CCNA Cyber Ops (Version 1.1) – Chapter 13: Incident Response and Handling

itexamanswers.net/ccna-cyber-ops-version-1-1-chapter-13-incident-response-and-handling.html

June 19, 2019

Contents

Objectives

Upon completion of this chapter, you will be able to answer the following questions:

- What are the steps in the Cyber Kill Chain?
- How do you classify an intrusion event using the Diamond Model?
- How do you apply the VERIS schema to an incident?
- What are the various goals of a given CSIRT?
- How do you apply the NIST 800-61r2 incident handling procedures to a given incident scenario?

Key Terms

This chapter uses the following key terms. You can find the definitions in the Glossary.

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

Introduction (13.0)

In cybersecurity, threat actors are always developing new techniques. New threats constantly emerge that must be detected and contained so that assets and communication are restored as quickly as possible. Many attackers use extortion, fraud, and identity theft for financial gain. The need to consistently defend against these attacks led to the creation of several incident response models.

This chapter covers incident response and handling models and procedures. These include the Cyber Kill Chain, the Diamond Model, the VERIS schema, and NIST guidelines for the structure of Computer Security Incident Response Teams (CSIRTs) and processes for handling an incident.

Incident Response Models (13.1)

In this section, you will learn how to apply incident response models to an intrusion event.

The Cyber Kill Chain (13.1.1)

In this topic, you will learn to identify the steps in the Cyber Kill Chain.

Steps of the Cyber Kill Chain (13.1.1.1)

The Cyber Kill Chain was developed by Lockheed Martin to identify and prevent cyber intrusions. As Figure 13-1 shows, there are seven steps to the Cyber Kill Chain, which help analysts understand the techniques, tools, and procedures of threat actors.

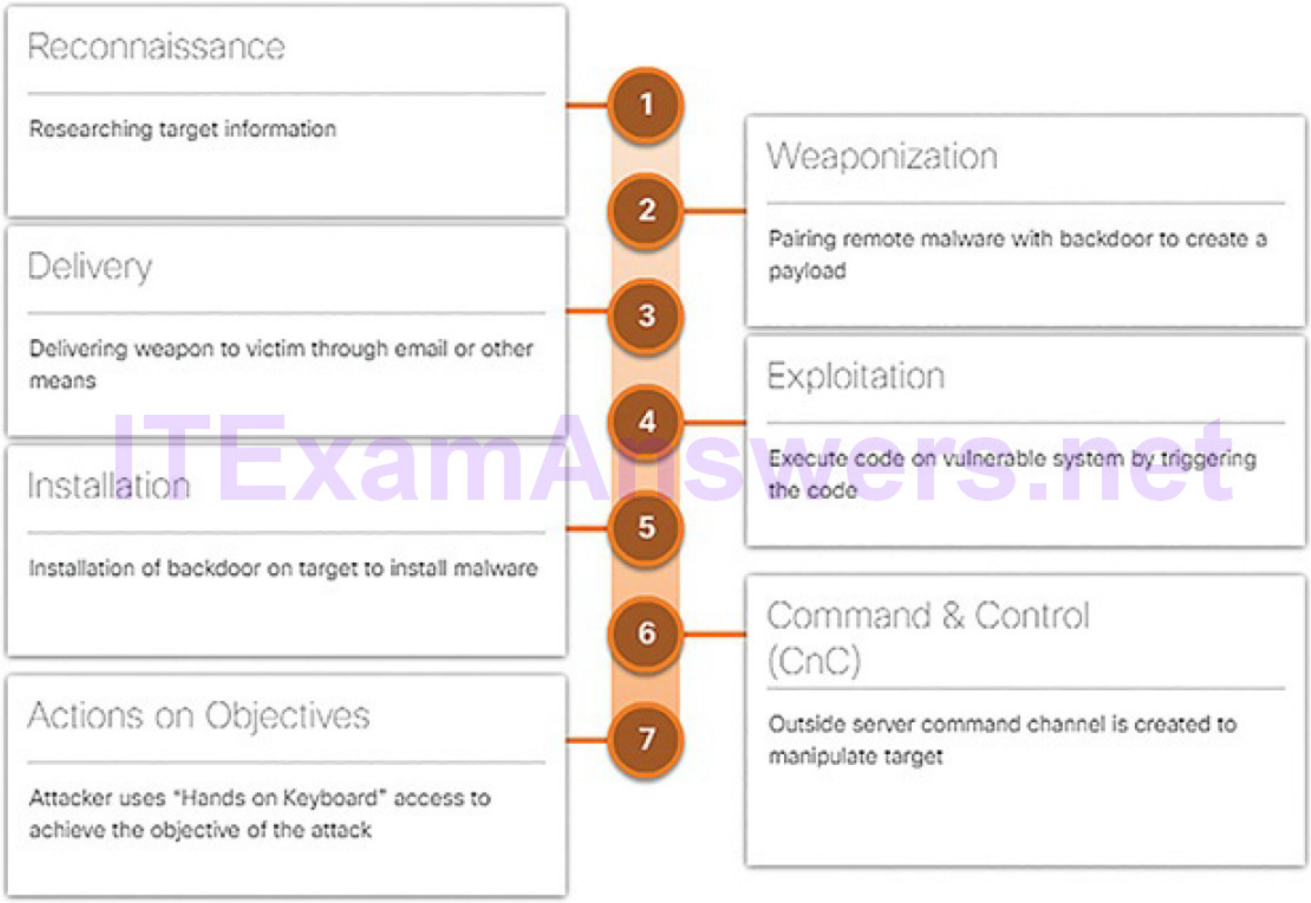

Reconnaissance
Researching target information
1
Weaponization
Pairing remote malware with backdoor to create a payload
2
Delivery
Delivering weapon to victim through email or other means
3
Exploitation
Execute code on vulnerable system by triggering the code
4
Installation
Installation of backdoor on target to install malware
5
Command & Control (CnC)
Outside server command channel is created to manipulate target
6
Actions on Objectives
Attacker uses "Hands on Keyboard" access to achieve the objective of the attack
7

Figure 13-1 The Cyber Kill Chain

When responding to an 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 specifies what an attacker must complete to accomplish their goal. The steps in the Cyber Kill Chain are as follows:

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command & Control (CnC)
7. Action on Objectives

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 reach Step 7.

