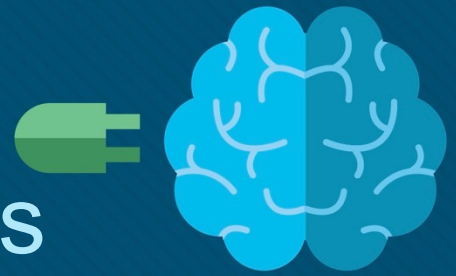


Chapter 12: Digital Forensics and Incident Analysis and Response

Information Security

Dr. Ayman Aljarbouh

Module Objectives

Module Title: Digital Forensics and Incident Analysis and Response

Module Objective: Explain how the CyberOps Associate responds to cyber 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 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

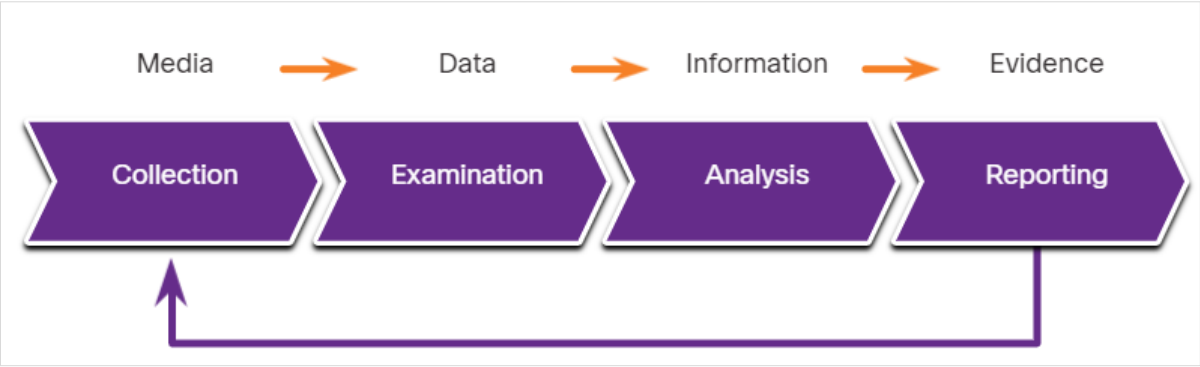
12.1 Evidence Handling and Attack Attribution

Digital Forensics

- 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.
- For example, under the US HIPAA regulations, if data breach has occurred involving patient information, then notification of the breach must be made to the affected individuals.
  - Digital forensic investigation must be used to determine the affected individuals and also to certify the number of affected individuals so that appropriate notification can be made in compliance with HIPAA regulations.
- At times, 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.

The Digital Forensics Process

- NIST describes the four phases of the digital evidence forensic process:
  - **Collection** - Identification of potential sources of forensic data and acquisition, handling, and storage of that data
  - **Examination** - Assessing and extracting relevant information from the collected data
  - **Analysis** - Drawing conclusions from the data and correlation of data from multiple sources
  - **Reporting** - Preparing and presenting information that resulted from the analysis phase.



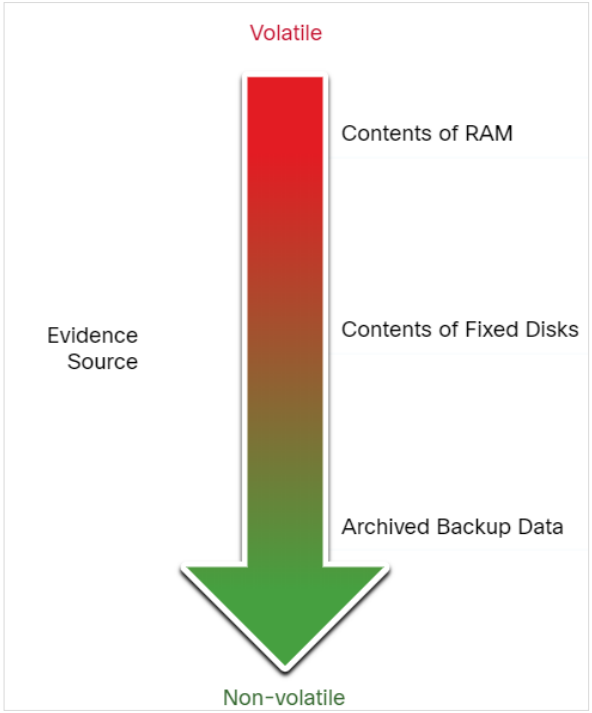
Types of Evidence

In legal proceedings, evidence is broadly classified as following:

