KPMG Learning Academy

CompTIA Cybersecurity Analyst CySA+ Certification Training

Module 1: Threat and Vulnerability Management

1.1 Explain the importance of threat data and intelligence

Intelligence sources

- Open-source intelligence
- Proprietary/closed-source intelligence
- Timeliness
- Relevancy
- Accuracy

Indicator management

- Structured Threat Information eXpression (STIX)
- Trusted Automated eXchange of Indicator Information (TAXII)
- OpenIoC

Threat classification

- Known threat vs. unknown threat
- Zero-day
- Advanced persistent threat

Threat actors

- Nation-state
- Hacktivist
- Organised crime
- Insider threat
- Intentional
- Unintentional

Intelligence cycle

- Requirements
- Collection
- Analysis
- Dissemination
- Feedback

Commodity malware

Information sharing and analysis communities

- Healthcare
- Financial
- Aviation
- Government
- Critical infrastructure

1.2 Given a scenario, utilise threat intelligence to support organisational security

Attack frameworks

- MITRE ATT&CK
- The Diamond Model of Intrusion Analysis
- Kill chain

Threat research

- Reputational
- Behavioural
- Indicator of compromise (IoC)
- Standard vulnerability scoring system (CVSS)

Threat intelligence sharing with supported functions

- Incident response
- Vulnerability management
- Risk management
- Security engineering
- Detection and monitoring

1.3 Given a scenario, perform vulnerability management activities

Vulnerability identification

- Asset criticality
- Active vs. passive scanning
- Mapping/enumeration

Validation

- True positive
- False positive - True negative
- False-negative

Remediation/mitigation

- Configuration baseline
- Patching
- Hardening
- Compensating controls
- Risk acceptance
- Verification of mitigation

Scanning parameters and criteria

- Risks associated with scanning activities
- Vulnerability feed
- Scope
- Credentialed vs. non-credentialed
- Server-based vs. agent-based
- Internal vs. external
- Special considerations
- Types of data
- Technical constraints
- Workflow
- Sensitivity levels
- Regulatory requirements
- Segmentation
- Intrusion prevention system (IPS), intrusion detection system (IDS), and firewall settings

Inhibitors to remediation

- Memorandum of Understanding (MOU)
- Service-level agreement (SLA)
- Organisational governance
- Business process interruption
- Degrading functionality
- Legacy systems

1.4 Given a scenario, analyse the output from standard vulnerability assessment tools

Web application scanner

- OWASP Zed Attack Proxy (ZAP)
- Burp suite
- Nikto
- Arachni

Infrastructure vulnerability scanner

- Nessus
- OpenVAS
- Qualys

Software assessment tools and techniques

- Static analysis
- Dynamic analysis
- Reverse engineering
- Fuzzing

Enumeration

- Nmap
- hoping
- Active vs. passive
- Responder

Wireless assessment tools

- Aircrack-ng
- Reaver
- oclHashcat

Cloud Infrastructure assessment tools

- ScoutSuite
- Prowler
- Pacu

1.5 Explain the threats and vulnerabilities associated with specialised technology

Mobile

Internet of Things (IoT)

Embedded

Real-time operating system (RTOS)

System-on-Chip (SoC)

Field programmable gate array (FPGA)

Physical access control

Building automation systems

Vehicles and drones

- CAN bus

Workflow and process automation systems

Industrial control system

Supervisory control and data acquisition (SCADA)

- Modbus

1.6 Explain the threats and vulnerabilities associated with operating in the cloud

Cloud service models

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

Cloud deployment models

- Public
- Private
- Community
- Hybrid

Function as a Service (FaaS)/ serverless architecture

Infrastructure as code (IaC)

Insecure application programming interface (API)

