP connection. Both endpoints will assume the other endpoint wants to terminate the connection. This process is called sniping. The goal is to get one of the endpoints to terminate the connection before an attack can succeed. Session sniping is not widely used as there are newer prevention capabilities that are more effective.

- **Inline Only**
  - Performing Inline Firewalling

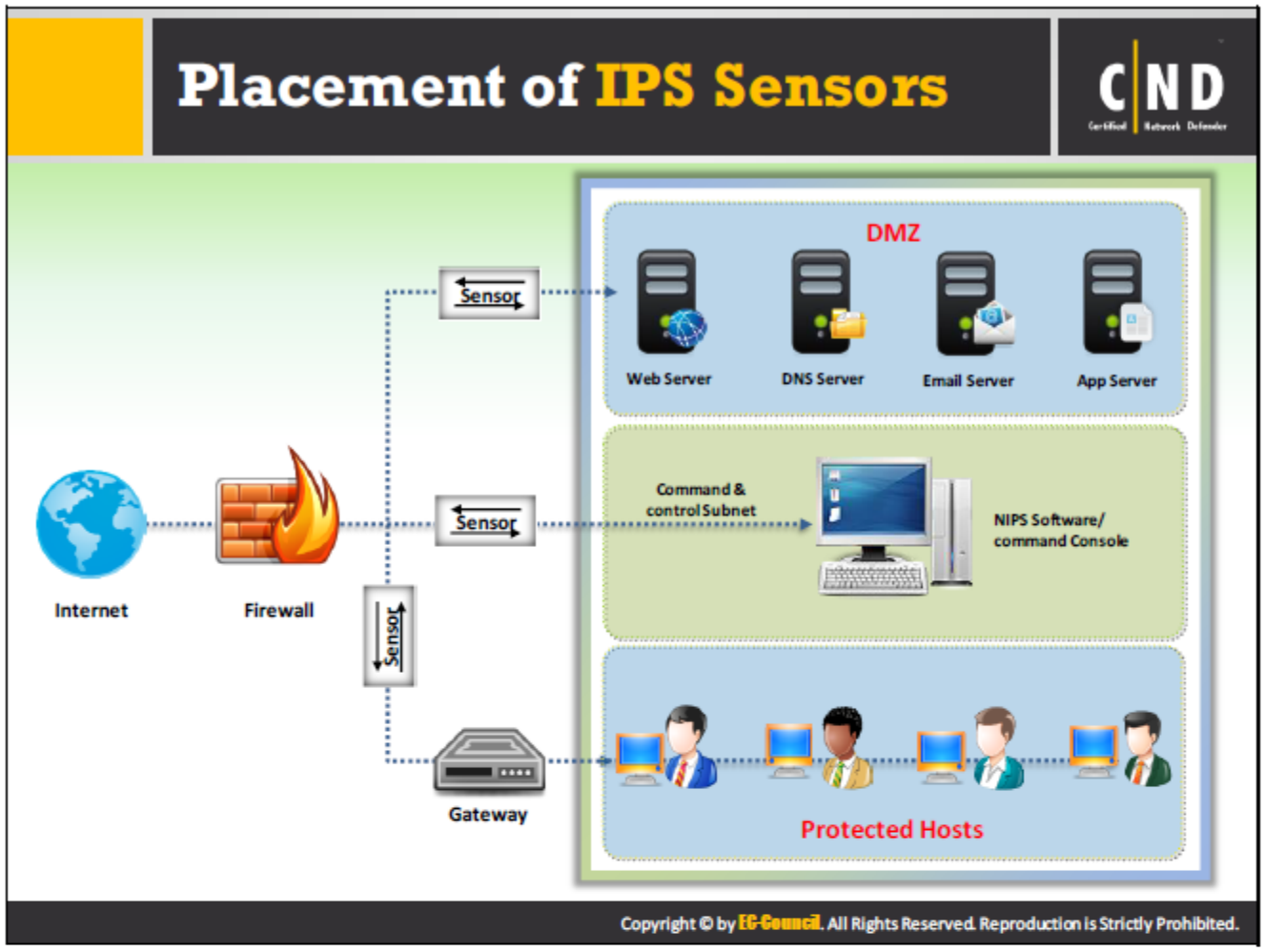
    A majority of inline IDPS sensors provide firewall capabilities for detecting and preventing attacks.
  - Throttling Bandwidth Usage

    Inline IPS sensors limit the percentage of network bandwidth usage by the protocol, with the precaution to prevent various attacks that may affect bandwidth usage such as a DoS attack, malware distribution, etc.
  - Altering Malicious Content

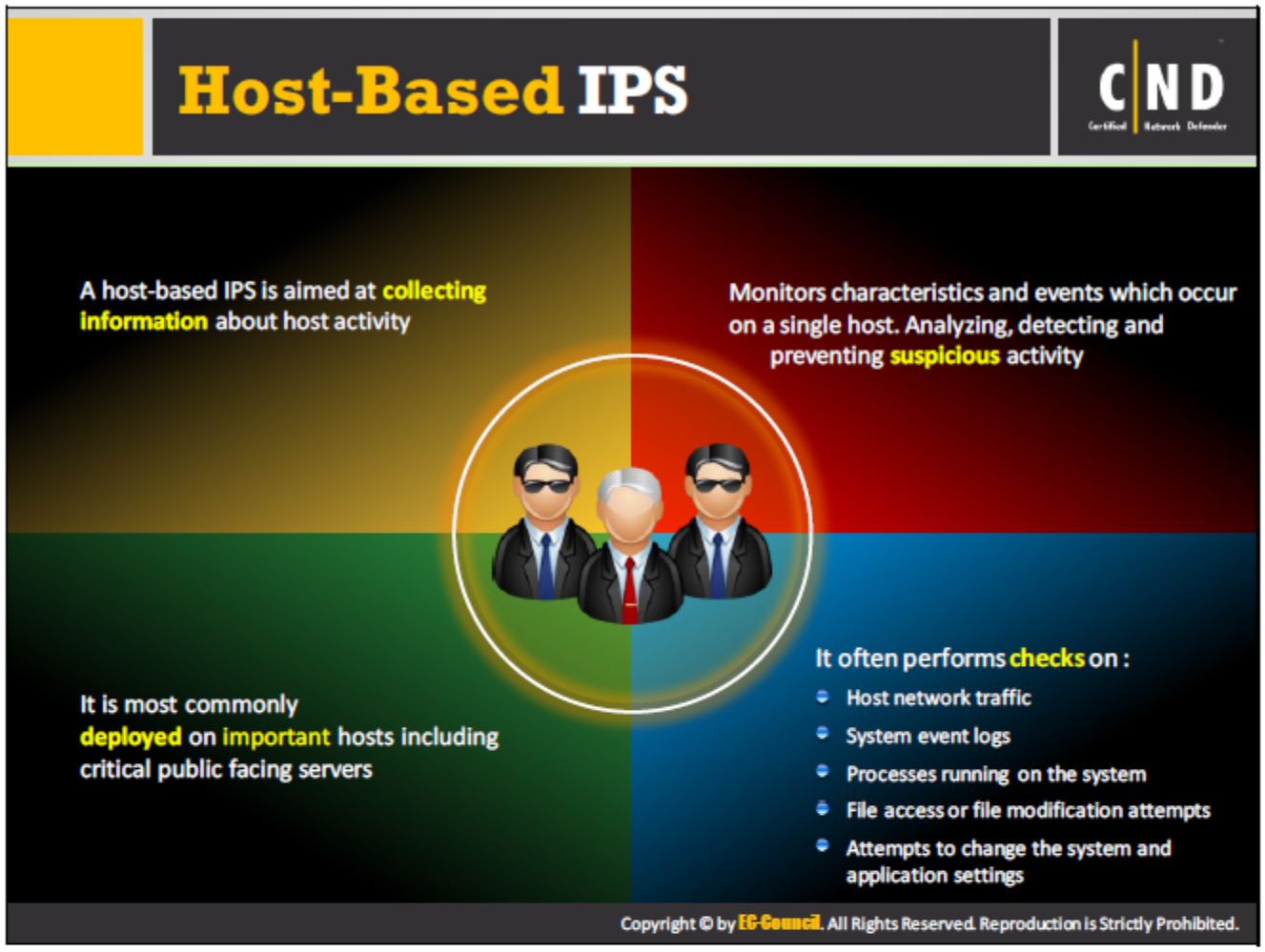
    There are a few inline IPS sensors that can replace the malicious content of a packet with trusted content and then send the decontaminated packet to the destination. Some sensors act as a proxy and perform normalization on the traffic to remove the malicious content from a packet. This sanitizes some attacks involving packet headers and application headers, irrespective of the attack detected by the IPS.
- **Both Passive and Inline**
  - Reconfiguring Other Network Security Devices

    Some sensors have the capability of informing other security devices such as firewall, router, switches, etc. about reconfiguring themselves to withstand against external attacks. It is useful when network traffic is analyzed using packet header characteristics such as IP addresses, port numbers, etc.
  - Running a Third-Party Program or Script

    When certain malicious activities are detected, some IPS sensors run an administrator-specified script or program triggering a prevention action, such as reconfiguration of security devices. Administrators desire third-party programs or scripts when the IPS does not support prevention actions. Some IPS sensors only indicate prevention actions to performed by suppressing all other actions.



As a single management station supports multiple sensors, each side of the firewall can therefore have an IPS sensor enabling the user to know what attacks the network is facing and how exactly the firewall is protecting the network from those attacks. An IPS sensor analyzes the attacks occurring on the external firewall, determines the potential attacks and stops them from entering the network. This kind of IPS configuration does not discover the internal threats. The IPS can work from a secondary location such as the DMZ and host segments to increase the visibility of the network traffic.



A host-based IPS monitors, detects, analyzes and prevents any intrusion activity on a particular host. It checks the system integrity, logs, programs, applications, file access and/or modification, traffic, etc. to detect intrusion attempts.

It has detection software known as agents installed on a single host instead of the whole network, that monitors activity on a host and conducts prevention functions. It monitors the status of key system files, triggers alerts on changes to file attributes, creation of new files, and deletion of any existing files. It monitors multiple systems by creating a host configuration file and making each HIPS report to a master console system.

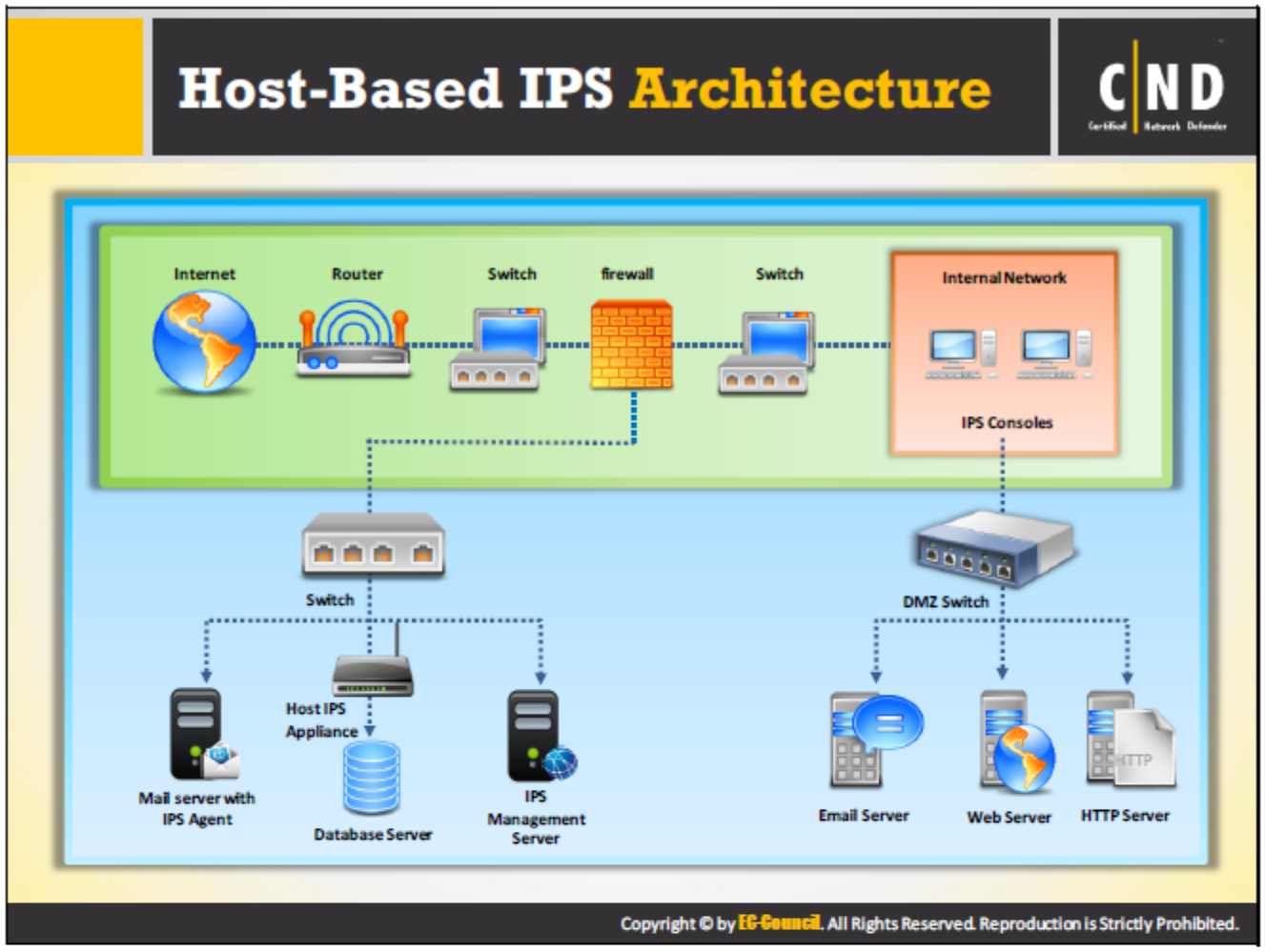
Advantages

- Detects local events and attacks on host systems, where encrypted traffic is decrypted and is available for processing.
- Not affected by using switched network protocols.
- Detects inconsistencies in the usage of applications and system programs by examining records stored in audit logs, to detect attacks including a Trojan horse.

