CompTIA Cybersecurity Analyst (CySA+)

Certification Exam
Pre-draft Exam Objectives
Exam Number: CS0-004

- Pre-draft Exam Objectives summarize the tasks and skills identified in the Job Task Analysis (JTA) workshop that provide directional information about the upcoming exam version.
- The Draft Exam Objectives will replace the Pre-draft Exam Objectives after approximately two months when the skills have been peer-evaluated and validated through a JTA survey of job role practitioners.
- Pre-draft Exam Objectives may contain typos and errata that will be corrected during the development process.
- CompTIA will not accept feedback on the Pre-draft Exam Objectives document. If errors are found, please wait until the Draft Exam Objectives are posted, and then provide feedback using the Draft Exam Objectives Feedback form.

1.0 Security Operations

1.1 Explain concepts related to system and network architecture in security operations.

- Logging concepts
  - Ingestion
  - Configurations
  - Integrity and security
  - Time synchronization
  - Retention
- Operating system concepts
  - System hardening
  - File structure
    - Critical files
  - System processes
- Infrastructure/system architecture concepts
  - Cloud-native
  - Virtualization
  - Containerization
  - Application programming interfaces (APIs)
- Device management concepts
  - Mobile
  - Endpoint
- Network architecture concepts
  - Zero Trust Network Architecture (ZTNA)
  - Secure Access Service Edge (SASE)
  - Hybrid cloud
- Identity and access management (IAM)
  - Privileged access management (PAM)
  - Authentication and authorization methods
  - Secrets management
- Encryption techniques
- Data protection concepts
- Critical infrastructure concepts
  - Operational technology (OT)
  - Industrial control systems (ICS)
  - Supervisory control and data acquisition (SCADA)

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

- Network-related indicators
  - Rogue devices
  - Enumeration
  - Anomalous activity
  - Activity on unexpected ports
- Host-related indicators
  - Resource consumption
  - Unauthorized software
  - Anomalous activity
    - Suspicious or rogue processes
    - LOLBins (Living off the Lan Binaries and Scripts)

        - File system changes
        - Data exfiltration
    - Unauthorized configuration
    - Application-related indicators
        - Service disruption
        - Anomalous activity
    - Cloud-related indicators
        - Anomalous activity
        - Resource compromise
    - Social engineering attacks
        - Typosquatting
        - URL shorteners
    - Identity-based indicators
        - IAM account compromise
        - Unauthorized access
        - Impossible travel
    - Email-related attacks
        - Business email compromise (BEC)

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

- Tools
    - Decoding/parsing
        - CyberChef
    - Packet analysis
        - Wireshark
        - tcpdump
        - Snort
        - Suricata
        - Zeek
    - Log analysis
        - Security information and event management (SIEM)
    - Threat-intelligence platforms
        - Open threat exchange (OTX)
        - Malware Information Sharing Platform (MISP)
        - Open Cyber Threat Intelligence (OpenCTI)
    - Endpoint security
        - EDR/XDR (Endpoint Detection Response/Extended Detection Response)
        - Mobile device management (MDM)
    - Domain and IP reputation
        - WHOIS
        - AbuseIPDB
        - Geolocation by IP Address (GEO-IP)
    - File analysis
        - Strings
        - VirusTotal
        - Yet Another Recursive Acronym (YARA)
    - Sandboxing
        - Joe Sandbox
        - Cuckoo Sandbox
    - Pattern recognition
        - Regular expressions
        - Interpreting suspicious commands

    - Email analysis
        - MXToolbox
    - User entity behavior analysis (UEBA)
        - OpenUBA
- File formats
    - JSON
    - XML
    - YAML
    - EVTX
- Programming/scripting languages
    - Python
    - PowerShell
    - Shell script

1.4 Explain threat intelligence and threat-hunting concepts.

- Threat actors
    - Advanced Persistent Threat (APT)
    - Insider threat
- Tactics, techniques and procedures (TTPs)
    - Heat maps
    - Pyramid of pain
    - MITRE ATT&CK
    - Attribution
- Confidence level impacts
    - Timeliness
    - Relevance
    - Accuracy
- Collection methods and sources
    - Open-source intelligence (OSINT)
    - Closed-source intelligence
    - Threat intelligence sharing
- Indicators of compromise (IoC)
    - Collection
    - Analysis
    - Application/usage
    - Types
        - Atomic
        - Behavioral
- Threat modeling
    - Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege (STRIDE)
- Threat mapping
- Cyber deception

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

- Standardize processes
    - Manage and facilitate team coordination
    - Playbook/runbook creation
- Streamline operations
    - Automation and orchestration
        - Security Orchestration, Automation and Response (SOAR)
        - Infrastructure as Code (IaC)

    - Data enrichment
        - Rule/alert tuning
        - Dashboard creation
- Technology and tool integration
    - APIs
    - Webhooks
    - Plug-ins

