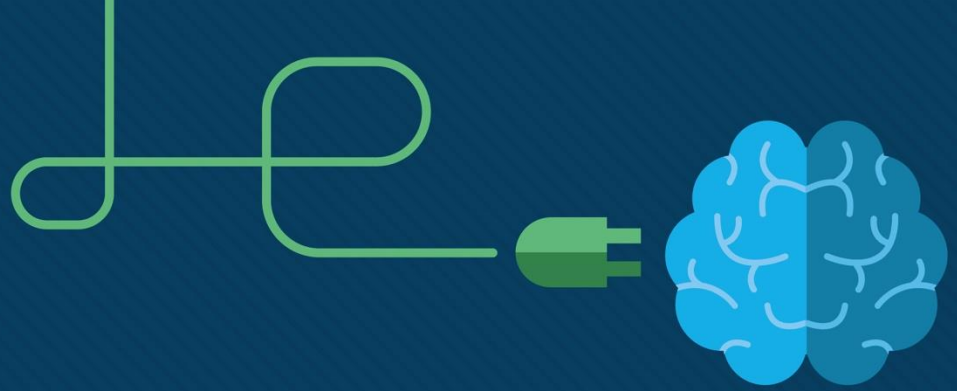


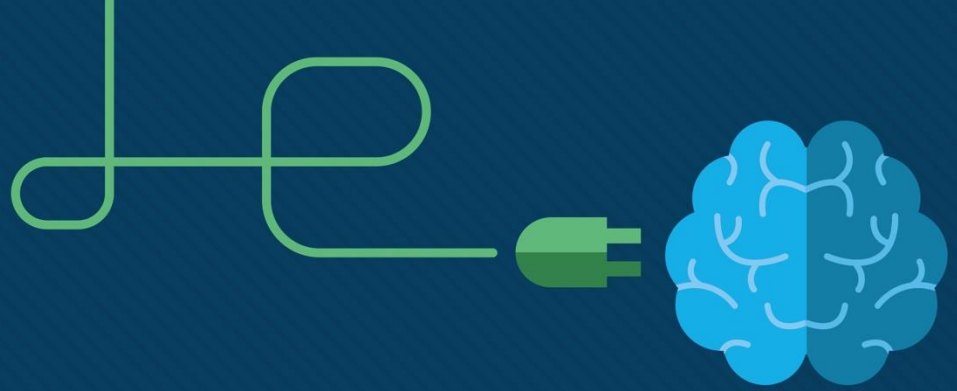
Chapter 13: Incident Response and Handling

Instructor Materials

CCNA Cybersecurity Operations v1.1

Chapter 13: Incident Response and Handling

CCNA Cybersecurity Operation v1.1
Planning Guide



Chapter 13: Incident Response and Handling

CCNA Cybersecurity Operations v1.1

Chapter 13 - Sections & Objectives

- 13.1 Incident Response Models
  - Apply incident response models to an intrusion event.
    - Identify the steps in the Cyber Kill Chain.
    - Classify an intrusion event using the Diamond Model.
    - Apply the VERIS Schema to an Incident.

- 13.2 Incident Handling
  - Apply standards specified in NIST 800-61r2 to a computer security incident.
    - Describe the goals of a given CSIRT
    - Apply the NIST 800-61r2 incident handling procedures to a given incident scenario.

13.1 Incident Response Models

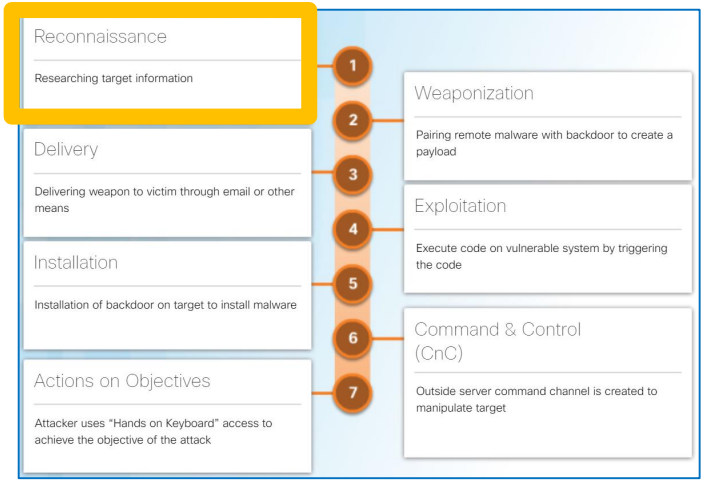
Steps of the Cyber Kill Chain®

- Developed by Lockheed Martin to identify and prevent cyber intrusions.
  - The steps of the Cyber Kill Chain help analysts understand the techniques, tools, and procedures of threat actors.
  - The threat actor gains more access to the target as they progress through the steps.
  - The goal is to stop them as early as possible to lessen the damage done.

Steps of the Cyber Kill Chain

Reconnaissance

- **Reconnaissance** is when the threat actor performs research, gathers intelligence, and selects targets.
- Organizations may provide information on websites, public-facing network devices, in news articles, conference proceedings, and social media outlets.



