Module 9: Défense-in-Depth and Incident Analysis and Response

Module Objectives

Module Title: Defense-in-Depth and Incident Analysis and Response

Module Objective: Explain how the CyberOps Associate responds to cyber security incidents.

Topic Title	Topic Objective
Defense-in-Depth	Explain how the defense-in-depth strategy is used to protect networks.
The Cyber Kill Chain	Identify the steps in the Cyber Kill Chain
The Diamond Model of Intrusion Analysis	Classify an intrusion event using the Diamond Model
Incident Response	Apply the NIST 800-61r2 incident handling procedures to a given incident scenario

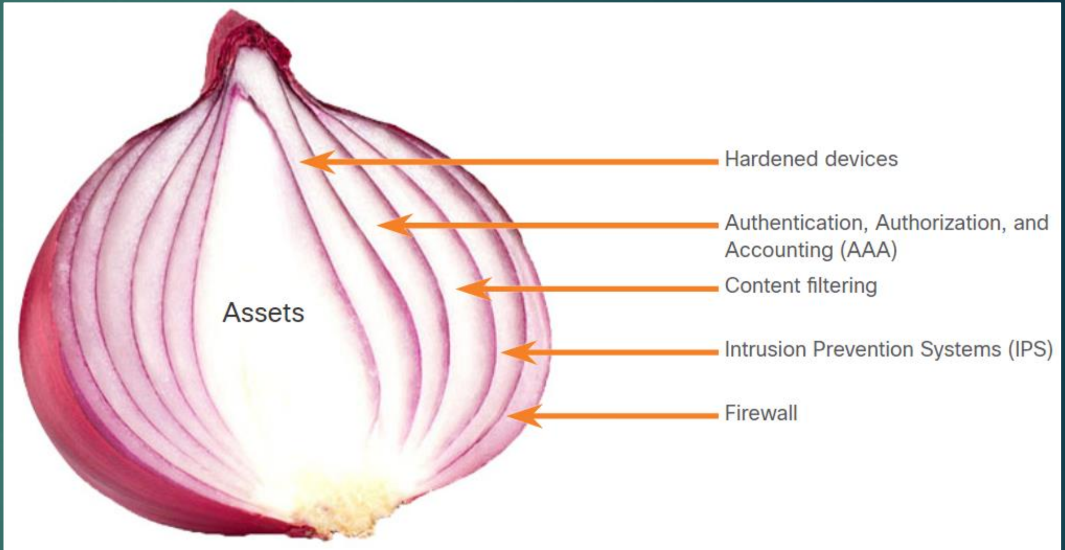
Understanding Defense

The Security Onion and The Security Artichoke

There are two common analogies that are used to describe a defense-in-depth approach.

Security Onion

- A common analogy used to describe a defense-in-depth approach is called "the security onion."
- As illustrated in figure, a threat actor would have to peel away at a network's defenses layer by layer in a manner similar to peeling an onion.
- Only after penetrating each layer would the threat actor reach the target data or system.


Assets
Hardened devices
Authentication, Authorization, and Accounting (AAA)
Content filtering
Intrusion Prevention Systems (IPS)
Firewall

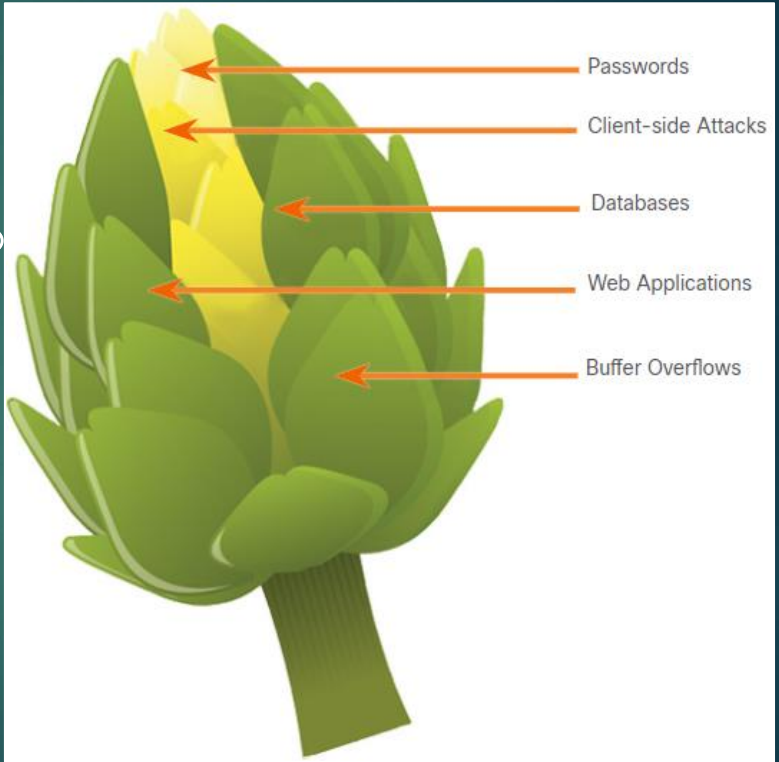
Note: *The security onion described on this page is a way of visualizing defense-in-depth. This is not to be confused with the Security Onion suite of network security tools.*

Understanding Defense

The Security Onion and The Security Artichoke (Contd.)

