Module 27: Digital Forensics and Incident Analysis and Response

Cybersecurity Essentials 3.0

Module Objectives

Module Title: Digital Forensics and Incident Analysis and Response

Module Objective: Use incident response models and forensic techniques to investigate security incidents.

Topic Title	Topic Objective
Evidence Handling and Attack Attribution	Explain the role of digital forensics processes.
The Cyber Kill Chain	Identify the steps in the Cyber Kill Chain.
The Diamond of Intrusion Analysis	Use the Diamond Model of Intrusion Analysis to classify intrusion events.
Incident Response	Apply the NIST 800-61r2 incident handling procedures to a given incident scenario.
Disaster Recovery	Use commands to back up files and restore network operations.

27.1 Evidence Handling and Attack Attribution

Digital Forensics

- Now that you have investigated and identified valid alerts, what do you do with the evidence? The cybersecurity analyst will inevitably uncover evidence of criminal activity. To protect the organization and to prevent cybercrime, it is necessary to identify threat actors, report them to the appropriate authorities, and provide evidence to support prosecution. Tier 1 cybersecurity analysts are often the first to uncover wrongdoing. Cybersecurity analysts must know how to properly manage evidence and attribute it to threat actors.

- Digital forensics is the recovery and investigation of information found on digital devices as it relates to criminal activity. Indicators of compromise are the evidence that a cybersecurity incident has occurred. This information could be data on storage devices, in volatile computer memory, or the traces of cybercrime that are preserved in network data, such as pcaps and logs. It is essential that all indicators of compromise be preserved for future analysis and attack attribution.

Digital Forensics (Cont.)

- Cybercriminal activity can be broadly characterized as originating from inside of or outside of the organization. Private investigations are concerned with individuals inside the organization. These individuals could simply be behaving in ways that violate user agreements or other non-criminal conduct. When individuals are suspected of involvement in criminal activity involving the theft or destruction of intellectual property, an organization may choose to involve law enforcement authorities, in which case the investigation becomes public. Internal users could also have used the organization's network to conduct other criminal activities that are unrelated to the organizational mission but are in violation of various legal statutes. In this case, public officials will conduct the investigation.

- When an external attacker has exploited a network and stolen or altered data, evidence needs to be gathered to document the scope of the exploit. Various regulatory bodies specify a range of actions that an organization must take when several types of data have been compromised. The results of forensic investigation can help to identify the actions that need to be taken.

Digital Forensics (Cont.)

- For example, under the US HIPAA regulations, if a data breach has occurred that involves patient information, notification of the breach must be made to the affected individuals. If the breach involves more than five hundred individuals in a state or jurisdiction, the media, as well as the affected individuals, must be notified. Digital forensic investigation must be used to determine which individuals were affected, and to certify the number of affected individuals so that appropriate notification can be made in compliance with HIPAA regulations.

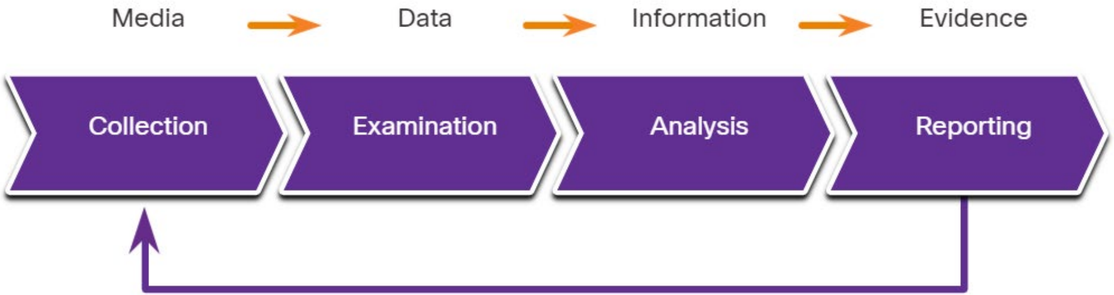
- It is possible that the organization itself could be the subject of an investigation. Cybersecurity analysts may find themselves in direct contact with digital forensic evidence that details the conduct of members of the organization. Analysts must know the requirements regarding the preservation and handling of such evidence. Failure to do so could result in criminal penalties for the organization and even the cybersecurity analyst if the intention to destroy evidence is established.

The Digital Forensics Process

- It is important that an organization develop well-documented processes and procedures for digital forensic analysis. Regulatory compliance may require this documentation, and this documentation may be inspected by authorities in the event of a public investigation.

- NIST Special Publication 800-86 *Guide to Integrating Forensic Techniques into Incident Response* is a valuable resource for organizations that require guidance in developing digital forensics plans. For example, it recommends that forensics be performed using the four-phase process.

The four basic phases of the digital evidence forensic process are:



The Digital Forensics Process (Cont.)

Step 1 – Collection: This is the identification of potential sources of forensic data and acquisition, handling, and storage of that data. This stage is critical because particular care must be taken not to damage, lose, or omit important data.

Step 2 – Examination: This entails assessing and extracting relevant information from the collected data. This may involve decompression or decryption of the data. Information that is irrelevant to the investigation may need to be removed. Identifying actual evidence in large collections of data can be very difficult and time-consuming.

Step 3 – Analysis: This entails drawing conclusions from the data. Salient features, such as people, places, times, events, and so on should be documented. This step may also involve the correlation of data from multiple sources.

Step 4 – Reporting: This entails preparing and presenting information that resulted from the analysis. Reporting should be impartial and alternative explanations should be offered if appropriate. Limitations of the analysis and problems encountered should be included. Suggestions for further investigation and next steps should also be made.

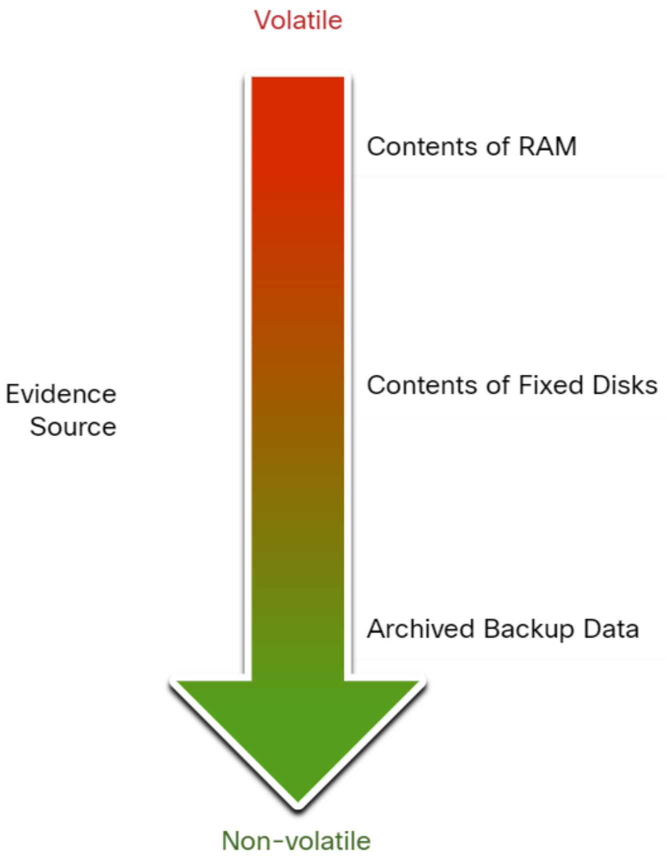
Types of Evidence

In legal proceedings, evidence is broadly classified as either direct or indirect. Direct evidence is evidence that was indisputably in the possession of the accused or is eyewitness evidence from someone who directly observed criminal behavior.

Evidence is further classified as:

- **Best evidence:** This is evidence that is in its original state. This evidence could be storage devices used by an accused, or archives of files that can be proven to be unaltered.
- **Corroborating evidence:** This is evidence that supports an assertion that is developed from best evidence.
- **Indirect evidence:** This is evidence that, in combination with other facts, establishes a hypothesis. This is also known as circumstantial evidence. For example, evidence that an individual has committed similar crimes can support the assertion that the person committed the crime of which they are accused.

Evidence Collection Order



IETF RFC 3227 provides guidelines for the collection of digital evidence. It describes an order for the collection of digital evidence based on the volatility of the data. Data stored in RAM is the most volatile, and it will be lost when the device is turned off. In addition, important data in volatile memory could be overwritten by routine machine processes. Therefore, the collection of digital evidence should begin with the most volatile evidence and proceed to the least volatile, as shown in the figure.

Evidence Collection Order (Cont.)

An example of most volatile to least volatile evidence collection order is as follows:

- Memory registers, caches
- Routing table, ARP cache, process table, kernel statistics, RAM
- Temporary file systems
- Non-volatile media, fixed and removable
- Remote logging and monitoring data
- Physical interconnections and topologies
- Archival media, tape or other backups

Details of the systems from which the evidence was collected, including who has access to those systems and at what level of permissions should be recorded. Such details should include hardware and software configurations for the systems from which the data was obtained.

Evidence Handling and Attack Attribution

Chain of Custody

Although evidence may have been gathered from sources that support attribution to an accused individual, it can be argued that the evidence could have been altered or fabricated after it was collected. To counter this argument, a rigorous chain of custody must be defined and followed.