Adversary Tactics	SOC Defenses
Plan and conduct research: • Harvest email addresses • Identify employees on social media networks • Collect all public relations information (press releases, awards, conference attendees, etc.) • Discover Internet-facing servers	Discover Adversary's intent: • Web log alerts and historical searching data • Data mine browser analytics • Build playbooks for detecting browser behavior that indicate recon activity • Prioritize defense around technologies and people that recon activity is targeting

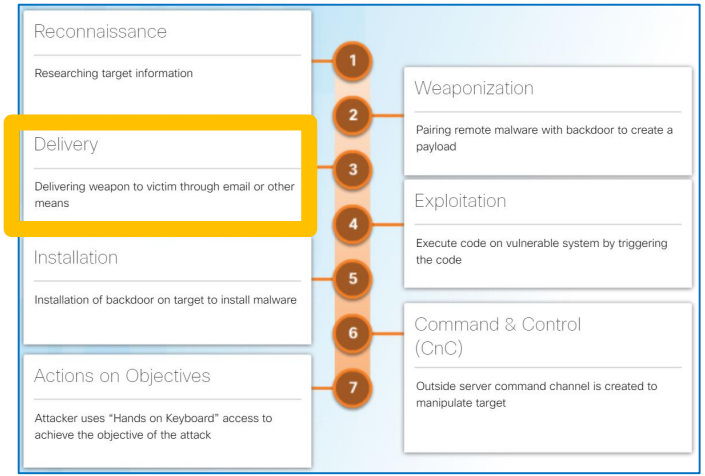
The Cyber Kill Chain
Weaponization

- **Weaponization** uses the vulnerability information gathered in the reconnaissance step to identify and develop a weapon against specific targeted systems in the organization.

Adversary Tactics	SOC Defenses
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 backdoor and command and control infrastructure.	Detect and collect weaponization artifacts: • Conduct full malware analysis. • Build detections for the behavior of known weaponizers. • Is malware old, "off the shelf" or new malware that might indicate a tailored attack? • Collect files and metadata for future analysis. • Determine which weaponizer artifacts are common to which campaigns.

The Cyber Kill Chain
Delivery

- **Delivery** is when the threat actor delivers the developed weapon using either a website, a removable USB media, or an email attachment.

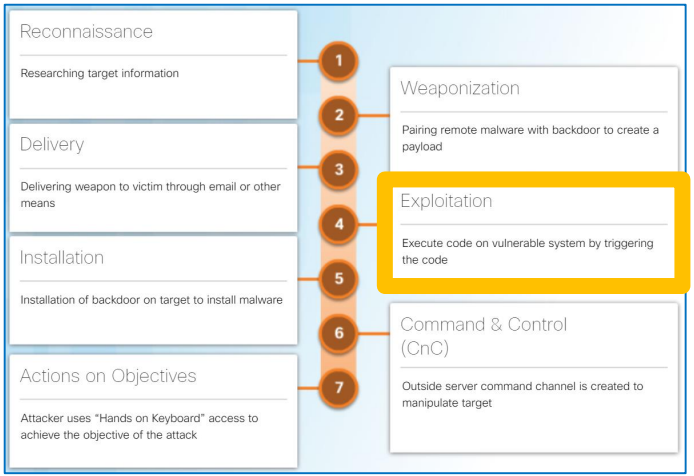


Adversary Tactics	SOC Defenses

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

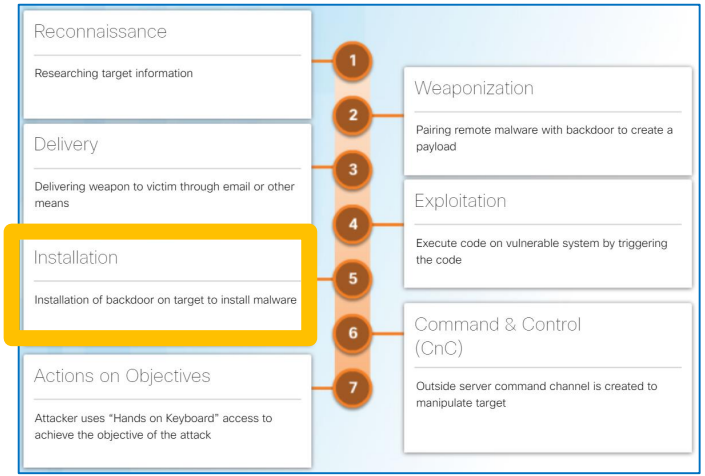
- **Exploitation** is when the threat actor triggers the weapon and executes it to compromise the vulnerability and gain control of the target.



Adversary Tactics	SOC Defenses
Exploit a vulnerability to gain access: • Use a 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 a malicious web link	Train employees, secure code, and harden devices: • Employee awareness training and 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

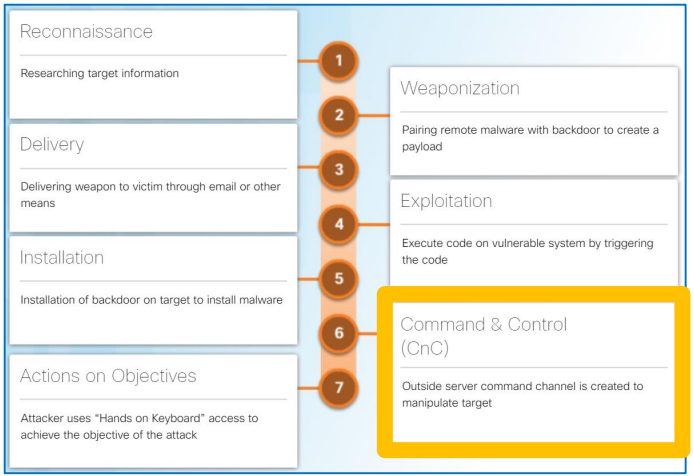
- **Installation** is when the threat actor establishes a back door into the system to allow for continued access to the target.