Security Artichoke

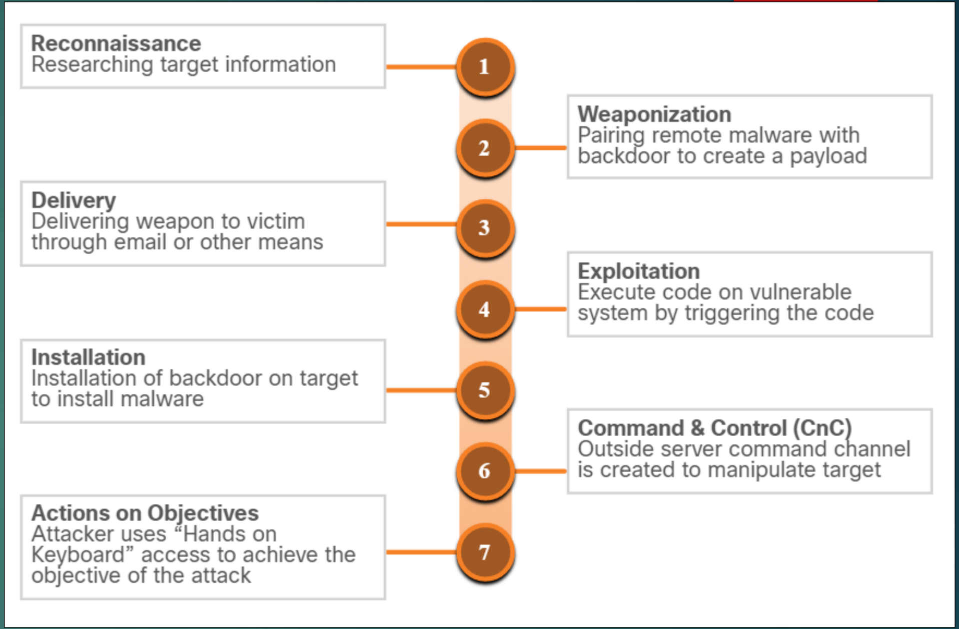
- The evolution of borderless networks has changed the analogy to the "security artichoke", which benefits the threat actor.
- As illustrated in the figure, threat actors no longer have to peel away each layer. They only need to remove certain "artichoke leaves."
- The bonus is that each "leaf" of the network may reveal sensitive data that is not well secured.
- In order to get at the heart of the artichoke, the hacker chips away at the security armor along the perimeter.
- While internet-facing systems are very well protected, persistent hackers do find a gap in that hard-core exterior through which they can enter.



The Cyber Kill Chain

Steps of the Cyber Kill Chain

- The Cyber Kill Chain was developed by Lockheed Martin to identify and prevent cyber intrusions.
- When responding to a security incident, the objective is to detect and stop the attack at the earliest in the kill chain progression to avoid further damage.
- If the attacker is stopped at any stage, the kill chain is broken and the defender successfully thwarted the threat actor's intrusion.



1 **Reconnaissance** Researching target information

2 **Weaponization** Pairing remote malware with backdoor to create a payload

3 **Delivery** Delivering weapon to victim through email or other means

4 **Exploitation** Execute code on vulnerable system by triggering the code

5 **Installation** Installation of backdoor on target to install malware

6 **Command & Control (CnC)** Outside server command channel is created to manipulate target

7 **Actions on Objectives** Attacker uses "Hands on Keyboard" access to achieve the objective of the attack

Steps of Cyber Kill Chain

Note: Threat actor refers to the party instigating the attack. However, Lockheed Martin uses the term "adversary" in Cyber Kill Chain. Therefore, the terms adversary and threat actor are used interchangeably in this topic.

The Cyber Kill Chain

Reconnaissance

- Reconnaissance is when the threat actor performs research, gathers intelligence, and selects targets.
- The threat actor will choose targets that have been neglected or unprotected because they will have a higher likelihood of becoming penetrated and compromised.
- The table summarizes the tactics and defenses used during the reconnaissance step.

Adversary Tactics	SOC Defences
Plan and conduct research: • Harvest email addresses • Identify employees on social media • Collect all public relations information (press releases, awards, conference attendees and so on) • Discover internet-facing servers • Conduct scans of the network to identify IP addresses and open ports	Discover adversary’s intent: • Web log alerts and historical searching data • Data mine browser analytics • Build playbooks for detecting behavior that indicate recon activity • Prioritize defense around technologies and people that reconnaissance activity is targeting

The Cyber Kill Chain

Weaponization

- Weaponization uses the information from reconnaissance to develop a weapon against specific targeted systems or individuals in the organization.
- It is often more effective to use a zero-day attack to avoid detection methods.
- A zero-day attack uses a weapon that is unknown to defenders and network security systems.
- The table summarizes the tactics and defenses used during the weaponization step.