- **Direct Evidence** - The evidence that was indisputably in the possession of the accused, or is eyewitness evidence from someone who directly observed criminal behavior.
- **Indirect evidence** - This evidence establishes a hypothesis in combination with other facts. It is also known as circumstantial evidence.
- **Best evidence** – This evidence could be storage devices used by an accused, or archives of files that can be proven to be unaltered.
- **Corroborating evidence** - This evidence supports an assertion that is developed from best evidence.

Evidence Collection Order

- IETF RFC 3227 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.
- The collection of digital evidence should begin with the most volatile evidence and proceed to the least volatile.
- 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.



Chain of Custody

- 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 regarding 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.

Data Integrity and Preservation

- Time stamping of files should be preserved. Hence, the original evidence should be copied, and analysis should only be conducted on copies of the original.
- The timestamps may be part of the evidence, opening files from the original media should be avoided.
- Archive and protect the original disk to keep it in its original, untampered with, condition.
- Special tools should be used to preserve forensic 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 malpractice will be preserved, and any indicators of compromise can be identified.

Attack Attribution

- 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.
- 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.
- 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 and the tools, and other techniques.
- For internal threats, asset management plays a major 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.

The MITRE ATT&CK Framework

- The MITRE Adversarial Tactics, Techniques & Common Knowledge (ATT&CK) Framework enables the ability to detect attacker's Tactics, Techniques, and Procedures (TTP) as a part of threat defense and attack attribution.
- Tactics consist of the technical goals that an attacker must accomplish to execute an attack.
- Techniques are the means by which the tactics are accomplished.
- Procedures are the specific actions taken by threat actors in the techniques that have been identified.
- The MITRE ATT&CK Framework is a global knowledge base of threat actor behavior.
- The framework is designed to enable automated information sharing by defining data structures for exchanging information between its community of users and MITRE.

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

The MITRE ATT&CK Framework (Contd.)

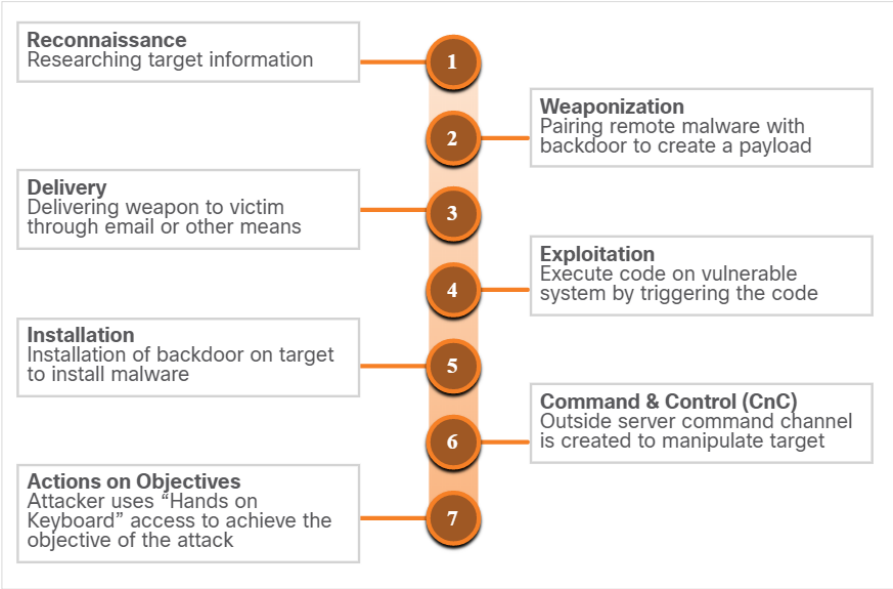
- The figure shows an analysis of a ransomware exploit from the ANY.RUN online sandbox. The columns show the enterprise attack matrix tactics, with the techniques that are used by the malware.