Adversary Tactics	SOC Defenses
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 admin privileges or only user. • Endpoint auditing to discover abnormal file creations. • Determine if malware is known threat or a new variant.

Command and Control

- **Command & Control** (CnC or C2) is when an outside server channel is used by the threat actor to manipulate a target by issuing commands to the software that they installed on the target.



Adversary Tactics	SOC Defenses
Open channel for target manipulation: • Open two way communications channel to CnC infrastructure. • Most common CnC channels are 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 thorough malware analysis. • Prevent impact by blocking or disabling CnC channel. • Consolidate the number of Internet points of presence. • Customize blocks of CnC protocols on web proxies.

Actions on Objectives

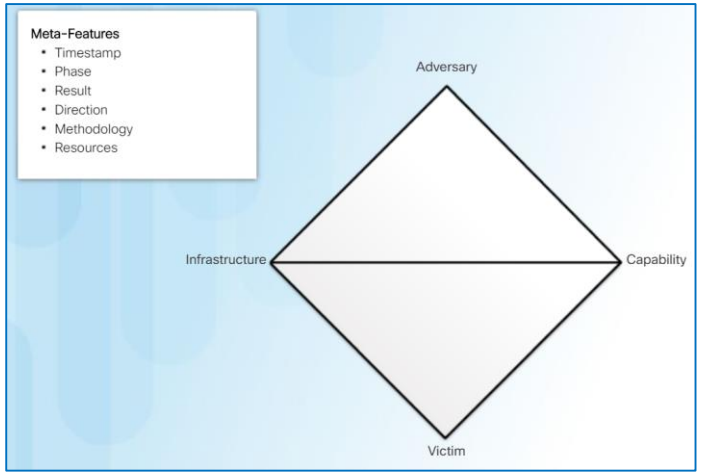
- **Actions on Objectives** is the final step of the kill chain and is when the attacker achieves attack objective.
  - Can be used for data theft, performing a DDoS attack, or using the compromised network to create and send spam.
  - Threat actor is deeply rooted in the systems of the organization and may be extremely difficult to remove from the network.

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

Diamond Model Overview

- The Diamond Model identifies four parts involved in a security incident.

Meta-features expand the model to include important elements.



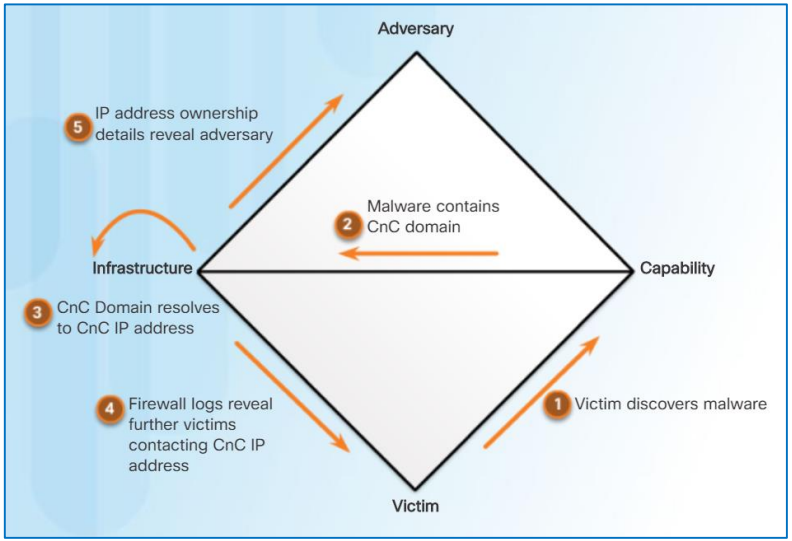
- **Adversary** – Parties responsible for the intrusion.
- **Capability** – Tool or technique used by the threat actor.
- **Infrastructure** – The network path(s) used by the threat actor to establish and maintain command and control.
- **Victim** – The target of the attack. The victim could then used as part of the infrastructure to launch other attacks.

- The ***adversary*** uses ***capabilities*** over ***infrastructure*** to attack the ***victim***.
  - Each line in the model shows how each part reached the other.

Pivoting Across the Diamond Model

- The Diamond Model is ideal for illustrating how the adversary pivots from one event to the next.