Improper key management

Unprotected storage

Logging and monitoring

- Insufficient logging and monitoring
- Inability to access

1.7 Given a scenario, implement controls to mitigate attacks and software vulnerabilities

Attack types

- Extensible markup language (XML) attack
- Structured query language (SQL) injection
- Overflow attack
    - Buffer
    - Integer
    - Heap
- Remote code execution
- Directory traversal
- Privilege escalation
- Password spraying
- Credential stuffing
- Impersonation
- Man-in-the-middle attack
- Session hijacking
- Rootkit
- Cross-site scripting
    - Reflected
    - Persistent
    - Document object model (DOM)

Vulnerabilities

- Improper error handling
- Dereferencing
- Insecure object reference
- Race condition
- Broken authentication
- Sensitive data exposure
- Insecure components - Insufficient logging and monitoring - Weak or default configurations - Use of insecure functions - strcpy

Module 2: Software and Systems Security

2.1 Given a scenario, apply security solutions for infrastructure management

Cloud vs. on-premises

Asset management

- Asset tagging

Segmentation

- Physical
- Virtual
- Jumpbox
- System isolation
- Air gap

Network architecture

- Physical
- Software-define
- Virtual private cloud (VPC)
- Virtual private network (VPN)
- Serverless

Change management

Virtualisation

- Virtual desktop infrastructure (VDI)

Containerisation

Identity and access management

- Privilege management
- Multifactor authentication (MFA)
- Single sign-on (SSO)
- Federation
- Role-based
- Attribute-based
- Mandatory
- Manual review

Cloud access security broker (CASB)

Honeypot

Monitoring and logging

Encryption

Certificate management

Active defence

2.2 Explain software assurance best practices

Platforms

- Mobile
- Web application
- Client/server
- Embedded
- System-on-chip (SoC)
- Firmware

Software development life cycle (SDLC) integration

DevSecOps

Software assessment methods

- User acceptance testing
- Stress test application
- Security regression testing
- Code review

Secure coding best practices

- Input validation
- Output encoding
- Session management
- Authentication
- Data protection
- Parameterised queries

Static analysis tools

Dynamic analysis tools

Formal methods for verification of critical software

Service-oriented architecture

- Security Assertions Markup Language (SAML)
- Simple Object Access Protocol (SOAP)
- Representational State Transfer (REST)
- Microservices

2.3 Explain hardware assurance best practices

Hardware root of trust

- Trusted platform module (TPM)
- Hardware security module (HSM)

eFuse

Unified Extensible Firmware Interface (UEFI)

Trusted foundry

Secure processing

- Trusted execution
- Secure Enclave
- Processor security extensions
- Atomic execution

Anti-tamper

Self-encrypting drive

Trusted firmware updates

Measured boot and attestation

Bus encryption

Module 3: Security Operations and Monitoring

3.1 Given a scenario, analyse data as part of security monitoring activities

Heuristics

Trend analysis

Endpoint

- Malware
- Reverse engineering
- Memory
- System and application behaviour
- Known-good behaviour
- Anomalous behaviour
- Exploit techniques
- File system
- User and entity behaviour analytics (UEBA)

Network

- Uniform Resource Locator (URL) and domain name system (DNS) analysis
- Domain generation algorithm
- Flow analysis
- Packet and protocol analysis
- Malware

Log review

- Event logs
- Syslog
- Firewall logs
- Web application firewall (WAF)
- Proxy
- Intrusion detection system (IDS)/ Intrusion prevention system (IPS)

Impact analysis

- Organisational impact vs. localised impact
- Immediate vs. total

Security information and event management (SIEM) review

- Rule writing
- Known-bad Internet protocol (IP)
- Dashboard

Query writing

- String search
- Script
- Piping

E-mail analysis

- Malicious payload
- Domain Keys Identified Mail (DKIM)
- Domain-based Message Authentication, Reporting, and Conformance (DMARC)
- Sender Policy Framework (SPF)
- Phishing
- Forwarding
- Digital signature
- E-mail signature block
- Embedded links
- Impersonation
- Header

3.2 Given a scenario, implement configuration changes to existing controls to improve security

Permissions

Safelisting

Denylisting

Firewall

Intrusion prevention system (IPS) rules

Data loss prevention (DLP)

Endpoint detection and response (EDR)