Note
Threat actor is the term used throughout this course to refer to the party instigating the attack. However, Lockheed Martin uses the term "adversary" in its description of the Cyber Kill Chain. The two terms, adversary and threat actor, are used interchangeably in this topic.

Reconnaissance (13.1.1.2)

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 attack could be performed, where it could be performed, and how it could 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.

Table 13-1 outlines some of the tactics and defenses used during this step.

Table 13-1 Examples of Reconnaissance Tactics and Defenses

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, conferences attendees, etc.). • Discover Internet-facing servers.	Discover adversary’s intent: • Investigate web log alerts and historical searching data. • Data mine browser analytics. • Build playbooks for detecting browser behavior that indicates recon activity. • Prioritize defense around technologies and people thatrecon activity is targeting.

Weaponization (13.1.1.3)

The goal of weaponization is to use the information from the earlier reconnaissance to develop a weapon against specific targeted systems 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.

It is not difficult to choose a weapon for the attack. The threat actor needs to look at what attacks are available for the vulnerabilities they have discovered. There are many attacks that have already been created and tested at large. One problem is that because these attacks are so well known, they are most likely also known by the defenders. It is often more effective to use a zero-day attack to avoid detection methods. The threat actor may wish to develop their own weapon that is specifically designed to avoid detection, using the information about the network and systems that they have learned.

Table 13-2 summarizes some of the tactics and defenses used during this step.

Table 13-2 Examples of Weaponization Tactics and Defenses

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. • Determine whether malware is old, “off the shelf,” or new malware that might indicate a tailored attack. • Collect files and metadata for futureanalysis. • Determine which weaponizer artifacts are common to which APT campaigns.

Delivery (13.1.1.4)

During this step, the weapon is transmitted to the target using a delivery vector. This may be through the use of 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 will 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.

Table 13-3 summarizes some of the tactics and defenses used during this step.

Table 13-3 Examples of Delivery Tactics and Defenses

Adversary Tactics	SOC Defenses
Launch malware at target: Directly 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 (13.1.1.5

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 very 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.

Table 13-4 summarizes some of the tactics and defenses used during this step.

Table 13-4 Examples of Exploitation Tactics and Defenses

Adversary Tactics	SOC Defenses
Initiate zero-day exploit: Directly against web servers Indirect delivery through: • Malicious email • Malware on USB stick • Social media interactions • Compromised websites	Train employees, secure code, and harden devices: • Conduct employee awareness training and email testing. • Conduct web developer training for securing code. • Perform regular vulnerability scanning and penetration testing. • Implement endpoint hardening measures. • Perform endpoint auditing to forensically determine origin of exploit.

Installation (13.1.1.6)

This step is where the threat actor establishes a backdoor 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. Theaccess 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.

Table 13-5 summarizes some of the tactics and defenses used during this step.

Table 13-5 Examples of Installation Tactics and Defenses

Adversary Tactics	SOC Defenses

Install persistent backdoor: • Install web shell on web server for persistent access. • Create point of persistence by adding services, AutoRun keys, etc. • Modify the timestamp of the malware to make it appear as part of the operating system.	Detect, log, and analyze installation activity: • Use a HIPS to alert or block on common installation paths. • Determine if malware requires admin privileges or only user privileges. • Perform endpoint auditing to discover abnormal file creations. • Determine if malware is a known threat or a new variant.

Command and Control (13.1.1.7)

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 in order 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 in order to discover the compromised host. This may be in the form of unauthorized Internet Relay Chat (IRC) traffic or excessive traffic to suspect domains.

Table 13-6 summarizes some of the tactics and defenses used during this step.

Table 13-6 Examples of Command & Control (CnC) Tactics and Defenses

Adversary Tactics	SOC Defenses
Open two-way communications channel to CnC infrastructure for target manipulation: • 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 number of Internet points of presence. • Customize blocks of CnC protocols on web proxies.

Actions on Objectives (13.1.1.8)

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. 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.

Table 13-7 summarizes some of the tactics and defenses used during this step.

Table 13-7 Examples of Actions on Objectives Tactics and Defenses

Adversary Tactics	SOC Defenses
Reap the rewards of successful attack: • Collect user credentials. • Escalate privileges. • Conduct internal reconnaissance. • Move laterally 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. • Ensure immediate analyst response of all alerts. • Conduct forensic analysis of endpoints for rapid triage. • Capture network packets to re-create activity. • Conduct damage assessment.

Activity 13.1.1.9: Identify the Kill Chain Step Refer to the online course to complete this Activity.

The Diamond Model of Intrusion (13.1.2)

In this topic, you will learn to classify an intrusion event using the Diamond Model.

Diamond Model Overview (13.1.2.1)

The Diamond Model was developed by Sergio Caltagirone, Andrew Pendergast, and Christopher Betz from the Center for Cyber Threat Intelligence and Threat Research. The Diamond Model is made up of four parts and represents a security incident or event, as shown Figure 13-2.