Adversary Tactics	**SOC Defence**
Prepare and stage the operation: • Obtain an automated tool to deliver the malware payload (weaponizer). • Select or create a document to present to the victim. • Select or create a backdoor and command and control infrastructure.	Detect and collect weaponization artifacts: • Ensure that IDS rules and signatures are up to date. • Conduct full malware analysis. • Build detections for the behavior of known weaponizers. • Is malware old, “off the shelf” or new malware that might indicate a tailored attack? • Collect files and metadata for future analysis. • Determine which weaponizer artifacts are common to which campaigns.

The Cyber Kill Chain

Delivery

- During this step, the weapon is transmitted to the target using a delivery vector. If the weapon is not delivered, the attack will be unsuccessful.
- The threat actor will use different methods to increase the odds of delivering the payload such as encrypting communications, making the code look legitimate, or obfuscating the code.
- Security sensors are so advanced that they can detect the code as malicious unless it is altered to avoid detection.
- The table summarizes the tactics and defenses used during the delivery step.

Adversary Tactics	SOC Defence
Launch malware at target: • Direct against web servers • Indirect delivery through: • Malicious email • Malware on USB stick • Social media interactions • Compromised websites	Block delivery of malware: • Analyze the infrastructure path used for delivery. • Understand targeted servers, people, and data available to attack. • Infer intent of the adversary based on targeting. • Collect email and web logs for forensic reconstruction.

The Cyber Kill Chain

Exploitation

- After the weapon has been delivered, the threat actor uses it to break the vulnerability and gain control of the target.
- The most common exploit targets are applications, operating system vulnerabilities, and users.
- The table summarizes the tactics and defenses used during the exploitation step.

Adversary Tactics	SOC Defence
Exploit a vulnerability to gain access: • Use software, hardware, or human vulnerability • Acquire or develop the exploit • Use an adversary-triggered exploit for server vulnerabilities • Use a victim-triggered exploit such as opening an email attachment or malicious web link	Train employees, secure code, and harden devices: • Employee security awareness training and periodic email testing • Web developer training for securing code • Regular vulnerability scanning and penetration testing • Endpoint hardening measures • Endpoint auditing to forensically determine origin of exploit

The Cyber Kill Chain

Installation

- In the Installation step, the threat actor establishes a back door into the system to allow for continued access to the target.
- To preserve this backdoor, the remote access should not alert cyber security analysts or users. The access method must survive through antimalware scans and rebooting of the computer to be effective.
- The table summarizes the tactics and defenses used during the installation step.

Adversary Tactics	SOC Defence
Install persistent backdoor: • Install webshell on web server for persistent access. • Create point of persistence by adding services, AutoRun keys, etc. • Some adversaries modify the timestamp of the malware to make it appear as part of the operating system.	Detect, log, and analyze installation activity: • HIPS to alert or block on common installation paths. • Determine if malware requires elevated privileges or user privileges • Endpoint auditing to discover abnormal file creations. • Determine if malware is known threat or new variant.

The Cyber Kill Chain

Command and Control

- The goal is to establish Command and Control (CnC or C2) with the target system.
- Compromised hosts usually beacon out of the network to a controller on the internet.
- Threat actors use CnC channels to issue commands to the software that they installed on the target.
- The cyber security analyst must be able to detect CnC communications to discover the compromised host.

Adversary Tactics	SOC Defence
Open channel for target manipulation: • Open two-way communications channel to CNC infrastructure • Most common CNC channels over web, DNS, and email protocols • CnC infrastructure may be adversary owned or another victim network itself	Last chance to block operation: • Research possible new CnC infrastructures • Discover CnC infrastructure though malware analysis • Isolate DNS traffic to suspect DNS servers, especially Dynamic DNS • Prevent impact by blocking or disabling CnC channel • Consolidate the number of internet points of presence • Customize rules blocking of CnC protocols on web proxies

- The table summarizes the tactics and defenses used during command and control step.

The Cyber Kill Chain

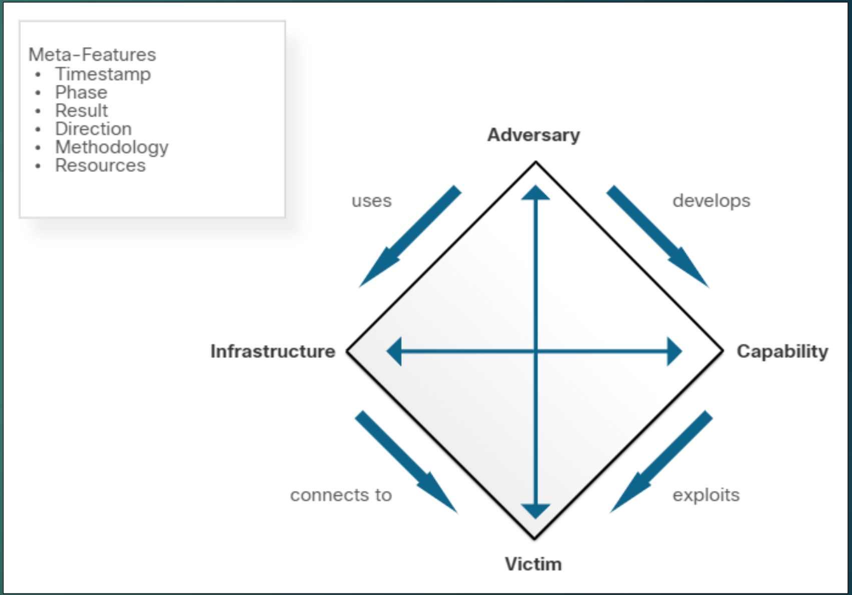
Actions on Objectives

- Actions on Objectives is the final step of the Cyber Kill Chain that describes the threat actor achieving their original objective.
- At this point, the threat actor is deeply rooted in the systems of the organization, hiding their moves and covering their tracks.
- It is extremely difficult to remove the threat actor from the network.
- The table summarizes the tactics and defenses used during the actions on objectives step.