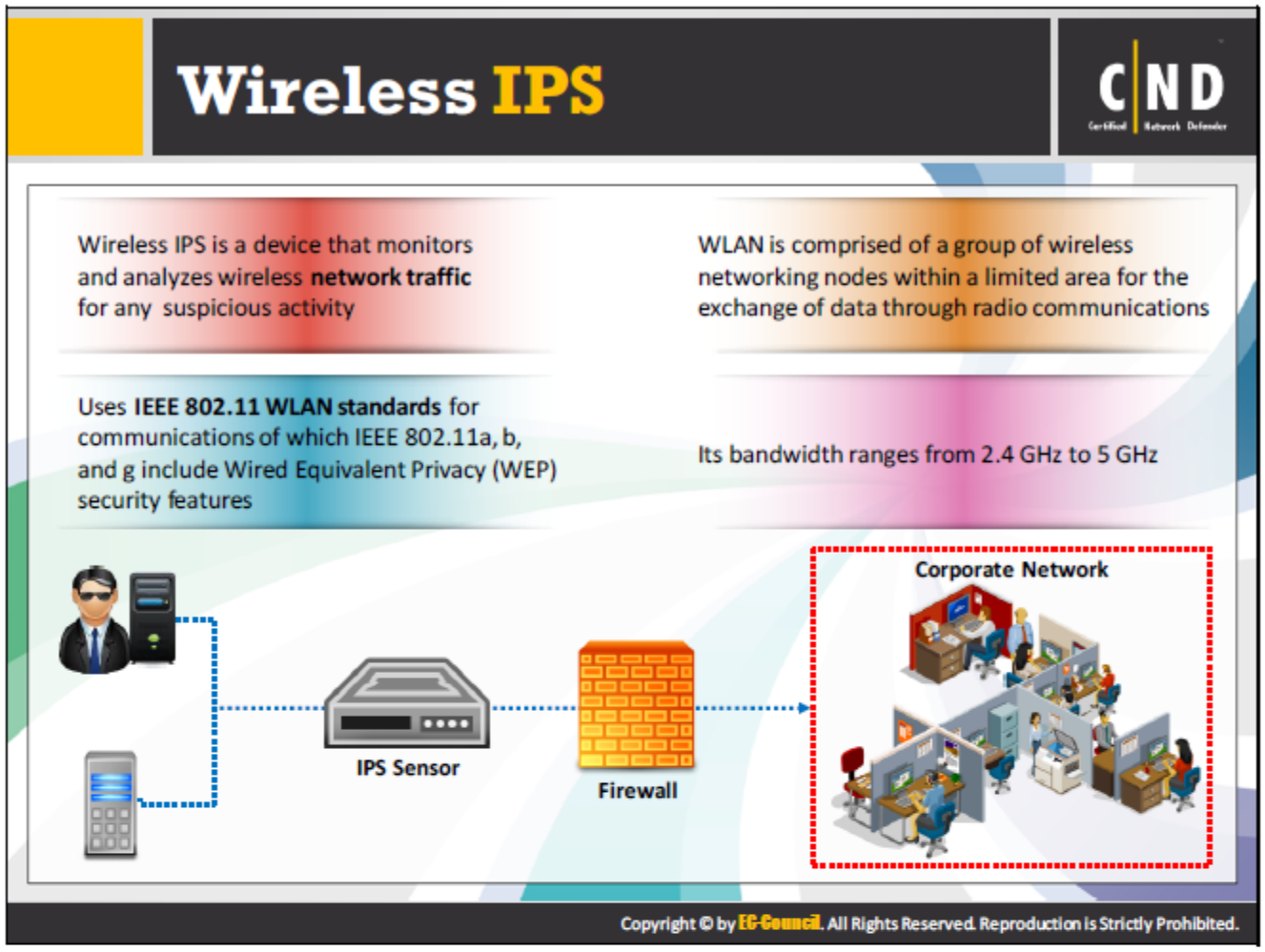
Disadvantages

- Management issues as it is configured on each monitored host.
- Vulnerable to host OS attacks.
- Cannot detect multi-host scanning.

- Vulnerable to denial-of-service attacks.
- Overhead on host systems reduce system performance below acceptable levels.

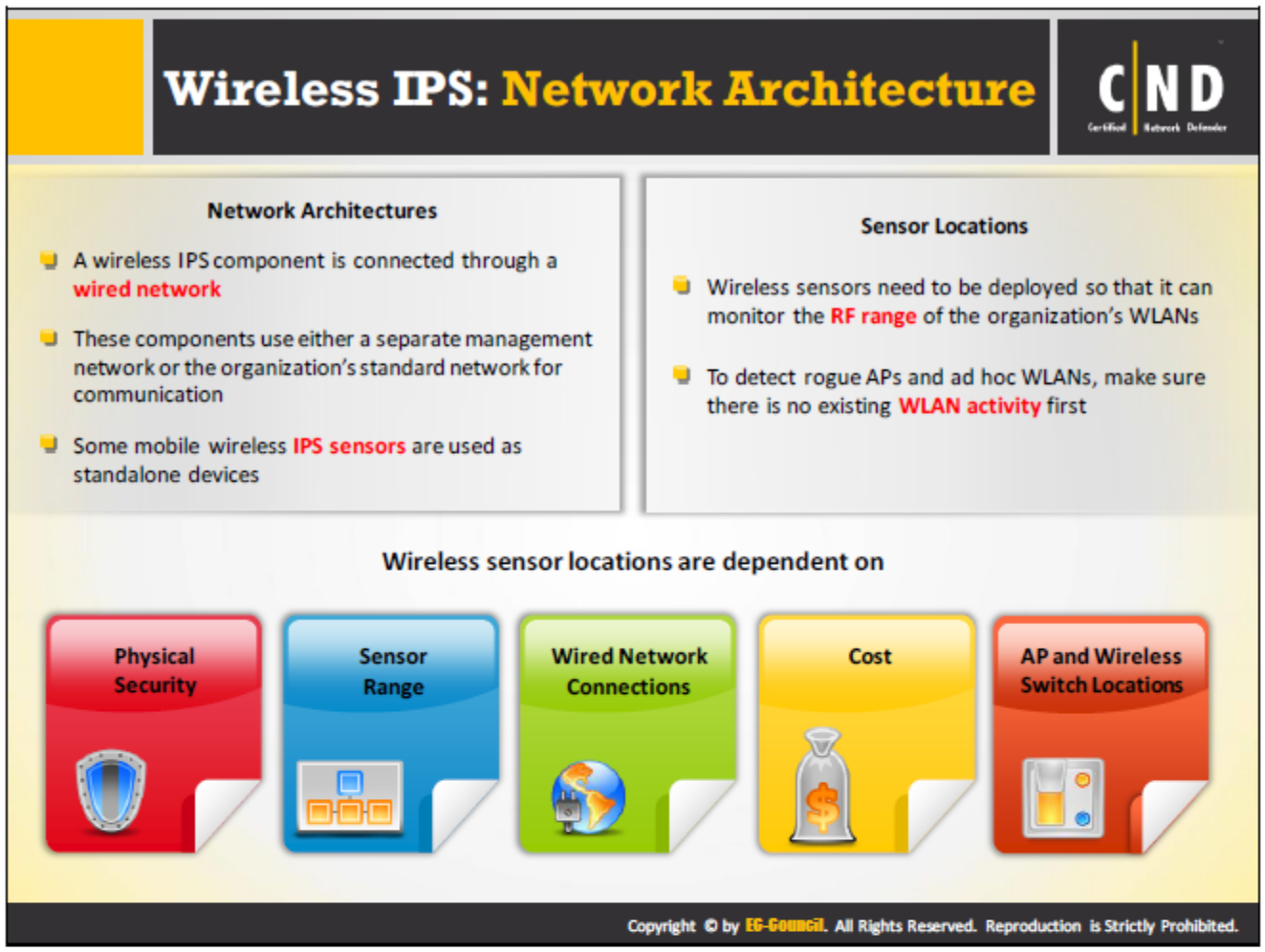


Host-based IPS architecture involves deploying a HIPS agent on each of the hosts in the organization. The system components communicate over an organization's network instead of using a separate management network. Most products encrypt their communications to prevent attackers from accessing the sensitive information. A host-based IPS architecture uses appliance based agents placed in front of the hosts it is protecting.



A wireless IPS is used to monitor wireless network traffic for detection and prevention of network intrusion activity. The system analyzes wireless networking protocols to identify and avert suspicious activities.

The wireless IPS covers devices, which connect over a wireless local area network (WLAN) through radio communications and distribute the signals within a limited geographic area. A wireless IPS detects abnormal activities in wireless network traffic which can be a device compromise attempt or an unauthorized access to the network. It will also identify any device that tries to spoof the identity of another device.



In an IPS, all the typical components use a wired network to connect with each other. The wireless IPS components communicate with each other using a separate management network or the organization's standard network. Some mobile wireless IPS sensors also act as standalone devices.

The network architecture for a wireless IPS also includes deciding where the sensor locations are in an IDPS. The location of the sensors should allow it to check regions where the WLAN activity should not exist as well as monitor all the channels and bands to detect rogue APs and ad-hoc WLANs.

Selection of wireless sensor locations depend on a wide array of criteria such as:

- **Physical Security:** Wireless sensors are prone to physical security threats because they are placed in open interior or external locations. The organization should consider some form of physical security for the sensors while deploying a WIPS. It is advisable to choose sensors with anti-tamper features.
- **Sensor Range:** The surrounding walls and doors may affect the range of WIPS sensors. It may add attenuation problems and reduce their range. It is advisable to use a Wireless IPS modeling software that helps administrators analyze building floor plans and features of walls, location of doors, etc.
- **Wired Network Connections:** Wired networks are required to connect sensors, which may require expanding the wired network in the area.

- **Cost:** Organizations should analyze the WLAN threats they face and choose a cost effective solution. Compare the cost of sensor purchases, deployment, and maintenance in order to define the solution that is capable of reducing the level of risk required.
- **AP and Wireless Switch Locations:** The locations of access points and wireless switches are crucial because they enable the implementation of wireless IPS software on themselves.

Wireless IPS: Security Capabilities

A wireless IPS offers different types of security capabilities, which are divided into **four categories** including:

- Wireless IPS **Information gathering capabilities**:
  - Identifying WLAN Devices by **enlisting** the inventory of WLAN devices
  - Identifying clients with the help of SSIDs and the **MAC addresses** for the devices
  - Identifying WLANs as **IPS sensors** track the WLANs through their **SSIDs**

- **Detection Capabilities** of a wireless IPS includes evaluation of:
  - Types of **events detected** by wireless IPS sensors include
    - Unauthorized WLAN devices
    - **Unsecure** WLAN devices
    - Unusual traffic behaviors
    - Wireless network **scanning attempts**
    - Denial of service (**DoS**) attempts
  - **Detection accuracy** of the wireless IPS is expected to be more accurate due to its limited scope
- Wireless IPS technology limitations include:
  - Inability to detect some **wireless protocol attacks**
  - **Susceptible** to evasion techniques
  - Cannot withstand **attacks** against an IPS

Wireless IPS: Security Capabilities (Cont'd)

Logging Capabilities

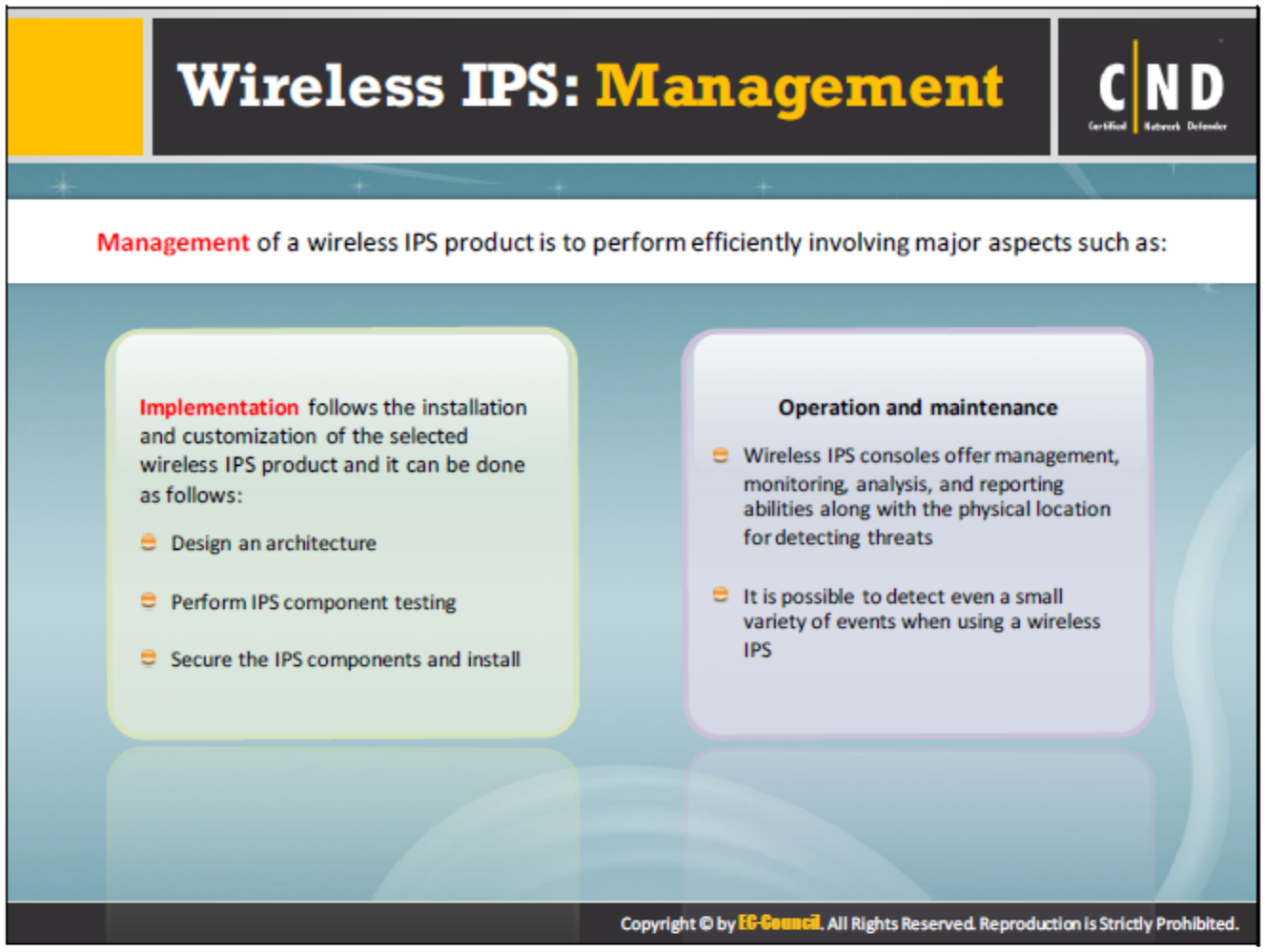
- Wireless IPS logging capabilities include **storing** log data for detected events
- It is helpful to confirm the **validity** of alerts by investigating incidents and correlating the log events with other logging sources

Prevention Capabilities

- Wireless IPS prevention capabilities include **averting** connections between a rogue or misconfigured STA and an authorized AP and vice-versa

Wireless IPSs offer various types of security capabilities including:

- **Information Gathering Capabilities:** Wireless IPS solutions are capable of collecting information on wireless devices. Wireless IPSs collect information in the following ways:
  - **Identifying WLAN Devices:** By listing the inventory of WLAN devices and clients noted by IPS sensors using SSIDs and the MAC addresses of wireless network interface cards.
  - **Identifying WLANs:** As IPS sensors track the WLANs through their SSIDs and the identification of new WLANs.
- **Detection Capabilities:** Detection Capabilities of a Wireless IPS include the evaluation of attacks, misconfigurations, and policy violations for a wireless network while accessing the IEEE 802.11 protocol communications. Other detection capabilities of the wireless IDPS include:
  - WIPS sensors detect the following types of events:
    - Unauthorized WLANs and WLAN devices
    - Unsecure WLAN devices
    - Unusual usage patterns
    - Wireless scanning activity
    - Denial of service (DoS) attacks and conditions
    - Impersonation and man-in-the-middle attacks
  - **Detection accuracy:** Detection accuracy of the wireless IPS is expected to be more accurate due to its limited scope.
  - **Technology limitations:** Technology limitations of the wireless IPS include:
    - Unable to detect some protocol attacks
    - Can be bypassed
    - Can be prone to attacks
- **Logging Capabilities:** Logging capabilities of a wireless IPS include storing the log data for detected events, which is used to confirm and investigate an incident.
- **Prevention Capabilities:** Prevention capabilities of a wireless IPS is to avert connections between a fake or improperly configured STA and an authorized AP and vice-versa. This includes both Wireless and Wired connections.
  - **Wireless:** Some sensors can terminate connections between a Station (STA) and an Access Point (AP) without any kind of direct connection, if there is a misconfiguration present in either of the components. The sensors send a message to the endpoint to disassociate the current session and then denies permission to create a new connection.
  - **Wired:** Certain sensors come with the ability to disconnect a switch on the wired network to block malicious or illicit network activity.



Management of a wireless IPS involves crucial tasks like implementation, operation, and maintenance of the products as well as providing guidelines for performing them effectively and efficiently.