MITRE ATT&CK Matrix for a Ransomware Exploit

12.2 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.



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.

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

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.

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.

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

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.

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.

Actions on Objectives

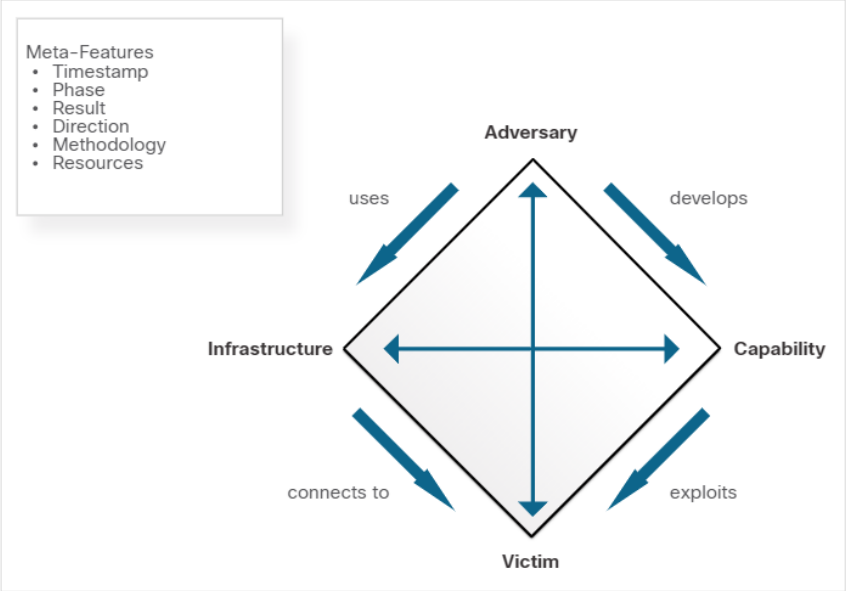
- Actions on Objectives is the final step of the Cyber Kill Chain that describes the threat actor achieving their original objective.
- At this point, the threat actor is deeply rooted in the systems of the organization, hiding their moves and covering their tracks.
- It is extremely difficult to remove 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