1.6 Summarize concepts related to the use of AI in security operations.

- AI risks
    - Hallucinations
    - Data exposure
    - Model poisoning
    - Malicious prompts
- Governance
    - Legal or regulatory compliance
    - AI usage policies
- Use cases
    - Comparing artifacts
    - Analyzing log files
    - Document creation
    - Incident investigation
    - Event correlation
    - Automation and orchestration

2.0 Vulnerability Management

2.1 Given a scenario, implement the appropriate vulnerability scanning method.

- Asset inventory
- Planning considerations
    - Scheduling
    - Operations
    - Performance
    - Sensitivity levels
    - Segmentation
    - Regulatory requirements
- Scan types
    - Internal vs. external
    - Agent vs. agentless
    - Credentialed vs. non-credentialed
    - Passive vs. active
    - Discovery
        - Mapping scans
        - Device fingerprinting
    - Security baseline scanning
        - PCI-DSS
        - CIS benchmarks
        - ISO 27000 series

2.2 Given a scenario, analyze output from vulnerability assessment tools.

- Network scanning and mapping
    - Angry IP Scanner
    - Masscan

- Multipurpose tools
  - Nmap
  - Metasploit Framework (MSF)
  - Maltego
  - Recon-ng
- Web application scanners
  - Burp Suite
  - Zed Attack Proxy (ZAP)
  - Nikto
- Vulnerability scanners
  - Nessus
  - Nuclei
  - OpenVAS
- Cloud infrastructure assessment tools
  - ScoutSuite
  - Prowler
  - Trivy
  - Checkov
- Breach attack simulation (BAS) tools
  - Atomic Red Team
  - Caldera

2.3 Given a scenario, analyze data to prioritize and mitigate vulnerabilities.

- Criteria
  - Exploitability
  - Active exploitation/threat intelligence
  - Asset value
  - Impact
  - Patch/remediation availability
  - True/false positives
  - True/false negatives
- Scoring methods
  - Common Vulnerability Scoring System (CVSS) metrics
  - First Exploitability Prediction Scoring System (EPSS)
- Context awareness
  - Internal
  - External
  - Isolated
- Mitigation strategies
  - Attack surface management
  - Secure coding best practices
  - Patching and configuration management
  - Exceptions
  - Compensating controls
- Validation of remediation

2.4 Explain concepts related to control types, risks, and vulnerability management.

- Control types
  - Administrative
  - Technical
  - Physical
- Control functions

    - Preventative
    - Detective
    - Responsive
    - Corrective
- Risk concepts
    - Risk appetite
    - Residual risk
    - Inherent risk
- Risk management strategies
    - Accept
    - Transfer
    - Avoid
    - Mitigate
- Policies, governance, and service-level objectives (SLOs)
- Application security
    - Static application security testing (SAST)
    - Dynamic application security testing (DAST)
    - Software Assurance Maturity Model (SAMM)
- Third-party risk
    - Supply chain
    - Software composition analysis (SCA)
    - Software bill of materials (SBoM)

3.0 Incident Response and Management

3.1 Summarize concepts related to attack methodology frameworks.

- Cyber Kill Chain
- Diamond Model of Intrusion Analysis
- MITRE ATT&CK

3.2 Summarize the incident response process.

- Preparation
- Detection
- Analysis
- Containment
- Eradication
- Recovery
- Post-incident

3.3 Given a scenario, implement incident response techniques.

- Analysis
    - Triage
    - Establish a timeline
- Evidence acquisition
    - Chain of custody
    - Validating data integrity
    - Preservation
    - Legal hold
- Containment
    - Scope
    - Impact
    - Isolation
- Escalation

- Eradication techniques
- Continuous monitoring

4.0 Reporting and Communication

4.1 Explain the importance of vulnerability management reporting and communication.

- Vulnerability scan reports
- Compliance findings
- Risk scorecards
- Action plans
  - Escalation
  - Dependencies
- Inhibitors to remediation
  - Contractual agreements
  - Organizational governance
  - Business process interruption
  - Degrading functionality
  - Legacy systems
  - Proprietary systems
  - Patch availability
- Stakeholder identification and communication
- Metrics and key performance indicators (KPIs)
  - Trends
  - Top risks
  - Service-level agreement (SLA)

4.2 Explain the importance of security operations and incident response reporting and communication.

- Incident declaration and escalation
- Executive summary
- Communication plan
  - Stakeholder identification
  - Legal team
  - Public relations
  - Regulatory reporting agencies
  - Law enforcement
  - Customers
- Operational security awareness
  - Communication channels
- Post-incident reporting
  - After-action report
  - Lessons learned
  - Root cause analysis
- Shift/incident handover
- Internal threat intelligence report
  - Tailored to organization/environment
- Metrics and KPIs
  - Alert volume
  - False-positive rate
  - True-positive rate
  - Mean time to close
  - Mean time to detect

- Mean time to respond
- Mean time to remediate
- Phishing campaign click rate