Adversary Tactics	SOC Defence
Reap the rewards of successful attack: • Collect user credentials • Privilege escalation • Internal reconnaissance • Lateral movement through environment • Collect and exfiltrate data • Destroy systems • Overwrite, modify, or corrupt data	Detect by using forensic evidence: • Establish incident response playbook • Detect data exfiltration, lateral movement, and unauthorized credential usage • Immediate analyst response for all alerts • Forensic analysis of endpoints for rapid triage • Network packet captures to recreate activity • Conduct damage assessment

Diamond Model Overview

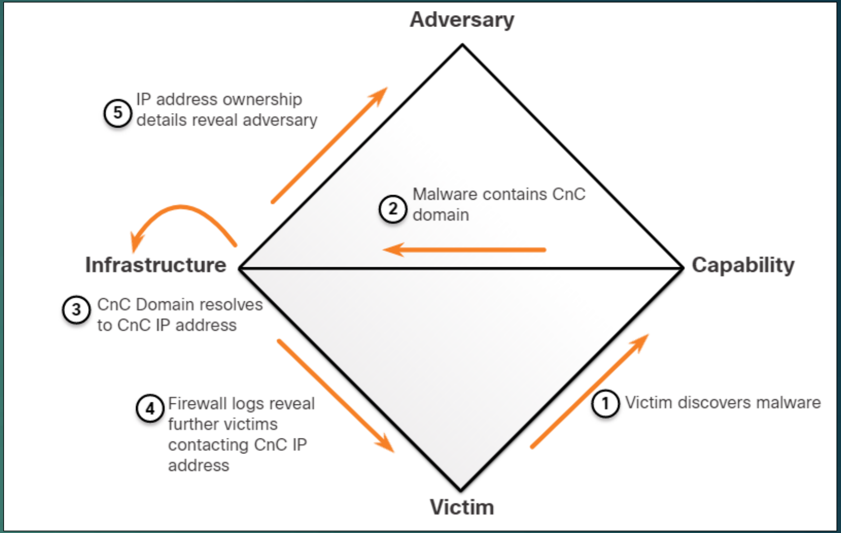
- The Diamond Model of Intrusion Analysis represents a security incident or event.
- The four core features of an intrusion event are:
  - **Adversary** - Parties responsible for the intrusion.
  - **Capability** - Tool or technique used by the adversary to attack the victim.
  - **Infrastructure** – Network path(s) used by the adversary to establish and maintain command and control over their capabilities.
  - **Victim** – Target of the attack.
- Meta-features expand the model slightly to include the important elements: **Timestamp**, **Phase**, **Result**, **Direction**, **Methodology**, and **Resources**



The Diamond Model of Intrusion Analysis

Pivoting Across the Diamond Model

- The Diamond Model is ideal for illustrating how the adversary pivots from one event to the next. For example:
  - An employee reports that his computer is acting abnormally. A host scan by the security technician indicates that the computer is infected with malware.
  - An analysis of the malware reveals that the malware contains a list of CnC domain names that resolve to a list of IP addresses.
  - These IP addresses are used to identify the adversary and investigate logs to determine if other victims in the organization are using the CnC channel.



Adversary
5 IP address ownership details reveal adversary
2 Malware contains CnC domain
Infrastructure
Capability
3 CnC Domain resolves to CnC IP address
4 Firewall logs reveal further victims contacting CnC IP address
1 Victim discovers malware
Victim

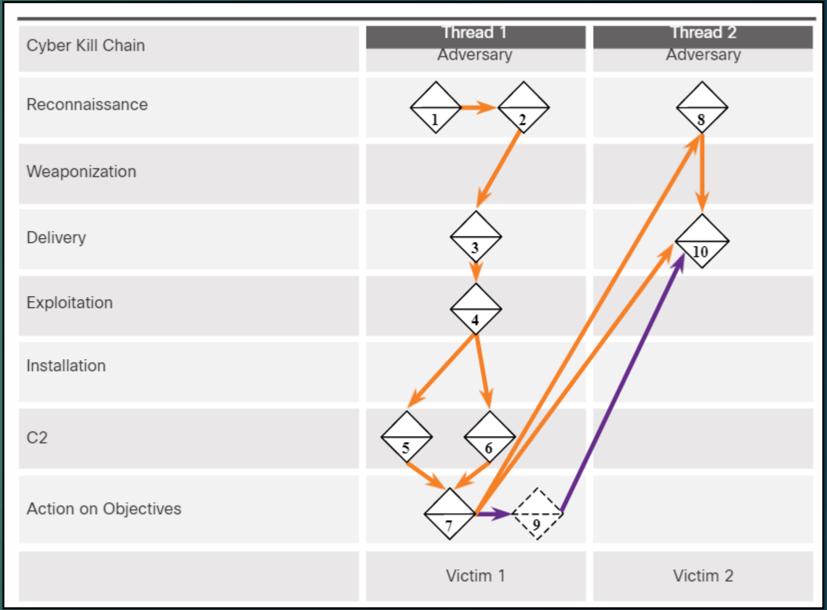
Diamond Model Characterization of an Exploit

The Diamond Model and the Cyber Kill Chain (Contd.)