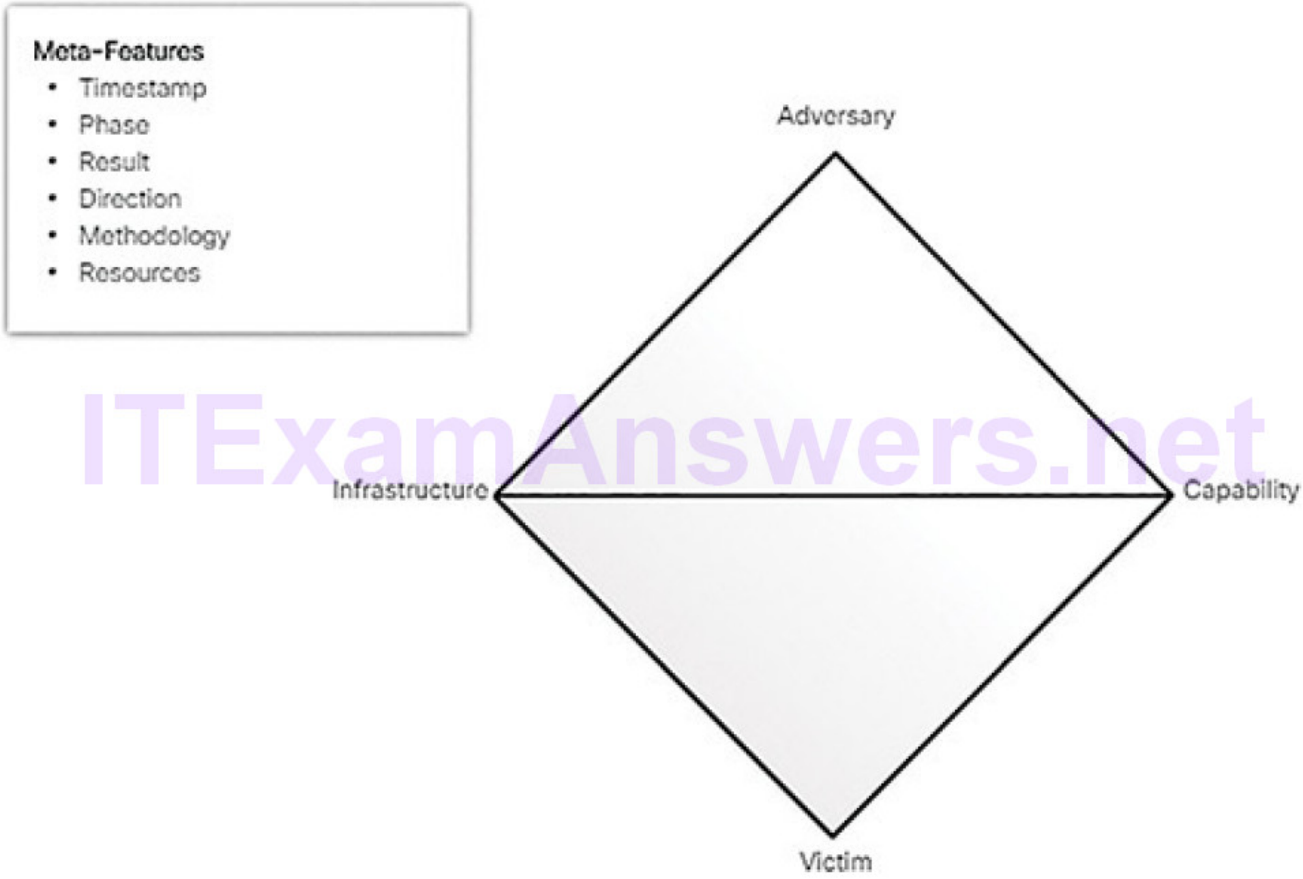


Figure 13-2 The Diamond Model

In the Diamond Model, an event is a time-bound activity restricted to a specific step where an adversary uses a capability over some infrastructure against a victim to achieve a specific result.

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

Adversary: This is the party 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 adversary uses 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.

The adversary uses capabilities over infrastructure to attack the victim. Each line in the model shows how each part reached the other. For example, a capability like malware might be used over email by an adversary to attack a victim.

Meta-features expand the model slightly to include the following importantelements:

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.

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.

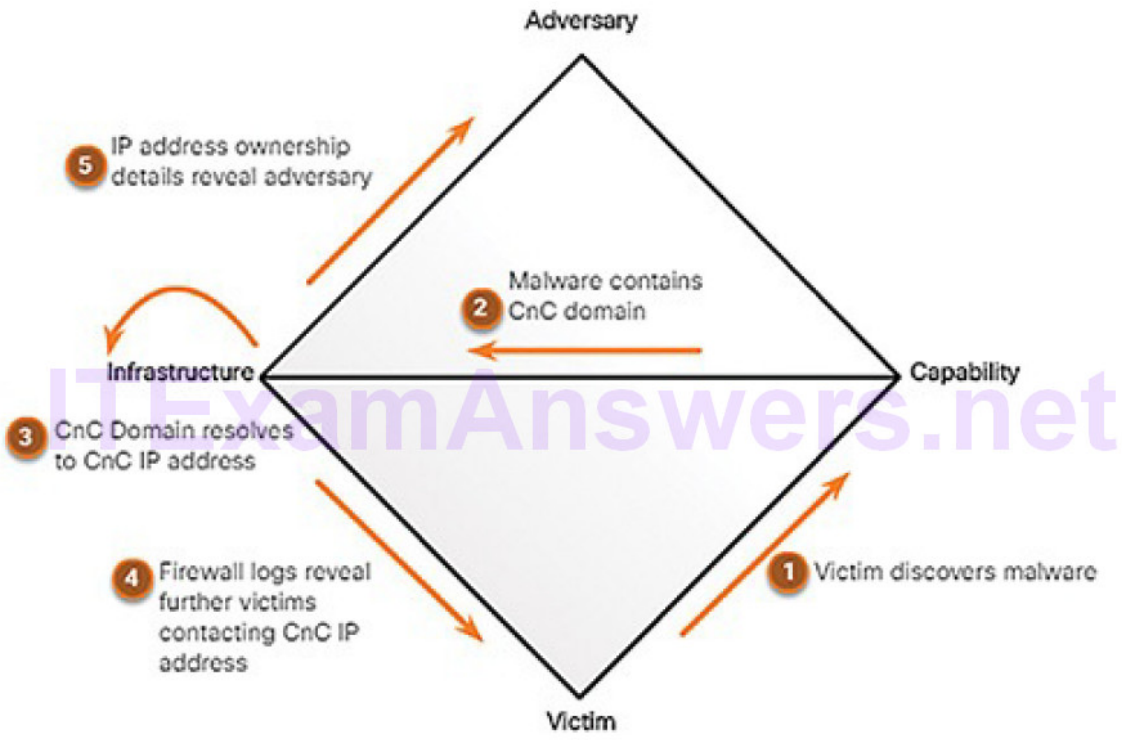
Methodology: This is used to classify the general type of event, such as port scan, phishing, content delivery attack, syn flood, etc.