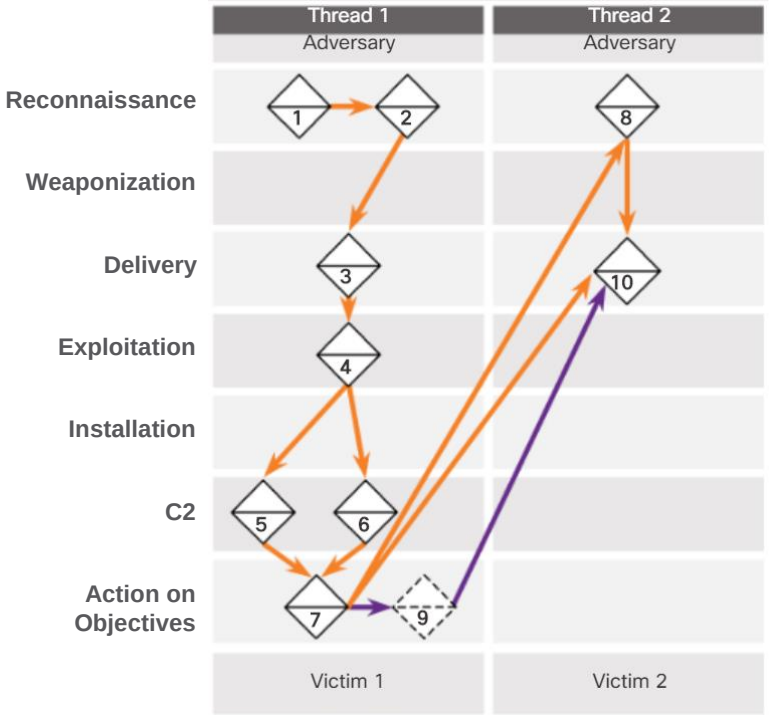
For example



1) An employee reports that his computer is acting abnormally and a scan indicates the computer is infected with malware.
2) An analysis of the malware reveals that the malware contains a list of CnC domain names.
3) These domain names resolve to a list of IP addresses.
4) These IP addresses are used to investigate logs to determine if other victims in the organization are using the CnC channel.
5) The IP addresses are also used to identify the adversary.

The Diamond Model and the Cyber Kill Chain

- The example illustrates the process used by an adversary as they traverse the Cyber Kill Chain.



1) Adversary conducts a web search for victim company Gadgets, Inc. receiving as part of the results their domain gadgets.com.

2) Adversary searches “network administrator gadget.com” and discovers the network administrators’ email addresses.

3) Adversary sends phishing emails with a Trojan horse attached to the network administrators.

4) One network administrator (NA1) opens the malicious attachment which executes the enclosed exploit.

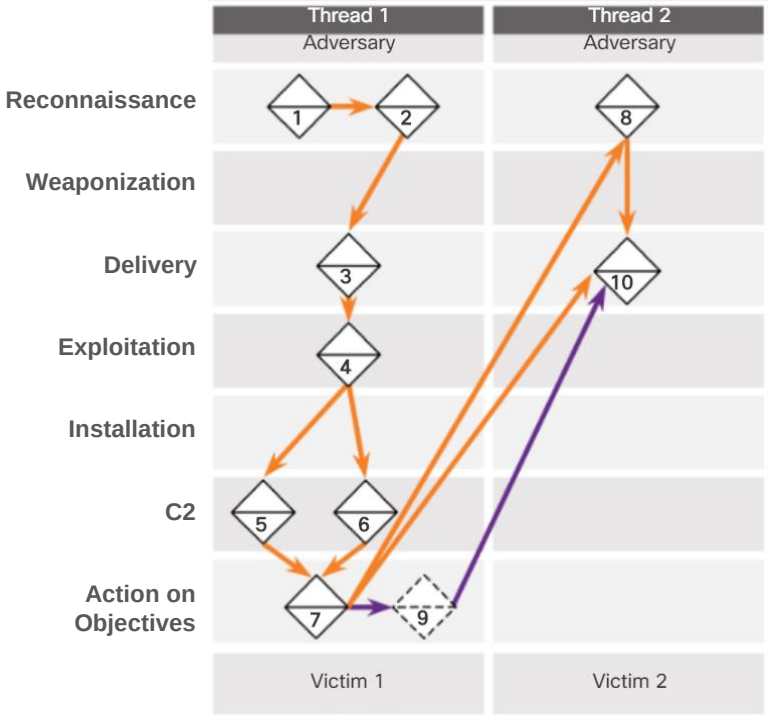
5) NA1’s host registers with a CnC controller by sending an HTTP Post message and receiving an HTTP Response in return.

6) Analysis of the malware identifies additional backup IP addresses.

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

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

- The example illustrates the process used by an adversary as they traverse the Cyber Kill Chain.



8) Through the proxy established on NA1's host, Adversary does a web search for "most important research ever" and finds Victim 2, Interesting Research Inc.

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

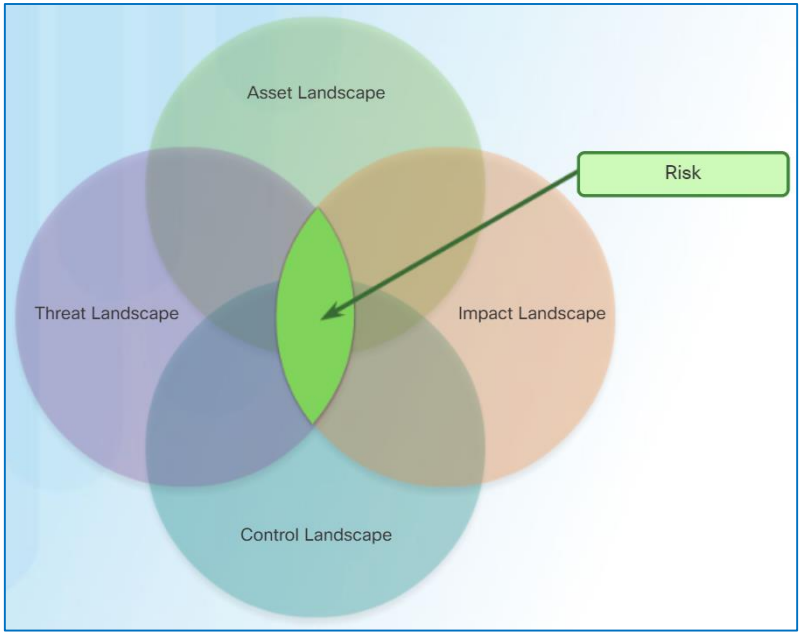
10) Chief Research Officer of Interesting Research Inc. receives a spear-phish email from Gadget Inc.'s NA1's email address sent from NA1's host with the same payload as observed in Event 3.