- Events are threaded together in a chain in which each event must be completed before the next event. This thread of events can be mapped to the Cyber Kill Chain.

- The example illustrates the end-to-end process of an adversary as they traverse the Cyber Kill Chain:

1. Adversary conducts a web search for victim company Gadgets, Inc. receiving as part of the results the domain name gadgets.com.
2. Adversary search “network administrator gadget.com” and discovers forum postings from users claiming to be network administrators of gadget.com and the profiles reveal their email addresses.
3. Adversary sends phishing emails with a Trojan horse attached to the network administrators.
4. One network administrator (NA1) opens the malicious attachment which executes the enclosed exploit.
5. NA1’s host registers with a CnC controller by sending an HTTP Post message and receiving an HTTP Response in return.



The Diamond Model of Intrusion Analysis

The Diamond Model and the Cyber Kill Chain (Contd.)

6. It is revealed from reverse engineering that the malware has additional backup IP addresses.

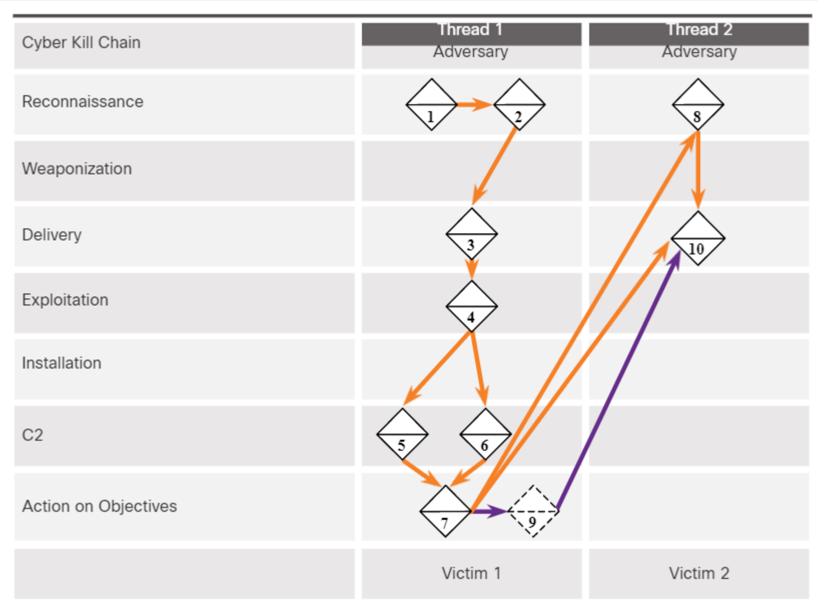
7. Through a CnC HTTP response message sent to NA1’s host, the malware begins to act as a proxy for new TCP connections.

8. Through information from the proxy that is running on NA1’s host, Adversary searches the web for “most important research ever” and finds Victim 2, Interesting Research Inc.

9. Adversary checks NA1’s email contact list for any contacts from Interesting Research Inc. and discovers the contact for the Interesting Research Inc. Chief Research Officer.

10. Chief Research Officer of Interesting Research Inc. receives a spear-phish email from Gadget Inc.’s NA1’s email address sent from NA1’s host with the same payload as observed in Event 3.

The adversary now has two compromised victims from which additional attacks can be launched.



Cyber Kill Chain	Thread 1 Adversary	Thread 2 Adversary
Reconnaissance	1, 2	8
Weaponization		
Delivery	3	10
Exploitation	4	
Installation		
C2	5, 6	
Action on Objectives	7, 9	
	Victim 1	Victim 2

Overview of Alert Evaluation

Evaluating Alerts

- Security incidents are classified using a scheme borrowed from medical diagnostics. This classification scheme is used to guide actions and to evaluate diagnostic procedures. The concern is that either diagnosis can be accurate, or true, or inaccurate, or false.
- In network security analysis, the cybersecurity analyst is presented with an alert. The cybersecurity analyst needs to determine if this diagnosis is true.
- Alerts can be classified as follows:
  - **True Positive**: The alert has been verified to be an actual security incident.
  - **False Positive**: The alert does not indicate an actual security incident. Benign activity that results in a false positive is sometimes referred to as a benign trigger.
- An alternative situation is that an alert was not generated. The absence of an alert can be classified as:
  - **True Negative**: No security incident has occurred. The activity is benign.
  - **False Negative**: An undetected incident has occurred.

Overview of Alert Evaluation

Evaluating Alerts (Contd.)