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).

Pivoting Across the Diamond Model (13.1.2.2)

As a cybersecurity analyst, you may be called on to use the Diamond Model 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 Figure 13-3 an employee reports that his computer is acting abnormally.


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

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 and the Cyber Kill Chain (13.1.2.3)

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, shown in Figure 13-4, 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:

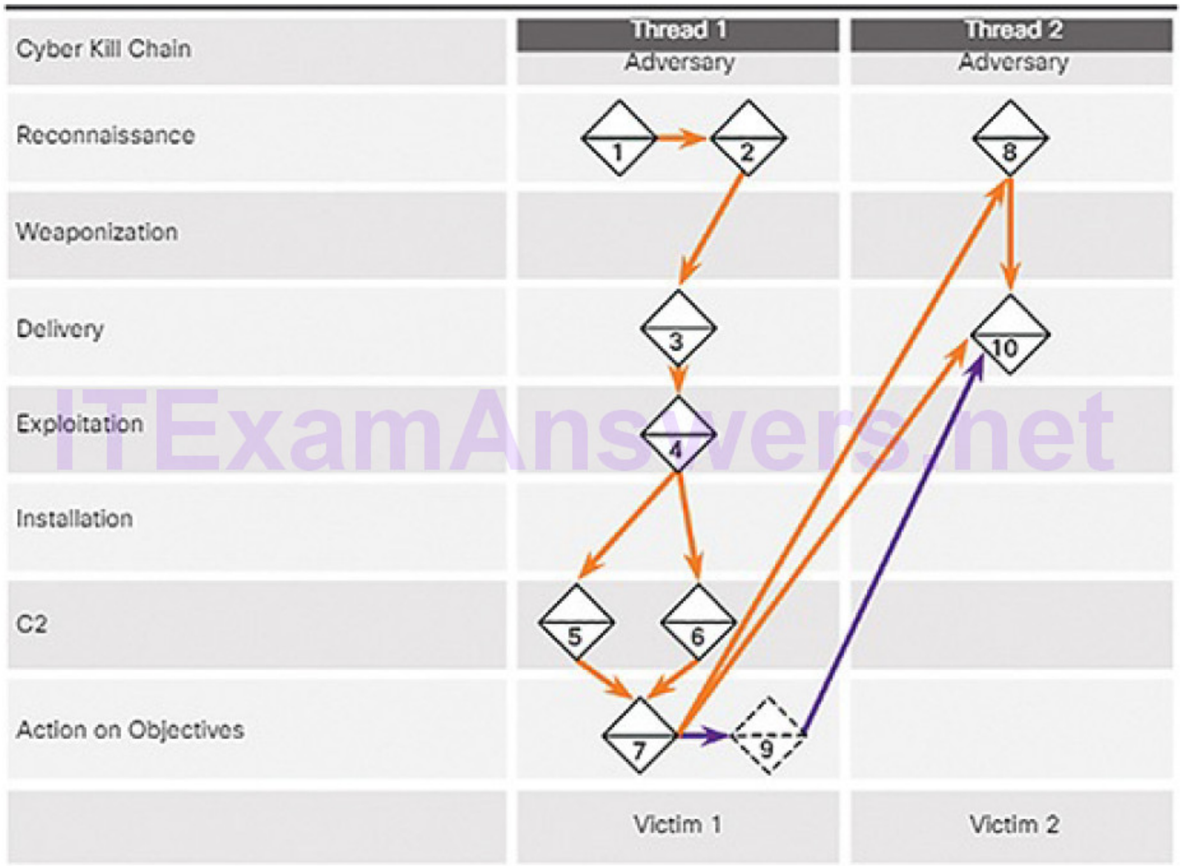


Figure 13-4 Activity Thread Example

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

2. Adversary uses the newly discovered domain gadets.com for a new search "network administrator gadgets.com" and discovers forum postings from users claiming to be network administrators of gadgets.com. The user profiles reveal their email addresses.

3. Adversary sends phishing emails with a Trojan horse attached to the network administrators of gadgets.com.

4. One network administrator (NA1) of gadgets.com opens the malicious attachment. This executes the enclosed exploit, allowing for further code execution.

5. 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.

6. 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.

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

8. Through the proxy established on NA1’s host, Adversary does a web searchfor “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 Gadgets, 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. For example, the adversary could mine the Chief Research Officer’s email contacts for additional potential victims. The adversary might also set up 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.”

Activity 13.1.2.4: Identify the Diamond Model Features Refer to the online course to complete this Activity.

The VERIS Schema (13.1.3)

In this topic, you will learn how to apply the VERIS Schema to an Incident.

What Is the VERIS Schema? (13.1.3.1)

Designed by Verizon and placed on the GitHub community coding site, the Vocabulary for Event Recording and Incident Sharing (VERIS) is a set of metrics designed to create a way to describe security incidents in a structured and repeatable way. VERIS was created to share quality information about security events to the community, anonymously. The VERIS Community Database (VCDB) is an open and free collection of publicly reported security incidents in VERIS format. You can use unformatted, raw data or the dashboard to find VERIS entries. The VCDB is a central location for the security community to learn from experience and help with decision making, before,during, and after a security incident.

In the VERIS schema, risk is defined as the intersection of four landscapes of Threat, Asset, Impact, and Control, as shown in Figure 13-5. 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.