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

What is the VERIS Schema?

- Vocabulary for Event Recording and Incident Sharing (VERIS) schema is a set of metrics to describe security incidents in a structured way.
- In the VERIS schema, risk is defined as the intersection of four landscapes of Threat, Asset, Impact, and Control.
- Information from each landscape helps to understand the level of risk to the organization.
- VERIS helps to determine these landscapes using real security incidents to help risk management assessment.

VERIS schema



Create a VERIS Record

- When creating records to add to the database, start with the basic facts about the incident and use the VERIS elements outlined by the community.
  - The only required fields in the record are those where the attribute is present.
  - As more is known about the incident, data can be added.

Variable	Value
timeline.incident.year	2017
schema_version	1.3
incident_id	1
security_incident	Confirmed
discovery_method	Unknown
action	Unknown
asset	Unknown
actor	Unknown
attribute	Unknown

- Additional information can be recorded by adding VERIS labels to the existing record.

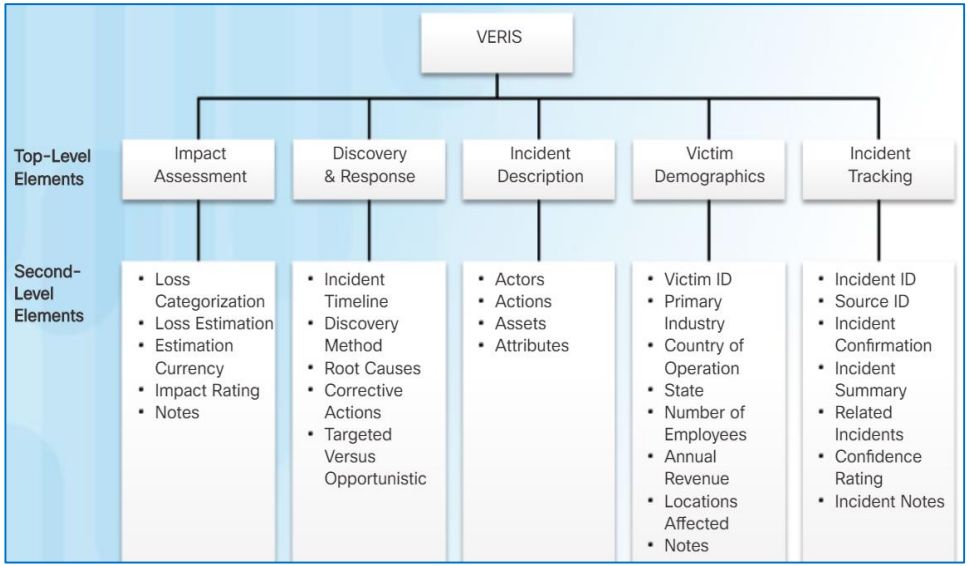
timeline.incident.year	2017
timeline.incident.month	06
timeline.incident.day	20

summary	Computer was infected with malware

discovery.notes	Reported by Debbie in sales
malware.notes	rootkit was found on Debbie's computer
social.notes	Debbie brought in an infected USB drive and used it on her company laptop

Top-Level and Second-Level Elements

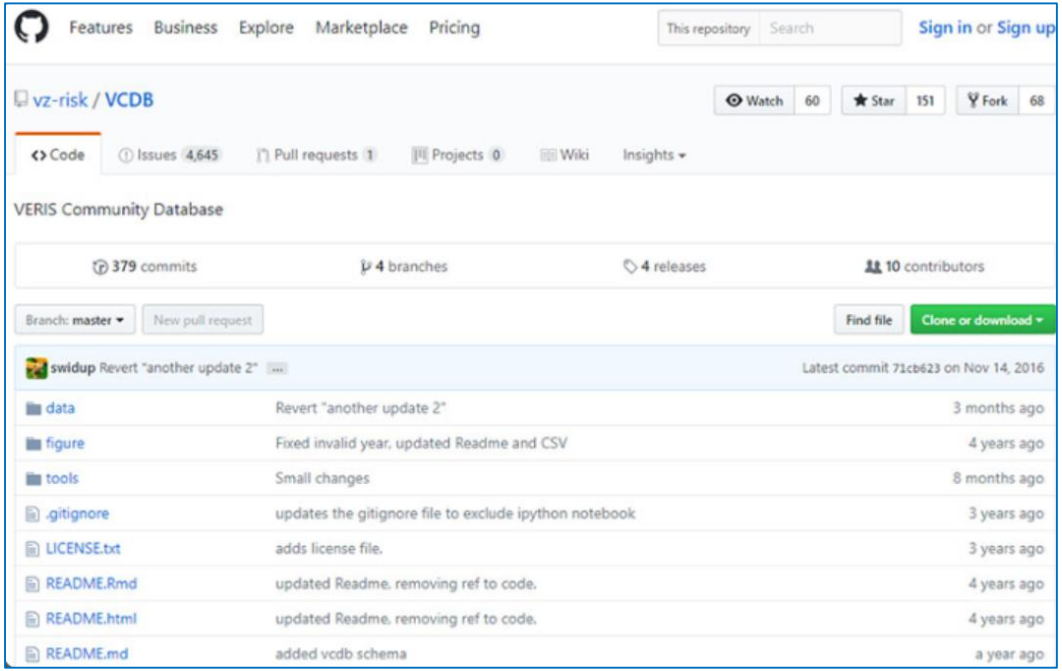
- The VERIS Schema identifies five top-level elements, providing a different aspect of the incident.
  - Each top-level element contains several second-level elements for classifying collected incident data.