When an alert is issued, it will receive one of four possible classifications:

	True	**False**
Positive (Alert exists)	Incident occurred	No incident occurred
Negative (No alert exists)	No incident occurred	Incident occurred

- **True positives** are the desired type of alert. They mean that the rules that generate alerts have worked correctly.
- **False positives** are not desirable. Although they do not indicate that an undetected exploit has occurred, they are costly because cybersecurity analysts must investigate false alarms.
- **True negatives** are desirable. They indicate that benign normal traffic is correctly ignored, and erroneous alerts are not being issued.
- **False negatives** are dangerous. They indicate that exploits are not being detected by the security systems that are in place.

Note: *"True" events are desirable. "False" events are undesirable and potentially dangerous.*

Overview of Alert Evaluation

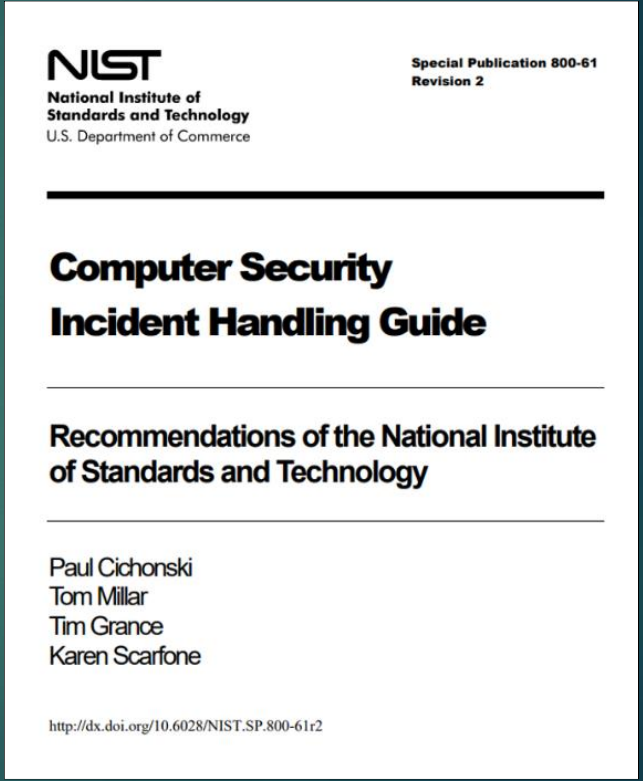
Evaluating Alerts (Contd.)

- Benign events are those that should not trigger alerts. Excess benign events indicate that some rules or other detectors need to be improved or eliminated.
- When true positives are suspected, a cybersecurity analyst is required to escalate the alert to a higher level for investigation.
- A cybersecurity analyst may also be responsible for informing security personnel that false positives are occurring to the extent that the cybersecurity analyst's time is seriously impacted.
- False negatives may be discovered well after an exploit has occurred. This can happen through retrospective security analysis (RSA). RSA can occur when newly obtained rules or other threat intelligence is applied to archived network security data.
- For this reason, it is important to monitor threat intelligence to learn of new vulnerabilities and exploits and to evaluate the likelihood that the network was vulnerable to them at some time in the past.

Incident Response

Establishing an Incident Response Capability

- Incident response aims to limit the impact of the attack, assess the damage caused, and implement recovery procedures.
- Incident Response involves the methods, policies, and procedures that are used by an organization to respond to a cyber attack.



NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Special Publication 800-61
Revision 2

Computer Security
Incident Handling Guide

Recommendations of the National Institute of Standards and Technology

Paul Cichonski
Tom Millar
Tim Grance
Karen Scarfone

http://dx.doi.org/10.6028/NIST.SP.800-61r2

Incident Response

Establishing an Incident Response Capability (Contd.)

- The below table summarizes the policy, plan and procedure elements in an incident response:

Policy Elements	Plan Elements	Procedure Elements
• Statement of management commitment • Purpose and objectives of the policy • Scope of the policy • Definition of computer security incidents and related terms • Organizational structure and definition of roles, responsibilities, and levels of authority • Prioritization of severity ratings of incidents • Performance measures • Reporting and contact forms	• Mission • Strategies and goals • Senior management approval • Organizational approach to incident response • How the incident response team will communicate with the rest of the organization and with other organizations • Metrics for measuring the incident response capacity • How the program fits into overall organization	• Technical processes • Using techniques • Filling out forms • Following checklists