Implementation

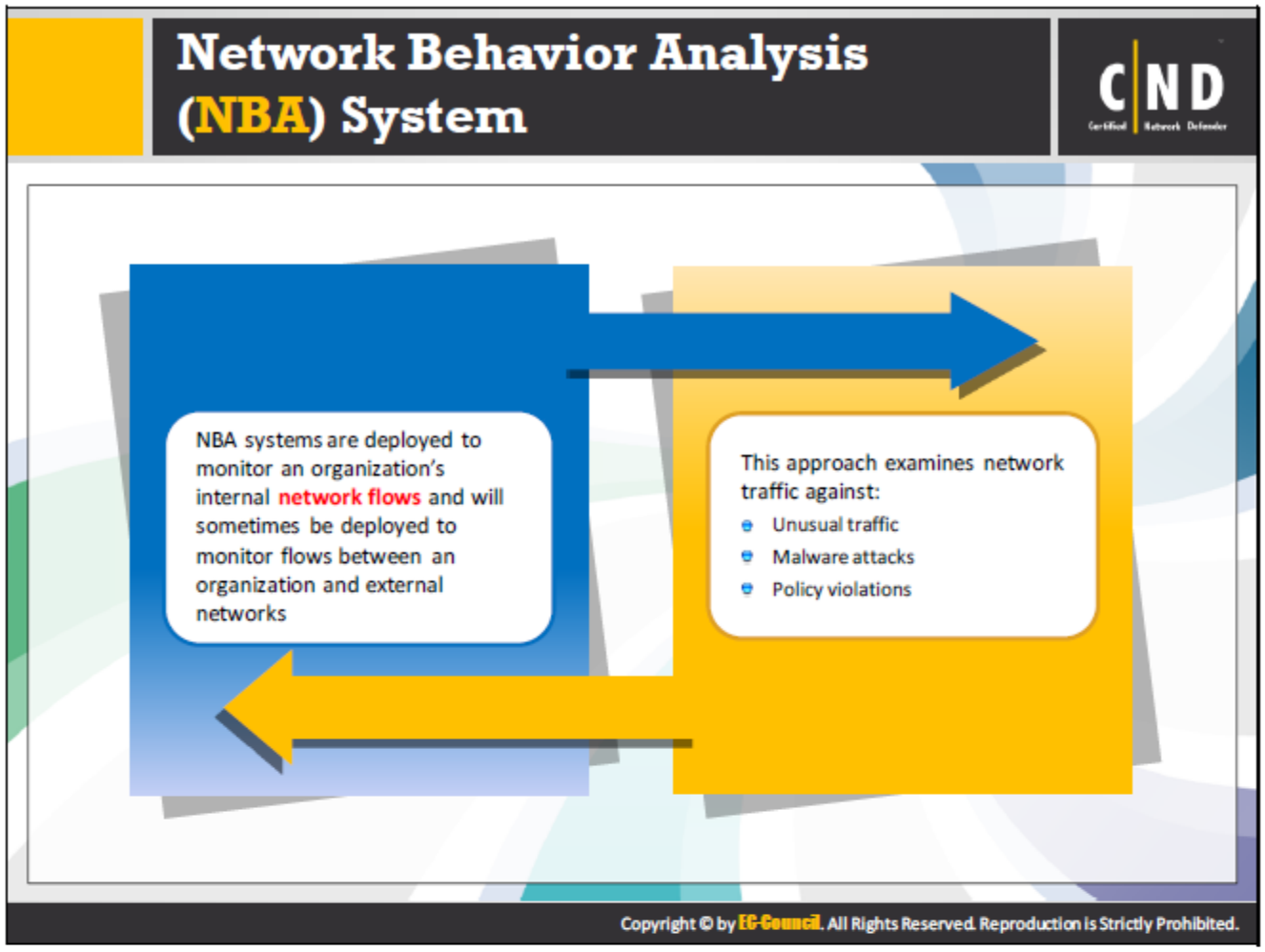
Implementation of a wireless IPS follows the installation and customization of the selected product.

Steps for implementing a wireless IPS include

- **Architecture Design**: Architecture includes planning the location of the IPS, number of sensors required, type of sensors and the process of connecting them.
- **Component Testing and Deployment:** Implementing a wireless IPS requires short network outages during installation of the sensors, network taps and load balancers.
- **Securing the IPS Components:** Do not assign IP addresses for both the passive and inline sensors used to monitor network traffic, as it keeps the sensors in stealth mode.

Operation and Maintenance

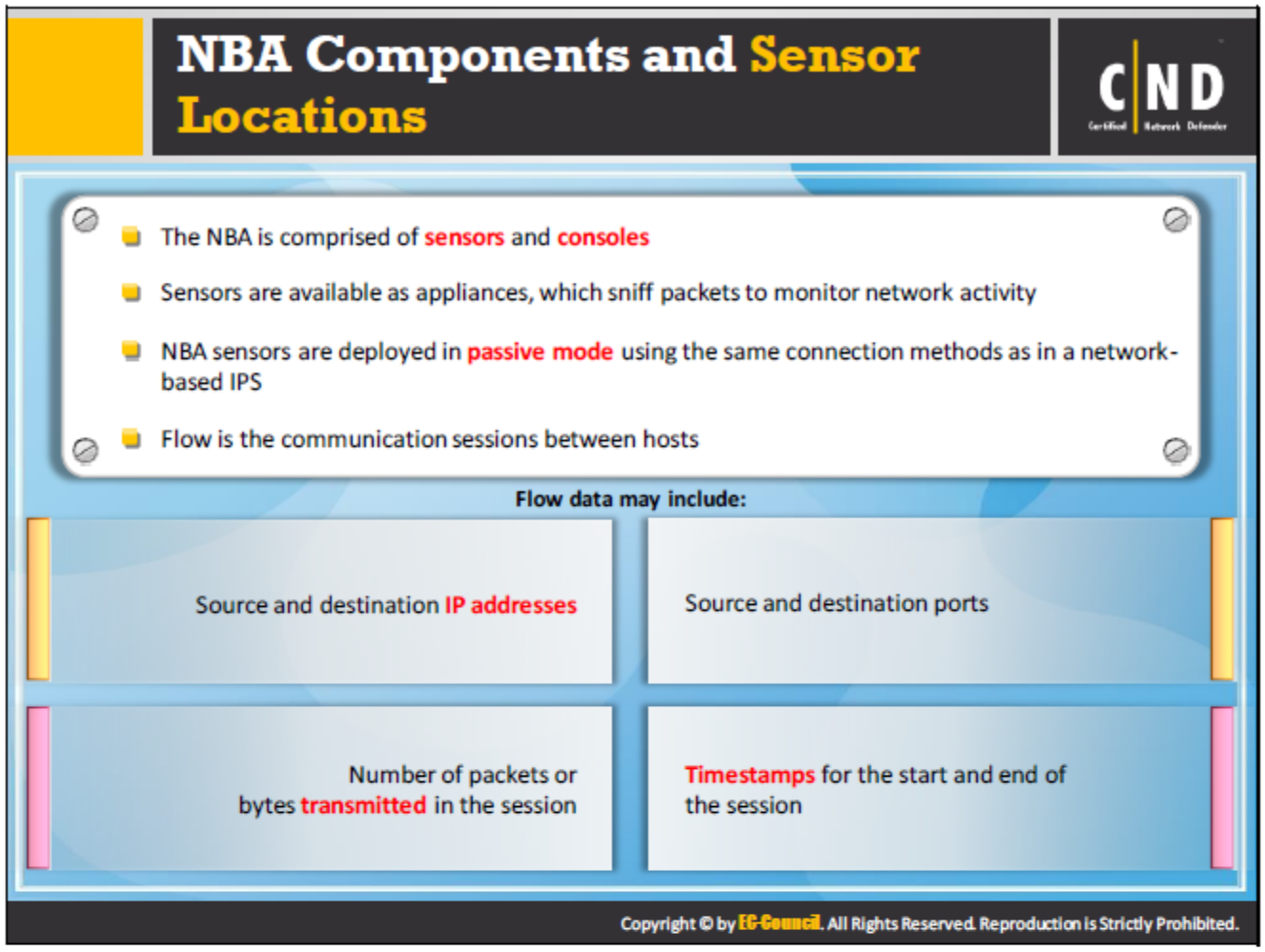
Wireless IPS consoles offer management, monitoring, analysis, and reporting abilities along with the physical location for detecting threats. The sensors have the ability to detect even a small variety of events.



A NBA system, also known as Network Behavior Anomaly Detection (NBAD) systems monitor an organization's internal network flows as well as flows between organizational and external networks. This approach evaluates and analyzes network traffic or its statistics on active devices such as switches, routers, firewalls etc. to identify:

- Unusual traffic
- Malware attacks
- Policy violations
- Advanced threats
- Undesirable behavior
- Anomalies

Some threats may evade an IDS and anti-virus software. The NBA system passively monitors the network traffic from many points and tries to identify such threats. The main advantage of using a NBA system is it focuses on the overall behavior of the network and flags new patterns that might indicate the presence of a threat. This allows the organization to address specific threats for which no signature is available. The NBA system is also capable of monitoring and recording the variations in the bandwidth and protocol usage.



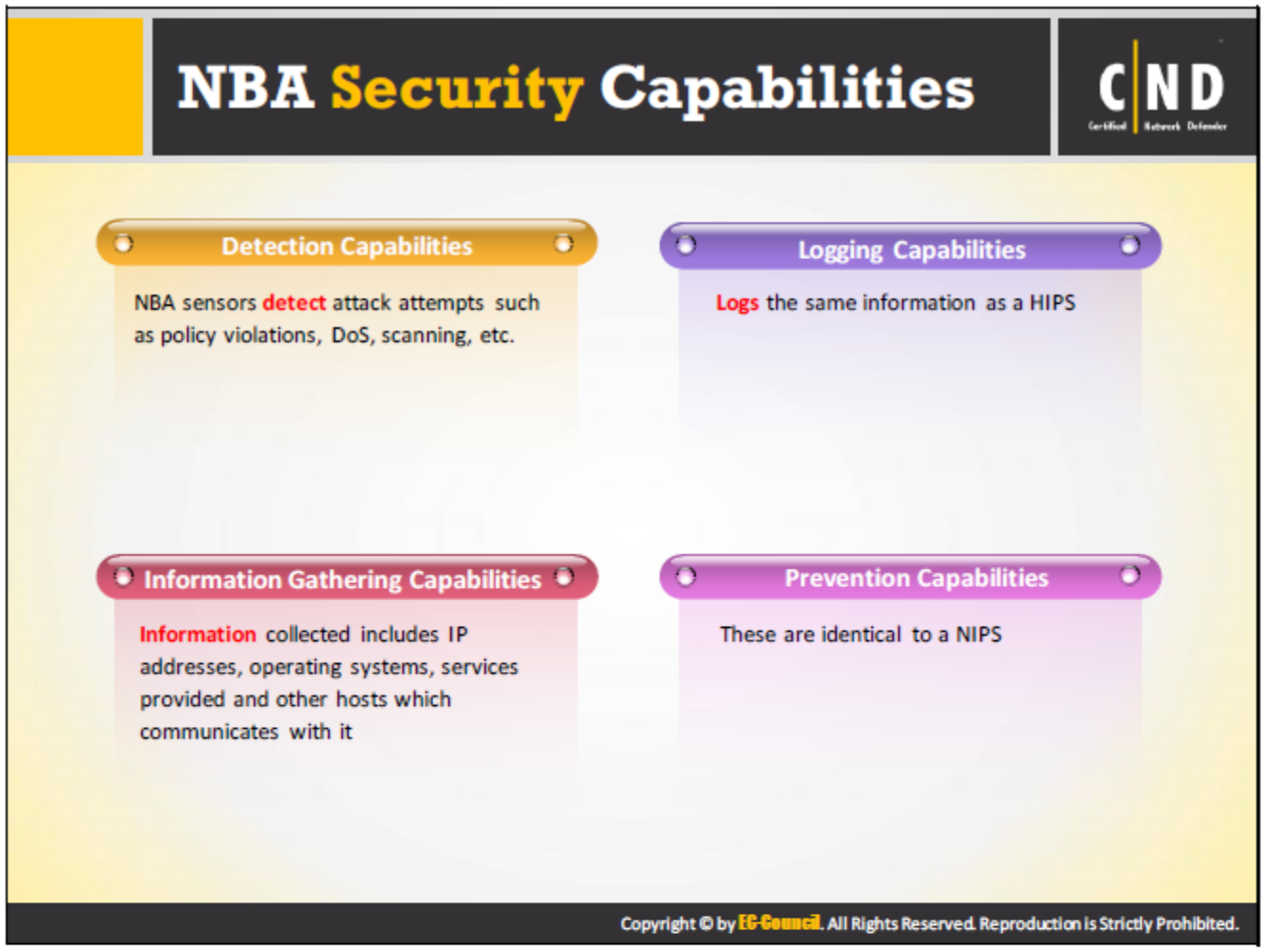
A NBA system can be deployed as a separate management network or as part of a corporate network. The NBA system is comprised of sensors and consoles, also some NBA products offer management servers (sometimes referred to as analyzers). Generally though, NBA sensors are available as a hardware appliance. Some sensors act similar to NIDPS to sniff packets and monitor traffic on network segments. Whereas, other senors depend on the network flow information given by routers, switches and other networking devices. Here, flow is the communication sessions taking place between hosts. Flow data formats have many standards, including NetFlow, sFlow etc. The intrusion detection is done based on:

- Source and destination IP addresses
- Source and destination TCP or UDP ports or ICMP types and codes
- Number of packets and number of bytes transmitted in the session
- Timestamps for the start and end of the session

Choosing the right place to deploy devices is equal to selecting the appropriate device in the network. Depending on the location, the NBA sensor can be either passive or inline. Most of the NBA sensors use the same connection techniques (such as network tap, switch spanning port) as NIDPS that can be deployed in passive mode. Passive sensors directly monitor the network traffic, so they can be placed in demilitarized zone (DMZ) subnets.

Inline sensors are placed at network boundaries or in close border firewalls. For instance, a NBA inline sensor deployed between the firewall and the Internet perimeter router is able to restrict

incoming attacks which overcome the firewall. Some products offer the combination of both NBA and IPS providing IPS or firewall functions. NBA sensors can be deployed in passive mode to collect the data from the switches.



The NBA system offers a variety of security capabilities that can be classified into four categories:

- Information capabilities
- Logging capabilities
- Detection capabilities
- Prevention capabilities

Information Capabilities

NBA systems gather information about hosts which is required for most of the NBA system's detection methods. NBA sensors have the ability to automatically create and maintain a list of hosts that are included across the organization's monitored network. These sensors gather detailed information by monitoring the port usage, implements passive fingerprinting and other techniques on the host. The information obtained for each host includes the IP address, operating system, services provided by it such as IP protocols, TCP and UDP ports used by it, other hosts interacting with this host, services used, IP protocols, and TCP or UDP ports it connects to. The NBA sensors monitor this information consistently for any changes.