Chain of custody involves the collection, handling, and secure storage of evidence. Detailed records should be kept of the following:

- Who discovered and collected the evidence?
- All details about the handling of evidence including times, places, and personnel involved.
- Who has primary responsibility for the evidence, when responsibility was assigned, and when custody changed?
- Who has physical access to the evidence while it was stored? Access should be restricted to only the most essential personnel.

Evidence Handling and Attack Attribution

Data Integrity and Preservation

- When collecting data, it is important that it is preserved in its original condition. Timestamping of files should be preserved. For this reason, the original evidence should be copied, and analysis should only be conducted on copies of the original. This is to avoid accidental loss or alteration of the evidence. Because timestamps may be part of the evidence, opening files from the original media should be avoided.

- The process used to create copies of the evidence that is used in the investigation should be recorded. Whenever possible, the copies should be direct bit-level copies of the original storage volumes. It should be possible to compare the archived disc image and the investigated disk image to identify whether the contents of the investigated disk have been tampered with. For this reason, it is important to archive and protect the original disk to keep it in its original, untampered with, condition.

- Volatile memory could contain forensic evidence, so special tools should be used to preserve that evidence before the device is shut down and evidence is lost. Users should not disconnect, unplug, or turn off infected machines unless explicitly told to do so by security personnel.

- Following these processes will ensure that any evidence of wrongdoing will be preserved, and any indicators of compromise can be identified.

Attack Attribution

- After the extent of the cyberattack has been assessed and evidence collected and preserved, incident response can move to identifying the source of the attack. As we know, a wide range of threat actors exist, ranging from disgruntled individuals, hackers, cybercriminals and criminal gangs, or nation states.

- Some criminals act from inside the network, while others can be on the other side of world. Sophistication of cybercrime varies as well. Nation states may employ large groups of highly trained individuals to conduct an attack and hide their tracks, while other threat actors may openly brag about their criminal activities.

- Threat attribution refers to the act of determining the individual, organization, or nation responsible for a successful intrusion or attack incident.

- Identifying responsible threat actors should occur through the principled and systematic investigation of the evidence. While it may be useful to also speculate as to the identity of threat actors by identifying potential motivations for an incident, it is important not to let this bias the investigation.

Attack Attribution (Cont.)

- In an evidence-based investigation, the incident response team correlates Tactics, Techniques, and Procedures (TTP) that were used in the incident with other known exploits. Cybercriminals, much like other criminals, have specific traits that are common to most of their crimes. Threat intelligence sources can help to map the TTP identified by an investigation to known sources of similar attacks.

- Some aspects of a threat that can aid in attribution are the location of originating hosts or domains, features of the code used in malware, the tools used, and other techniques. Sometimes, at the national security level, threats cannot be openly attributed because doing so would expose methods and capabilities that need to be protected.

- For internal threats, asset management plays a significant role. Uncovering the devices from which an attack was launched can lead directly to the threat actor. IP addresses, MAC addresses, and DHCP logs can help track the addresses used in the attack back to a specific device. AAA logs are especially useful in this regard, as they track who accessed what network resources at what time.

The MITRE ATT&CK Framework

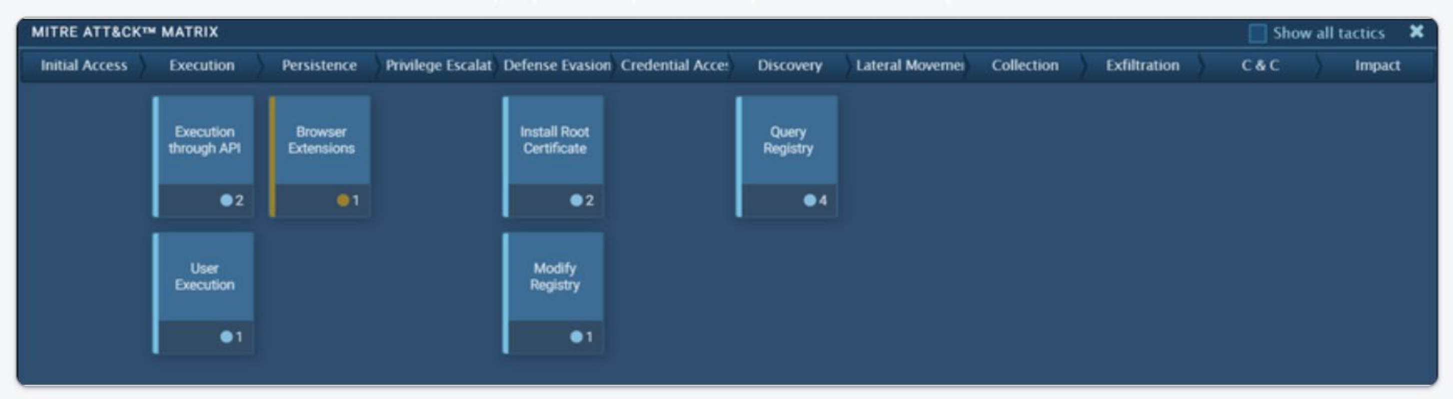
- One way to attribute an attack is to model threat actor behavior. The MITRE Adversarial Tactics, Techniques & Common Knowledge (ATT&CK) Framework enables the ability to detect attacker tactics, techniques, and procedures (TTP) as part of threat defense and attack attribution. This is done by mapping the steps in an attack to a matrix of generalized tactics and describing the techniques that are used in each tactic. Tactics consist of the technical goals that an attacker must accomplish to execute an attack and techniques are how the tactics are accomplished. Finally, procedures are the specific actions taken by threat actors in the techniques that have been identified. Procedures are the documented real-world use of techniques by threat actors.

- The MITRE ATT&CK Framework is a global knowledge base of threat actor behavior. It is based on observation and analysis of real-world exploits with the purpose of describing the behavior of the attacker, not the attack itself. It is designed to enable automated information sharing by defining data structures for the exchange of information between its community of users and MITRE.

The MITRE ATT&CK Framework (Cont.)

- The figure shows an analysis of a ransomware exploit from the excellent ANY.RUN online sandbox. The columns show the enterprise attack matrix tactics, with the techniques that are used by the malware arranged under the columns. Clicking the technique then lists details of the procedures that are used by the specific malware instance with a definition, explanation, and examples of the technique.

Note: Do an internet search on MITRE ATT&CK to learn more about this tool.



Initial Access	Execution	Persistence	Privilege Escalat	Defense Evasion	Credential Acce:	Discovery	Lateral Moveme	Collection	Exfiltration	C & C	Impact
	Execution through API ● 2	Browser Extensions ● 1		Install Root Certificate ● 2		Query Registry ● 4					
	User Execution ● 1			Modify Registry ● 1							

Lab - Gather System Information After an Incident

In this Lab, you will complete the following objectives:

- Collect system information after an incident has occurred.
- View logs for potential intrusions.

27.2 The Cyber Kill Chain

Steps of the Cyber Kill Chain

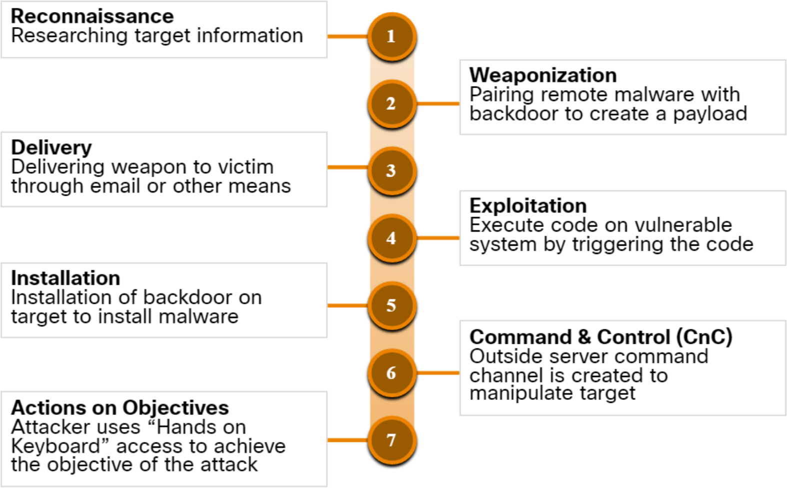
- Lockheed Martin developed the Cyber Kill Chain to identify and prevent cyber intrusions. There are seven steps to the Cyber Kill Chain. Focusing on these steps helps analysts understand the techniques, tools, and procedures of threat actors. When responding to a security incident, the objective is to detect and stop the attack as early as possible in the kill chain progression. The earlier the attack is stopped; the less damage is done and the less the attacker learns about the target network.

The Cyber Kill Chain

Steps of the Cyber Kill Chain (Cont.)

The Cyber Kill Chain specifies what an attacker must complete to accomplish their goal. The steps in the Cyber Kill Chain are shown in the figure.

If the attacker is stopped at any stage, the chain of attack is broken. Breaking the chain means the defender successfully thwarted the threat actor’s intrusion. Threat actors are successful only if they complete Step 7.



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

Reconnaissance

- Reconnaissance is when the threat actor performs research, gathers intelligence, and selects targets. This will inform the threat actor if the attack is worth performing. Any public information may help to determine what, where, and how of the attack to be performed. There is a lot of publicly available information, especially for larger organizations including news articles, websites, conference proceedings, and public-facing network devices. Increasing amounts of information surrounding employees is available through social media outlets.