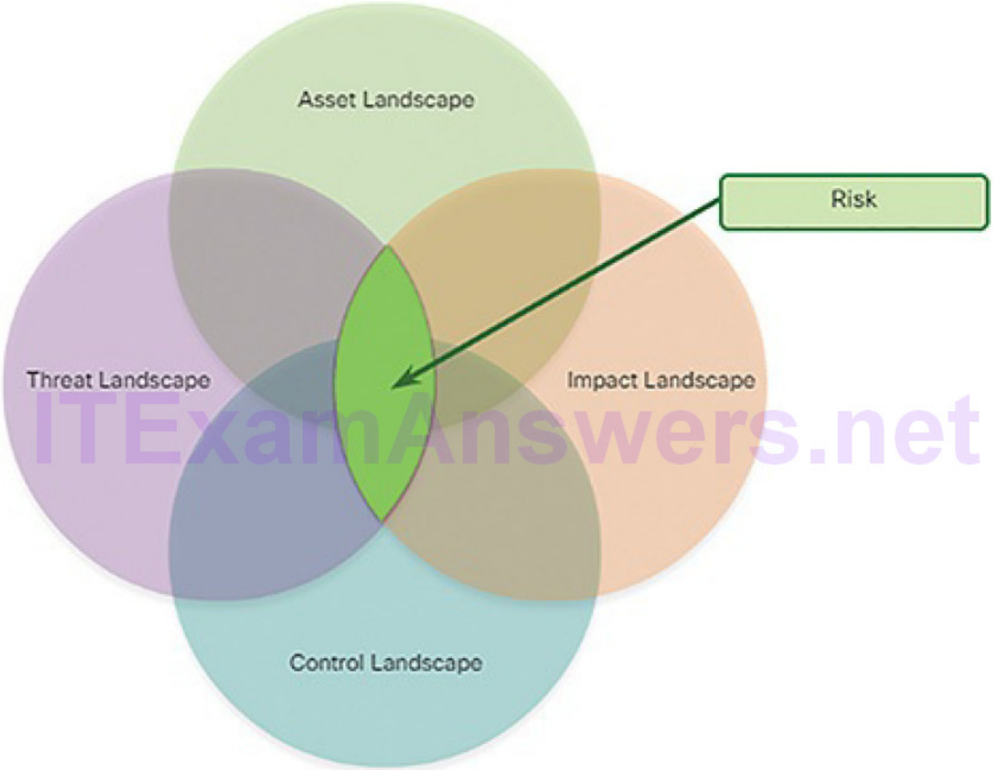


Figure 13-5 Risk at the Intersection of Four Landscapes

Create a VERIS Record (13.1.3.2)

When creating records to add to the database, start with the basic facts about the incident. It is helpful to use the VERIS elements outlined by the community.

Table 13-8 shows the most basic record that can exist. The framework does not need to be complicated. 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.

Table 13-8 A Basic VERIS Record

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

When an incident is recorded, it is most likely that you will have more specific information than just the year when the incident occurred. For example, the month and day can be documented by adding VERIS labels to the existing record, as shown in Table 13-9. The way the incident was discovered, a summary of what happened, and any other notes about the type of incident should also be recorded using VERIS labels. Any variable, data, or text can be recorded as part of the VERIS record using VERIS labels. For example, in Table 13-9 variables were added to document that Debbie in Sales reported that her computer was infected with malware. It was determined, through an interview with Debbie and a scan of her computer, that a rootkit was installed via an infected USB drive.

Table 13-9 Adding Information to the VERIS Record

Variable	Value
timeline.incident.year	2017
timeline.incident.month	6
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.

After the initial records are created, additional details should be added to aid in data analysis. The only two required in the VERIS schema are whether the incident was a real security incident, and how the incident was discovered. Most ticketing systems will allow new fields to be added to forms. To add more details to the record, just add a new field and designate a VERIS enumeration for it. A Word document, Excel spreadsheet, or other software can be used to create these records as well. You could also create a dedicated reporting tool for incident recording.

After the major details have been recorded, even more detail can be added as you continue to document the incident. Every bit of information that can be entered into the record may be helpful to your organization and others who respond to the incident and may help to prevent and detect future incidents of this type. The more data available to the community, the better chance there is of preventing future incidents.

VERIS can record the details of the organization that was affected such as industry, number of employees, or the country of the organization. This information can be useful in the overall picture when multiple organizations have a record of a similar incident. This demographic information can be shared without revealing specific, private information about the affected organization.

Top-Level and Second-Level Elements (13.1.3.3)

There are five top-level elements of the VERIS schema, each of which provides a different aspect of the incident. Each top-level element contains several second-level elements, as shown in Figure 13-6. These elements are useful for classifying data that has been collected about an incident.