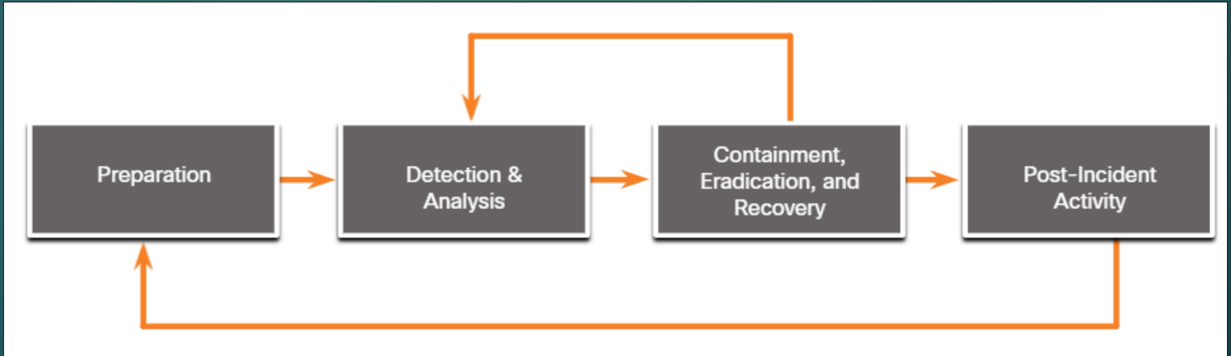
Incident Response Stakeholders

- The stakeholders involved in handing a security incident are as follows:
    - Management
    - Information Assurance
    - IT Support
    - Legal Department
    - Public Affairs and Media Relations
    - Human Resources
    - Business Continuity Planners
    - Physical Security and Facilities Management

Incident Response

NIST Incident Response Life Cycle

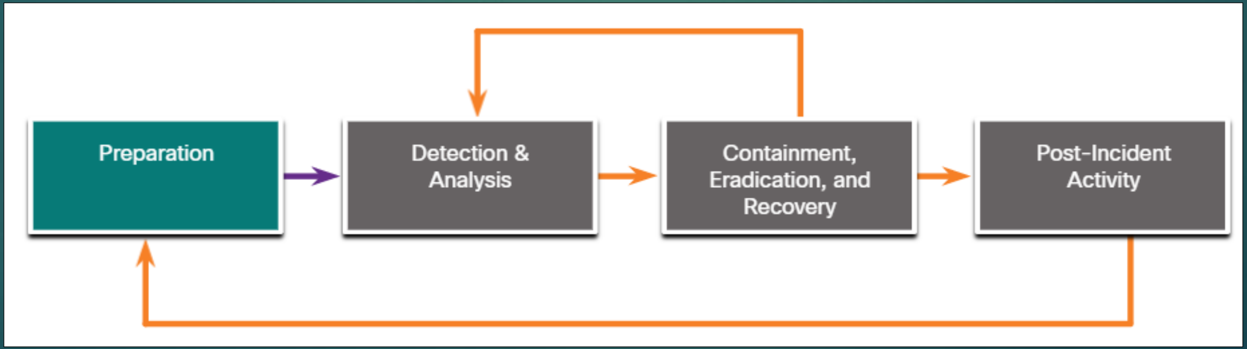
- NIST defines four steps in the incident response process life cycle:
  - **Preparation** - The members of the CSIRT are trained in how to respond to an incident.
  - **Detection and Analysis** – CSIRT quickly identifies, analyzes, and validates an incident.
  - **Containment, Eradication, and Recovery** – CSIRT implements procedures to contain the threat, eradicate the impact on organizational assets, and use backups to restore data and software.
  - **Post-Incident Activities** – CSIRT documents how the incident was handled, recommends changes for future response, and specifies how to avoid a reoccurrence.



Incident Response

Preparation

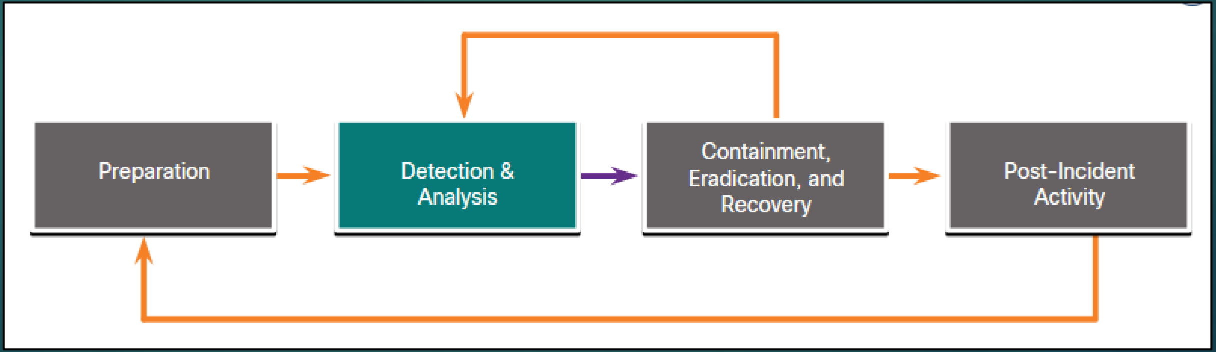
- The preparation phase is when the CSIRT is created and trained. The tools and assets that will be needed by the team to investigate incidents are acquired and deployed.
- The examples of actions in the preparation phase are as follows:
  - Facilities to host the response team and the SOC are created.
  - Risk assessments are used to implement controls that will limit the number of incidents.
  - User security awareness training materials are developed.
  - Necessary hardware and software for incident analysis and mitigation is acquired.



