Incident Response

Objective 4.8: Explain appropriate incident response activities

- **Incident Response**
  - *Incident Response*
    - Systematic approach to managing and mitigating security incidents
    - Goals
      - Minimize impact
      - Reduce detection and containment time
      - Facilitate recovery
    - Key Steps
      - Detection
      - Classification
      - Containment
      - Eradication
      - Evidence preservation
      - Communication
      - Lessons learned
  - Study Topics
    - Incident Response Process
      - Steps
        - Preparation
        - Detection
        - Analysis
        - Containment

        - Eradication
        - Recovery
        - Lessons Learned
- *Threat Hunting*
    - Proactive cybersecurity approach for continuous threat identification
    - Purpose
        - Identify hidden or emerging threats
- *Root Cause Analysis*
    - Systematic process to investigate incidents and identify underlying factors
    - Purpose
        - Understand the cause of security breaches or operational issues
- Incident Response Training and Testing
    - Methods
        - Tabletop Exercises
        - Simulations
        - Drills
        - Live Exercises
    - Purpose
        - Prepare personnel and systems for effective incident response
- *Digital Forensic Procedures*
    - Systematic techniques to gather, analyze, and preserve digital evidence
    - Purpose
        - Investigate cybercrimes or security incidents
- *Data Collection Procedures*
    - Established methods for gathering relevant information during incident response

- Concept
  - Order of volatility (prioritizing data collection based on volatility)
- *Disk Imaging and Analysis*
  - Creating a bit-by-bit copy (image) of a storage device, examining content
  - Purpose
    - Recover data
    - Investigate incidents
    - Identify security issues

- **Incident Response Process**
  - *Incident*
    - An act violating a security policy
  - Phases of Incident Response
    - NIST (National Institute for Standards and Technology) defines a four-phase incident response process
      - Preparation
      - Detection and Analysis
      - Containment, Eradication and Recovery
      - Post-Incident Activity
    - In the CompTIA model, "Detection and Analysis" is divided into two phases, and "Containment, Eradication, and Recovery" is divided into three, creating a seven-phase model
  - Seven Phases of Incident Response
    - *Preparation*
      - Gets an organization ready for future incidents
      - Focuses on making systems resilient to attacks by hardening systems and

networks

- Involves creating policies, procedures, and a communication plan

- *Detection*
  - Determines if a security incident has occurred
  - Identifies a security incident
  - Cybersecurity and triage analysts play a vital role in assessing incident severity
- *Analysis*
  - Thoroughly examines and evaluates the incident
  - Provides insights into the incident's scope and impact
  - Notifies stakeholders and initiates containment
- *Containment*
  - Limits the incident's scope by securing data and minimizing business impact
  - Prevents the spread of malicious activity
- *Eradication*
  - Starts after containment
  - Focuses on removing malicious activity from systems or networks
  - May involve reimaging affected systems
- *Recovery*
  - Restores affected systems and services to their secure state
  - Includes restoring from backups, patching, and updating configurations
  - Ensures resilience against future threats
- *Post-Incident Activity*
  - Occurs after containment, eradication, and recovery
  - Identifies the initial incident source and improvements to prevent future

incidents

- Involves
    - Root cause analysis
        - Identifies the incident's source and how to prevent it in the future
        - Steps
            - Define/scope the incident
            - Determine the causal relationships that led to the incident
            - Identify an effective solution
            - Implement and track the solutions
    - Lessons learned
        - Documents experiences during incidents in a forma
    - After-action report
        - Collects formalized information about what occurred

- *Incident Response Team*
    - The core team includes cybersecurity professionals with incident response experience
        - Temporary members may be added as needed (e.g., database administrators)
    - Large organizations have full-time incident response teams
        - Smaller organizations form temporary teams for specific incidents
    - Team Roles
        - Leader
        - Subject Matter Experts
        - IT Support

- Legal Counsel
- HR
- Public Relations

■ Leadership and management ensure the incident response team has necessary funding, resources ,and expertise

■ Management makes crucial decisions and communicates them during the incident response

○ Outsourcing Incident Response

■ Some organizations outsource incident response to specialized teams

■ Effective but expensive; external teams may not be familiar with the organization's network