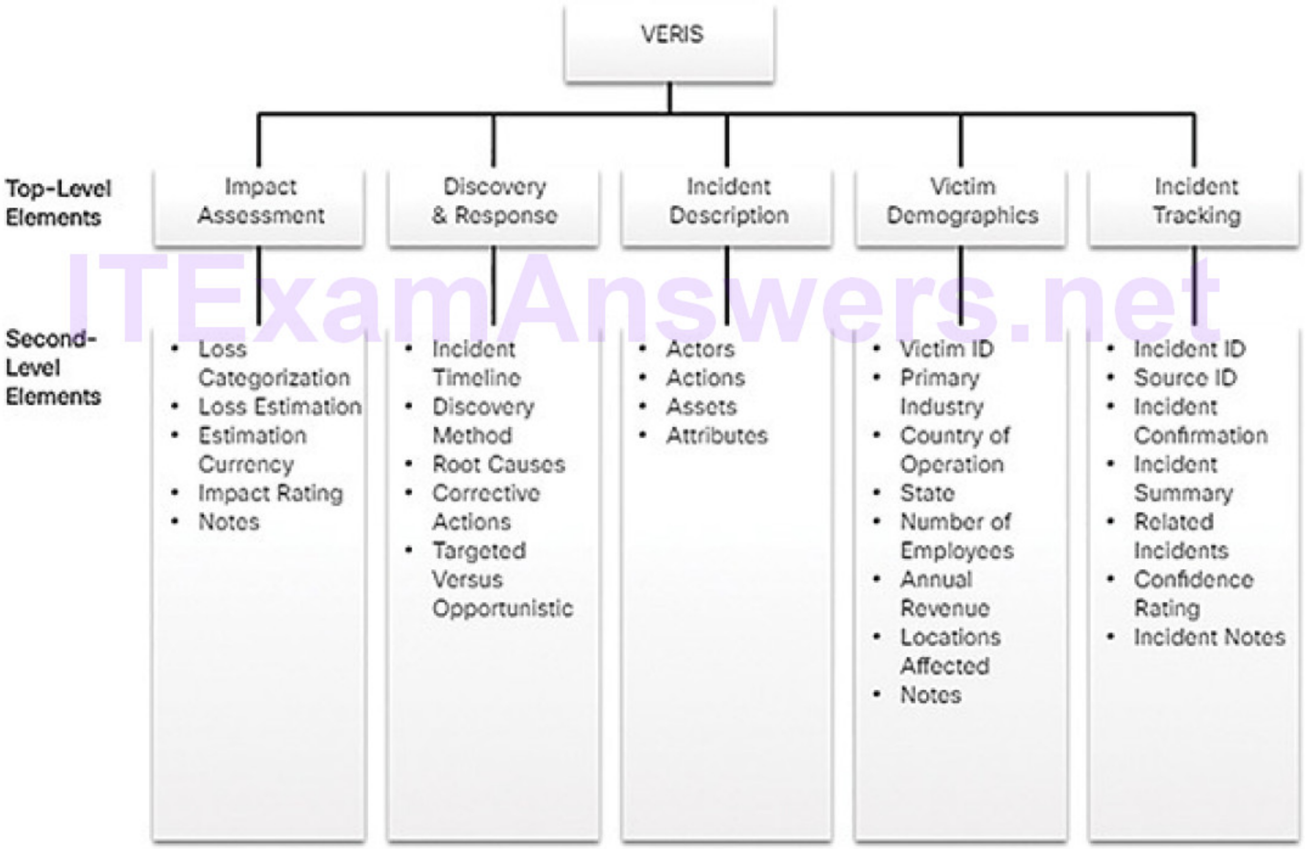


Figure 13-6 VERIS Schema Elements

Impact Assessment

For any incident, there is impact, whether it is minor or widespread. It is often very difficult to determine the scope of the impact until well after an incident has occurred, or even after it has been remediated. The second-level elements used for impact assessment are as follows:

Loss Categorization: Identifies the types of losses that occurred due to the incident.
Loss Estimation: This is an estimate of the total losses that were incurred because of the incident.
Estimation Currency: Uses the same currency when multiple types are involved.

Impact Rating: This is a rating that indicates the overall impact of the incident. It could be a number between 1 and 100, or another scale such as a grading scale.
Notes: Additional details that may be of use are recorded here.

Discovery and Response

This section is for recording the timeline of events, the method of incident discovery, and what the response was to the incident, including how it was remediated. The second-level elements used for discovery and response are as follows:

Incident Timeline: The timeline of all events from the discovery of the incident to the time the incident has been contained or restored to a fully functional state. This section is very important for gathering metrics such as readiness, the actions of the threat actors, and the response of the affected organization, along with many others.
Discovery Method: Identifies the way in which the incident was discovered. This may be accidental or by design.
Root Causes: Identifies any weakness or failure in security allowing the incident to take place.
Corrective Actions: This variable is for recording what will be done to detect or prevent this type of incident in the future.
Targeted vs. Opportunistic: Identifies if the incident was a deliberate, targeted attack, or if it was a random incident, based on a found opportunity by an attacker.

Incident Description

To describe an incident completely, VERIS uses the A4 threat model that was developed by the RISK team at Verizon. The second-level elements used for incident description, also known as the 4 As, are as follows:

Actors: Whose actions affected the asset?
Actions: What actions affected the asset?
Assets: Which assets were affected?
Attributes: How was the asset affected?

Each of these elements should be further refined through the use of their associated subelements by answering the questions in Table 13-10.

Table 13-10 Incident Description for Subelements

Actors	
Variable	**Question**
actor.external	Was there an external threat actor?
actor.internal	Was there an internal threat actor?

actor.partner	Was there a partner threat actor?
actor.unknown	Was there a threat actor but you don’t know what kind?

Actions

Variable	**Question**
action.hacking	Was there evidence of hacking?
action.malware	Was there evidence of malware?
action.social	Was there evidence of social engineering?
action.misuse	Was there evidence of misuse of privileges?
action.error	Was there an error that lead to the incident?
action.physical	Was there evidence of physical attack?
action.environmental	Was there an act of God that lead to the incident?
action.unknown	Are we unsure what happened?

Attributes

Variable	**Question**
attribute.confidentiality	Is it possible that confidential information was exposed?
attribute.integrity	Was the integrity of any system affected?
attribute.availability	Was there an availability loss?
attribute.unknown	Are we unsure what was affected?

Assets

Variable	**Question**
asset.assets.server	Was a server affected by the incident?
asset.assets.network	Was a network device affected?
asset.assets.user	Were any end-user devices affected?
asset.assets.terminal	Were any terminal devices affected (e.g., ATM, Kiosk, etc.)?
asset.assets.media	Did the incident affect any paper documents, or storage media?
asset.assets.people	Were any people compromised (e.g., Social Engineering)?

asset.assets.unknown	Are we unsure what was affected?

Victim Demographics

This section is for describing the organization that has experienced the incident. The characteristics of the organization can be compared to other organizations to determine if there are aspects of an incident that are common. The second-level elements used for victim demographics are as follows:

Victim ID: Identifies incidents with the organization that experienced them.
Primary Industry: Identifies the industry in which the affected organization conducts business. The six-digit North American Industry Classification System (NAICS) code is entered here.
Country of Operation: Used to record the country where the primary location of the organization operates.
State: Only used when the organization operates in the United States.
Number of Employees: This is for recording the size of the entire organization, not a department or branch.
Annual Revenue: This variable can be rounded for privacy.Locations Affected: Identifies any additional regions or branches that were affected by the incident.
Notes: Additional details that may be of use are recorded here.