- The threat actor will choose targets that have been neglected or unprotected because they will have a higher likelihood of becoming penetrated and compromised. All information obtained by the threat actor is reviewed to determine its importance and if it reveals possible additional avenues of attack.

Reconnaissance (Cont.)

The table summarizes some of the tactics and defenses used during the reconnaissance step.

Adversary Tactics	SOC Defenses
Plan and conduct research: • Harvest email addresses • Identify employees on social media • Collect all public relations information (press releases, awards, conference attendees, etc.) • 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

- The goal of this step is to use the information from reconnaissance to develop a weapon against specific targeted systems or individuals in the organization.
  - To develop this weapon, the designer will use the vulnerabilities of the assets that were discovered and build them into a tool that can be deployed.
  - After the tool has been used, it is expected that the threat actor has achieved their goal of gaining access into the target system or network, degrading the health of a target, or the entire network.
  - The threat actor will further examine network and asset security to expose additional weaknesses, gain control over other assets, or deploy additional attacks.
  - A zero-day attack uses a weapon that is unknown to defenders and network security systems.
  - Attackers have learned how to create numerous variants of their attacks to evade network defenses.

Weaponization (Cont.)

The table summarizes some of the tactics and defenses used during the weaponization step.

Adversary Tactics	SOC Defense
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.

Delivery

- During this step, the weapon is transmitted to the target using a delivery vector.
- This may be using a website, removable USB media, or an email attachment.
- If the weapon is not delivered, the attack will be unsuccessful.
- The threat actor will use many 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 code may be altered to seem innocent, yet still perform the necessary actions, even though it may take longer to execute.

Delivery (Cont.)

The table summarizes some of the tactics and defenses used during the delivery step.

Adversary Tactics	SOC Defense
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 attacker must use an exploit that gains the effect they desire.
- This is especially important because if the wrong exploit is conducted, obviously the attack will not work, but unintended side effects such as a DoS or multiple system reboots will cause undue attention that could easily inform cybersecurity analysts of the attack and the threat actor's intentions.

Exploitation (Cont.)

The table summarizes some of the tactics and defenses used during the exploitation step.

Adversary Tactics	SOC Defense
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 weblink	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

- This step is where the threat actor establishes a back door into the system to allow for continued access to the target.
- To preserve this backdoor, it is important that remote access does not alert cybersecurity analysts or users.
- The access method must survive through antimalware scans and rebooting of the computer to be effective.
- This persistent access can also allow for automated communications, especially effective when multiple channels of communication are necessary when commanding a botnet.

The Cyber Kill Chain

Installation (Cont.)

The table summarizes some of the tactics and defenses used during the installation step.

Adversary Tactics	SOC Defense
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

- In this step, 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.
- This is because most malware requires manual interaction to exfiltrate data from the network.
- CnC channels are used by the threat actor to issue commands to the software that they installed on the target.
- The cybersecurity analyst must be able to detect CnC communications to discover the compromised host.
- This may be in the form of unauthorized Internet Relay Chat (IRC) traffic or excessive traffic to suspect domains.

Command and Control (Cont.)

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

Adversary Tactics	SOC Defense
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

Actions on Objectives

- The final step of the Cyber Kill Chain describes the threat actor achieving their original objective.
- This may be data theft, performing a DDoS attack, or using the compromised network to create and send spam or mine Bitcoin.
- 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 Cyber Kill Chain

Actions on Objectives (Cont.)

The table summarizes some of the tactics and defenses used during the actions on objectives step.

Adversary Tactics	SOC Defense
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

27.3 The Diamond Model of Intrusion Analysis

Diamond Model Overview

The Diamond Model of Intrusion Analysis is made up of four parts. The model represents a security incident or event. In the Diamond Model, an event is a time-bound activity that is restricted to a specific step in which an adversary uses a capability over infrastructure to attack a victim to achieve a specific result.

The four core features of an intrusion event are adversary, capability, infrastructure, and victim:

- **Adversary:** These are the parties responsible for the intrusion.
- **Capability:** This is a tool or technique that the adversary uses to attack the victim.
- **Infrastructure:** This is the network path or paths that the adversaries use to establish and maintain command and control over their capabilities.
- **Victim:** This is the target of the attack. However, a victim might be the target initially and then used as part of the infrastructure to launch other attacks.

Diamond Model Overview (Cont.)

The adversary uses capabilities over infrastructure to attack the victim. The model can be interpreted as saying, “The adversary uses the infrastructure to connect to the victim. The adversary develops capability to exploit the victim.” For example, a capability like malware might be used over the email infrastructure by an adversary to exploit a victim.

Meta-features expand the model slightly to include the following essential elements:

- **Timestamp:** This indicates the start and stop time of an event and is an integral part of grouping malicious activity.
- **Phase:** This is analogous to steps in the Cyber Kill Chain; malicious activity includes two or more steps executed in succession to achieve the desired result.
- **Result:** This delineates what the adversary gained from the event. Results can be documented as one or more of the following: confidentiality compromised, integrity compromised, and availability compromised.

Diamond Model Overview (Cont.)

Direction: This indicates the direction of the event across the Diamond Model. These include Adversary-to-Infrastructure, Infrastructure-to-Victim, Victim-to-Infrastructure, and Infrastructure-to-Adversary.

Methodology: This is used to classify the general type of event, such as port scan, phishing, content delivery attack, syn flood, etc.

Resources: These are one or more external resources used by the adversary for the intrusion event, such as software, adversary’s knowledge, information (e.g., username/passwords), and assets to carry out the attack (hardware, funds, facilities, network access).

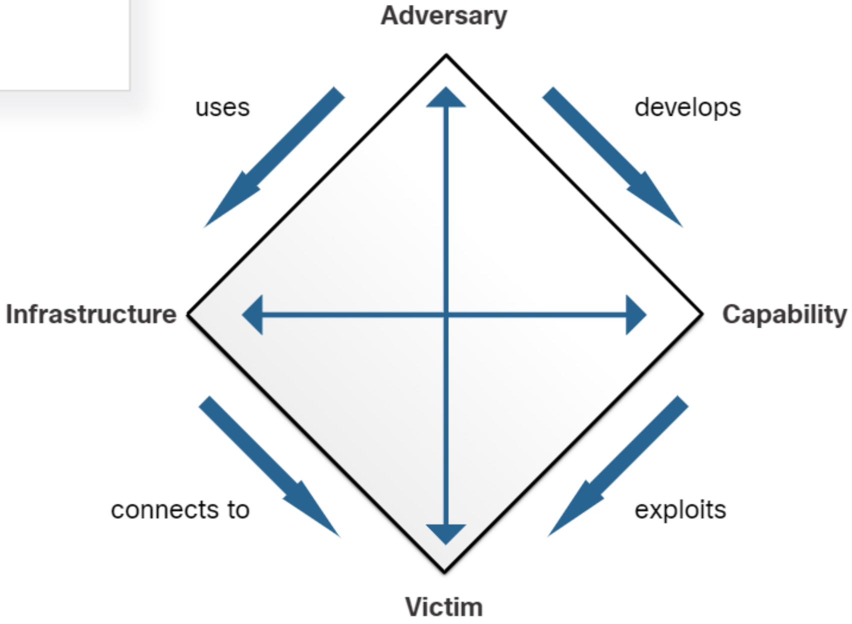
The Diamond Model of Intrusion Analysis

Diamond Model Overview (Cont.)

The Diamond Model

Meta-Features

- Timestamp
- Phase
- Result
- Direction
- Methodology
- Resources



Pivoting Across the Diamond Model

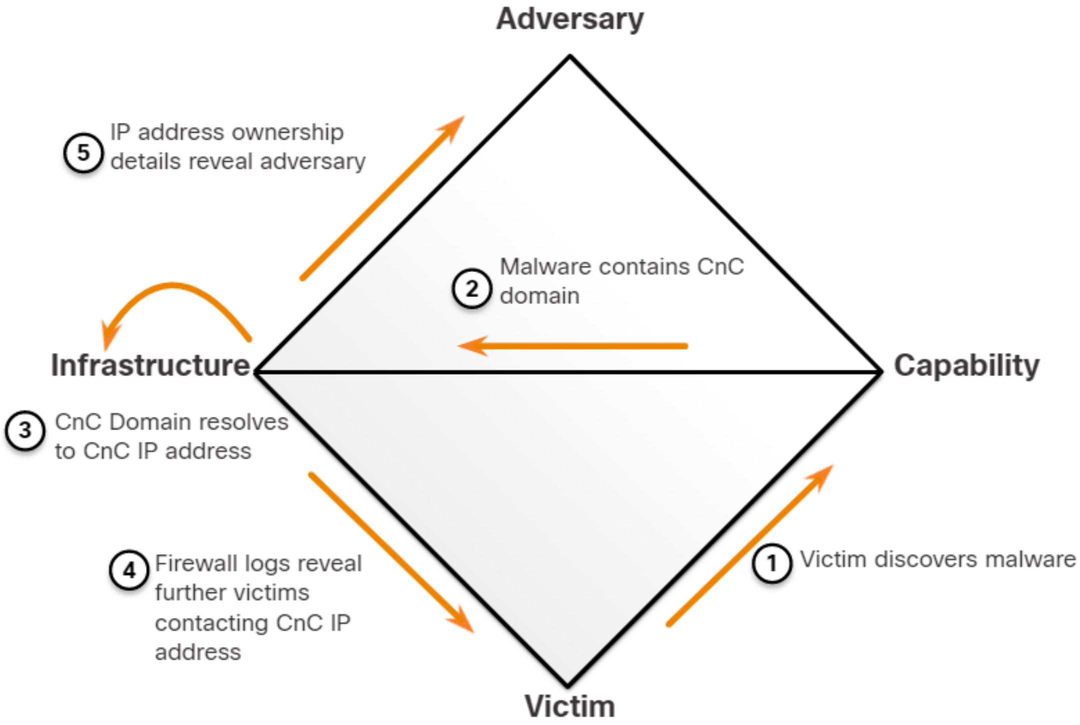
- As a cybersecurity analyst, you may be called on to use the Diamond Model of Intrusion Analysis to diagram a series of intrusion events. The Diamond Model is ideal for illustrating how the adversary pivots from one event to the next.