12.3 The Diamond Model of Intrusion Analysis

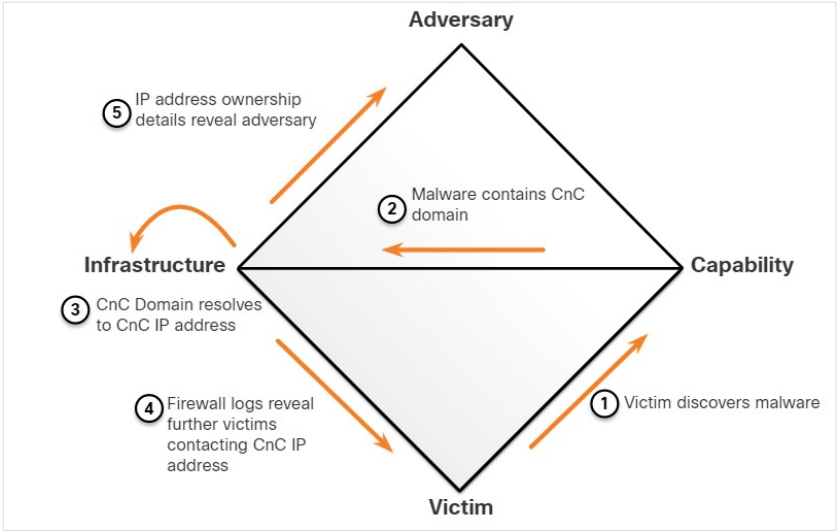
Diamond Model Overview

- 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**



Pivoting Across the Diamond Model

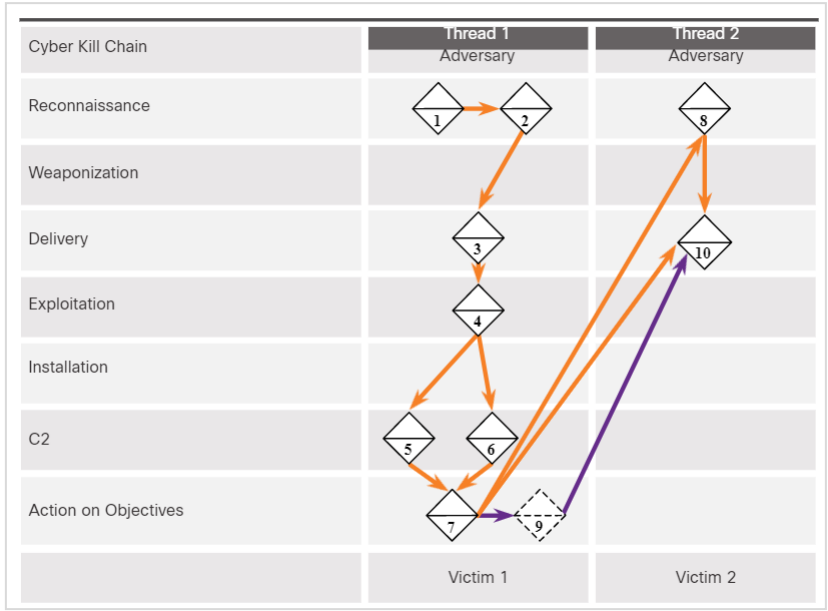
- The Diamond Model is ideal for illustrating how the adversary pivots from one event to the next. For example:
  - An employee reports that his computer is acting abnormally. A host scan by the security technician indicates that the computer is infected with malware.
  - An analysis of the malware reveals 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.



Diamond Model Characterization of an Exploit

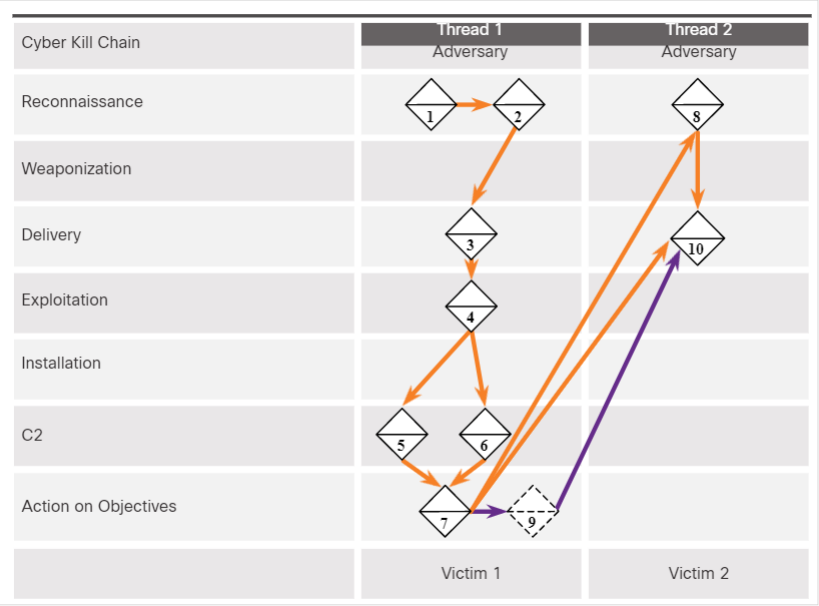
The Diamond Model and the Cyber Kill Chain (Contd.)

- 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:
  - Adversary conducts a web search for victim company Gadgets, Inc. receiving as part of the results the domain name gadgets.com.
  - 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.
  - Adversary sends phishing emails with a Trojan horse attached to the network administrators.