Incident Tracking

This is for recording general information about the incident so organizations can identify, store, and retrieve incidents over time. The second-level elements used for incident tracking are as follows:

Incident ID: This is a unique identifier for storage and tracking.
Source ID: Identifies the incident in the context of who reported it.
Incident Confirmation: Differentiates the incident from those that are known or suspected as being non-incidents.
Incident Summary: Provides a short description of the incident.
Related Incidents: Allows the incident to be associated with similar incidents.
Confidence Rating: Provides a rating as to how accurate the reported incident information is.
Incident Notes: Allows recording of any information not captured in other VERIS fields.

The VERIS Community Database (13.1.3.4)

There are some organizations that collect data for security incidents, but either the data is not available to the public for free or it is not in a format that allows for manipulation or transformation that may be required to make it useful. This makes it difficult for researchers who study security incident trends and organizations to make reliable risk management calculations.

This is where the VERIS Community Database (VCDB) is useful. Through the proper use of the VERIS schema and a willingness 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.

Like any database, it can be used to determine answers to questions. It can also be used to find out how one organization compares to another when it is of the same approximate size and operating in the same kind of industry.

Activity 13.1.3.5: Apply the VERIS Schema to an Incident Refer to the online course to complete this Activity.

Incident Handling (13.2)

In this section, you will learn how to apply standards specified in NIST 800-61r2 to a computer security incident.

CSIRTs (13.2.1)

In this topic, you will learn the various goals of a given CSIRT.

CSIRT Overview (13.2.1.1)

A computer security incident can be defined differently across organizations. Generally, a computer security incident is any malicious or suspicious act which violates a security policy or any event that threatens the security, confidentiality, integrity, or availability of an organization's assets, information systems, or data network. Although this definition may be considered vague, these are some common computer security incidents:

- Malicious code
- Denial of service
- Unauthorized entry
- Device theft
- Malicious scans or probes
- Security breach
- Violation of any security policy item

When a security incident takes place, an organization needs a way to respond. A Computer Security Incident Response Team (CSIRT) is an internal group commonly found within an organization that provides services and functions to secure the assets of that organization. A CSIRT does not necessarily only respond to incidents that have already happened. A CSIRT may also provide proactive services and functions such as penetration testing, intrusion detection, or even security awareness training. These types of services can help to prevent incidents, but also increase response time and mitigate damage. In the case where a security incident needs to be contained and mitigated, the CSIRT coordinates and oversees these efforts.

Types of CSIRTs (13.2.1.2)

In larger organizations, the CSIRT will focus on investigating computer security incidents. Information security teams (InfoSec) will focus on implementing security policies and monitoring for security incidents. Many times in smaller organizations, the CSIRT will handle the tasks of the InfoSec team. Every organization is different. The goals of the CSIRT must be in alignment with the goals of the organization. There are many different types of CSIRTs and related organizations:

Internal CSIRT: Provides incident handling for the organization in which the CSIRT resides. Any organization, such as a hospital, bank, university, or construction company, can have an internal CSIRT.

National CSIRT: Provides incident handling for a country.

Coordination center: Coordinates incident handling across multiple CSIRTs. One example is US-CERT. US-CERT responds to major incidents, analyzes threats, and exchanges information with other cybersecurity experts and partners around the world.

Analysis center: Uses data from many sources to determine incident activity trends. Trends help to predict future incidents and provide early warning to prevent and mitigate damages as quickly as possible. The VERIS community is an example of an analysis center.

Vendor team: Provides remediation for vulnerabilities in an organization’s software or hardware. These teams often handle customer reports concerning security vulnerabilities. A vendor team may also act as theinternal CSIRT for an organization.

Managed security service provider (MSSP): Provides incident handling to other organizations as a fee-based service. Cisco, Symantec, Verizon, and IBM are all examples of managed security service providers.

CERT (13.2.1.3)

Computer Emergency Response Teams (CERTs) are similar to CSIRTs, but are not the same. CERT is a trademarked acronym owned by Carnegie Mellon University. A CSIRT is an organization responsible for receiving, reviewing, and responding to security incidents. A CERT provides security awareness, best practices, and security vulnerability information to their populations. CERTs do not directly respond to security incidents.

Many countries have asked for permission to use the CERT acronym. These are some of the more prominent CERTs:

- US-CERT: https://www.us-cert.gov
- Japan CERT Coordination Center: http://www.jpcert.or.jp/english/
- Indian Computer Emergency Response Team: http://www.cert-in.org.in
- Singapore Computer Emergency Response Team: https://www.csa.gov.sg/singcert
- CERT Australia: https://www.cert.gov.au

Activity 13.2.1.4: Match the CSIRT with the CSIRT Goal Refer to the online course to complete this Activity.

NIST 800-61r2 (13.2.2)

In this topic, you will learn how to apply the NIST 800-61r2 incident handling procedures to a given incident scenario.

Establishing an Incident Response Capability (13.2.2.1)

The NIST recommendations for incident response are detailed in Special Publication 800-61, revision 2, entitled Computer Security Incident Handling Guide.

Note
Although this chapter summarizes much of the content in the NIST 800-61r2 standard, you should also read the entire publication as it covers six major exam topics for the Cybersecurity CCNA SECOPS exam. Search the Internet for "NIST 800-61r2", download the PDF, and study it.

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 particular 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.

Policy

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 are as follows:

- 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 or severity ratings of incidents
- Performance measures
- Reporting and contact forms

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 capability and its effectiveness
- Roadmap for maturing the incident response capability
- How the program fits into the overall organization

Procedure Elements

The procedures that are followed during an incident response should follow the incident response plan. Procedures such as following technical processes, using techniques, filling out forms, and following checklists are 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 who 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 (13.2.2.2)

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 CSIRT to handle 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 are in charge of staffing all of the departments. Management must coordinate the incident response with other stakeholders and minimize the damage of an incident.