- For example, in the figure 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.
- These domain names resolve to a list of IP addresses.
- These IP addresses are then used to identify the adversary, as well as investigate logs to determine if other victims in the organization are using the CnC channel.

The Diamond Model of Intrusion Analysis

Pivoting Across the Diamond Model (Cont.)

Diamond Model Characterization of an Exploit



Adversary

Infrastructure

Capability

Victim

1 Victim discovers malware

2 Malware contains CnC domain

3 CnC Domain resolves to CnC IP address

4 Firewall logs reveal further victims contacting CnC IP address

5 IP address ownership details reveal adversary

The Diamond Model and the Cyber Kill Chain

Adversaries do not operate in just a single event. Instead, events are threaded together in a chain in which each event must be successfully completed before the next event. This thread of events can be mapped to the Cyber Kill Chain previously discussed in the chapter.

The following example illustrates the end-to-end process of an adversary as they vertically traverse the Cyber Kill Chain, use a compromised host to horizontally pivot to another victim, and then begin another activity thread:

- Adversary conducts a web search for victim company Gadgets, Inc. receiving as part of the results the domain name gadgets.com.
- Adversary uses the newly discovered domain gadets.com for a new search “network administrator gadget.com” and discovers forum postings from users claiming to be network administrators of gadget.com. The user profiles reveal their email addresses.
- Adversary sends phishing emails with a Trojan horse attached to the network administrators of gadget.com.

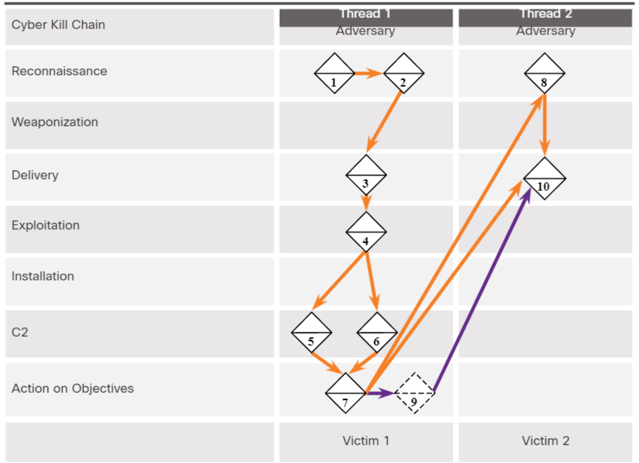
The Diamond Model and the Cyber Kill Chain (Cont.)

- One network administrator (NA1) of gadget.com opens the malicious attachment. This executes the enclosed exploit allowing for further code execution.
- NA1's compromised host sends an HTTP Post message to an IP address, registering it with a CnC controller. NA1's compromised host receives an HTTP Response in return.
- It is revealed from reverse engineering that the malware has additional IP addresses configured which act as a back-up if the first controller does not respond.
- Through a CnC HTTP response message sent to NA1's host, the malware begins to act as a web proxy for new TCP connections.
- Through information from the proxy that is running on NA1's host, Adversary does a web search for "most important research ever" and finds Victim 2, Interesting Research Inc.
- 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.
- 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 Diamond Model and the Cyber Kill Chain (Cont.)

The adversary now has two compromised victims from which additional attacks can be launched. For example, the adversary could mine the Chief Research Officer’s email contacts for the additional potential victims. The adversary might also setup another proxy to exfiltrate all of the Chief Research Officer’s files.

Note: This example is a modification of the U.S. Department of Defense’s example in the publication “The Diamond Model of Intrusion Analysis".



Lab - Attack Analysis

In this Lab, you will meet the following objectives:

- Part 1: Investigate IOCs
- Part 2: Investigate the Malicious Activity
- Part 3: Investigate the More Malicious Activity

27.4 Incident Response

Establishing an Incident Response Capability

- Incident Response involves the methods, policies, and procedures that are used by an organization to respond to a cyberattack. The aims of incident response are to limit the impact of the attack, assess the damage caused, and implement recovery procedures. Because of the potential large-scale loss of property and revenue that can be caused by cyberattacks, it is essential that organizations create and maintain detailed incident response plans and designate personnel who are responsible for executing all aspects of that plan.

- The U.S. National Institute of Standards and Technology (NIST) recommendations for incident response are detailed in their Special Publication 800-61, revision two entitled “Computer Security Incident Handling Guide,” which is shown the figure.

- **Note:** Although this chapter summarizes much of the content in the NIST 800-61r2 standard, you should be familiar with the entire publication as it covers four major exam topics for the Understanding Cisco Cybersecurity Operations Fundamentals exam.

Establishing an Incident Response Capability (Cont.)

- The NIST 800-61r2 standard provides guidelines for incident handling, particularly for analyzing incident-related data, and determining the appropriate response to each incident. The guidelines can be followed independently of hardware platforms, operating systems, protocols, or applications.

- The first step for an organization is to establish a computer security incident response capability (CSIRC). NIST recommends creating policies, plans, and procedures for establishing and maintaining a CSIRC.

Establishing an Incident Response Capability (Cont.)

Policy Elements: An incident response policy details how incidents should be handled based on the organization's mission, size, and function. The policy should be reviewed regularly to adjust it to meet the goals of the roadmap that has been laid out. Policy elements include the following:

- 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

Establishing an Incident Response Capability (Cont.)

Plan Elements: A good incident response plan helps to minimize damage caused by an incident. It also helps to make the overall incident response program better by adjusting it according to lessons learned. It will ensure that each party involved in the incident response has a clear understanding of not only what they will be doing, but what others will be doing as well. Plan elements are as follows:

- 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

Establishing an Incident Response Capability (Cont.)

Procedure Elements: The procedures that are followed during an incident response should follow the incident response plan. Procedures elements are as follows:

- Technical processes
- Using techniques
- Filling out forms,
- Following checklists

These are typical standard operating procedures (SOPs). These SOPs should be detailed so that the mission and goals of the organization are in mind when these procedures are followed. SOPs minimize errors that may be caused by personnel that are under stress while participating in incident handling. It is important to share and practice these procedures, making sure that they are useful, accurate, and appropriate.

Incident Response Stakeholders

Other groups and individuals within the organization may also be involved with incident handling. It is important to ensure that they will cooperate before an incident is underway. Their expertise and abilities can help the Computer Security Incident Response Team (CSIRT) to manage the incident quickly and correctly. These are some of the stakeholders that may be involved in handing a security incident:

Management: Managers create the policies that everyone must follow. They also design the budget and oversee staffing of all the departments. Management must coordinate the incident response with er stakeholders and minimize the damage of an incident.

Incident Response Stakeholders (Cont.)

Information Assurance: This group may need to be called in to change things such as firewall rules during some stages of incident management such as containment or recovery.

IT Support: This is the group that works with the technology in the organization and understands it the most. Because IT support has a deeper understanding, it is more likely that they will perform the correct action to minimize the effectiveness of the attack or preserve evidence properly.

Legal Department: It is a best practice to have the legal department review the incident policies, plans, and procedures to make sure that they do not violate any local or federal guidelines. Also, if any incident has legal implications, a legal expert will need to become involved. This might include prosecution, evidence collection, or lawsuits.

Incident Response Stakeholders (Cont.)

Public Affairs and Media Relations: There are times when the media and the public might need to be informed of an incident, such as when their personal information has been compromised during an incident.

Human Resources: The human resources department might need to perform disciplinary measures if an incident caused by an employee occurs.

Business Continuity Planners: Security incidents may alter an organization’s business continuity. It is important that those in charge of business continuity planning are aware of security incidents and the impact they have had on the organization. This will allow them to make any changes in plans and risk assessments.

Physical Security and Facilities Management: When a security incident happens because of a physical attack, such as tailgating or shoulder surfing, these teams might need to be informed and involved. It is also their responsibility to secure facilities that contain evidence from an investigation.

Incident Response Stakeholders (Cont.)

The Cybersecurity Maturity Model Certification

The Cybersecurity Maturity Model Certification (CMMC) framework was created to assess the ability of organizations that perform functions for the U.S. Department of Defense (DoD) to protect the military supply chain from disruptions or losses due to cybersecurity incidents. Security breaches related to DoD information indicated that NIST standards were not sufficient to mitigate against the increasing and evolving threat landscape, especially from nation-state threat actors. For companies to receive contracts from the DoD, those companies must be certified. The certification consists of five levels, with various levels required depending on the degree of security required by the project.

Incident Response Stakeholders (Cont.)