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

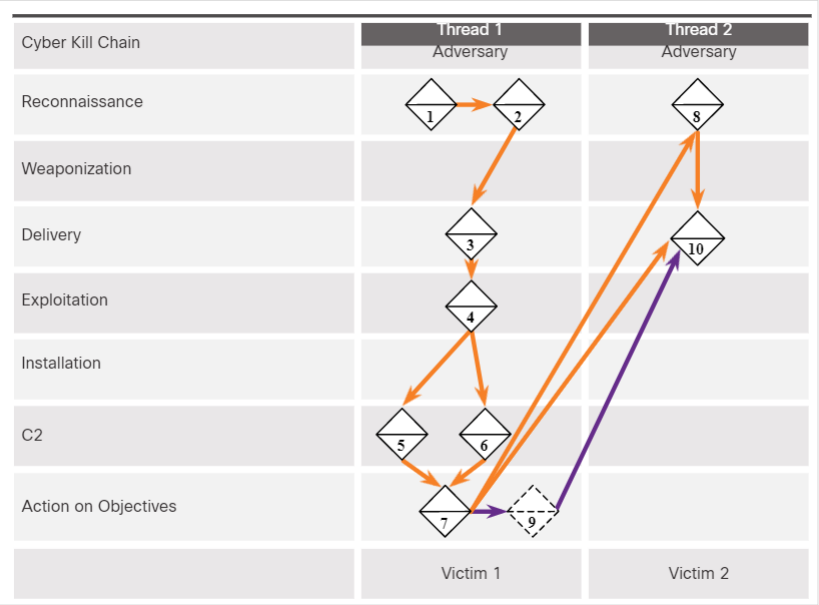
- One network administrator (NA1) opens the malicious attachment which executes the enclosed exploit.
- NA1's host registers with a CnC controller by sending an HTTP Post message and receiving an HTTP Response in return.
- It is revealed from reverse engineering that the malware has additional backup IP addresses.
- Through a CnC HTTP response message sent to NA1's host, the malware begins to act as a proxy for new TCP connections.



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

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

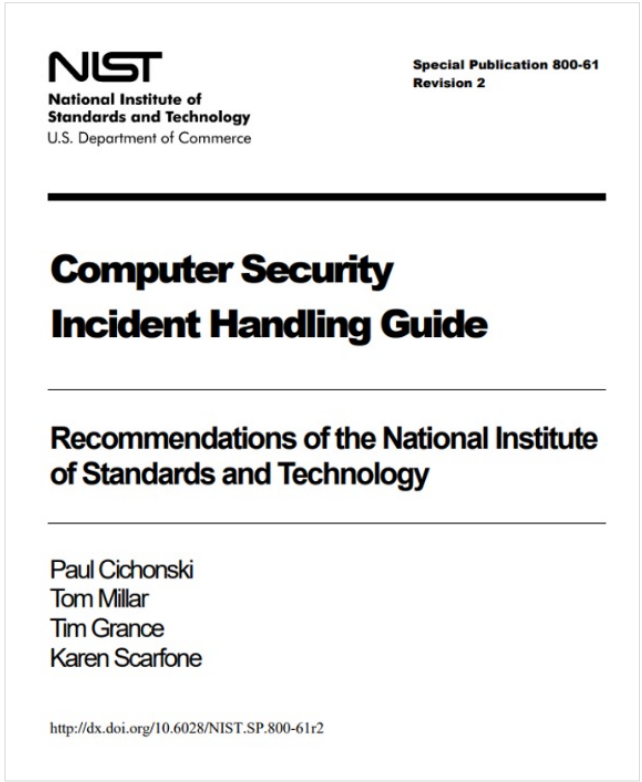


12.4 Incident Response

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.