- **Threat Hunting**
  - *Threat Hunting*
    - Proactive cybersecurity technique to detect threats that haven't been discovered by normal security monitoring
    - Involves actively seeking out potential threats within your network, as opposed to waiting for them to trigger alerts
  - Steps in Threat Hunting
    - Establishing a Hypothesis
      - Conduct threat modeling to identify potential threats with high impact
      - Use threat intelligence to form hypotheses about threat actors or campaigns that may target your organization
    - Profiling Threat Actors and Activities
      - Create scenarios to understand how attackers might attempt an intrusion
      - Determine the type of threat actor (insider, hacktivist, criminal, nation

state)
- Identify their objectives and potential targets

■ Threat Hunting Process
- Utilizes security monitoring and incident response tools
- Analyzes logs, system data, file systems, and registry information
- Focuses on finding threats not detected by existing rules
- Start by assuming that the current rules haven't flagged potential threats
- Seeks new tactics, techniques, and procedures used by threat actors

○ Key Considerations
■ Threat hunters must stay updated on the latest attacks and threats
■ Use advisories and bulletins published by vendors and researchers to identify new TTPs and vulnerabilities
■ Utilize intelligence fusion and threat data, combining SIEM logs with real-world threat feeds

○ Benefits of Threat Hunting
■ Improves detection capabilities by identifying threats that bypass existing defenses
■ Enhances threat intelligence by correlating external threat feeds with internal logs
■ Provides actionable intelligence to strengthen security measures

- **Root Cause Analysis**
  - *Root Cause Analysis (RCA)*
    - Systematic process to identify the initial source of an incident and prevent it from recurring

- Steps in Root Cause Analysis
  - Define and Scope the Incident
    - Determine the initial cause and scope of the incident
    - Understand how many systems/users have been affected and the operational impact
  - Determine Causal Relationships
    - Identify the causal relationships that led to the incident
    - Understand how the incident occurred, such as through malware infection via USB drive or other vectors
  - Identify Effective Solutions
    - Find solutions to prevent the incident from recurring
    - Solutions may include adding antivirus, restricting data transfer from USB devices, or applying software patches
  - Implement and Track Solutions
    - Execute the solutions and ensure the incident is fully resolved
    - Use change management processes to update systems and configurations
    - Look across the network and see if there are any other machines that could have been affected
- Benefits of Root Cause Analysis
  - Identifies vulnerabilities and weaknesses in security practices
  - Creates more robust protections against cyber threats
  - Encourages a no-blame culture, focusing on solutions and improvements rather than assigning fault
    - *No-Blame Approach*
      - RCA should not assign blame to individuals or teams

    - Encourages open and honest reporting to improve cybersecurity practices
    - Recognizes that human errors often result from systemic issues within organizations, such as training procedures or regulatory oversight

- **Incident Response Training and Testing**
    - *Training*
        - Education to ensure employees and staff understand incident response processes, procedures, and priorities
        - Training should be tailored to different roles (e.g., first responders, managers, executives, end users) with specific needs
            - End user training includes teaching them how to report incidents and remedial training for those who make mistakes
        - Capture and incorporate lessons learned from previous incidents into training to prevent their recurrence
        - Soft skills and relationship building are important in high-functioning incident response teams
    - *Testing*
        - Practical exercise of incident response procedures to ensure the practical application of knowledge
        - Testing helps assess the effectiveness of your response procedures
        - It can be costly, complex, and resource-intensive, depending on the scenario
    - *Tabletop Exercise (TTX)*
        - A theoretical exercise that presents an incident response scenario
        - Discussion based

- Participants discuss and role-play their response actions
- Cost-effective but lacks hands-on experience
- Useful for exploring decision-making and response planning

- *Penetration Test (Pen Test)*
  - A red team (attacker) attempts network intrusion based on a specific threat modeling scenario
  - Rules of engagement and clear methodology are established beforehand
  - Popular tools and operating systems
    - Metasploit
    - Cobalt Strike
    - Kali Linux
    - ParrotOS
    - Commando OS
  - Awareness of these tools is crucial, as they can be used by both penetration testers and attackers
- *Simulation*
  - Goes beyond tabletop discussions, involving realistic, hands-on scenarios
  - Mimics actual incidents
    - Simple
      - Phishing attacks,
      - Ransomware infections
    - Complex
      - Multi-stage attacks
      - Data breaches in coordination with external parties
  - Tests technical skills, decision-making under pressure, and effective communication