The CMMC specifies seventeen domains, each of which has a varying number of capabilities that are associated with it. The organization is rated by the maturity level that has been achieved for each of the domains. One of the domains concerns incident responses. The capabilities that are associated with the incident response domain are as follows:

- Plan incident response
- Detect and report events
- Develop and implement a response to a declared incident
- Perform post incident reviews
- Test incident response

The CMMC certifies organizations by level. For most domains, there are five levels, however for incident response, there are only four. The higher the level that is certified, the more mature the cybersecurity capability of the organization. A summary of the incidence response domain maturity levels is shown below.

Incident Response Stakeholders (Cont.)

Level 2: Establish an incident response plan that follows the NIST process. Detect, report, and prioritize events. Respond to events by following predefined procedures. Analyze the cause of incidents to mitigate future issues.

Level 3: Document and report incidents to stakeholders that have been identified in the incident response plan. Test the incident response capability of the organization.

Level 4: Use knowledge of attacker tactics, techniques, and procedures (TTP) to refine incident response planning and execution. Establish a security operation center (SOC) that facilitates a 24/7 response capability.

Level 5: Utilize accepted and systematic computer forensic data gathering techniques including the secure handling and storage of forensic data. Develop and utilize manual and automated real-time responses to potential incidents that follow known patterns.

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. CSIRT members should continually develop knowledge of emerging threats.

Detection and Analysis: Through continuous monitoring, the CSIRT quickly identifies, analyzes, and validates an incident.

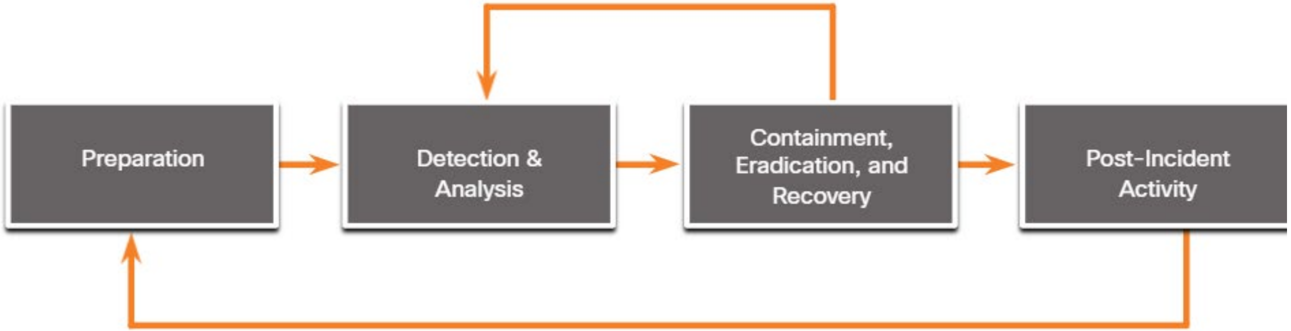
Containment, Eradication, and Recovery: The CSIRT implements procedures to contain the threat, eradicate the impact on organizational assets, and use backups to restore data and software. This phase may cycle back to detection and analysis to gather more information, or to expand the scope of the investigation.

Post-Incident Activities: The CSIRT then documents how the incident was managed, recommends changes for future response, and specifies how to avoid a reoccurrence.

Incident Response

NIST Incident Response Life Cycle (Cont.)

The incident response life cycle is meant to be a self-reinforcing learning process whereby each incident informs the process for handling future incidents. Each of these phases are discussed in more detail in this topic.



Preparation

The preparation phase is when the CSIRT is created and trained. This phase is also when the tools and assets that will be needed by the team to investigate incidents are acquired and deployed. The following list has examples of actions that also take place during the preparation phase:

- Organizational processes are created to address communication between people on the response team. This includes such things as contact information for stakeholders, other CSIRTs, and law enforcement, an issue tracking system, smartphones, encryption software, etc.
- Facilities to host the response team and the SOC are created.
- Necessary hardware and software for incident analysis and mitigation is acquired. This may include forensic software, spare computers, servers and network devices, backup devices, packet sniffers, and protocol analyzers.
- Risk assessments are used to implement controls that will limit the number of incidents.
- Validation of security hardware and software deployment is performed on end-user devices, servers, and network devices.
- User security awareness training materials are developed.

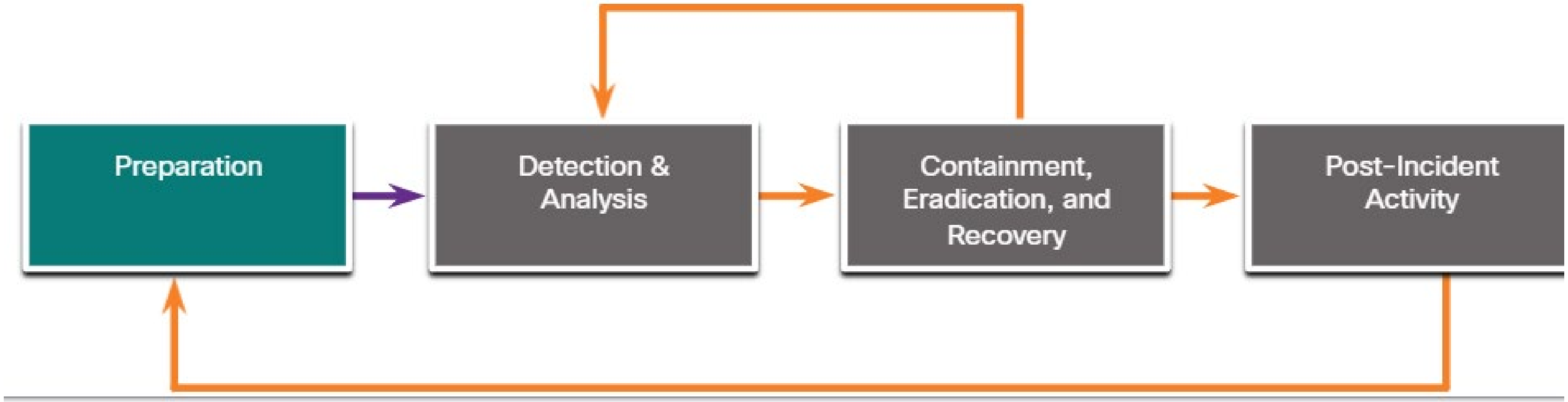
Preparation (Cont.)

- Additional incident analysis resources might be required. Examples of these resources are a list of critical assets, network diagrams, port lists, hashes of critical files, and baseline readings of system and network activity. Mitigation software is also an important item when preparing to manage a security incident. An image of a clean OS and application installation files may be needed to recover a computer from an incident.

- Often, the CSIRT may have a jump kit prepared. This is a portable box with many of the items listed above to help in establishing a swift response. Some of these items may be a laptop with appropriate software installed, backup media, and any other hardware, software, or information to help in the investigation. It is important to inspect the jump kit on a regular basis to install updates and make sure that all the necessary elements are available and ready for use. It is helpful to practice deploying the jump kit with the CSIRT to ensure that the team members know how to use its contents properly.

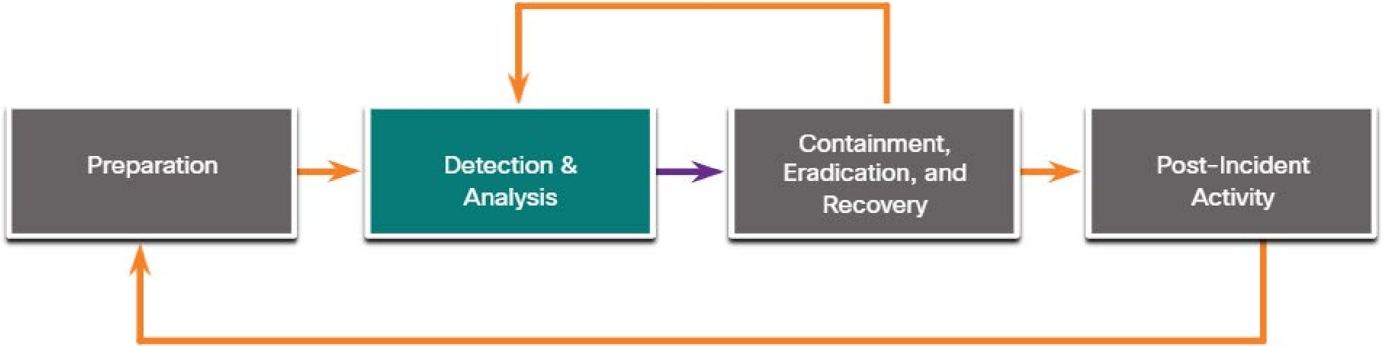
Preparation (Cont.)

Preparation Phase:



Detection and Analysis

Detection and Analysis Phase:



Because there are so many ways in which a security incident can occur, it is impossible to create instructions that completely cover each step to follow to manage them. Different types of incidents will require different responses.

Detection and Analysis (Cont.)

Attack Vectors:

An organization should be prepared to manage any incident but should focus on the most common types of incidents so that they can be dealt with swiftly. These are some of the more common types of attack vectors:

- **Web** - Any attack that is initiated from a website or application hosted by a website.
- **Email** - Any attack that is initiated from an email or email attachment.
- **Loss or Theft** - Any equipment that is used by the organization such as a laptop, desktop, or smartphone can provide the required information for someone to initiate an attack.
- **Impersonation** - When something or someone is replaced for the purpose of malicious intent.
- **Attrition** - Any attack that uses brute force to attack devices, networks, or services.
- **Media** - Any attack that is initiated from external storage or removable media.