***Note**: Although this chapter summarizes 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.*


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

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

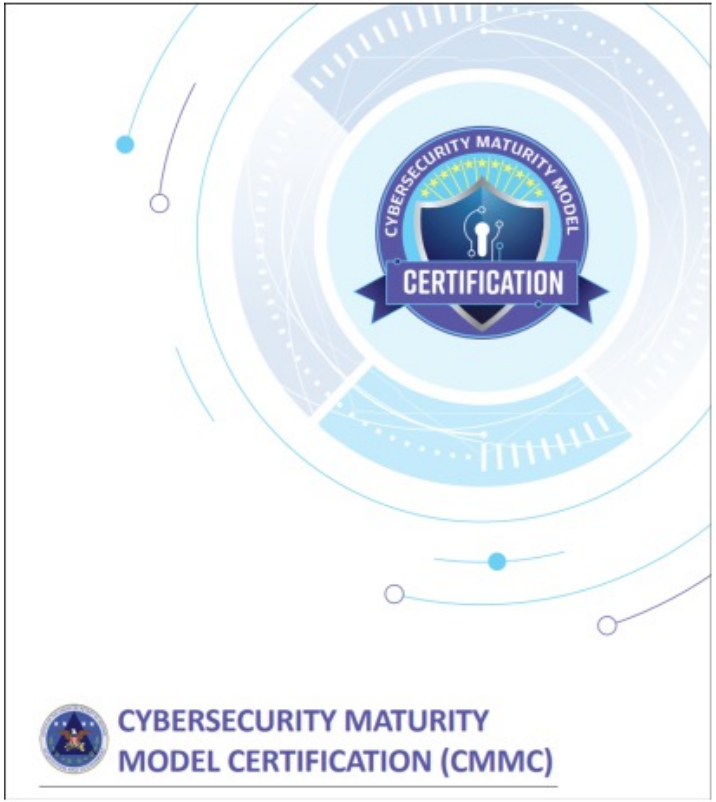
Incident Response Stakeholders

- 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 Stakeholders (Contd.)

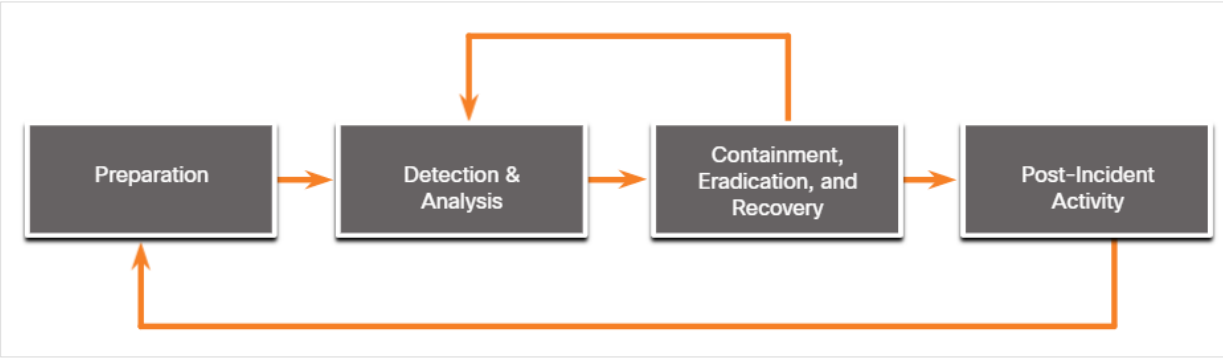
The Cybersecurity Maturity Model Certification (CMMC)

- The CMMC certifies organizations by level. For most domains, there are five levels, however for incident response, there are only four:
  - **Level 2 -** Establish an incident response plan that follows the NIST process.
  - **Level 3** - Document and report incidents to stakeholders identified in the incident response plan.
  - **Level 4 -** Use knowledge of attacker TTP to refine incident response planning and execution.
  - **Level 5 -** Utilize accepted and systematic computer forensic data gathering techniques.



