1.0 Security Operations

1.1 Explain the importance of system and network architecture concepts in security operations.

- **Log ingestion**
  - Time synchronization
  - Logging levels
- **Operating system (OS) concepts**
  - Windows Registry
  - System hardening
  - File structure
    - Configuration file locations
  - System processes
  - Hardware architecture
- **Infrastructure concepts**
  - Serverless
  - Virtualization
  - Containerization
- **Network architecture**
  - On-premises
  - Cloud
  - Hybrid
  - Network segmentation
  - Zero trust
  - Secure access secure edge (SASE)
  - Software-defined networking (SDN)
- **Identity and access management**
  - Multifactor authentication (MFA)
  - Single sign-on (SSO)
  - Federation
  - Privileged access management (PAM)
  - Passwordless
  - Cloud access security broker (CASB)
- **Encryption**
  - Public key infrastructure (PKI)
  - Secure sockets layer (SSL) inspection
- **Sensitive data protection**
  - Data loss prevention (DLP)
  - Personally identifiable information (PII)
  - Cardholder data (CHD)

1.2 Given a scenario, analyze indicators of potentially malicious activity.

- **Network-related**
  - Bandwidth consumption
  - Beaconing
  - Irregular peer-to-peer communication
  - Rogue devices on the network
  - Scans/sweeps
  - Unusual traffic spikes
  - Activity on unexpected ports
- **Host-related**
  - Processor consumption
  - Memory consumption
  - Drive capacity consumption
  - Unauthorized software
  - Malicious processes
  - Unauthorized changes
  - Unauthorized privileges
  - Data exfiltration
  - Abnormal OS process behavior
  - File system changes or anomalies
  - Registry changes or anomalies
  - Unauthorized scheduled tasks
- **Application-related**
  - Anomalous activity
  - Introduction of new accounts
  - Unexpected output
  - Unexpected outbound communication
  - Service interruption
  - Application logs
- **Other**
  - Social engineering attacks
  - Obfuscated links

1.3 Given a scenario, use appropriate tools or techniques to determine malicious activity.

- **Tools**
  - Packet capture
    - Wireshark
    - tcpdump
  - Log analysis/correlation
    - Security information and event management (SIEM)
    - Security orchestration, automation, and response (SOAR)
  - Endpoint security
    - Endpoint detection and response (EDR)
  - Domain name service (DNS) and Internet Protocol (IP) reputation
    - WHOIS
    - AbuseIPDB
  - File analysis
    - Strings
    - VirusTotal
  - Sandboxing
    - Joe Sandbox
    - Cuckoo Sandbox
- **Common techniques**
  - Pattern recognition
    - Command and control
  - Interpreting suspicious commands
  - Email analysis
    - Header
    - Impersonation
    - DomainKeys Identified Mail (DKIM)
    - Domain-based Message Authentication, Reporting, and Conformance (DMARC)
    - Sender Policy Framework (SPF)
    - Embedded links
  - File analysis
    - Hashing
  - User behavior analysis
    - Abnormal account activity
    - Impossible travel
- **Programming languages/scripting**
  - JavaScript Object Notation (JSON)
  - Extensible Markup Language (XML)
  - Python
  - PowerShell
  - Shell script
  - Regular expressions

1.4 Compare and contrast threat-intelligence and threat-hunting concepts.

- **Threat actors**
  - Advanced persistent threat (APT)
  - Hacktivists
  - Organized crime
  - Nation-state
  - Script kiddie
  - Insider threat
    - Intentional
    - Unintentional
  - Supply chain
- **Tactics, techniques, and procedures (TTP)**
- **Confidence levels**
  - Timeliness
  - Relevancy
  - Accuracy
- **Collection methods and sources**
  - Open source
    - Social media
    - Blogs/forums
    - Government bulletins
    - Computer emergency response team (CERT)
    - Cybersecurity incident response team (CSIRT)
    - Deep/dark web
  - Closed source
    - Paid feeds
    - Information sharing organizations
    - Internal sources
- **Threat intelligence sharing**
  - Incident response
  - Vulnerability management
  - Risk management
  - Security engineering
  - Detection and monitoring
- **Threat hunting**
  - Indicators of compromise (IoC)
    - Collection
    - Analysis
    - Application
  - Focus areas
    - Configurations/ misconfigurations
    - Isolated networks
    - Business-critical assets and processes
  - Active defense
  - Honeypot

1.5 Explain the importance of efficiency and process improvement in security operations.

- **Standardize processes**
  - Identification of tasks suitable for automation
    - Repeatable/do not require human interaction
  - Team coordination to manage and facilitate automation
- **Streamline operations**
  - Automation and orchestration
    - Security orchestration, automation, and response (SOAR)
  - Orchestrating threat intelligence data
    - Data enrichment
    - Threat feed combination
  - Minimize human engagement
- **Technology and tool integration**
  - Application programming interface (API)
  - Webhooks
  - Plugins
- **Single pane of glass**