- Align simulations with the organization's threat landscape and risk profile
- Identifies gaps in incident response plans, improves team coordination, and ensures role clarity during real incidents
- Regularly incorporating simulations improves an organization's readiness for cybersecurity incidents

- **Digital Forensic Procedures**
  - *Digital Forensics*
    - Systematic process of investigating and analyzing digital devices and data to uncover evidence for legal purposes
  - Four Main Phases of Digital Forensic Procedures
    - *Identification*
      - Focus on scene safety, prevention of evidence contamination, and scope determination
      - Secure the scene, preserve evidence, and document the scene
      - Identify where relevant data might be stored (e.g., tablets, smartphones, servers)
    - *Collection*
      - Requires proper authorization (e.g., warrant, executive authorization)
      - Order of volatility
        - Dictates the sequence in which data sources should be collected and preserved based on their susceptibility to modification or loss
        - Following order of volatility minimizes data loss
        - 5 Steps of Order of Volatility
          - Collect data from the system's memory
          - Capture data from the system state

        - Collect data from storage devices
        - Capture network traffic and logs
        - Collect remotely stored or archived data
    - *Chain of Custody*
        - Documented and verifiable record that tracks the handling, transfer, and preservation of digital evidence from the moment it is collected until it is presented in a court of law
    - Evidence Collecting techniques
        - *Disk imaging*
            - Involves creating a bit-by-bit or logical copy of a storage device, preserving its entire content, including deleted files and unallocated space
        - *File Carving*
            - Focuses on extracting files and data fragments from storage media without relying on the file system
- *Analysis*
    - Examine the forensically sound evidence copy
    - Systematically scrutinize data for relevant information, timestamps, user interactions, and signs of criminal activity
    - Follow strict procedures and documented protocols for consistency and objectivity
- *Reporting*
    - Document methods, tools used, actions performed, findings, and conclusions in a final report
    - The report serves as crucial evidence in legal proceedings, and the forensic analyst may need to testify

- Additional Concepts
  - *Legal Hold*
    - Issued when litigation is expected and preserves potentially relevant electronic data
    - Ensures evidence is not tampered with, deleted, or lost
    - Requires the implementation of preservation practices to protect systems and evidence
  - *E-Discovery (Electronic Discovery)*
    - Process of identifying, collecting, and presenting electronically stored information for potential legal proceedings
    - Involves searching, analyzing, and formatting electronic data for litigation
- Ethical Considerations
  - Adherence to a code of ethics that emphasizes avoiding bias, repeatable actions, and evidence preservation
    - Avoiding bias
      - Analysis should be performed without bias or prejudice and be based solely on the evidence
      - Use forensic analysts who are removed from the situation to avoid potential bias
    - Repeatable actions
      - All analysis must be based on repeatable processes documented in the final report
      - Ensuring the original evidence remains unchanged is critical to maintaining evidentiary integrity
    - Evidence preservation
      - Evidence includes both the device (e.g., laptop hard disk) and the

data recovered from it

- Perform analysis on a disk image, not the original drive, to prevent modifications or alterations

- **Data Collection Procedures**
  - Digital Forensic Collection Techniques
    - Involve making forensic images of data for later analysis
    - This approach allows incident response teams to resume operations quickly while maintaining evidence
    - Evidence may be required for potential legal action and cooperation with law enforcement
  - Data collection involves the following
    - Capturing and hashing system images
    - Analyzing data with forensic tools
      - FTK (Forensic Toolkit)
      - EnCase
    - Capturing machine screenshots
    - Reviewing network logs
    - Collecting CCTV video
  - *Order of Volatility*
    - Guides the sequence of collecting data, from most volatile (CPU registers and cache) to least volatile (archival media)
  - Licensing and documentation reviews ensure system configurations align with their design
  - *Data Acquisition*
    - The method and tools used to create a forensically sound copy of data from a

source device, such as system memory or a hard disk

- Policies for bringing one's own device (BYOD) complicate data acquisition because it may not be legally possible to search or seize the devices
- Some data can only be collected once the system is shutdown or the power is disconnected
- Order of Volatility
    - CPU registers and cache memory
    - System memory (RAM), routing tables, ARP caches, process table, temporary swap files
    - Data on persistent mass storage
    - Remote logging and monitoring data
    - Physical configuration and network topology
    - Archival data
- WARNING
    - Some Windows registry keys, like HKLM/Hardware, are only in memory and require a memory dump to analyze