Incident Response

Detection and Analysis

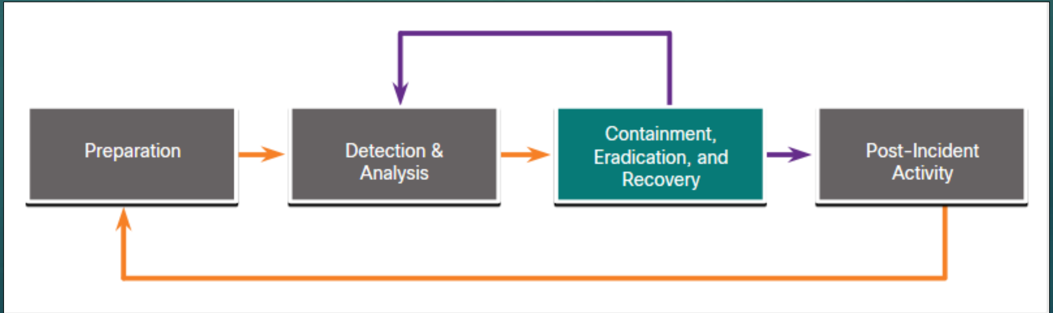
- Different types of incidents will require different responses.
  - **Attack Vectors**: Web, Email, Loss or Theft, Impersonation, Attrition and Media.
  - **Detection:** Automated detection - Antivirus software, IDS, manual detection - user reports.
  - **Analysis**: Use Network and System Profiling to determine the validity of security incidents.
  - **Scoping**: Provide information on the containment of the incident and deeper analysis of the effects of the incident.
  - **Incident Notification**: Notify appropriate stakeholders and outside parties, once the incident is analyzed and prioritized,



Incident Response

Containment, Eradication, and Recovery

- After determining the validity of the incident through detection and analysis, it must be contained.
  - **Containment Strategy**: For every type of incident, a containment strategy should be created and enforced depending on some conditions.
  - **Evidence**: During an incident, evidence must be gathered to resolve it. It is required for subsequent investigation by authorities.
  - **Attacker Identification**: Identifying attackers will minimize the impact on critical business assets and services.
  - **Eradication, recovery, and remediation**: to eradicate, identify all hosts that need remediation; to recover hosts, use clean and recent backups, or rebuild them with installation media.



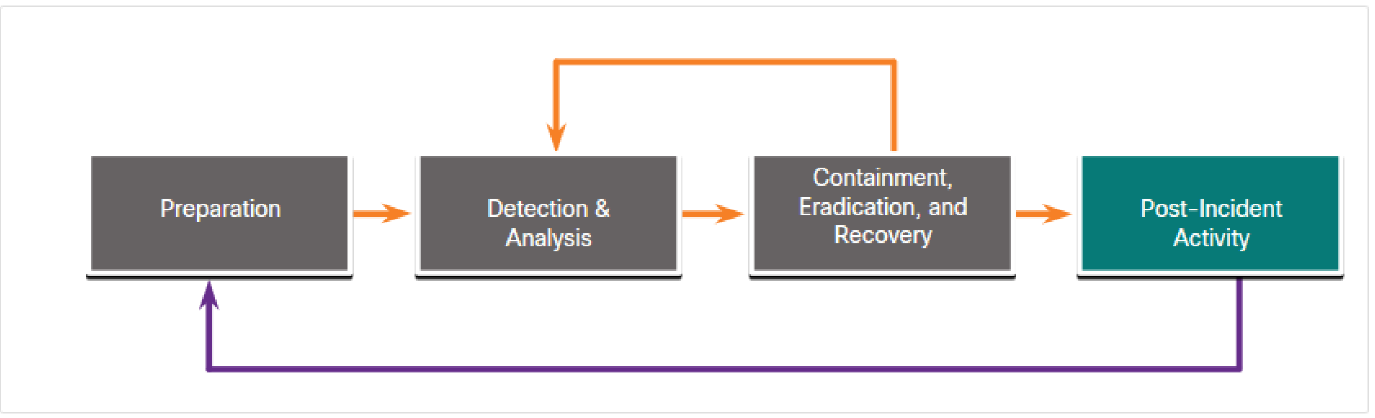
Incident Response

Post-Incident Activities

- It is important to periodically meet with all the parties involved to discuss the events that took place and the actions of all of the individuals while handling the incident.

Lessons-based hardening:

- The organization should hold a “lessons learned” meeting to:
  - Review the effectiveness of the incident handling process.
  - Identify necessary hardening needed for existing security controls and practices.



Digital Forensics and Incident Analysis and Response Summary

What Did I Learn in this Module?

- Organizations must use a defense-in-depth approach to identify threats and secure vulnerable assets.
- The Cyber Kill Chain was developed to identify and prevent cyber intrusions.
- The steps in the Cyber Kill Chain are reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives.
- The Diamond Model of Intrusion Analysis represents a security incident or event.
- The four core features of an intrusion event are adversary, capability, infrastructure and victim.
- Alerts can be classified as True Positive (The alert has been verified to be an actual security incident) or False Positive (The alert does not indicate an actual security incident).
- An alternative situation is that an alert was not generated. The absence of an alert can be classified as: True Negative (No security incident has occurred. The activity is benign.) and False Negative (An undetected incident has occurred).
- Incident Response involves the methods, policies, and procedures that are used by an organization to respond to a cyber attack.