Logging Capabilities

NBA systems log detected anomalies. The data fields logged by the NBA system are:

- timestamp (date and time)

- Alert type
- Source and destination IP addresses
- Rating priority, severity, etc.
- Protocols at application, transport and network layers
- Source and destination TCP or UDP ports or ICMP types and codes
- Additional packet header fields such as IP time-to-live
- Number of bytes and packets
- Prevention action

Detection Capabilities

An NBA system detects different types of malicious behavior that has significant deviations from normal behavior. To monitor and analyze the network activity most of the NBA system uses anomaly-based detection and stateful protocol analysis methods. NBA sensors can detect the following types of events:

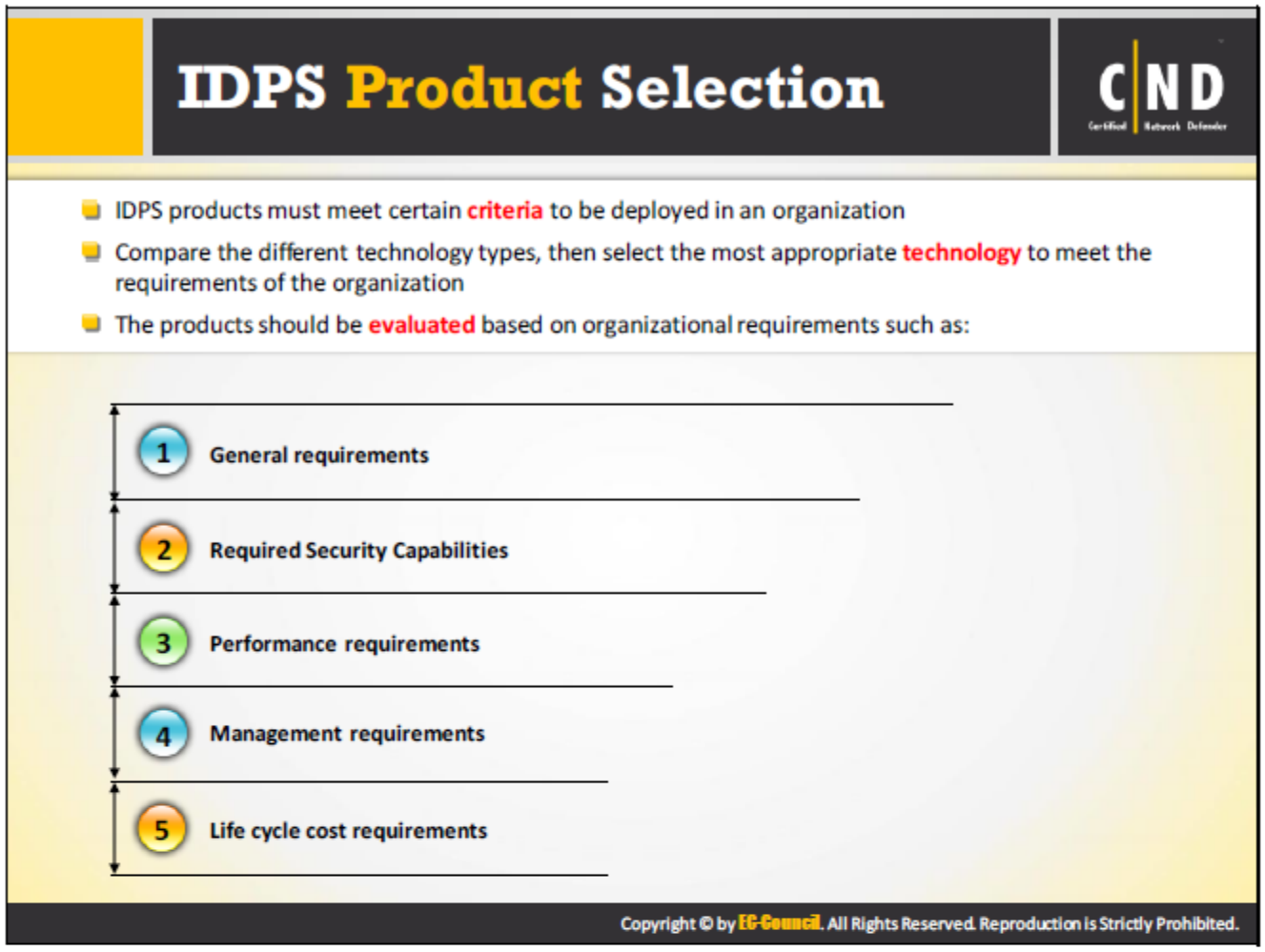
- **Denial of Service (Dos) and Distributed Denial of Service (DDoS) Attack:** If a host utilizes increased bandwidth, the NBA analyzes this type of activity and determines if it violates the normal traffic behavior to detect these types of attacks.
- **Scanning:** The IDS detects scanning attacks by noticing abnormal flow patterns at different layers, such as banner grabbing at the application layer, TCP and UDP port scanning at the transport layer and ICMP scanning at the network layer.
- **Worms:** The IDS can detect worms in more than one way as it depends on the behavior of a worm, such as its propagation, causing hosts to use undesirable ports, etc. For example, if a network has a worm infection, the NBA sensor can examine the worm's flow and identify the host that first transmitted the worm in the network.
- **Unexpected Application Services:** To detect unexpected application services such as tunneled protocols, backdoors, use of prohibited application protocols etc., The NBA uses stateful protocol analysis techniques.
- **Policy Violations:** In most NBA sensors, it is possible to create detailed policies such as hosts, groups of hosts, communication between them, permitted activity, time period etc. They also have the ability to detect policy violations such as running unauthorized services etc.

Prevention Capabilities

The NBA system provides various intrusion prevention capabilities. The configuration of a NBA sensor considers different types of alerts raised by NBA sensors in order to determine the kind of prevention capability required to block a specific known threat. According to the type of sensor, the following are the prevention capabilities of a NBA sensor:

- **Passive sensor**: Terminates the session by sending a TCP reset (RST) packet to both endpoints of a communication line.
- **Inline sensor**: Performs inline firewall functions to allow or deny any suspicious network traffic.
- **Both passive and inline**: Most NBA sensors have the ability to instruct network security devices to perform reconfiguration to restrict certain types of attacks.
- **Running a third-party program or script**: If any malicious activity is detected, some NBA sensors have the ability to run as an administrator-specified script or program.

Most NBA systems use limited prevention capabilities because of false positives, as blocking a single false positive may disturb the entire network.

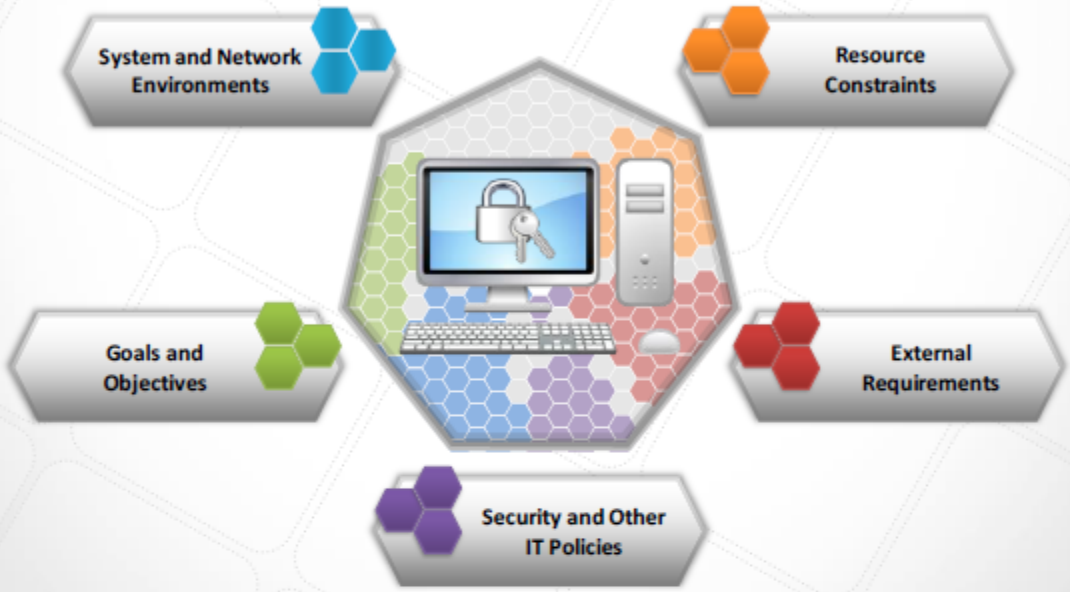


The selection of any IDPS product depends on whether the IDPS products meet certain requirements. The selection process consists of assessing the four aspects of IDPS technologies, they include security capabilities, performance, management, and life cycle cost.

Organizations should determine a particular type of IDPS technology such as network-based, wireless, network behavior analysis (NBA), or host-based that best suits their requirement. The organization should conduct a risk management to identify security measures required to mitigate the risk identified.

IDPS Product Selection: General Requirements

- Evaluate the general requirements the IDPS products will have to meet post deployment
- Size of an organization also modifies the number of IDPS products needed



IDPS Product Selection: General Requirements (Cont'd)

System and Network Environments

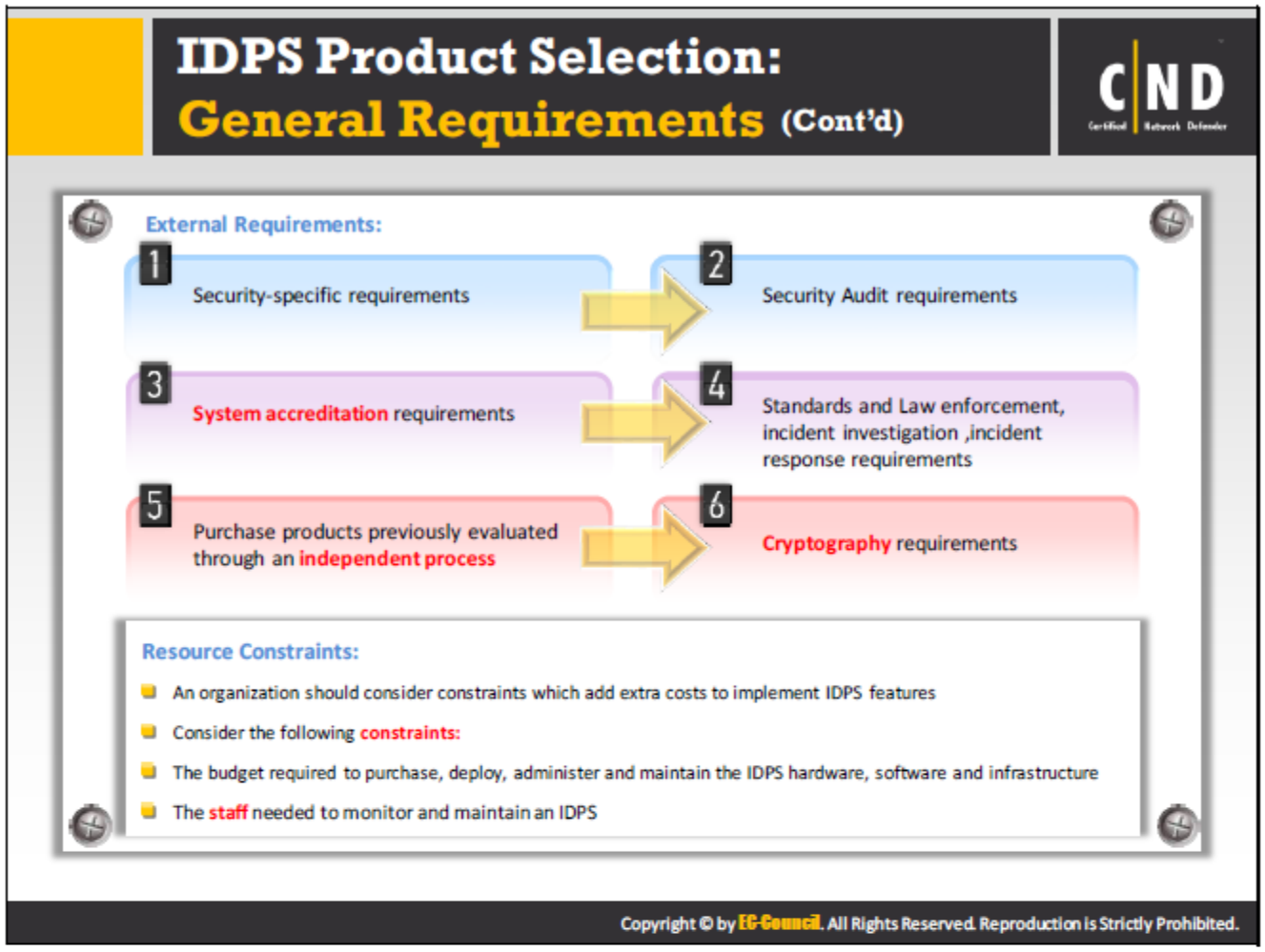
- An organization's characteristics such as system and network environments should be evaluated and examined if the selected IDPS is compatible with them and the capabilities include event monitoring
- Consider the following characteristics
  - Technical specifications of the IT environment
  - Technical specifications of the existing security protections

Goals and Objectives

- An organization should decide whether a particular IDPS solution satisfies their technical, operational, business goals and objectives behind the reason for implementing an IDPS
- Consider the following questions while articulating goals and objectives
  - Which type of threats does an IDPS protect against?
  - Will an IDPS be able to monitor activities against acceptable use, violations, non-security reasons, etc.?

Security and Other IT Policies

- Review the current security and IT policies and evaluate whether a certain IDPS will offer the specified protection to meet an organization's policies
- Consider the following points when selecting and IDPS product:
  - Policy goals
  - Reasonable use policies
  - Policy violations and consequences



An organization needs to have a clear baseline of the requirements for an IDPS product. Each IDPS solution may differ in features and services. An organization needs to determine which IDPS product will suit their requirements the best. For example, there are situations where a single IDPS product may not satisfy the requirements of an organization. This scenario encourages the use of multiple IDPS products. Wireless IDPS products have certain general requirements such as a method of detecting anomalies and the process of connecting to other components that decide if the product can satisfy the company's requirements.

The selection of an IDPS depends on the following general requirements:

System and Network Environments

The network administrator should be able to select the IDPS product according to the requirements of an organization and its network configuration. Also, the selected IDPS product should be able to detect and log interesting events that the organization wants to evaluate and examine. Consider the following characteristics:

- Technical specifications of the IT environment.
- Technical specifications of the existing security protections.

Goals and Objectives

The network administrator must evaluate their product for the technical, operational, business goals and objectives. Consider the following characteristics:

- Which type of threats will the IDPS monitor?
- Will it monitor acceptable use violations?

Security and Other IT Policies

The network administrator should review their security policies prior to selecting the IDPS product. Consider the following characteristics:

- Policy Goals
- Reasonable use policies
- Consequences of no compliance with policies

External Requirements

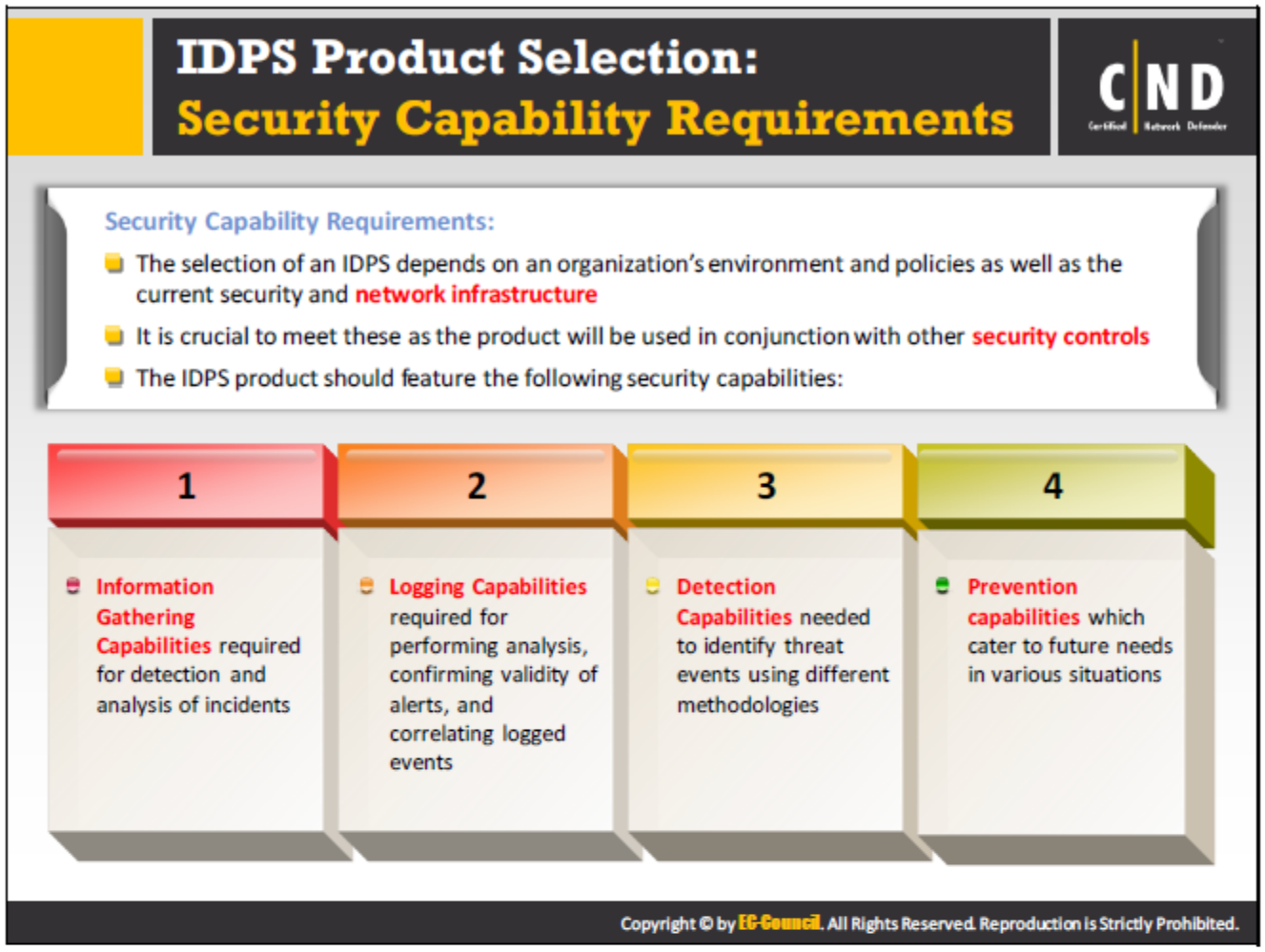
If the organization is supposed to undergo a review by other organizations, an administrator will need to assess whether they can review the IDPS implementation in their organization.