- **Impact Assessment –** All incidents have an impact, whether it is minor or widespread, which can only be determined after an incident has occurred.
- **Discovery and Response –** Identifies the timeline of events, the method of incident discovery, and what the response was to the incident, including how it was remediated.
- **Incident Description** - Describes an incident completely, using the A4 threat model developed by Verizon.
- **Victim Demographics –** Describes the organization that has experienced the incident and its characteristics.
- **Incident Tracking** – Records general information about the incident so organizations can identify, store, and retrieve incidents over time.

The VERIS Community Database

- The VERIS Community Database (VCDB) is a very useful shared database for organizations willing to participate.
  - Organizations can submit security incident details to the VCDB for the community to use.
  - The larger and more robust the VCDB becomes, the more useful it will be in prevention, detection, and remediation of security incidents.
  - It will also become a very useful tool for risk management, saving organizations data, time, effort, and money.



13.2 Incident Handling

CSIRT Overview

- A Computer Security Incident Response Team (CSIRT) is a group commonly found within an organization that provides services and functions to secure the assets of that organization.

- A CSIRT:
  - Responds to incidents that have already happened.
  - Provides proactive services and functions such as penetration testing, intrusion detection, or even security awareness training.

Types of CSIRTs

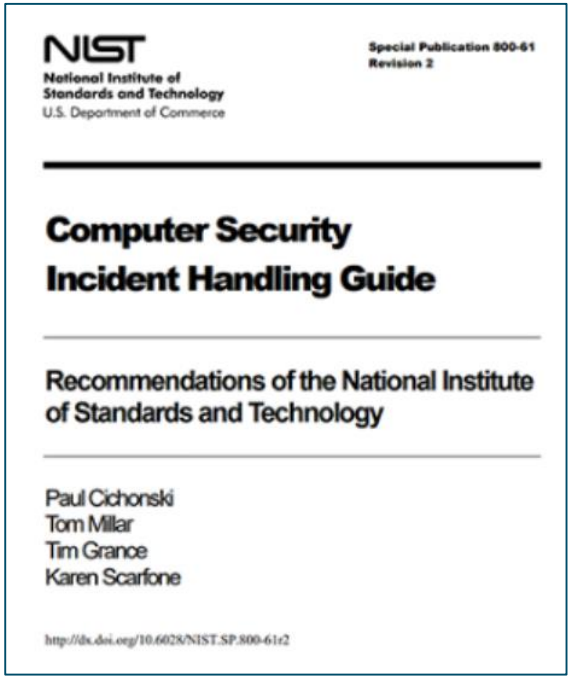
- There are many different types of CSIRTs and related organizations:
  - **Internal** – used in banks, hospitals, universities, etc.
  - **National** – handles incidents for a country
  - **Coordination center** – incident handling across multiple CSIRTs
  - **Analysis centers** – data from many sources to identify trends
  - **Vendor teams** – remediation for vulnerabilities in hardware/software
  - **Managed security service providers** – a fee-based service

CERT

- Computer Emergency Response Team (CERT) is a trademarked acronym owned by Carnegie Mellon University.
- A CERT provides security awareness, best practices, and security vulnerability information, but does not respond to security incidents.
- Other countries have asked for permission to use the CERT acronym.

Establishing an Incident Response Capability

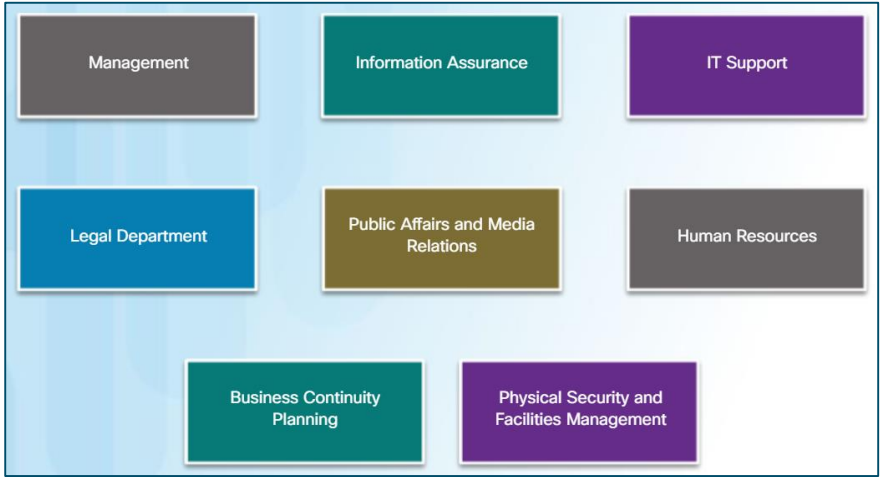
- The NIST “Computer Security Incident Handling Guide” Special Publication 800-61, revision 2 (800-61r2) provides guidelines for:
  - Incident handling
  - Analyzing incident-related data
  - Determining the appropriate response to each incident



- NIST recommends establishing a computer security incident response capability (CSIRC) and creating:
  - **Incident Response Policies**
  - **Incident Response Plans**
  - **Incident Response Procedures**

