
# 2.0 Security Operations

## 2.1 Given a scenario, perform threat management activities.

- **Intelligence types**
  - Tactical
    - Commodity malware
  - Strategic
    - Targeted attacks
  - Operational
    - Threat hunting
    - Threat emulation
- **Actor types**
  - Advanced persistent threat (APT)/nation-state
  - Insider threat
  - Competitor
  - Hacktivist
  - Script kiddie
  - Organized crime
- **Threat actor properties**
  - Resource
    - Time
    - Money
  - Supply chain access
  - Create vulnerabilities
  - Capabilities/sophistication
  - Identifying techniques
- Intelligence collection methods
  - Intelligence feeds
  - Deep web
  - Proprietary
  - Open-source intelligence (OSINT)
  - Human intelligence (HUMINT)
- **Frameworks**
  - MITRE Adversarial Tactics, Techniques, & Common knowledge (ATT&CK)
    - ATT&CK for industrial control system (ICS)
  - Diamond Model of Intrusion Analysis
  - Cyber Kill Chain

## 2.2 Given a scenario, analyze indicators of compromise and formulate an appropriate response.

- **Indicators of compromise**
  - Packet capture (PCAP)
  - Logs
    - Network logs
    - Vulnerability logs
    - Operating system logs
    - Access logs
    - NetFlow logs
  - Notifications
    - FIM alerts
    - SIEM alerts
    - DLP alerts
    - IDS/IPS alerts
    - Antivirus alerts
  - Notification severity/priorities
  - Unusual process activity
- **Response**
  - Firewall rules
  - IPS/IDS rules
  - ACL rules
  - Signature rules
  - Behavior rules
  - DLP rules
  - Scripts/regular expressions

## 2.3 Given a scenario, perform vulnerability management activities.

- **Vulnerability scans**
  - Credentialed vs. non-credentialed
  - Agent-based/server-based
  - Criticality ranking
  - Active vs. passive
- **Security Content Automation Protocol (SCAP)**
  - Extensible Configuration Checklist Description Format (XCCDF)
  - Open Vulnerability and Assessment Language (OVAL)
  - Common Platform Enumeration (CPE)
  - Common Vulnerabilities and Exposures (CVE)
  - Common Vulnerability Scoring System (CVSS)
  - Common Configuration Enumeration (CCE)
  - Asset Reporting Format (ARF)
- **Self-assessment vs. third-party vendor assessment**
- **Patch management**
- **Information sources**
  - Advisories
  - Bulletins
  - Vendor websites
  - Information Sharing and Analysis Centers (ISACs)
  - News reports

## 2.4 Given a scenario, use the appropriate vulnerability assessment and penetration testing methods and tools.

- **Methods**
  - Static analysis
  - Dynamic analysis
  - Side-channel analysis
  - Reverse engineering
    - Software
    - Hardware
  - Wireless vulnerability scan
  - Software composition analysis
  - Fuzz testing
  - Pivoting
  - Post-exploitation
  - Persistence
- **Tools**
  - SCAP scanner
  - Network traffic analyzer
  - Vulnerability scanner
  - Protocol analyzer
  - Port scanner
  - HTTP interceptor
  - Exploit framework
  - Password cracker
- **Dependency management**
- **Requirements**
  - Scope of work
  - Rules of engagement
  - Invasive vs. non-invasive
  - Asset inventory
  - Permissions and access
  - Corporate policy considerations
  - Facility considerations
  - Physical security considerations
  - Rescan for corrections/changes