- Security-specific requirements help in the investigation of security violations incidents.
- Audit requirements are specific functions an IDPS must support.
- System accreditation requirements help an administrator address the accreditation authority's requirements.
- Law enforcement investigations and the resolution of security incident requirements.
- Purchase products previously evaluated through an independent process requirement.

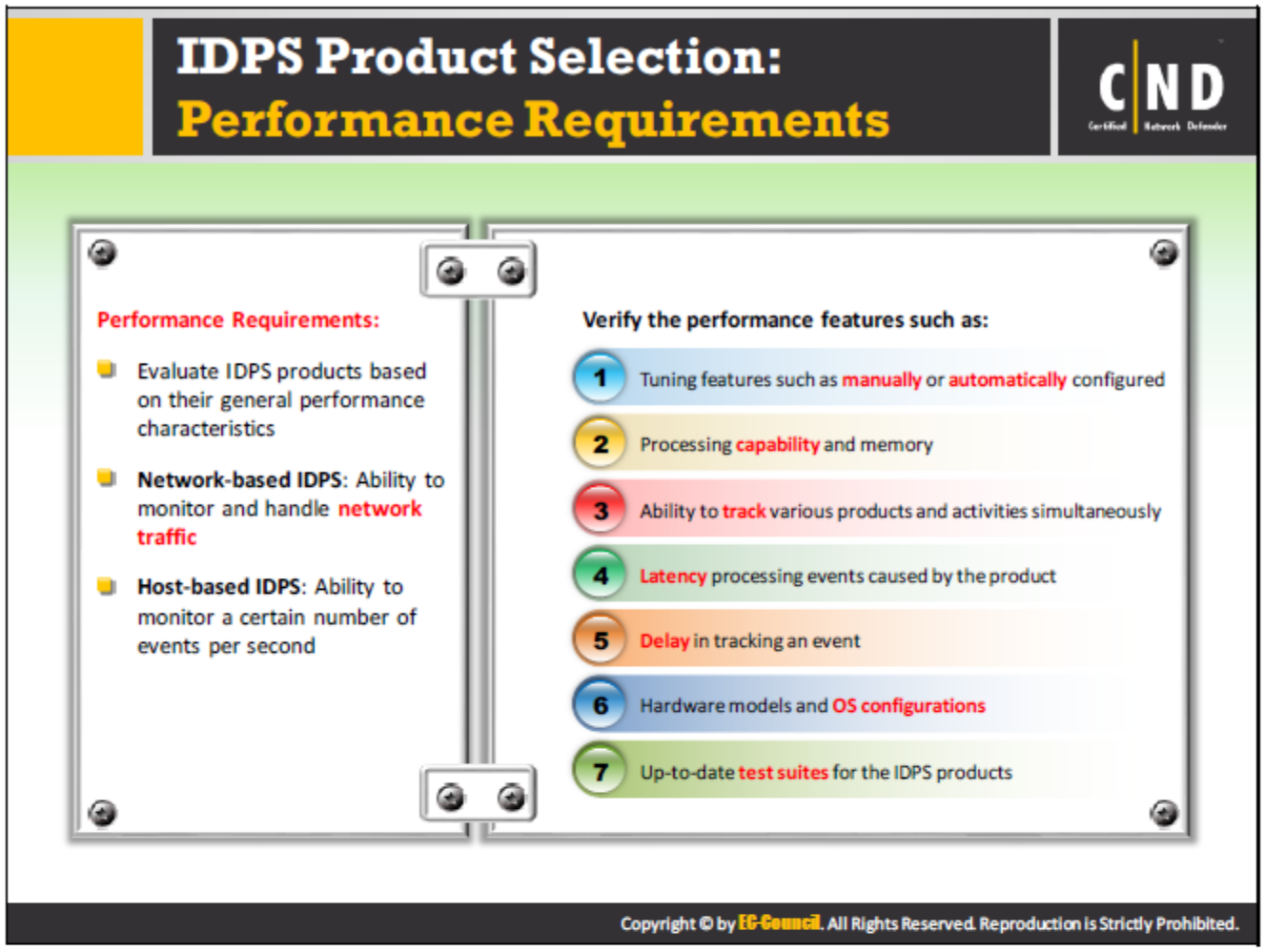
Resource Constraints

Administrators should also consider their adequacy in terms of system or personnel to handle the IDPS feature that they are thinking of implementing. Expenses on additional IDPS features will be in vain, if the organizations do not have enough resources to handle them. Network administrators must consider the following constraints:

- The budget for purchasing, implementing and maintaining IDPS hardware, software and structure.
- The staff needed to monitor and maintain an IDPS.



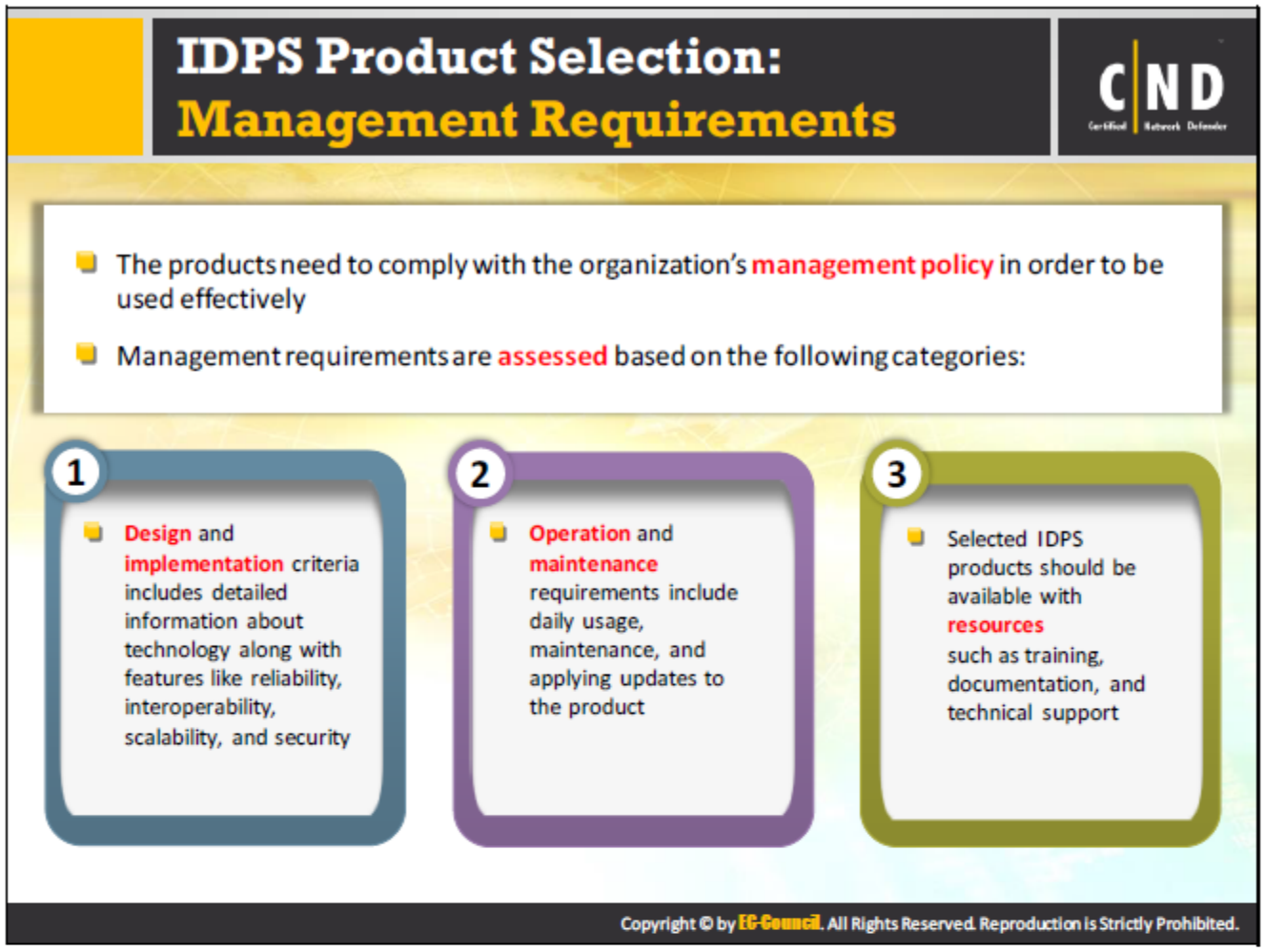
In addition to defining general requirements, the network administrator needs to define a specialized set of requirements. Organizations should evaluate IDPS security capability requirements as a baseline for creating a specific set of criteria. This is done by taking their environment, security policies and network infrastructure into consideration. It is important to check and confirm the security capabilities of an IDPS product. The IDPS products that do not meet the required security capabilities is of no use as a security control and an administrator must select a different product or use that product in combination with another security control. The IDPS product should feature security capabilities such as information gathering, logging, detection and prevention.



Network administrators must evaluate an IDPS product's general performance characteristics by assessing the capacity to handle the network traffic or packet monitoring capabilities for network-based IDPS and event monitoring capabilities for host-based IDPS.

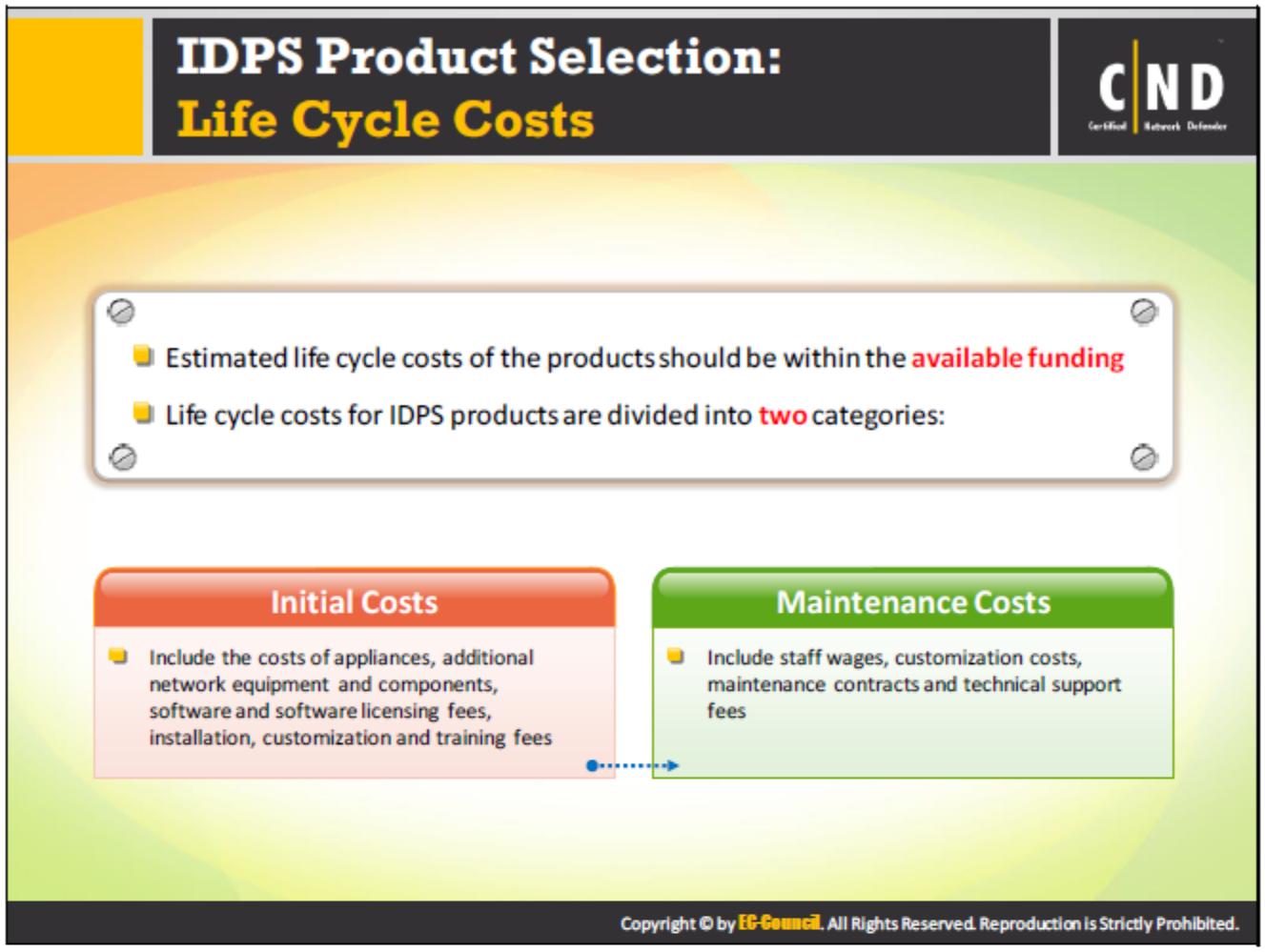
Verify the performance features such as:

- Verify tuning features of an IDPS as its performance is dependent on product configuration and tuning.
- Check for the processing capability and memory.
- Ability to track various product state activities simultaneously.
- Latency of processing events caused by the product.
- Delay in tracking an event.
- Hardware models and OS configurations.
- Up-to-date test suites for the IDPS products.



The products need to comply with the organization's management policy in order to offer better performance. If the products do not comply with the company's policy, it would be difficult to handle and make it work effectively. Management requirements for an IDPS include categories such as:

- Design and implementation criteria include detailed information about the technology type used in the product along with features like reliability, interoperability, scalability and security.
- Operation and maintenance requirements include daily usage, maintenance and applying updates to the product.
- The IDPS product should offer better interoperability, which refers to the process of offering effective performance while working in combination with existing systems.
- Selected IDPS products should be available with resources such as training, documentation, and technical support.
- The products should offer scalability, so that the company would be able to increase or decrease the product quantity to meet future requirements.