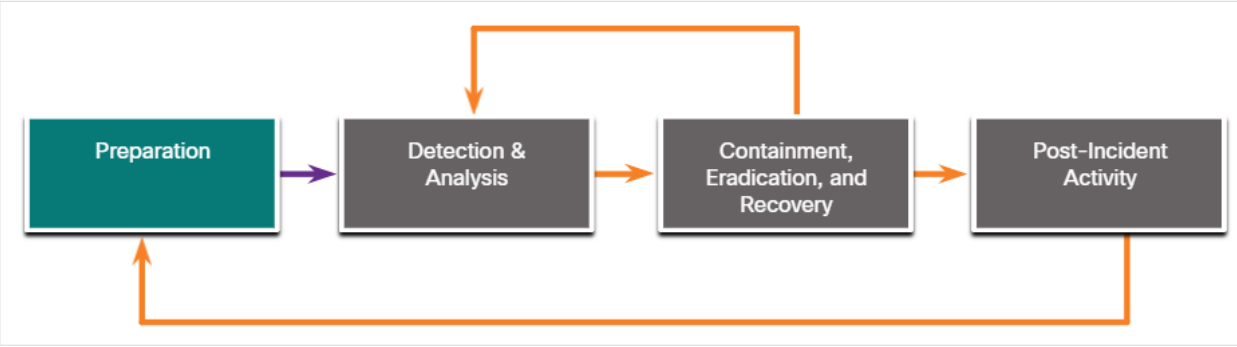
NIST Incident Response Life Cycle

- 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.



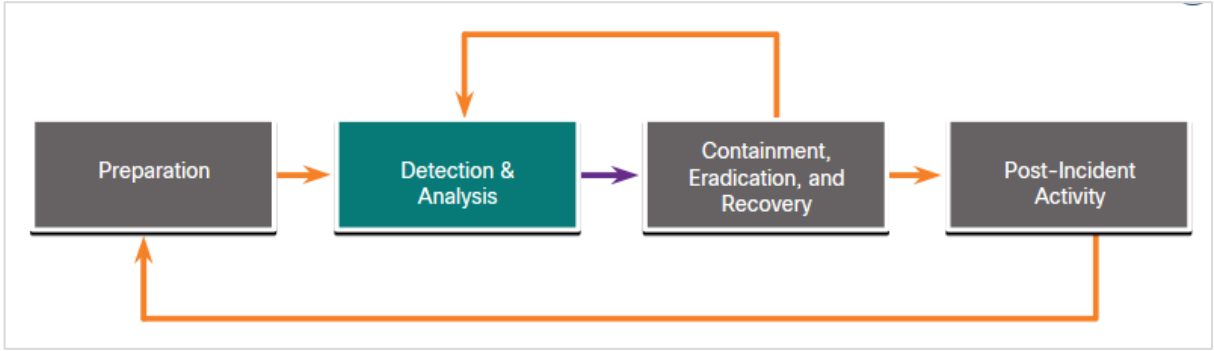
Preparation

- 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.



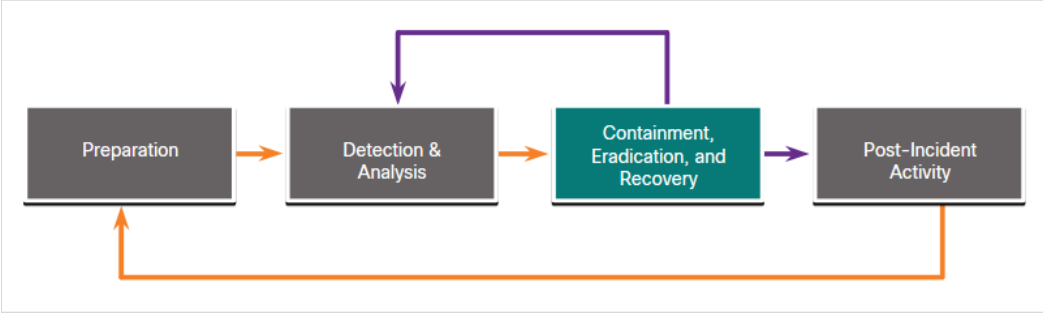
Detection and Analysis

- 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.



