4.0 Security Operations

4.1 Given a scenario, analyze data to enable monitoring and response activities.

- **Security information event management (SIEM)**
  - Event parsing
  - Event duplication
  - Non-reporting devices
  - Retention
  - Event false positives/false negatives
- **Aggregate data analysis**
  - Correlation
  - Audit log reduction
  - Prioritization
  - Trends
- **Behavior baselines and analytics**
  - Network
  - Systems
  - Users
  - Applications/services
- **Incorporating diverse data sources**
  - Third-party reports and logs
  - Threat intelligence feeds
  - Vulnerability scans
  - CVE details
  - Bounty programs
  - DLP data
  - Endpoint logs
  - Infrastructure device logs
  - Application logs
  - Cloud security posture management (CSPM) data
- **Alerting**
  - False positives/false negatives
  - Alert failures
  - Prioritization factors
    - Criticality
    - Impact
    - Asset type
    - Residual risk
    - Data classification
  - Malware
  - Vulnerabilities
- **Reporting and metrics**
  - Visualization
  - Dashboards

4.2 Given a scenario, analyze vulnerabilities and attacks, and recommend solutions to reduce the attack surface.

- **Vulnerabilities and attacks**
  - Injection
  - Cross-site scripting (XSS)
  - Unsafe memory utilization
  - Race conditions
  - Cross-site request forgery
  - Server-side request forgery
  - Insecure configuration
  - Embedded secrets
  - Outdated/unpatched software and libraries
  - End-of-life software
  - Poisoning
  - Directory service misconfiguration
  - Overflows
  - Deprecated functions
  - Vulnerable third parties
  - Time of check, time of use (TOCTOU)
  - Deserialization
  - Weak ciphers
  - Confused deputy
  - Implants
- **Mitigations**
  - Input validation
  - Output encoding
  - Safe functions
    - Atomic functions
    - Memory-safe functions
    - Thread-safe functions
  - Security design patterns
  - Updating/patching
    - Operating system (OS)
    - Software
    - Hypervisor
    - Firmware
    - System images
  - Least privilege
  - Fail secure/fail safe
  - Secrets management
    - Key rotation
  - Least function/functionality
  - Defense-in-depth
  - Dependency management
  - Code signing
  - Encryption
  - Indexing
  - Allow listing

4.3 Given a scenario, apply threat-hunting and threat intelligence concepts.

- **Internal intelligence sources**
  - Adversary emulation engagements
  - Internal reconnaissance
  - Hypothesis-based searches
  - Honeypots
  - Honeynets
  - User behavior analytics (UBA)
- **External intelligence sources**
  - Open-source intelligence (OSINT)
  - Dark web monitoring
  - Information sharing and analysis centers (ISACs)
  - Reliability factors
- **Counterintelligence and operational security**
- **Threat intelligence platforms (TIPs)**
  - Third-party vendors
- **Indicator of compromise (IoC) sharing**
  - Structured Threat Information eXchange (STIX)
  - Trusted automated exchange of indicator information (TAXII)
- **Rule-based languages**
  - Sigma
  - Yet Another Recursive Acronym (YARA)
  - Rita
  - Snort
- **Indicators of attack**
  - TTPs

4.4 Given a scenario, analyze data and artifacts in support of incident response activities.

- **Malware analysis**
  - Detonation
  - IoC extractions
  - Sandboxing
  - Code stylometry
    - Variant matching
    - Code similarity
    - Malware attribution
- **Reverse engineering**
  - Disassembly and decompilation
  - Binary
  - Byte code
- **Volatile/non-volatile storage analysis**
- **Network analysis**
- **Host analysis**
- **Metadata analysis**
  - Email header
  - Images
  - Audio/video
  - Files/filesystem
- **Hardware analysis**
  - Joint test action group (JTAG)
- **Data recovery and extraction**
- **Threat response**
- **Preparedness exercises**
- **Timeline reconstruction**
- **Root cause analysis**
- **Cloud workload protection platform (CWPP)**
- **Insider threat**