## 2.5 Given a scenario, analyze vulnerabilities and recommend risk mitigations.

- **Vulnerabilities**
  - Race conditions
  - Overflows
    - Buffer
    - Integer
  - Broken authentication
  - Unsecure references
  - Poor exception handling
  - Security misconfiguration
  - Improper headers
  - Information disclosure
  - Certificate errors
  - Weak cryptography implementations
  - Weak ciphers
  - Weak cipher suite implementations
  - Software composition analysis
  - Use of vulnerable frameworks and software modules
  - Use of unsafe functions
  - Third-party libraries
    - Dependencies
  - Code injections/malicious changes
  - End of support/end of life
  - Regression issues
- **Inherently vulnerable system/application**
  - Client-side processing vs. server-side processing
  - JSON/representational state transfer (REST)
  - Browser extensions
    - Flash
    - ActiveX
  - Hypertext Markup Language 5 (HTML5)
  - Asynchronous JavaScript and XML (AJAX)
  - Simple Object Access Protocol (SOAP)
  - Machine code vs. bytecode or interpreted vs. emulated
- **Attacks**
  - Directory traversal
  - Cross-site scripting (XSS)
  - Cross-site request forgery (CSRF)
  - Injection
    - XML
    - LDAP
    - Structured Query Language (SQL)
    - Command
    - Process
  - Sandbox escape
  - Virtual machine (VM) hopping
  - VM escape
  - Border Gateway Protocol (BGP)/ route hijacking
  - Interception attacks
  - Denial-of-service (DoS)/DDoS
  - Authentication bypass
  - Social engineering
  - VLAN hopping

## 2.6 Given a scenario, use processes to reduce risk.

- **Proactive and detection**
  - Hunts
  - Developing countermeasures
  - Deceptive technologies
    - Honeynet
    - Honeypot
    - Decoy files
    - Simulators
    - Dynamic network configurations
- **Security data analytics**
  - Processing pipelines
    - Data
    - Stream
  - Indexing and search
  - Log collection and curation
  - Database activity monitoring
- **Preventive**
  - Antivirus
  - Immutable systems
  - Hardening
  - Sandbox detonation
- **Application control**
  - License technologies
  - Allow list vs. block list
  - Time of check vs. time of use
  - Atomic execution
- **Security automation**
  - Cron/scheduled tasks
  - Bash
  - PowerShell
  - Python
- **Physical security**
  - Review of lighting
  - Review of visitor logs
  - Camera reviews
  - Open spaces vs. confined spaces

## 2.7 Given an incident, implement the appropriate response.

- **Event classifications**
  - False positive
  - False negative
  - True positive
  - True negative
- **Triage event**
- **Preescalation tasks**
- **Incident response process**
  - Preparation
  - Detection
  - Analysis
  - Containment
  - Recovery
  - Lessons learned
- **Specific response playbooks/processes**
  - Scenarios
    - Ransomware
    - Data exfiltration
    - Social engineering
  - Non-automated response methods
  - Automated response methods
    - Runbooks
    - SOAR
- **Communication plan**
- **Stakeholder management**

## 2.8 Explain the importance of forensic concepts.

- **Legal vs. internal corporate purposes**
- **Forensic process**
  - Identification
  - Evidence collection
    - Chain of custody
    - Order of volatility
      - Memory snapshots
      - Images
    - Cloning
  - Evidence preservation
    - Secure storage
    - Backups
  - Analysis
    - Forensics tools
  - Verification
  - Presentation
- **Integrity preservation**
  - Hashing
- **Cryptanalysis**
- **Steganalysis**

## 2.9 Given a scenario, use forensic analysis tools.

- **File carving tools**
  - Foremost
  - Strings
- **Binary analysis tools**
  - Hex dump
  - Binwalk
  - Ghidra
  - GNU Project debugger (GDB)
  - OllyDbg
  - readelf
  - objdump
  - strace
  - ldd
  - file
- **Analysis tools**
  - ExifTool
  - Nmap
  - Aircrack-ng
  - Volatility
  - The Sleuth Kit
  - Dynamically vs. statically linked
- **Imaging tools**
  - Forensic Toolkit (FTK) Imager
  - dd
- **Hashing utilities**
  - sha256sum
  - ssdeep
- **Live collection vs. post-mortem tools**
  - netstat
  - ps
  - vmstat
  - ldd
  - lsof
  - netcat
  - tcpdump
  - conntrack
  - Wireshark