Chapter 13

Dealing with Incidents

Episode 13.01

Episode title: **Incident Response Overview**

Objective: **Overview**

Episode 13.02

Episode title: **Incident Response Plans (IRPs)**

Objective: **4.2 Summarize the importance of policies, processes, and procedures for incident response.**

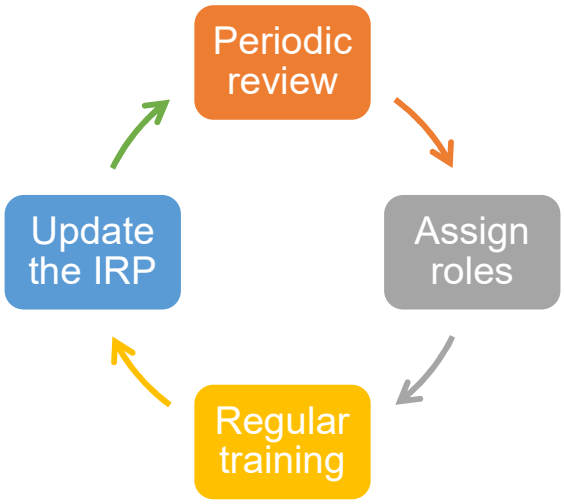
Indicators of Compromise (IoC)

- Suspicious occurrence that raises a red flag
- Examples
  - Excessive outbound traffic to a single unknown host
  - Newly detected Linux device on a Windows network
  - Log/IDS/IPS alerts

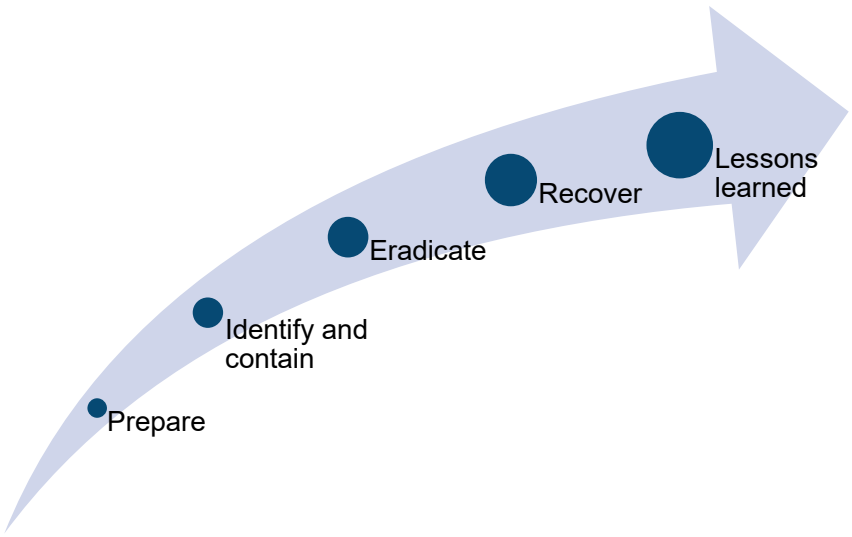
Incident Response Plan (IRP)

- Proactive preparation for reacting to an attack
  - Step-by-step procedures
  - Document(s)
- Response to threats
  - Detection
  - Containment
  - Eradication
- Contact list
- When to escalate

IRP Life Cycle



IRP Process


Lessons learned
Recover
Eradicate
Identify and contain
Prepare

IRP Testing

- Designed to detect, contain, and eradicate threats
- Walkthroughs
- Simulations
- Tabletop exercises

Quick Review

- An Incident Response Plan (IRP) is a proactive way to minimize downtime and impacts caused by security events
- Incident response tasks include proactive preparation, identification and containment, eradication, and applying lessons learned
- IRPs must be reviewed periodically

Episode 13.03

Episode title: **Threat Analysis and Mitigating Actions**

Objective: **4.2 Summarize the importance of policies, processes, and procedures for incident response.**

Cyber Kill Chain Analysis

- Trace steps taken for a successful compromise/data exfiltration event
- Security compromise knowledge can help prevent future breaches