Incident Response Stakeholders

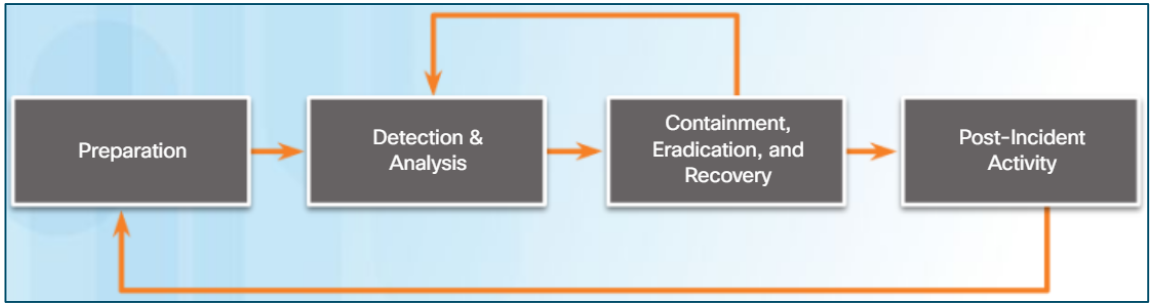
- The following groups and individuals may also be involved with incident handling.



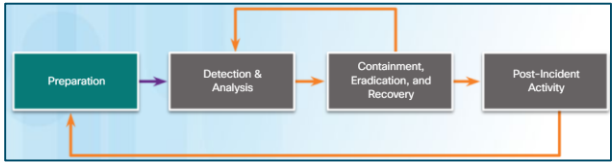
- It is important to ensure their cooperation before an incident is underway as their expertise and abilities can help the CSIRT to handle the incident quickly and correctly.

NIST Incident Response Life Cycle

- NIST defines the following 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** – 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.
  - **Post-Incident Activities** – The CSIRT then documents how the incident was handled, recommends changes for future response, and specifies how to avoid a reoccurrence.



Preparation

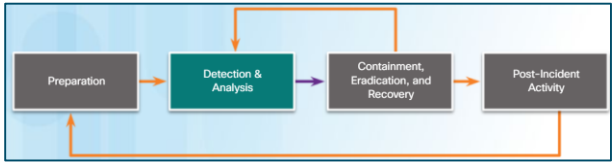


- The preparation phase is when the CSIRT is:
  - Created and trained
  - Tools and assets that will be needed to investigate incidents are acquired and deployed.

- The following are examples of actions that also take place during the preparation phase:
  - Organizational processes are created to address communication between people on the response team.
  - Facilities to host the response team and the SOC are created.
  - Necessary hardware and software for incident analysis and mitigation is acquired.
  - Risk assessments are used to implement controls that will limit the number of incidents.
  - Validation of security hardware and software deployment is performed on devices.
  - User security awareness training materials are developed.

NIST 800-61r2

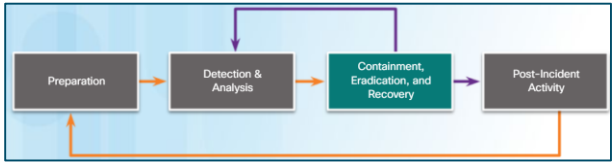
Detection and Analysis



- Different types of incidents will require different responses and organizations need to be prepared for incidents from various attack vectors including the Web, Email, loss or theft, impersonation, attrition, or media.
- Some incidents are easy to detect while others may go undetected for months.
  - There are automated ways of detection such as antivirus software or an IDS.
  - There are also manual detections through user reports.
  - There are two categories for the signs of an incident; precursor and indicator.
- Incident analysis is difficult because not all of the indicators are accurate and the CSIRT must react quickly to validate and analyze incidents.
- Incident notification is when an incident is analyzed and prioritized, the incident response team needs to notify the appropriate individuals so that all who need to be involved will play their roles.

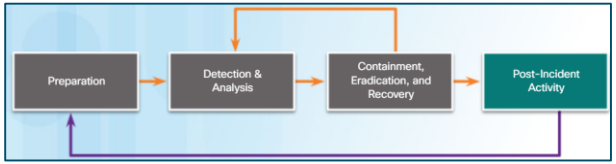
NIST 800-61r2

Containment, Eradication, and Recovery



- Containment ensures the incident does not continue.
  - Different types of incidents will require different strategies.
  - For every type of incident, a containment strategy should be created and enforced.
  - During an incident, evidence must be gathered and documented in a clear and concise manner for subsequent investigation by authorities.
- Eradication is identifying all of the hosts that need remediation and all of the effects of the security incident must be eliminated.
  - Exploited vulnerabilities must be corrected or patched so that the incident does not occur again.
- Recovery of hosts requires clean and recent backups, or they will have to be rebuilt with installation media.

Post-Incident Activity Phase



- It is important to perform a post-mortem and periodically meet with all of the parties involved to discuss the events that took place and the actions of all of the individuals while handling the incident.
- After a major incident has been handled, 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

- In the ‘lessons learned’ meetings, the collected data can be used to:
  - Determine the cost of an incident for budgeting reasons.
  - Determine the effectiveness of the CSIRT.
  - Identify possible security weaknesses throughout the system.
- NIST Special Publication 800-61 provides examples of performing an objective assessment of an incident.
- There should be an evidence retention policy that outlines how long evidence of an incident should be retained.
  - Evidence is often retained for many months or many years after an incident has taken place.
  - Reasons affecting evidence retention include prosecution, the type of data, and the cost of storage.