IDPS products are environment specific and can be a tedious task for organizations to quantify the cost of IDPS solutions. The cost of the IDPS product should be proportional to the available budget of the organization. Estimated life cycle costs of the selected IDPS products should be in the range of the available funding. Selecting an IDPS based on cost is difficult as the environment, security and other networking criteria are liable to dominate the situation. Life cycle costs of the IDPS products include categories such as:

Initial Costs

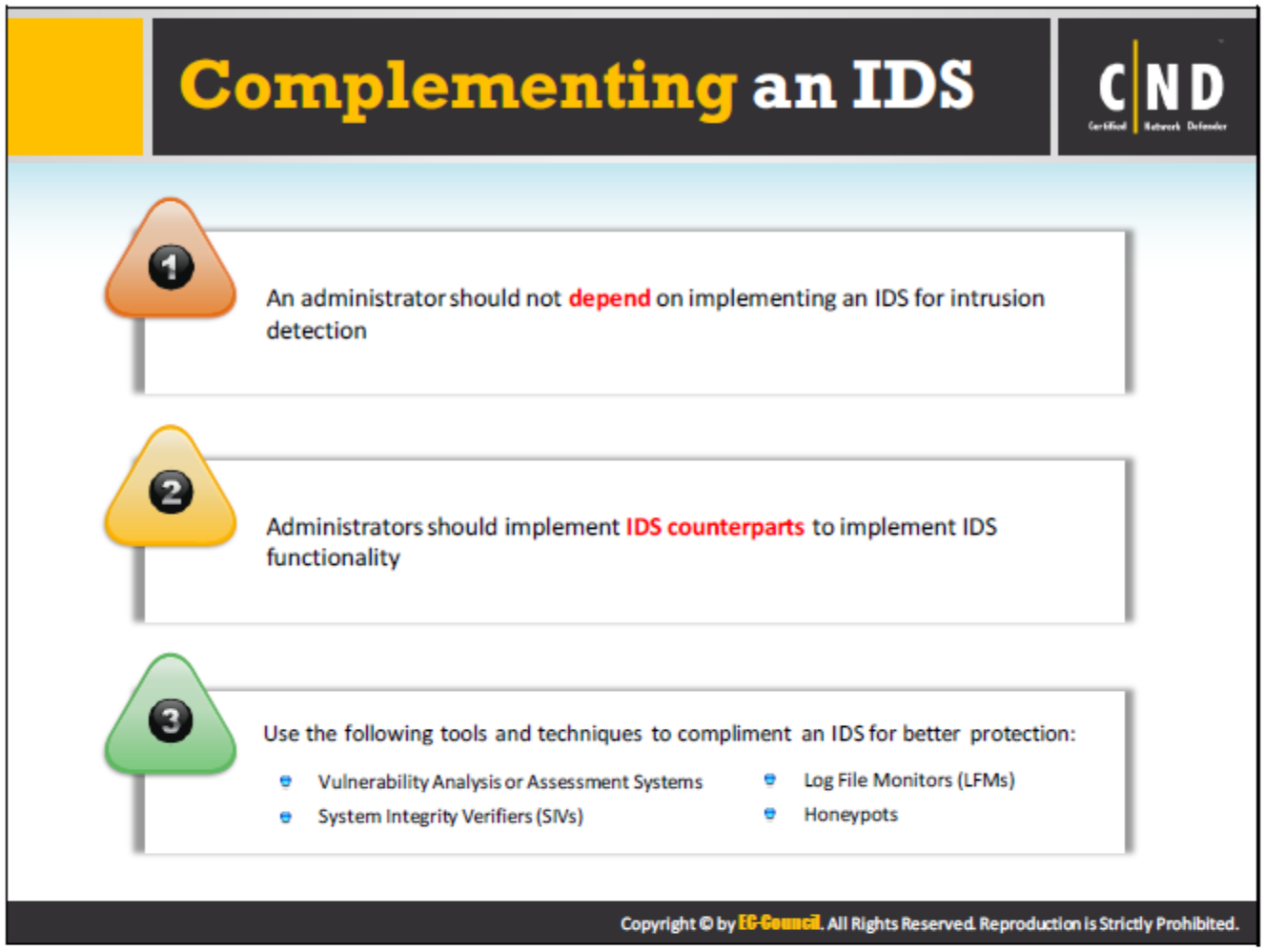
Initial cost is the starting point for all IDPS product calculations. It includes:

- Cost for deploying hardware or software tools: It involves the cost of network appliances, IDS load balancers, software tools such as reporting tools, database software, etc.
- Installation and configuration costs: This cost includes internal or external labor for fixing systems, network appliances or installing network or system accessories.
- Cost of application customization: This type of cost involves the programmers or developers who develop scripts or applications for maintaining the security.
- Cost for training and awareness: It involves the cost for training and its awareness among the administrators.

Cost of maintenance

Usually organizations do not have a standard for measuring the cost of maintenance, this results in different costs of maintenance within the same organization. The cost of maintenance within the organization includes:

- Cost of Labor: Cost of labor includes the cost of staff handling the IDPS solutions and the administration.
- Cost of technical support: Organizations using external technical support from the third-party services are required to pay costs for technical support services.
- Cost of professional services: Technical support vendors that do not provide IDPS solution services fall under professional services. Organizations using service support from these IDPS vendors or third-parties are required to pay the costs of these professional services.



Although various types of IDPS and their hybrid solutions are used to detect and prevent intrusions on a network, they are not always sufficient to detect specific types of intrusions. Solutions are required which specialize in detecting a specific type of intrusions. There are other technologies and solutions that act as counterparts to an IDS and help you detect various types of intrusions on the network. IDPS solutions are more generalized whereas these solutions are meant for targeting specific types of intrusions and therefore are more specialized. These solutions, if implemented can provide add-on security to the network. Some of the specialized intrusion detection systems are:

- Vulnerability Analysis or Assessment Systems
- System Integrity Verifiers (SIVs)
- Log File Monitors (LFMs)
- Honeypots

Vulnerability Analysis or Assessment Systems

- Vulnerability Assessment is performed to test whether a network or host is vulnerable to known attacks

Vulnerability analysis are classified as

Host-based Vulnerability Analysis

- It involves checking system data sources such as file contents, configuration settings, and other status information to identify possible vulnerabilities
- A vulnerability analyzer is considered as having permission to access the host as a result is also known as credential-based assessment

Network-Based Vulnerability Analysis

- It involves simulating various attacks and recording the responses to identify possible vulnerabilities
- A vulnerability analyzer performing vulnerability analysis regardless of whether it has permission to access the target system or not, is known as a non-credential-based assessment

Advantages & Disadvantages of a Vulnerability Analysis

Advantages

- Helps detect problems on systems where an IDS cannot be deployed
- Supports security testing capabilities
- Spot changes in security states reliably
- Mitigates a set of security problems

Disadvantages

- Expensive to build, maintain and manage a vulnerability analysis system
- Less accurate and has a high false alarm rate
- Some vulnerability checks can crash the system

A vulnerability assessment helps the network administrator decide whether a host or a network is susceptible to any kind of attack. These tests help the company design a framework for how vulnerabilities affect the system and provide details about the intrusion detection process.

The vulnerability assessment should address issues related to human errors and also monitor for any compliance issues with existing devices.

Vulnerability analysis processes include the following categories:

- **Host-based Vulnerability Analysis:** The system determines vulnerabilities by assessing system data sources such as file contents, configuration settings, and other status information.

  The credential-based assessment system gathers information from different hosts, as it has access to those hosts. Information is usually accessible using standard system queries and inspection of system attributes.

- **Network-based Vulnerability Analysis:** These vulnerability analysis systems require a remote connection to the target system. They re-enact system attacks, noting and recording responses to these attacks or simply probe different targets to infer weaknesses from their responses regardless of whether it has permission to access the target system.

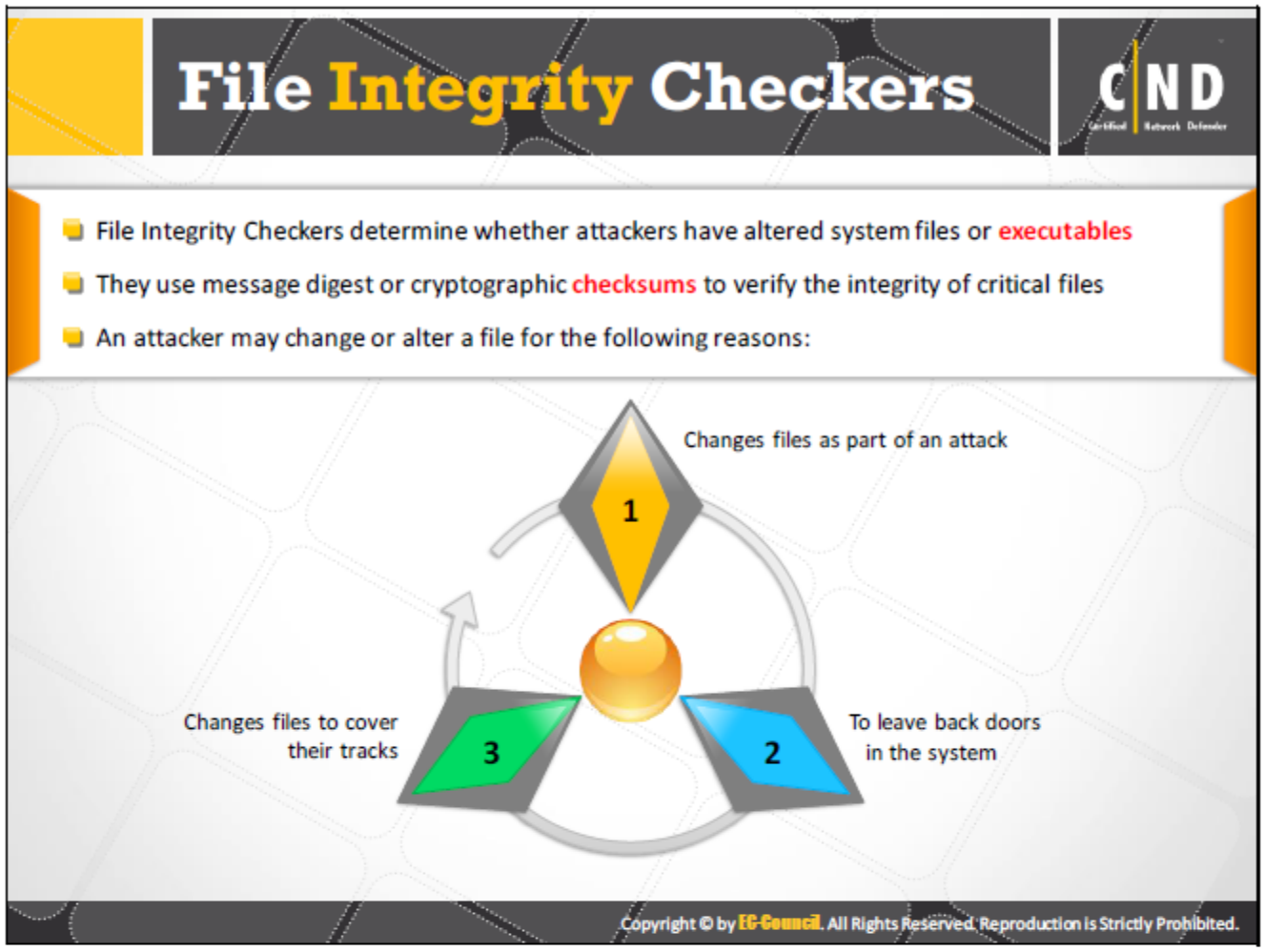
This type of vulnerability analysis is a non-credential assessment and is capable of deploying an interference method.

Advantages

- Vulnerability analysis allows detection of problems on systems that cannot support an IDS.
- Provide security-specific testing capabilities that record the current security state of the systems.
- Vulnerability analysis systems spot changes in the security state and offer correction procedures, when used on a regular basis.
- The tests help the companies to ensure mitigation of security problems and provide methods to double-check the changes made to systems.

Disadvantages

- Vulnerability analysis systems are costly to build, maintain, and manage, as they require specific operating systems and applications.
- Certain vulnerability analysis systems are platform-independent and less accurate.
- Some systems that analyze denial-of-service attacks are liable to crash the systems they are testing.
- Repeated network-based assessments are liable to train certain IDSs to ignore real attacks.



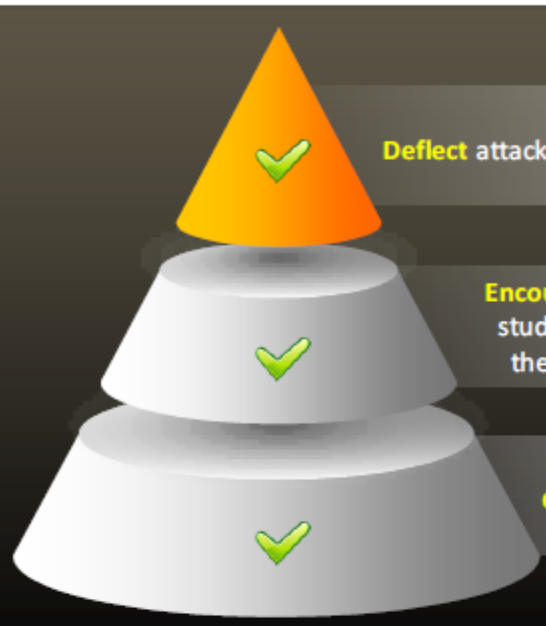
File Integrity Checkers are security tools that complement an IDS and are used to determine a change in system files or executables. They utilize message digest or cryptographic checksums for critical files and objects and compare them to reference values for flagging differences or changes.

The checkers also help determine whether vendor-supplied bug patches or other changes are made to system binaries. Cryptographic checksums are important, as attackers often alter system files, at three stages of an attack such as:

- They alter system files as the goal of the attack.
- They attempt to leave back doors in the system through which they can re-enter system.
- They attempt to cover their tracks so that system owners will be unaware of the attack.

Honey Pot & Padded Cell Systems

Honey pots are decoy systems that are designed to:



- **Deflect** attackers from gaining access to critical systems
- **Encourage attackers** to stay on the system in order to study their unauthorized attempts and respond to them
- **Gather information** on an attacker's activity

Honey Pot & Padded Cell Systems (Cont'd)

- A padded cell is a simulated environment where attackers are contained once they are detected.
- The simulated environment is different from a live environment and it contains fake data and attackers cannot harm the actual live environment
- A padded cell and a traditional IDS operate simultaneously i.e. When the IDS detects the intrusion from the attacker, it seamlessly transfers the attackers to a special padded cell host

Advantages	Disadvantages
Helps divert attackers to different targets they cannot damage	Legal implications for these devices are not well defined
Gives extra time to decide when responding to the incident	Attackers may be encouraged to launch a more hostile attack
Easy and extensive monitoring helps to refine threat models and improve system protections	A high level of expertise is required to use these systems
Effective at catching employees who are snooping around the network	

Honey pots

Honey pots are decoy systems designed to lure potential attackers away from critical systems and encourage attacks against themselves. The defender may lure them away from actual targets, perhaps detect their presence, and then block access. This approach has the risk of perhaps luring attackers into the defender's network. Honey pots are decoy systems which perform important tasks such as:

- Diverting attackers from accessing critical systems.
- Gather information on an attacker's activity.
- Encourages an attacker to stay on the system for a long time.

The system stores information to make it seem crucial to the attacker and lures them to attempt an attack. The system features monitors and event loggers that detect attacker attempts to access the honey pot and collect information.

Padded cell Systems

A padded cell is a protected honey pot that cannot be compromised easily. In addition to attracting attackers with tempting data, a padded cell operates in tandem with a traditional IDS. When the IDS detects an attacker, it seamlessly transfers them to a special simulated environment where they can cause no harm—the nature of this host environment is what gives the approach its name, padded cell.

A padded cell system is similar to the honey pot as it performs intrusion isolation using a different approach. Padded cell and a traditional IDS operate simultaneously, i.e., when the IDS detects an attacker, it seamlessly transfers them to a special padded cell host. Once attackers are in the padded cell, they are captured within a simulated environment where they can cause no harm and keep on thinking that the attack has been successful.

Commercial production of padded cell systems has not started, as these systems need certain permissions from legal counsel for operating in a live environment.