Detection and Analysis (Cont.)

Detection: Some incidents are easy to detect while others may go undetected for months. The detection of security incidents might be the most difficult phase in the incident response process. Incidents are detected in many ways and not all these ways are very detailed or provide detailed clarity. There are automated ways of detection such as antivirus software or an IDS. There are also manual detections through user reports.

It is important to accurately determine the type of incident and the extent of the effects. There are two categories for the signs of an incident:

- **Precursor** - This is a sign that an incident might occur in the future. When precursors are detected, an attack might be avoided by altering security measures to specifically address the type of attack detected. Examples of precursors are log entries that show a response to a port scan, or a newly discovered vulnerability to an organization's web server.
- **Indicator** - This is a sign that an incident might already have occurred or is currently occurring. Some examples of indicators are a host that has been infected with malware, multiple failed logins from an unknown source, or an IDS alert.

Detection and Analysis (Cont.)

Analysis: Incident analysis is difficult because not all the indicators are accurate. In a perfect world, each indicator should be analyzed to find out if it is accurate. This is nearly impossible due to the number and variety of logged and reported incidents. The use of complex algorithms and machine learning often help to determine the validity of security incidents. This is more prevalent in large organizations that have thousands or even millions of incidents daily. One method that can be used is network and system profiling. Profiling is measuring the characteristics of expected activity in networking devices and systems so that changes to it can be more easily identified.

When an indicator is found to be accurate, it does not necessarily mean that a security incident has occurred. Some indicators happen for other reasons besides security. A server that continually crashes, for example, may have bad RAM instead of a buffer overflow attack occurring. To be safe, even ambiguous, or contradictory symptoms must be analyzed to determine if a legitimate security incident has taken place. The CSIRT must react quickly to validate and analyze incidents. This is performed by following a predefined process and documenting each step.

Detection and Analysis (Cont.)

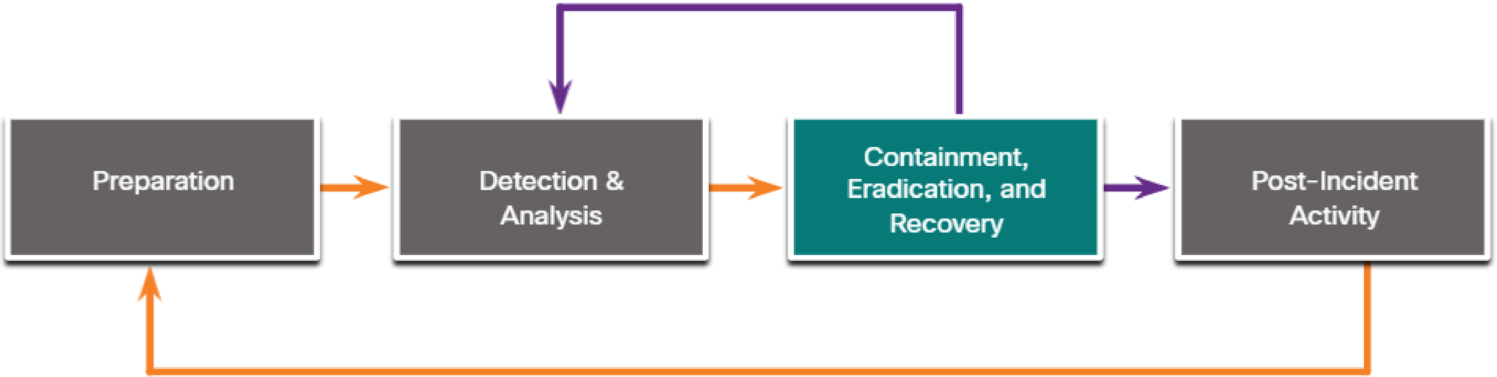
Scoping: When the CSIRT believes that an incident has occurred, it should immediately perform an initial analysis to determine the incident's scope, such as which networks, systems, or applications are affected, who or what originated the incident, and how the incident is occurring. This scoping activity should provide enough information for the team to prioritize subsequent activities, such as containment of the incident and deeper analysis of the effects of the incident.

Detection and Analysis (Cont.)

Incident notification: When an incident is analyzed and prioritized, the incident response team needs to notify the appropriate stakeholders and outside parties so that all who need to be involved will play their roles. Examples of parties that are typically notified include:

- Chief Information Officer (CIO)
- Head of information security
- Local information security officer
- Other incident response teams within the organization
- External incident response teams (if appropriate)
- System owner
- Human resources (for cases involving employees, such as harassment through email)
- Public affairs (for incidents that may generate publicity)
- Legal department (for incidents with potential legal ramifications)
- US-CERT (required for Federal agencies and systems operated on behalf of the Federal government)
- Law enforcement (if appropriate)

Containment, Eradication, and Recovery



After a security incident has been detected and sufficient analysis has been performed to determine that the incident is valid, it must be contained to determine what to do about it. Strategies and procedures for incident containment need to be in place before an incident occurs and implemented before there is widespread damage.

Containment, Eradication, and Recovery (Cont.)

Containment Strategy: For every type of incident, a containment strategy should be created and enforced. These are some conditions to determine the type of strategy to create for each incident type:

- How long it will take to implement and complete a solution?
- How much time and how many resources will be needed to implement the strategy?
- What is the process to preserve evidence?
- Can an attacker be redirected to a sandbox so that the CSIRT can safely document the attacker's methodology?
- What will be the impact to the availability of services?
- What is the extent of damage to resources or assets?
- How effective is the strategy?

During containment, additional damage may be incurred. For example, it is not always advisable to unplug the compromised host from the network. The malicious process could notice this disconnection to the CnC controller and trigger a data wipe or encryption on the target. This is where experience and expertise can help to contain an incident beyond the scope of the containment strategy.

Containment, Eradication, and Recovery (Cont.)

Evidence: During an incident, evidence must be gathered to resolve it. Evidence is also important for subsequent investigation by authorities. Clear and concise documentation surrounding the preservation of evidence is critical. For evidence to be admissible in court, evidence collection must conform to specific regulations. After evidence collection, it must be accounted for properly. This is known as the chain of custody. These are some of the most important items to log when documenting evidence used in the chain of custody:

- Location of the recovery and storage of all evidence
- Any identifying criteria for all evidence such as serial number, MAC address, hostname, or IP address
- Identification information for all the people that participated in collecting or managing the evidence
- Time and date that the evidence was collected and each instance it was handled
- It is vital to educate anyone involved in evidence managing on how to preserve evidence properly.

Containment, Eradication, and Recovery (Cont.)

Attacker Identification: Identifying attackers is secondary to containing, eradicating, and recovering hosts and services. However, identifying attackers will minimize the impact to critical business assets and services. These are some of the most important actions to perform to attempt to identify an attacking host during a security incident:

- Use incident databases to research related activity. This database may be in-house or located at organizations that collect data from other organizations and consolidate it into incident databases such as the VERIS community database.
- Validate the attacker’s IP address to determine if it is a viable one. The host may or may not respond to a request for connectivity. This may be because it has been configured to ignore the requests, or the address has already been reassigned to another host.
- Use an internet search engine to gain additional information about the attack. There may have been another organization or individual that has released information about an attack from the identified source IP address.
- Monitor the communication channels that some attackers use, such as IRC. Because users can be disguised or anonymized in IRC channels, they may talk about their exploits in these channels. Often, the information gathered from this type of monitoring is misleading and should be treated as leads and not facts.

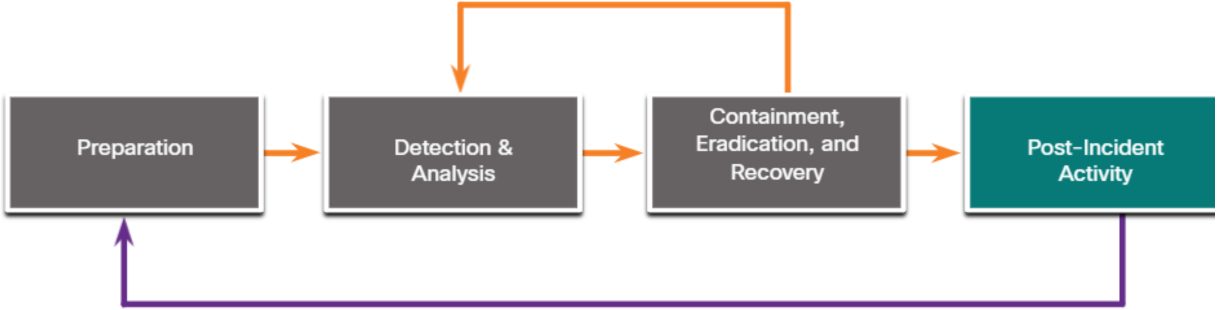
Containment, Eradication, and Recovery (Cont.)

Eradication, recovery, and remediation: After containment, the first step to eradication is identifying all the hosts that need remediation. All the effects of the security incident must be eliminated. This includes malware infections and user accounts that have been compromised. All the vulnerabilities that were exploited by the attacker must also be corrected or patched so that the incident does not occur again.