Reporting Requirements and Information Sharing

- An organization may have reporting requirements.
  - There could be governmental regulations which the organization must adhere to.
  - Management may also have to report to stakeholders, customers, vendors, partners, etc.
- NIST recommends organizations share incident information with VERIS, however:
  - 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

Networking Academy

Lab – Incident Handling

Objectives

Apply your knowledge of security incident handling procedures to formulate questions about given incident scenarios.

Background / Scenario

Computer security incident response has become a vital part of any organization. The process for handling a security incident can be complicated and involve many different groups. An organization must have standards for responding to incidents in the form of policies, procedures, and checklists. To properly respond to a security incident, the security analyst must be trained to understand what to do, and must also follow all of the guidelines outlined by the organization. There are many resources available to help organizations create and maintain a computer incident response handling policy, but the NIST Special Publication 800-61 is specifically called by the CCNA CyberOps SECOPS exam topics. This publication can be found here:

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Scenario 1: Worm and Distributed Denial of Service (DDoS) Agent Infestation

Study the following scenario and discuss and determine the incident response handling questions that should be asked at each stage of the incident response process. Consider the details of the organization and the CSIRC when formulating your questions.

13.3 Chapter Summary

Summary

- The Cyber Kill Chain outlines the steps an attacker must complete to accomplish their goal. These steps are reconnaissance, weaponization, delivery, exploitation, installation, command & control.
- The Diamond Model of intrusion is used to diagram a series of intrusion events. It is ideal for showing how the adversary pivots from one event to the next.
- The Diamond Model has 4 parts used to represent a security incident or event: adversary, capability, infrastructure, and victim.
- VERIS can be used to submit security incident details to the VCDB for community use.
- The VERIS schema top level elements include impact assessment, discovery & response, incident description, victim demographics, and incident tracking.

Summary (Cont.)

- A CSIRT is a group that provides services and functions in response to security incidents.
- Types of CSIRTs include internal, national, coordination centers, analysis centers, vendor teams, and managed security service providers.
- CERT is a trademarked acronym owned by Carnegie Mellon University, but used with permission by other countries. A CERT provides security awareness, best practices, and security vulnerability information; a CERT does not respond to security incidents.
- The NIST 800-61r2 standard provides guidelines for incident handling. The phases of an incident response process life cycle are preparation; detection and analysis; containment, eradication, and recovery; and post-incident activities.

New Terms and Commands

- command and control (CnC or C2)
- Computer Emergency Response Team (CERT)
- Computer Security Incident Response Team (CSIRT)
- Cyber Kill Chain
- Diamond Model
- NIST 800-61r2
- Vocabulary for Event Recording and Incident Sharing (VERIS)
- weaponization

Cybersecurity Operations Certification

This chapter covers the following areas in the Cybersecurity Operations Certification:

From 210-250 SECOPS – Implementing Cybersecurity Security Operations:

- **Domain 3: Incidence Response**
  - 3.1 Describe the elements that should be included in an incident response plan as stated in NIST.SP800-61 r2
  - 3.2 Map elements to the following steps of analysis based on the NIST-SP800-61R2:
    - Preparation
    - Detection & Analysis
    - Containment, Eradication, & Recovery
    - Post-incident analysis (lessons learned)

Cybersecurity Operations Certification (Cont.)

This chapter covers the following areas in the Cybersecurity Operations Certification:

From 210-250 SECOPS – Implementing Cybersecurity Security Operations:

- **Domain 3: Incidence Response**
  - 3.3 Map the organization stakeholders against the NIST IR categories (C2M2 page 2, NIST.SP800-61r2 p.21-p.41):
    - Preparation
    - Detection & Analysis
    - Containment, Eradication, & Recovery
    - Post-incident analysis (lessons learned)

Cybersecurity Operations Certification (Cont.)

This chapter covers the following areas in the Cybersecurity Operations Certification:

From 210-250 SECOPS – Implementing Cybersecurity Security Operations:

- **Domain 3: Incidence Response**
  - 3.4 Describe the goals of the given CSIRT
    - Internal CSIRT
    - National CSIRT
    - Coordination Centers
    - Analysis Centers
    - Vendor Teams
    - Incident Response Providers (MSSP)

Cybersecurity Operations Certification (Cont.)

This chapter covers the following areas in the Cybersecurity Operations Certification:

From 210-250 SECOPS – Implementing Cybersecurity Security Operations:

- **Domain 5: Incidence Handling**
  - 5.1 Classify intrusion events into the following categories as defined in the Diamond Model of Intrusion:
    - Reconnaissance
    - Weaponization
    - Delivery
    - Exploitation
    - Installation
    - Command and Control
    - Action on Objectives

Cybersecurity Operations Certification (Cont.)

This chapter covers the following areas in the Cybersecurity Operations Certification:

From 210-250 SECOPS – Implementing Cybersecurity Security Operations:

- **Domain 5: Incidence Handling**
  - 5.2 Apply the NIST.SP800-61 r2 incident handling process to an event
  - 5.3 Define the following activities as they relate to incident handling:
    - Identification
    - Scoping
    - Containment
    - Remediation
    - Lessons based hardening
    - Reporting

Cybersecurity Operations Certification (Cont.)

This chapter covers the following areas in the Cybersecurity Operations Certification:

From 210-250 SECOPS – Implementing Cybersecurity Security Operations:

- **Domain 5: Incidence Handling**
  - 5.4 Describe the following concepts as they are documented in NIST SP800-86:
    - Evidence collection order
    - Data integrity
    - Data preservation
    - Volatile data collection
  - 5.5 Apply the VERIS schema categories to a given incident


CISCO