Advantages

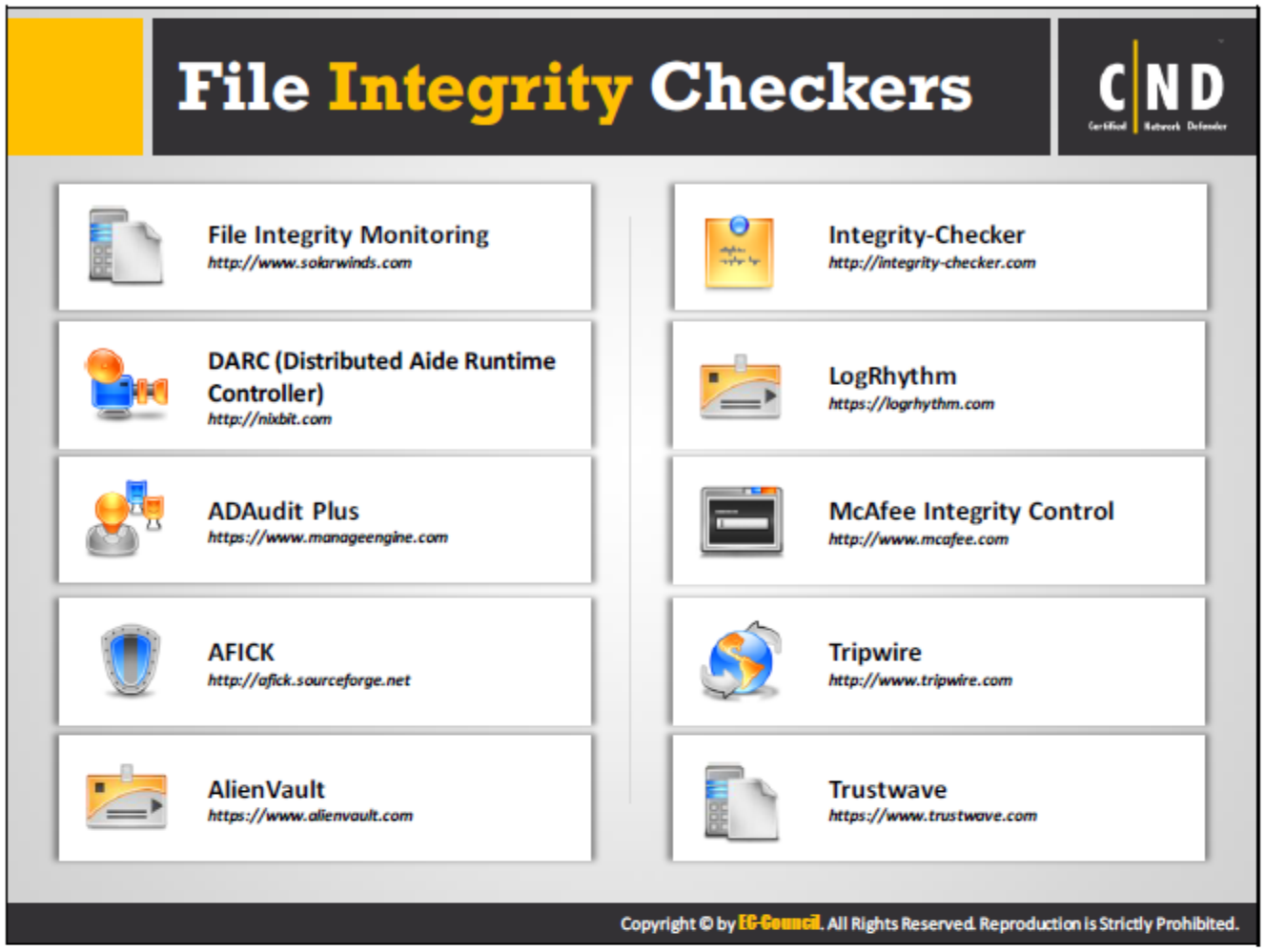
Usage of honey pots and padded cell systems enables various functions such as:

- Attackers can be diverted to system targets that they cannot damage
- Administrators have additional time to decide how to respond to an attacker
- Easy and extensive monitoring helps to refine threat models and improve system protections
- Effective at catching employees who are snooping around the network

Disadvantages

Disadvantages of using honey pots and padded cell systems are:

- The legal implications of using such devices are not well defined.
- An expert attacker, once diverted into a decoy system, may become angry and launch a more hostile attack against an organization's system.
- In order to use these systems, a high level of expertise is needed.



File Integrity Monitoring

File Integrity Monitoring

Source: *http://www.solarwinds.com*

File Integrity Monitoring is used to detect and alert when there are changes to key files, folders and registry settings.

DARC (Distributed Aide Runtime Controller)

Source: *http://nixbit.com*

Distributed Aide Runtime Controller detects file system changes in UNIX environments, which is useful for forensics on compromised systems and tracing illicit system configuration changes. DARC provides a mechanism to run AIDE integrity checks across many UNIX systems from a single management station.

ADAudit Plus

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

ADAudit Plus's File Integrity Monitoring (FIM) feature is critical for Microsoft Windows network security, with respect to changes to configurations, files and file attributes (DLL, exe and other system files).

AFICK

Source: *http://afick.sourceforge.net*

AFICK is a portable security tool that monitors the changes on your file systems, and can detect intrusions.

AlienVault

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

AlienVault's File Integrity Monitoring (FIM) alerts you to changes in critical system files, configuration files, and content files.

Integrity-Checker

Source: *http://integrity-checker.com*

Integrity-Checker verifies the integrity of files on your Windows server. It supports WSSX integration so you can access all functionality directly from the server's dashboard on Server 2012 Essentials, Windows Home Server 2011, SBS 2011 Essentials, and Storage Server 2008 R2.

LogRhythm

Source: *https://logrhythm.com*

LogRhythm's File Integrity Monitoring protects your organization's critical files, wherever they're stored. It sends alerts on malware-related registry changes, improper access of confidential files, and theft of sensitive data.

McAfee Integrity Control

Source: *http://www.mcafee.com*

McAfee Integrity Control checks files and directories for changes to content and permissions. It provides continuous file integrity monitoring, essential for verifying the security of an environment and meeting compliance requirements.

Tripwire

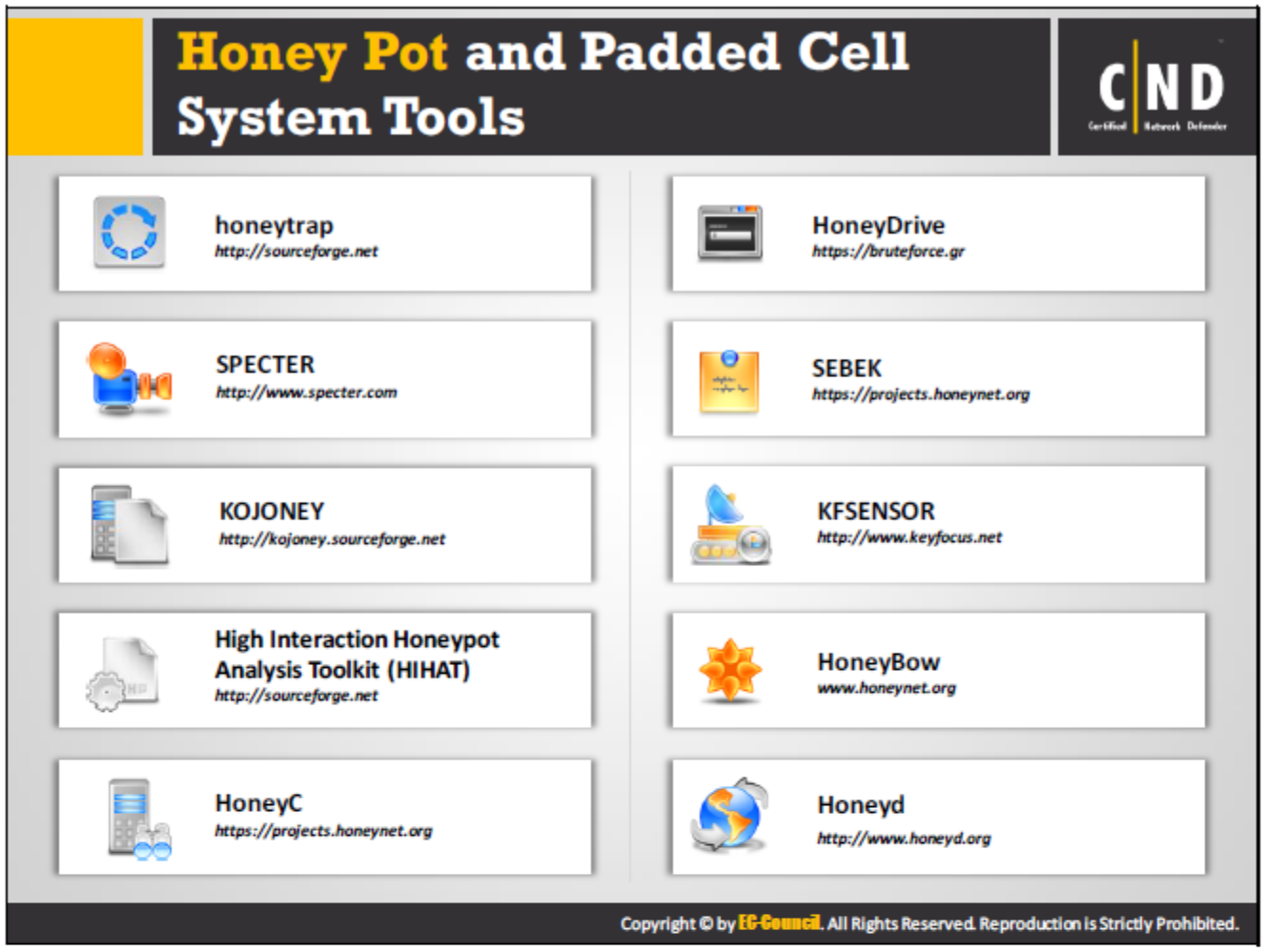
Source: *http://www.tripwire.com*

Tripwire File Integrity Monitoring is available as a standalone solution or as part of Tripwire's Security Configuration Management suite. With Tripwire, you have continual assurance of the integrity of security configurations, complete visibility and control of all changes for your continuous monitoring, change audit and compliance demands. Tripwire File Integrity Monitoring (FIM) has the unique, built-in capability to reduce noise by providing multiple ways of determining low-risk change from high-risk change as part of assessing, prioritizing and reconciling detected change.

Trustwave

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

Trustwave File Integrity Monitoring monitors OS and registry file data on Windows-based POS devices, laptops, desktops and servers.



honeytrap

Source: *http://sourceforge.net*

Honeytrap is a low-interaction honeypot daemon for observing attacks against network services. It monitors the network stream for incoming sessions and starts appropriate listeners just in time. Each listener can handle multiple connections and terminates itself after being idle for a certain length of time.

SPECTER

Source: *http://www.specter.com*

SPECTER is a honeypot-based intrusion detection system that simulates a vulnerable computer, providing an interesting target to lure hackers away from production machines.

KOJONEY

Source: *http://kojoney.sourceforge.net*

Kojoney is a low-level interaction honeypot that emulates an SSH server, and the daemon written in Python using the Twisted Conch libraries.

High Interaction Honeypot Analysis Toolkit (HIHAT)

Source: *http://sourceforge.net*

The High Interaction Honeypot Analysis Toolkit (HIHAT) allows transforming arbitrary PHP applications into web-based high-interaction Honeypots. Furthermore, it provides a graphical user interface, which supports the process of monitoring the Honeypot and analyzing the acquired data. A typical use could be the transformation of PHPNuke, PHPMyAdmin or OSCommerce into a full functional Honeypot, which offers the complete functionality of the application to the users but performs comprehensive logging and monitoring in the background.

HoneyC

Source: *https://projects.honeynet.org*

HoneyC is a low interaction client honeypot / honeyclient that allows the identification of rogue servers on the web.

HoneyDrive

Source: *https://bruteforce.gr*

HoneyDrive is the premier honeypot Linux distro. It is a virtual appliance (OVA) with Xubuntu Desktop 12.04.4 LTS edition installed. It contains over 10 pre-installed and pre-configured honeypot software packages such as Kippo SSH honeypot, Dionaea and Amun malware honeypots, Honeyd low-interaction honeypot, Glastopf web honeypot and Wordpot, Conpot SCADA/ICS honeypot, Thug and PhoneyC honeyclients and more.

SEBEK

Source: *https://projects.honeynet.org*

Sebek is a kernel module installed on high-interaction honeypots for the purpose of extensive data collection. It allows administrators to collect activities such as keystrokes on the system in encrypted environments and mainly used for Win32 and Linux systems.

KFSENSOR

Source: *http://www.keyfocus.net*

KFSensor is a Windows based honeypot Intrusion Detection System (IDS) that acts as a honeypot to attract and detect hackers and worms by simulating vulnerable system services and Trojans. By acting as a decoy server, it can divert attacks from critical systems and provide a higher level of information than can be achieved by using firewalls and NIDS alone. Windows based corporate environments use KFSensor and it contains unique features such as remote management, a Snort compatible signature engine and emulations of Windows networking protocols. With its GUI based management console, extensive documentation and low maintenance, KFSensor provides a cost effective way of improving an organization's network security.

HoneyBow

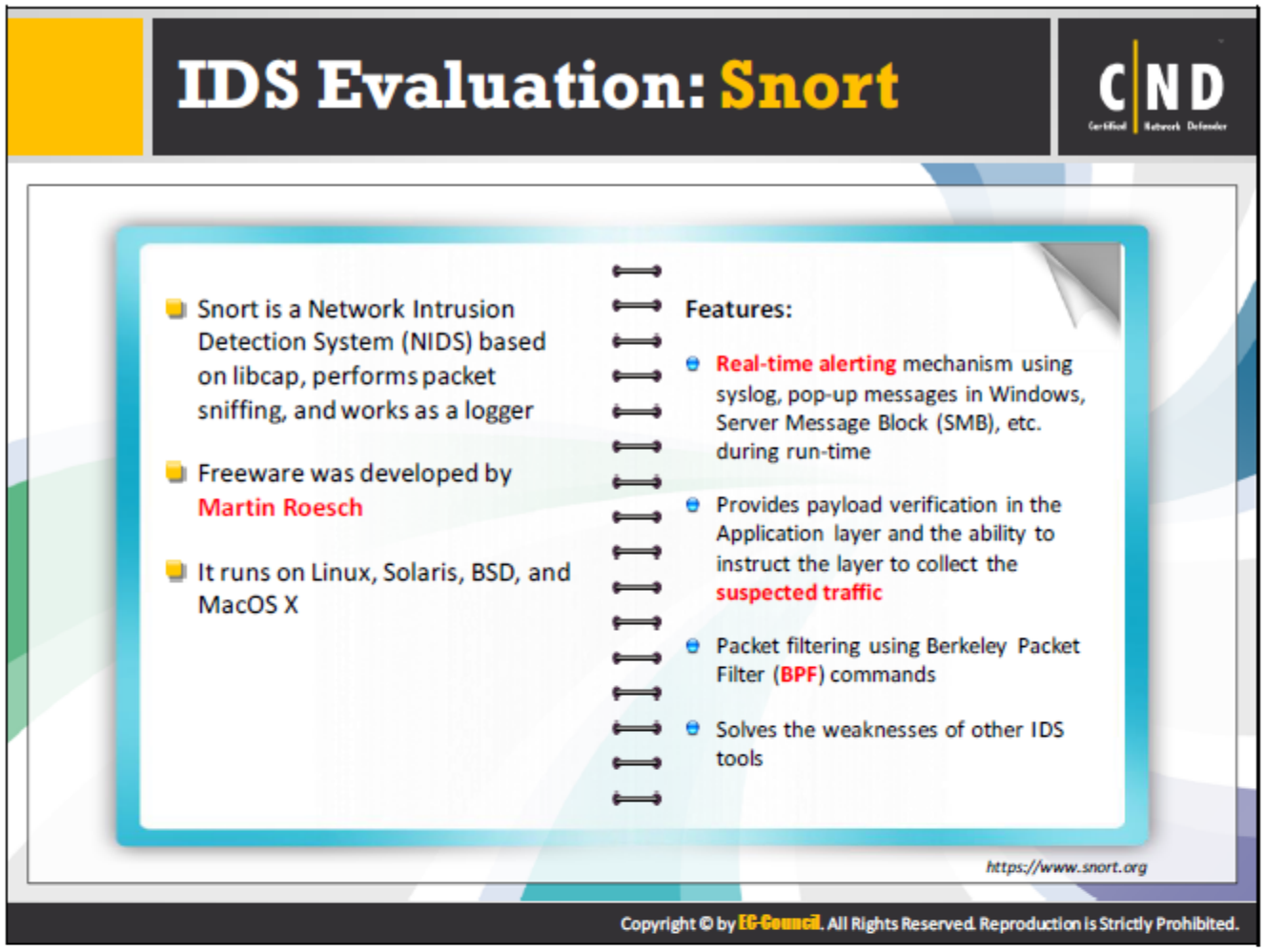
Source: *https://www.honeynet.org*

HoneyBow is a high-interaction malware collection toolkit with integration with nepenthes and the mwcollect Alliance's GOTEK architecture.