To recover hosts, use clean and recent backups, or rebuild them with installation media if no backups are available or they have been compromised. Also, fully update and patch the operating systems and installed software of all hosts. Change all host passwords and passwords for critical systems in accordance with the password security policy. This may be a suitable time to validate and upgrade network security, backup strategies, and security policies. Attackers often attack the systems again, or use a similar attack to target additional resources, so be sure to prevent this as best as possible. Focus on what can be fixed quickly while prioritizing critical systems and operations.

Post-Incident Activities

Post-Incident Activity Phase



After incident response activities have eradicated the threats and the organization has begun to recover from the effects of the attack, it is important to take a step back and periodically meet with all the parties involved to discuss the events that took place and the actions of all the individuals while managing the incident. This will provide a platform to learn what was done right, what was done wrong, what could be changed, and what should be improved upon.

Post-Incident Activities (Cont.)

Lessons-based hardening: After a major incident has been handled, the organization should hold a “lessons learned” meeting to review the effectiveness of the incident handling process and identify necessary hardening needed for existing security controls and practices. Examples of good questions to answer during the meeting include the following:

- Exactly what happened, and when?
- How well did the staff and management perform while dealing with the incident?
- Were the documented procedures followed? Were they adequate?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurs?
- How could information sharing with other organizations be improved?
- What corrective actions can prevent similar incidents in the future?
- What precursors or indicators should be watched for in the future to detect similar incidents?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

Incident Data Collection and Retention

- By having ‘lessons learned’ meetings, the collected data can be used to determine the cost of an incident for budgeting reasons, as well as to determine the effectiveness of the CSIRT, and identify security weaknesses throughout the system. The collected data needs to be actionable. Only collect data that can be used to define and refine the incident handling process.

- A higher number of incidents handled can show that something in the incidence response methodology is not working properly and needs to be refined. It could also show incompetence in the CSIRT. A lower number of incidents might show that network and host security has been improved. It could also show a lack of incident detection. Separate incident counts for each type of incident may be more effective at showing strengths and weakness of the CSIRT and implemented security measures. These subcategories can help to target where a weakness resides, rather than whether there is a weakness at all.

Incident Data Collection and Retention (Cont.)

The time of each incident provides insight into the total amount of labor used and the total time of each phase of the incident response process. The time until the first response is also important, as well as how long it took to report the incident and escalate it beyond the organization, if necessary.
It is important to perform an objective assessment of each incident. The response to an incident that has been resolved can be analyzed to determine how effective it was. NIST Special Publication 800-61 provides the following examples of activities that are performed during an objective assessment of an incident:

- Reviewing logs, forms, reports, and other incident documentation for adherence to established incident response policies and procedures.
- Identifying which precursors and indicators of the incident were recorded to determine how effectively the incident was logged and identified.
- Determining if the incident caused damage before it was detected.
- Determining if the actual cause of the incident was identified, and identifying the vector of attack, the vulnerabilities exploited, and the characteristics of the targeted or victimized systems, networks, and applications.

Incident Data Collection and Retention (Cont.)

- Determining if the incident is a recurrence of a previous incident.
- Calculating the estimated monetary damage from the incident (e.g., information and critical business processes negatively affected by the incident).
- Measuring the difference between the initial impact assessment and the final impact assessment.
- Identifying which measures, if any, could have prevented the incident.
- Subjective assessment of each incident requires that incident response team members assess their own performance, as well as that of other team members and of the entire team. Another valuable source of input is the owner of a resource that was attacked, in order to determine if the owner thinks the incident was managed efficiently and if the outcome was satisfactory.

Incident Data Collection and Retention (Cont.)

There should be a policy in place in each organization that outlines how long evidence of an incident is retained. Evidence is often retained for many months or many years after an incident has taken place. In some cases, compliance regulations may mandate the retention period. These are some of the determining factors for evidence retention:

Prosecution: When an attacker will be prosecuted because of a security incident, the evidence should be retained until after all legal actions have been completed. This may be several months or many years. In legal actions, no evidence should be overlooked or considered insignificant. An organization's policy may state that any evidence surrounding an incident that has been involved with legal actions must never be deleted or destroyed.

Incident Data Collection and Retention (Cont.)

Data Type: An organization may state that types of data should be kept for a specific period. Items such as email or text may only need to be kept for 90 days. More important data such as that used in an incident response (that has not had legal action), may need to be kept for three years or more.

Cost: If there is a lot of hardware and storage media that needs to be stored for a long time, it can become costly. Also remember that as technology changes, functional devices that can use outdated hardware and storage media must be stored as well.

Reporting Requirements and Information Sharing

The legal team should consult governmental regulations to precisely determine the organization’s responsibility for reporting the incident. In addition, management will need to determine what additional communication is necessary with other stakeholders, such as customers, vendors, partners, etc.

Beyond the legal requirements and stakeholder considerations, NIST recommends that an organization coordinate with organizations to share details for the incident. For example, the organization could log the incident in the VERIS community database.

The critical recommendations from NIST for sharing information are as follows:

- Plan incident coordination with external parties before incidents occur.
- Consult with the legal department before initiating any coordination efforts.
- Perform incident information sharing throughout the incident response life cycle.
- Attempt to automate as much of the information sharing process as possible.
- Balance the benefits of information sharing with the drawbacks of sharing sensitive information.

Share as much of the appropriate incident information as possible with other organizations.

Lab - Incident Handling

In this lab, you will apply your knowledge of security incident handling procedures to formulate questions about given incident scenarios.

27.5 Disaster Recovery

Types of Disasters

A disaster includes any natural or human-caused event that damages assets or property and impairs the ability of the organization to continue operating.

Natural disasters differ depending on location and are sometimes difficult to predict. They fall into the following categories:

- Geological disasters such as earthquakes, landslides, volcanoes, and tsunamis.
- Meteorological disasters such as hurricanes, tornadoes, snowstorms, lightning, and hail.
- Health disasters such as widespread illnesses, quarantines, and pandemics.
- Miscellaneous disasters such as fires, floods, solar storms, and avalanches.

Types of Disasters (Cont.)

Human-caused disasters involve people or organizations and fall into the following categories:

- Labor events such as strikes, walkouts and slowdowns.
- Sociopolitical events such as vandalism, blockades, protests, sabotage, terrorism, and war.
- Materials events such as hazardous spills and fires.
- Utility disruptions such as power failures, communication outages, fuel shortages and radioactive fallout.

Disaster Recovery Plan

An organization puts its **Disaster Recovery Plan (DRP)** into action while the disaster is ongoing, and employees are scrambling to ensure critical systems are online.

The DRP includes the activities the organization takes to assess, salvage, repair and restore damaged facilities or assets.

To create the DRP, answer the following questions:

- Who is responsible for this process?
- What does the individual need to perform the process?
- Where does the individual perform this process?
- What is the process?
- Why is the process critical?

Implementing Disaster Recovery Controls

Disaster recovery controls minimize the effects of a disaster so that the organization can resume operation. The three types of IT disaster recovery controls are:

- **Preventive controls:** preventive measures include controls that prevent a disaster from occurring. They aim to identify and mitigate risks.
- **Detective controls:** Detective measures include controls that discover unwanted events. These measures uncover new potential threats.
- **Corrective controls:** Corrective measures include controls that restore the system after a disaster or an event.

Business Continuity Planning

- Business continuity is one of the most important concepts in computer security. Having plans in place will ensure business continuity regardless of what may occur.

- A business continuity plan (BCP) is a broader plan than a disaster recovery plan (DRP) because it can include getting critical systems to another location while the repair of the original facility is underway. In such a scenario, personnel continue to perform all business processes in an alternate manner until normal operations resume.

- Creating a business continuity plan starts with conducting a business impact analysis (BIA) to identify critical business processes, resources, and relationships between systems. The BIA focuses on the consequences of the interruption to critical business functions and examines the key considerations listed below.

Business Continuity Planning (Cont.)

Recovery time objectives (RTOs): The maximum tolerable length of time that a system, network, or application can be unavailable after a failure or disaster.

Recovery point objectives (RPOs): The average lifespan of a given asset before it fails.

Mean time to repair (MTTR): The average time required to repair a failed component.

Mean time between failures (MTBF): The average time that elapses between one failure and the next.

Business Continuity Considerations

Business continuity controls are more than just backing up data and providing redundant hardware. Organizations need employees to properly configure and operate systems. Data can be useless until it provides information.

An organization should look at the following:

- Getting the right people to the right places.
- Documenting configurations.
- Establishing alternate communication channels for both voice and data.
- Providing power.
- Identifying all dependencies for applications and processes so that they are properly understood.
- Understanding how to conduct automated tasks manually.

Business Continuity Best Practices

The National Institute of Standards and Technology (NIST) developed best practices in relation to business continuity. NIST recommendations are as follows:

1. Develop the policy statement: Write a policy that provides guidance to develop the business continuity plan and assigns roles to carry out the tasks.
2. Conduct the business impact assessment: Identify critical systems and processes and prioritize them based on necessity.
3. Calculate risk: Identify vulnerabilities, threats and calculate risks.
4. Identify preventative controls: Identify and implement controls and countermeasures to reduce risk.
5. Develop recovery strategies: Devise methods to bring back critical systems quickly.
6. Develop the contingency plan: Write procedures to keep the organization functioning in a chaotic state.
7. Test the plan: Verify how effective the plan is in real-time scenarios.
8. Maintain the plan: Update the plan regularly.