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.

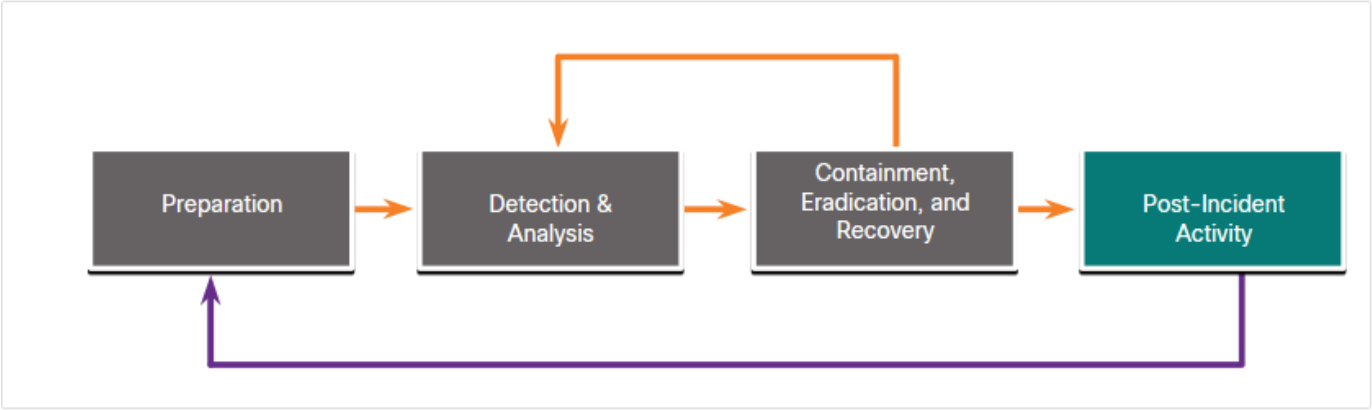


Post-Incident Activities

- 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.



Incident Data Collection and Retention

- The below table summarizes the incident data collection and retention:

Incident Data Collection	Retention

• The collected data after the lessons-learned meeting can be used to:
  • Determine the incident cost for budgeting
  • Determine the effectiveness of the CSIRT
  • Identify possible security weaknesses throughout the system
• The time of each incident provides an insight into the total amount of labor used and the total time of each phase of the incident response process.
• Only collect data that can be used to define and refine the incident handling process.
• Perform an objective assessment of each Incident.
	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.
	• **Data Type** - An organization may specify that specific types of data should be kept for a specific period of time.
	• **Cost** - If there is a lot of hardware and storage media that needs to be stored for a long time, it can become costly.

Reporting Requirements and Information Sharing

- Governmental regulations should be consulted by the legal team to determine the organization's responsibility for reporting the incident.
- Management needs to determine what additional communication is necessary with other stakeholders, such as customers, vendors, partners and so on.
- NIST recommends that an organization coordinate with organizations to share details for the incident. 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.

New Terms and Commands

- Digital Forensic
- Corroborating evidence
- Best evidence
- Chain of Custody
- Threat Attribution
- Tactics, Techniques and Procedures (TTP)
- MITRE Adversarial Tactics, Techniques & Common Knowledge (ATT&CK)
- Cyber Kill Chain
- Adversary
- Diamond Model of Intrusion Analysis
- Incident Response Capability
- Computer Security Incident Handling Guide
- Computer Security Incident Response Capability (CSIRC)
- Incident Response policy
- Incident Response Plan
- Standard Operating Procedures(SOD)
- Cyber security Maturity Model Certification(CMMC)
- Containment
- Eradication
- Precursor
- Lessons-based hardening

Lab 41 - Incident Handling

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

Lab 42 - Investigating an Attack on a Windows Host

In this lab, you will complete the following objectives:

- Investigate an attack on a Windows host.
- Use Sguil, Kibana, and Wireshark in Security Onion to investigate the attack.
- Examine exploit artifacts.