Cyber Kill Chain Analysis

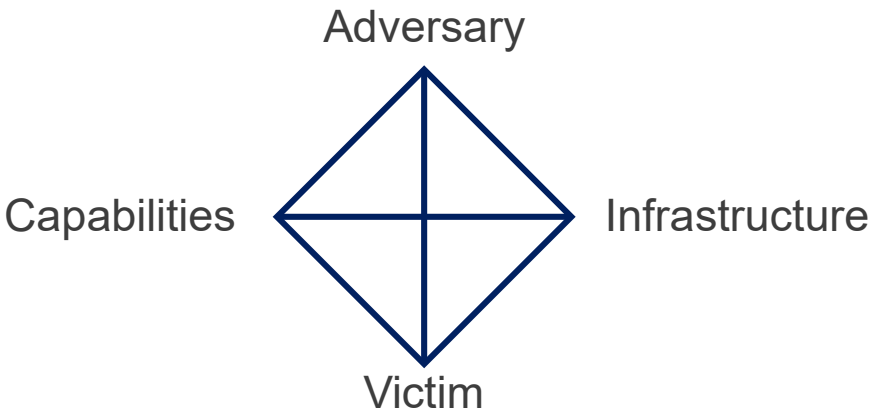
MITRE ATT&CK Framework

- Used for post-compromise identification and analysis
  - Threat detection
  - What was done and how was it done?
- Identify attacker techniques
- Mitigation
  - Modify existing firewall, IDS/IPS alert rules
  - Deploy honeypot traps

The Diamond Model of Intrusion Analysis

- Shows how malicious actors (adversaries) use exploit capabilities over an infrastructure against victims
- Data can stem from the use of honeypots

The Diamond Model of Intrusion Analysis



Security Orchestration, Automation, and Response (SOAR)

- Automate incident response using playbooks
  - Firewall rules, content filters
  - Application allow/deny lists
  - Revoke certificates
- Reduce incident response time

Quick Review

- Cyber Kill Chain analysis is used to trace steps taken for a successful security compromise
- The MITRE ATT&CK framework is used to analyze how security events occurred
- The Diamond Model of Intrusion analysis describes attacker methods and techniques
- SOAR is used to automate incident response

Episode 13.04

Episode title: **Digital Forensics**

Objective: **2.8 Summarize the basics of cryptographic concepts.**
4.5 Explain the key aspects of digital forensics.

Digital Forensics

- Applying science to the collection and preservation of evidence for legal use
- Follow proper evidence gathering and retention procedures
  - Technological solutions
  - Interviews for parties related to a security incident

E-discovery

- Discovery of electronic information
- On-premises
- Cloud
- Investigations
- Legal hold
- Freedom of Information Act

Mobile Device Forensics

- Prevent wireless communications
  - Enable airplane mode
  - Faraday bag/cage
- Geolocation GPS tagging
  - When/where pictures and video were taken
  - Social media posts

Steganography

- Hiding in plain sight
  - A form of obfuscation
  - Example: Message embedded in a benign picture

Quick Review

- Digital forensics is the application of science to digital evidence gathering
- Legal holds ensure potential evidence is not modified or deleted
- Steganography hides messages within benign files or network transmissions

Episode 13.05

Episode title: **Gathering Digital Evidence**

Objective: **4.1 Given a scenario, use the appropriate tool to assess organizational security.**

4.5 Explain the key aspects of digital forensics.

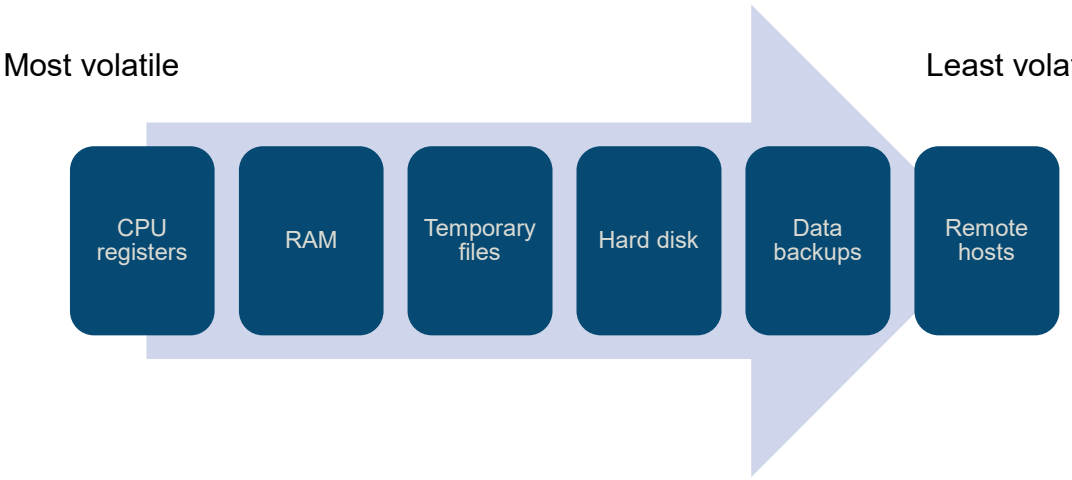
Chain of Custody

- Documents evidence acquisition
  - Document the original state of everything
  - On-premises and in the cloud
  - Tools and techniques used
  - Date and time stamps
  - Evidence collection, tagging, transfer and storage