Exercising Your Disaster Recovery Plan

There are several different methods available to train staff and assess the organization’s disaster recovery plan.

Tabletop exercises: The simplest is a tabletop exercise in which participants sit around a table with a facilitator who supplies information related to a scenario incident and processes that are being examined. No actual processes or procedures are invoked; they are just discussed. This may result in the realization that a certain type of incident is not currently covered in existing plans.

Functional tests: Another type of exercise is a functional test where certain aspects of a plan are tested to see how well they work (and how well-prepared personnel is).

Operational exercises: At the most extreme are full operational exercises, or simulations. These are designed to interrupt services to verify that all aspects of a plan are in place and sufficient to respond to the type of incident that is being simulated.

Packet Tracer - Investigate Disaster Recovery

In this Packet Tracer activity, you will meet the following objectives:

- Part 1: Review a Switch Configuration
- Part 2: Backup Files to a TFTP Server
- Part 3: Replace a Failed Switch
- Part 4: Restore Network Operations

Lab - Recommend Disaster Recovery Measures

In this Lab, you will meet the following objectives:

- Part 1: Natural Disaster
- Part 2: DDoS Attack
- Part 3: Loss of Data

27.6 Digital Forensics and Incident Analysis and Response Summary

What Did I Learn in this Module?

Evidence Handling and Attack Attribution:

- Digital forensics is the recovery and investigation of information found on digital devices as it relates to criminal activity.
- Indicators of compromise are the evidence that a cybersecurity incident has occurred.
- These must be preserved for future analysis and attack attribution.
- An organization must develop well-documented processes and procedures for digital forensic analysis.
- NIST Special Publication 800-86 Guide to Integrating Forensic Techniques into Incident Response is a valuable resource.
- The forensic process includes four steps: collection, examination, analysis, and reporting.
- IETF RFC 3227 describes an order for the collection of digital evidence based on the volatility of the data.
- Chain of custody involves the collection, handling, and secure storage of evidence.

What Did I Learn in this Module? (Cont.)

Evidence Handling and Attack Attribution:

- Identifying responsible threat actors (called threat attribution) should occur through the principled and systematic investigation of the evidence.
- In an evidence-based investigation, the incident response team correlates Tactics, Techniques, and Procedures (TTP) that were used in the incident with other known exploits.
- Threat intelligence sources can help to map the TTP identified by an investigation to known sources of similar attacks.
- For internal threats, uncovering the devices from which an attack was launched can lead directly to the threat actor.
- One way to attribute an attack is to model threat actor behavior.
- The MITRE Adversarial Tactics, Techniques & Common Knowledge (ATT&CK) Framework enables cybersecurity technicians to detect attacker tactics, techniques, and procedures (TTP) as part of threat defense and attack attribution.

What Did I Learn in this Module? (Cont.)

The Cyber Kill Chain:

- There are seven steps to the Cyber Kill Chain.
- These steps help analysts understand the techniques, tools, and procedures of threat actors.
- When responding to a security incident, the objective is to detect and stop the attack as early as possible in the kill chain progression.
- The steps in the Cyber Kill Chain are reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives.
- Reconnaissance is when the threat actor performs research, gathers intelligence, and selects targets.
- Weaponization is using the information from reconnaissance to develop a weapon against specific targeted systems or individuals in the organization.
- During Delivery, the weapon is transmitted to the target using a delivery vector.

What Did I Learn in this Module? (Cont.)

The Cyber Kill Chain:

- After the weapon has been delivered, the threat actor Exploits it to gain control of the target.
- Installation is when the threat actor establishes a back door into the system to allow for continued access to the target.
- To preserve this backdoor, it is important that remote access does not alert cybersecurity analysts or users.
- Command and Control, or CnC, establishes the threat actor's control over the target system.
- CnC channels are used by the threat actor to issue commands to the software that they installed on the target.
- Actions on Objectives describes the threat actor achieving their original objective.
- This may be data theft, performing a DDoS attack, or using the compromised network to create and send spam or mine Bitcoin

What Did I Learn in this Module? (Cont.)

The Diamond Model of Intrusion Analysis:

- The Diamond Model of Intrusion Analysis represents a security incident or event.
- An event is a time-bound activity that is restricted to a specific step in which an adversary uses a capability over infrastructure to attack a victim to achieve a specific result.
- The four core components of an intrusion event are the adversary, the capability, the infrastructure, and the victim.
- Meta-features, which expand the model slightly, include Timestamp, Phase, Result, Direction, Methodology, and Resources.
- As a cybersecurity analyst, you may be called on to use the Diamond Model of Intrusion Analysis to diagram a series of intrusion events.
- Adversaries do not operate in just a single event. Instead, events are threaded together in a chain in which each event must be successfully completed before the next event.
- This thread of events can be mapped to the Cyber Kill Chain.

What Did I Learn in this Module? (Cont.)

Incident Response involves the methods, policies, and procedures that are used by an organization to respond to a cyberattack.

- The goals of incident response are to limit the impact of the attack, assess the damage caused, and implement recovery procedures.
- It is essential that organizations create and maintain detailed incident response plans and designate personnel who are responsible for executing all aspects of that plan.
- NIST recommendations for incident response are detailed in their Special Publication 800-61, revision two entitled “Computer Security Incident Handling Guide”.
- The first step for an organization is to establish a computer security incident response capability (CSIRC).
- NIST recommends creating policies, plans, and procedures for establishing and maintaining a CSIRC.
- Some of the CSIRC stakeholders include Management, Information Assurance, IT Support, the Legal Department, Public Affairs and Media Relations, Human Resources, Business Continuity Planners, Physical Security and Facilities Management.

What Did I Learn in this Module? (Cont.)

Incident Response:

- The legal team should consult governmental regulations to determine the organization’s responsibility for reporting the incident.
- Beyond the legal requirements and stakeholder considerations, NIST recommends that an organization coordinate with organizations to share details for the incident.
- There should be a policy in place in each organization that outlines how long evidence of an incident is retained.
- The CMMC framework was created to assess the ability of organizations that perform functions for the U.S. DoD to protect the military supply chain from disruptions or losses due to cybersecurity incidents.
- The CMMC specifies seventeen domains, each of which has a varying number of capabilities that are associated with it.
- The organization is rated by the maturity level that has been achieved for each of the domains.
- The CMMC certifies organizations by level.

What Did I Learn in this Module? (Cont.)

Incident Response:

- NIST defines four steps in the incident response process life cycle:
  1. Preparation
  2. Detection and Analysis
  3. Containment, Eradication, and Recovery
  4. Post-Incident Activities.
- The preparation phase is when the CSIRT is created and trained.
- This phase is also when the tools and assets that will be needed by the team to investigate incidents are acquired and deployed. Incidents are detected in many ways and not all these ways are detailed or provide detailed clarity.
- There are two categories for the signs of an incident: Precursor and Indicator.
- The use of complex algorithms and machine learning often help to determine the validity of security incidents.
- One method that can be used is network and system profiling.

What Did I Learn in this Module? (Cont.)

Incident Response:

- When the CSIRT believes that an incident has occurred, it should immediately perform an initial analysis to determine the incident's scope, such as which networks, systems, or applications are affected, who or what originated the incident, and how the incident is occurring.
- When an incident is analyzed and prioritized, the incident response team needs to notify the appropriate stakeholders and outside parties so that all who need to be involved will play their roles.
- Clear and concise documentation surrounding the preservation of evidence is critical.
- Identifying attackers is secondary to containing, eradicating, and recovering hosts and services.
- After containment, the first step to eradication is identifying all the hosts that need remediation.
- All the effects of the security incident and all the vulnerabilities that were exploited by the attacker must also be corrected or patched so that the incident does not occur again.
- Following an incident, the organization should debrief to review the effectiveness of the incident handling process and identify necessary hardening needed for existing security controls and practices.

What Did I Learn in this Module? (Cont.)

Disaster Recovery:

- Natural disasters differ depending on location and are sometimes difficult to predict.
- Human-caused disasters involve people or organizations.
- An organization’s DRP includes the activities the organization takes to assess, salvage, repair and restore damaged facilities or assets.
- Preventive measures include controls that prevent a disaster from occurring.
- Detective measures include controls that discover new potential threats.
- Corrective measures include controls that restore the system after a disaster or an event.
- Business continuity controls are more than just backing up data and providing redundant hardware.
- Creating a business continuity plan starts with conducting a business impact analysis (BIA) to identify critical business processes, resources, and relationships between systems.
- The BIA focuses on the consequences of the interruption to critical business functions and examines the key considerations listed here: RTOs, RPOs, MTTR, and MTBF.
- The National Institute of Standards and Technology (NIST) developed best practices in relation to business continuity.

What Did I Learn in this Module? (Cont.)

Disaster Recovery:

- Training for the disaster recovery plan can use several methods.
- Consider a tabletop exercise in which participants sit around a table with a facilitator who supplies information related to a scenario incident and processes that are being examined.
- No actual processes or procedures are invoked; they are just discussed.
- Another type of exercise is a functional test where certain aspects of a plan are tested to see how well they work (and how well-prepared personnel is).
- At the most extreme are full operational exercises, or simulations.
- These are designed to interrupt services to verify that all aspects of a plan are in place and sufficient to respond to the type of incident that is being simulated.