Honeyd

Source: *www.honeyd.org*

This is a low-interaction honeypot used for capturing attacker activity. Honeyd is a small daemon that creates virtual hosts on a network configured to run arbitrary services, and their personality can be adapted so they appear to be running certain operating systems. Honeyd enables a single host to claim multiple addresses. Honeyd improves cyber security by providing mechanisms for threat detection and assessment. It also deters adversaries by hiding real systems in the middle of virtual systems.



Snort is an open source network intrusion detection and prevention system developed by Martin Roesch. It is capable of performing live traffic analysis, packet sniffing, and packet logging on IP networks. It can perform protocol analysis and content searching/matching. It can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting, attempts etc. Snort supports various platforms such as Windows, Linux, Solaris, BSD, and Mac OS X.

The NIDS functionality of snort is based on libcap. Snort uses a flexible rules language to describe traffic that it should collect or pass, as well as a detection engine that utilizes a modular plug-in architecture. Snort has a live alerting capability as well, incorporating alerting mechanisms for syslog, a user specified file, a UNIX socket, or WinPopup messages to Windows clients.

Snort has three primary uses: a straight packet sniffer like tcpdump, a packet logger (useful for network traffic debugging, etc.), or a full-blown network intrusion prevention system.

Features

- Live alert mechanism using syslog, pop-up messages in Windows, Server Message Block (SMB), etc. during run-time.
- Provides pay load verification in the Application layer and the ability to instruct the layer to collect the suspected traffic.
- Packet filtering using Berkeley Packet Filter (BPF) commands.

- Solves the weaknesses of other IDS tools.

Snort: Installation

Snort is a "lightweight" NIDS, non-intrusive, easily configured, utilizes familiar methods for rule development and takes only a few minutes to install.

SNORTSNARF is a script for alerts from the Snort IDS which is run at regular intervals to generate a convenient HTML output of all the alerts. SNORTSNARF comes with a load of options that performs automatic review.

Planning a Deployment

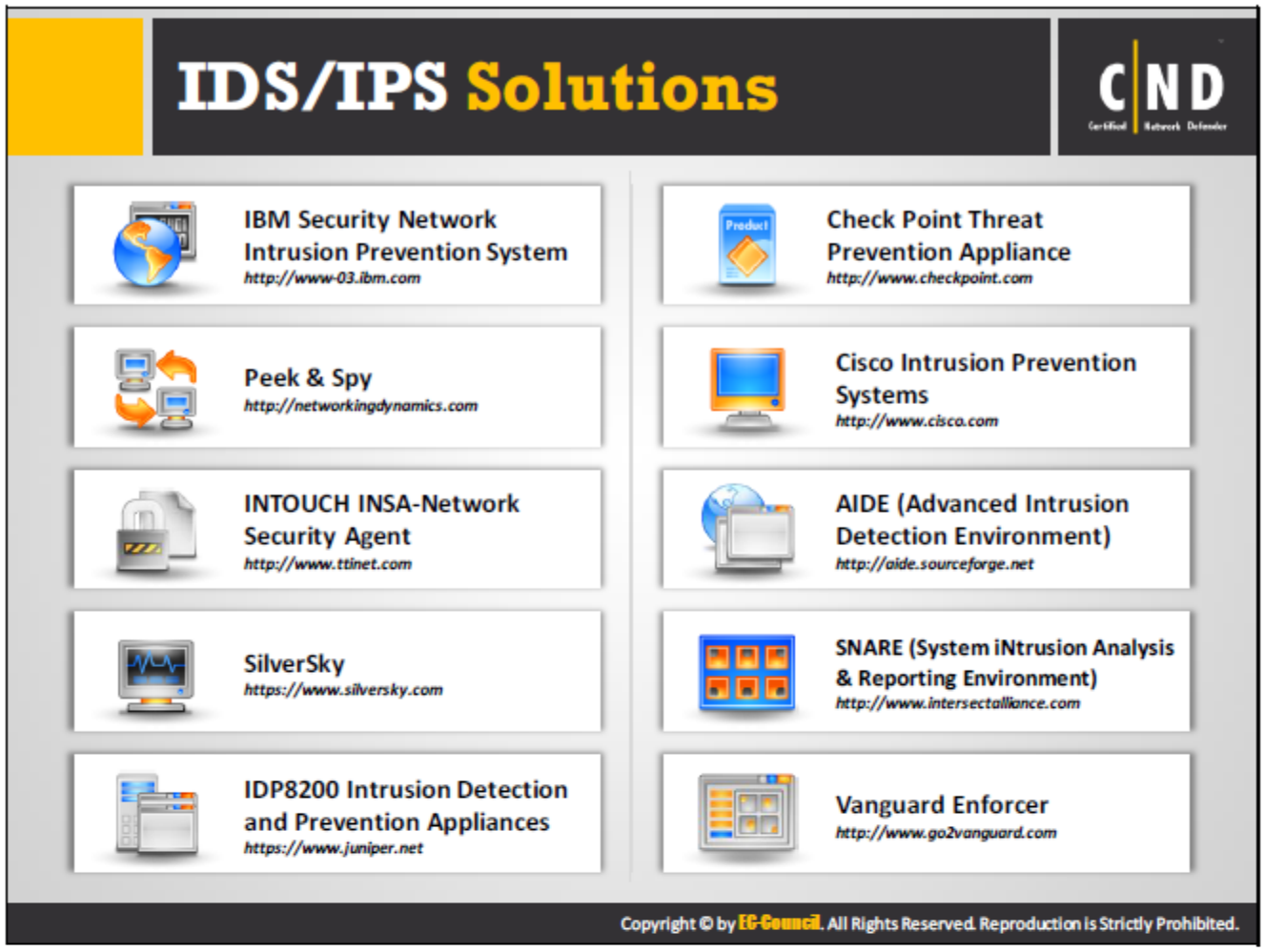
In order to install snort IDS, it is important to locate the position of the IDS in the network.

- Initially, plan the deployment by identifying the type of sensors which will be used either passive, inline or both.
- Choose which assets will be secured and maintain transparency between the sensors and other network devices.
- Check the policies and access control for the communication of snort in the network.
- The installation platform of snort includes an operating system and hardware considerations such as CPU, memory, motherboard etc.

Software Requirements

- Download Snort IDS
- Supported software of snort includes: Database - MySQL, Web server - Apache and PHP
- Snort prerequisites:
  - Snort engine - (prefer the most recent release)
  - Snort rules - ./oinkmaster.pl -o $RULE_PATH 2>&1 | logger -t oinkmaster , downloads the snort rules in $RULE_PATH
  - pcap-library or WinPcap library should be installed prior to Snort installation (Available at http://www.tcpdump.org/)
  - PCRE
  - Libnet-1.0.2.a
  - Unified output processing tool
  - Other tools such as BASE and ADODB

Source: *http://www.snort.org*



IBM Security Network Intrusion Prevention System

Source: *http://www-03.ibm.com*

IBM Security Network Intrusion Prevention System appliances stop constantly evolving threats before they affect your business. This means providing both high levels of protection and performance, while lowering the overall cost and complexity associated with deploying and managing a large number of point solutions.

Peek & Spy

Source: *http://networkingdynamics.com*

PEEK & SPY lets a privileged user see exactly what is on another user's terminal and then permits them to either take control of that terminal to fix the problem from their own computer or let the user have control while they give the needed instructions. If the PEEK & SPY user chooses to fix it by themselves, then the privileged user can display the input on the user's screen to show them how to fix it. Where PEEK informs users that they may have watched, SPY does not. In addition, SPY gives system managers documented proof of security breaches and provides a tool to lock out unauthorized users.

INTOUCH INSA–Network Security Agent

Source: *http://www.ttinet.com*

INTOUCH INSA - Network Security Agent scans all user activity on your networks, seven days a week, 24 hours a day. Whether the intrusion is from the outside (firewall failure) or from the inside (unauthorized insider activity). With INTOUCH INSA–Network Security Agent, the Network manager and Network Security Officer have a tool that allows for the automated tracking and logging of unauthorized or suspicious activity.

SilverSky

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

Intrusion Detection and Prevention (IDS/IPS) systems analyze complex network traffic in real-time and proactively block malicious internal traffic and sophisticated attacks that might not be prevented with firewalls alone. SilverSky reduces the costs and complexity of managing IDS/IPS Systems while improving your ability to respond to evolving threats.

IDP8200 Intrusion Detection and Prevention Appliances

Source: *https://www.juniper.net*

The IDP8200 Intrusion Detection and Prevention Appliances are the ideal network intrusion detection and application security management solution for large enterprise networks and service providers that require the highest throughput levels and reliability.

Check Point Threat Prevention Appliance

Source: *http://www.checkpoint.com*

The Check Point Threat Prevention Appliance prevents advanced threats and malware attacks and enables an organization to control access to millions of web sites easily and confidently. Protections include stopping application-specific attacks, botnets, targeted attacks, APTs, and zero-day threats.

Cisco Intrusion Prevention Systems

Source: *http://www.cisco.com*

Cisco IOS Intrusion Prevention System (IPS) is an inline, deep-packet inspection-based solution that enables Cisco IOS Software to effectively mitigate a wide range of network attacks. Although it is common practice to defend against attacks by inspecting traffic at data centers and corporate headquarters, distributing the network level defense to stop malicious traffic close to its entry point at branch or telecommuter offices is also critical.

AIDE (Advanced Intrusion Detection Environment)

Source: *http://aide.sourceforge.net*

AIDE (Advanced Intrusion Detection Environment) is a file and directory integrity checker. It creates a database from the regular expression rules that it finds from the configuration file(s). Initialization of this database helps verify the integrity of the files. It has several message digest algorithms to check the integrity of the file. You can also check the inconsistencies of all usual file attributes.

SNARE (System iNtrusion Analysis & Reporting Environment)

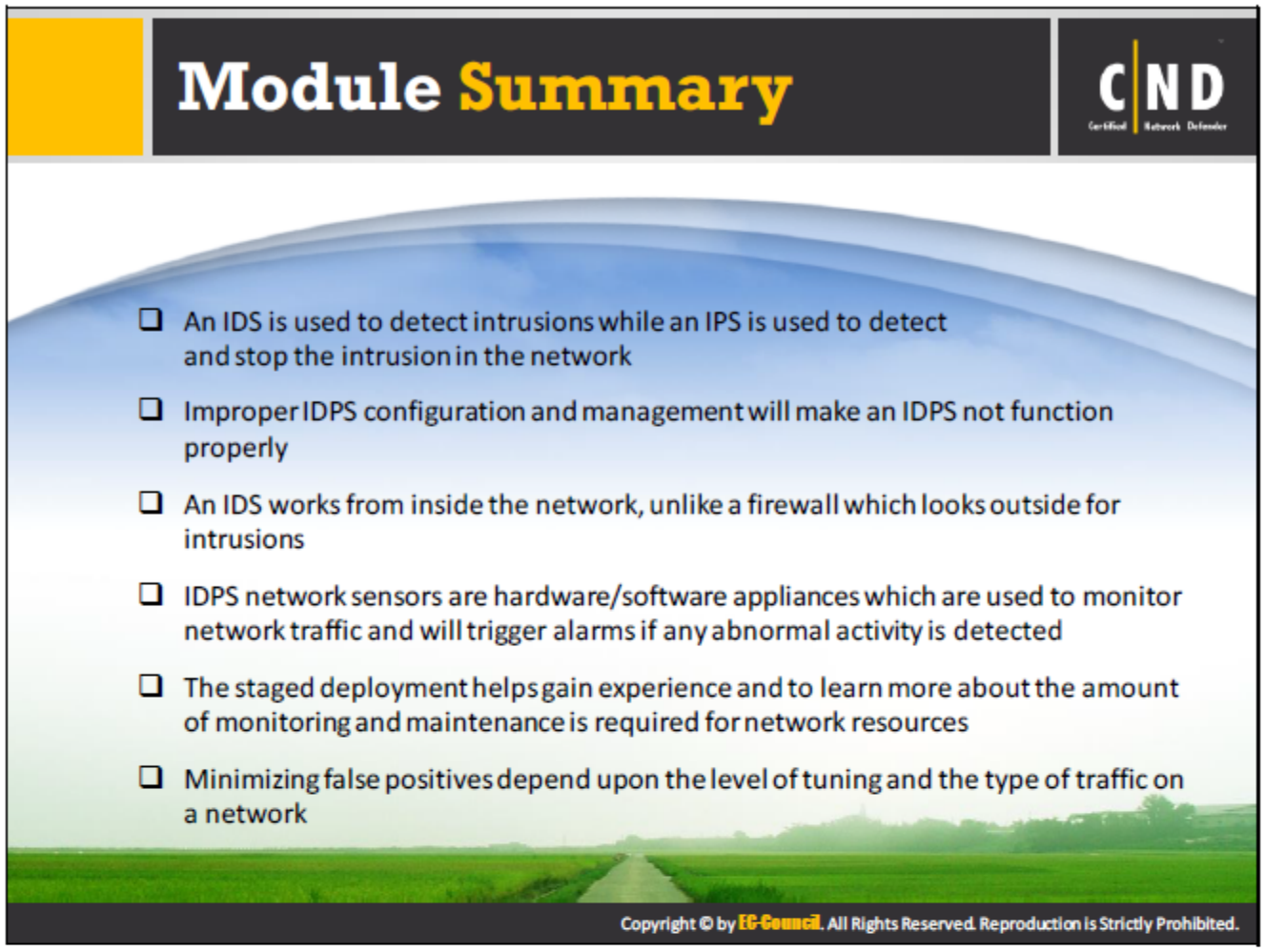
Source: *http://www.intersectalliance.com*

SNARE (System iNtrusion Analysis & Reporting Environment) consists of the centrally installed Snare Server and individual device-based Snare Agents. The Snare Server's role is to give your system administrator all the tools needed to define, gather, index, track, report on and store all relevant IT network security events input from Snare and open source agents. Snare Agents examine all IT events at their source. SSNARE (System iNtrusion Analysis and Reporting Environment) is a series of log collection, forwarding, filtering agents that facilitate centralized analysis of audit log data.

Vanguard Enforcer

Source: *http://www.go2vanguard.com*

Vanguard Enforcer provides real-time intrusion protection, detection and management solutions for the z/OS mainframe that prevent human error and deliberate attacks. By providing 24/7 protections for critical information and resources hosted on mainframes, Vanguard Enforcer guarantees that z/OS and RACF® security standards, profiles, rules and settings should not become compromised. In less than two seconds, the software can automatically detect and notify personnel when threat events on the mainframe and network occur, and then respond to deviations from the security baseline with corrective actions that reassert the approved security policy.



In this module, you have learned the importance of implementing and deploying an IDPS solution in the network. The module also explained important concepts about an IDPS including types of IDPS systems, working, components, deployment strategies, etc. With this module, you will able to determine an appropriate IDPS solution, implement the right IDPS deployment strategy, configure them properly, reduce false positive and negative rates of an IDPS, etc.