Common Forensic Tools

- Create forensic disk images
  - Linux dd command
  - FTK imager
- Analyze disk images, recover data
  - Autopsy
  - WinHex
- RAM memory dumps
  - Memdump
  - HELIX

Order of Volatility



Quick Review

- Chain of custody refers to the proper gathering, storage, and transferring of digital evidence
- The order of volatility determines the order in which digital evidence is gathered
- The state of the original copy of digital evidence must be preserved

Episode 13.06

Episode title: **Business Continuity and Alternate Sites**

Objective:

2.1 Explain the importance of security concepts in an enterprise environment.

4.2 Summarize the importance of policies, processes, and procedures for incident response.

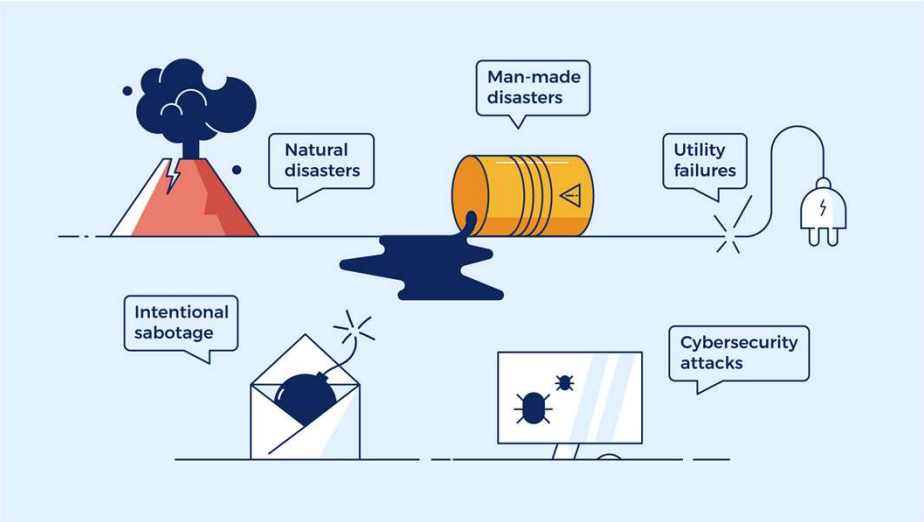
Planning for Disasters

- Business continuity plan (BCP)
  - Continuity of operations (COOP)
  - Broad scope
- Disaster Recovery Plan (DRP)
  - Narrow scope such as specific server

Planning for Disasters

- Organizational policies
  - Change management
  - Asset management
  - Security

Disaster Types



Source: https://smallbiztrends.com/2019/02/what-is-a-business-continuity-plan.html

Disaster Recovery Sites

- Site risk assessment
  - Geographical location
- Site components
  - Hardware
  - Software
  - Data
  - Personnel
- The public cloud is often used as an alternate site

Hot Site

- Hardware
- Software
- Networking in place
- Up-to-date data
  - Continuous replication with primary site
- Personnel
- Quickest switchover time, most expensive

Warm Site

- Hardware
- Software
- Networking in place
- No up-to-date data
- Longer switchover time than hot, less expensive than hot
- Personnel may be present

Cold Site

- Basic IT infrastructure in place
  - Networking
- No hardware
- No software
- No data
- No personnel
- Longest switchover time, cheapest type of recovery site

Quick Review

- The BCP scope is broad, DRP scope is focused on returning a specific system back to a functional state
- Hot alternate sites are more expensive than warm and cold because switchover can be immediate

Episode 13.07

Episode title: **Data Backup**

Objective: **2.5 Given a scenario, implement cybersecurity resilience.**

Data Backup Considerations

- On-premises
  - Tape
  - Network attached storage (NAS)
  - Storage area network (SAN)
- Offsite
  - Cloud
- Compression
- Encryption
- Type of backup
- Virtual machine
  - Snapshots
  - Custom images

Full/Copy Backup

- All data is backed up
  - Longest time for backup
  - Shortest time for restore
- Example: Weekly full backup

Incremental Backup

- New/modified data since the last incremental backup
  - Shortest time to backup
  - Longest time to restore
- Example: Full backup weekly, incremental nightly

Differential Backup

- New/modified data since last full backup
  - Longer to backup than incremental, shorter than full
  - Quicker to restore than incremental, slower than full

Quick Review

- Data backups increase data availability in case of a disaster
- Backups can be compressed and encrypted
- Full backups are the longest to backup and the quickest to restore
- Differential backups copy new and modified data since the last full backup
- Incremental backups copy new and modified data since the last incremental backup