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.

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 Planning: 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 as a whole. 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.

NIST Incident Response Life Cycle (13.2.2.3)

NIST defines four steps in the incident response process life cycle, as shown inFigure 13-7.

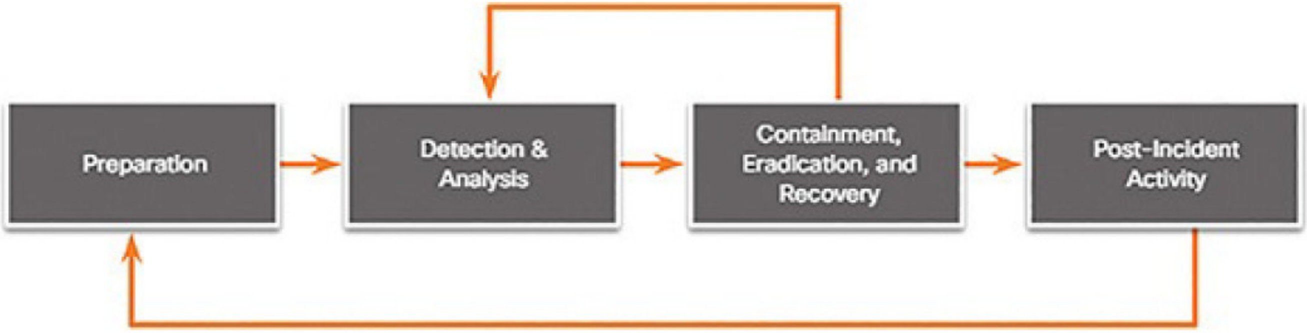


Figure 13-7 Incident Response Life Cycle

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. 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 handled, recommends changes for future response, and specifies how to avoid a reoccurrence.

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 is discussed in more detail in this topic.

Preparation (13.2.2.4)

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 compiling contactinformation for stakeholders, other CSIRTs, and law enforcement, establishing an issue tracking system, and distributing smartphones, encryption software, etc.
- Facilities to host the response team and the SOC are created.
- Necessary hardware and software for incident analysis and mitigation are 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.

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 handle 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.

Detection and Analysis (13.2.2.5)

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

Attack Vectors

An organization should be prepared to handle 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

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 different ways and not all of 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.

Analysis

Incident analysis is difficult because not all of 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 being the target of a buffer overflow attack. 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.

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.

Incident Notification

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. 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 (13.2.2.6)

After a security incident has been detected and sufficient analysis has been performed to determine that the incident is valid, it must be contained in order 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 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.

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 of the people who participated in collecting or handling 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 handling on how to preserve evidence properly.

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 organizationsand 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. Another organization or individual may have 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.

Eradication, Recovery, and Remediation

After containment, the first step to eradication is identifying all of the hosts that need remediation. All of the effects of the security incident must be eliminated. This includes malware infections and user accounts that have been compromised. All of 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 good 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 (13.2.2.7)

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 of the parties involved to discuss the eventsthat took place and the actions of all of the individuals while handling 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.

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 at what times?
- 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 (13.2.2.8)

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 possible 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 incidenceresponse 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.

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 800-61r2 provides the following examples of performing 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 whether the incident caused damage before it was detected
- Determining whether 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
- Determining whether 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 aresource that was attacked, in order to determine if the owner thinks the incident was handled efficiently and if the outcome was satisfactory.

There should be a policy in place in each organization 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. 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.

Data Retention: An organization may specify that specific types of data should be kept for a specific period of time. 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, storage management can become costly. Remember also that as technology changes, functional devices that can use outdated hardware and storage media must be stored as well.

Reporting Requirements and Information Sharing (13.2.2.9)

Governmental regulations should be consulted by the legal team to determine precisely 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.

Activity 13.2.2.10: Identify the Incident Response Plan Elements Refer to the online course to complete this Activity.

Activity 13.2.2.11: Identify the Incident Handling Term Refer to the online course to complete this Activity.

Activity 13.2.2.12: Identify the Incident Handling Step Refer to the online course to complete this Activity.

Lab 13.2.2.13: Incident Handling

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

Summary (13.3)

In this chapter, you learned about incident response models commonly used by cybersecurity analysts to manage network security incidents.

The Cyber Kill Chain specifies the steps that an attacker must complete to accomplish their goal. The steps in the Cyber Kill Chain are as follows:

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command and Control
7. Action on Objectives

If the attacker is stopped at any stage, the chain of attack is broken.

The Diamond Model of intrusion is made up of four parts and represents a security incident or event: adversary, capability, infrastructure, and victim. As a cybersecurity analyst, you may be called on to use the Diamond Model to diagram a series of intrusion events. The Diamond Model is ideal for illustrating how the adversary pivots from one event to the next.

In the VERIS schema, risk is defined as the intersection of four landscapes of Threat, Asset, Impact, and Control. Through the proper use of the VERIS schema and a willingness to participate, organizations can submit security incident details to the VCDB for the community to use.

Generally, a computer security incident is any malicious or suspicious act which violates a security policy, or any event that threatens the security, confidentiality, integrity, or availability of an organization's assets, information systems, or data network.

A CSIRT is an internal group commonly found within an organization that provides services and functions to respond to security incidents.

The types of CSIRTs are

- Internal CSIRT
- National CSIRT
- Coordination centers
- Analysis centers
- Vendor teams
- Managed security service providers

Unlike CSIRTs, CERTs provide security awareness, best practices, and security vulnerability information to their populations. CERTs do not directly respond to security incidents.

NIST 800-61r2 defines four phases in the incident response process life cycle:

- Preparation
- Detection and analysis
- Containment, eradication, and recovery
- Post-incident activities

Practice

The following Lab provides practice with the topics introduced in this chapter.
All the Labs, Class Activities, and Packet Tracer Activities are available in the companion CCNA Cybersecurity Operations Lab Manual (ISBN: 9781587134388). The PKA files are found in the online course.

Labs

Lab 13.2.2.13: Incident Handling