Network access control (NAC)

Sinkholing

Malware signatures

- Development/rule writing

Sandboxing

Port security

3.3 Explain the importance of proactive threat hunting

Establishing a hypothesis

Profiling threat actors and activities

Threat hunting tactics

- Executable process analysis

Reducing the attack surface area

Bundling critical assets

Attack vectors

Integrated intelligence

Improving detection capabilities

3.4 Compare and contrast automation concepts and technologies

Workflow orchestration

- Security Orchestration, Automation, and Response (SOAR)

Scripting

Application programming interface (API) integration

Automated malware signature creation

Data Enrichment

Threat feed combination

Machine learning

Use of automation protocols and standards

- Security Content Automation Protocol (SCAP)

Continuous integration

Continuous deployment/delivery

Module 4: Incident Response

4.1 Explain the importance of the incident response process

Communication plan

- Limiting communication to trusted parties
- Disclosing based on regulatory/ legislative requirements
- Preventing inadvertent release of information
- Using a secure method of communication
- Reporting requirements

Response coordination with relevant entities

- Legal Human resources
- Public relations
- Internal and external
- Law enforcement
- Senior leadership
- Regulatory bodies

Factors contributing to data criticality

- Personally identifiable information (PII)
- Personal health information (PHI)
- Sensitive personal information (SPI)
- High-value asset
- Financial information
- Intellectual property
- Corporate information

4.2 Given a scenario, apply the appropriate incident response procedure

Preparation

- Training
- Testing
- Documentation of procedures

Detection and analysis

- Characteristics contributing to severity level classification
- Downtime
- Recovery time
- Data integrity
- Economic
- System process criticality
- Reverse engineering
- Data correlation

Containment

- Segmentation
- Isolation

Eradication and Recovery

- Vulnerability mitigation
- Sanitisation
- Reconstruction/reimaging
- Secure disposal
- Patching
- Restoration of permissions
- Reconstitution of resources
- Restoration of capabilities and services
- Verification of logging/ communication to security monitoring

Post-incident activities

- Evidence retention
- Lessons learned report
- Change control process
- Incident response plan update
- Incident summary report
- IoC generation
- Monitoring

4.3 Given an incident, analyse potential indicators of compromise

Network-related

- Bandwidth consumption
- Beaconing
- Irregular peer-to-peer communication
- The rogue device on the network
- Scan/sweep
- Unusual traffic spike
- Common protocol over a non-standard port

Host-related

- Processor consumption
- Memory consumption
- Drive capacity consumption
- Unauthorised software
- Malicious process
- Unauthorised change

- Unauthorised privilege
- Data exfiltration
- Abnormal OS process behaviour
- File system change or anomaly
- Registry change or anomaly
- Unauthorised scheduled task

Application-related

- Anomalous activity
- Introduction of new accounts
- Unexpected output
- Unexpected outbound communication
- Service interruption
- Application log

4.4 Given a scenario, utilise basic digital forensics techniques

Network

- Wireshark
- tcpdump

Endpoint

- Disk
- Memory

Mobile

Cloud

Virtualisation

Legal hold

Procedures

Hashing

- Changes to binaries

Carving

Data acquisition

Module 5: Compliance and Assessment

5.1 Understand the importance of data privacy and protection

Privacy vs. security

Non-technical controls

- Classification
- Ownership
- Retention
- Data types
- Retention standards
- Confidentiality
- Legal Requirements
- Data sovereignty
- Data minimisation
- Purpose limitation
- A non-disclosure agreement (NDA)

Technical controls

- Encryption
- Data loss prevention (DLP)
- Data masking
- Deidentification
- Tokenisation
- Digital rights management (DRM)?
- Watermarking
- Geographic access requirements
- Access controls

5.2 Given a scenario, apply security concepts to support organisational risk mitigation

Business impact analysis

Risk identification process

Risk calculation

- Probability
- Magnitude

Communication of risk factors

Risk prioritisation

- Security controls
- Engineering tradeoffs

Systems assessment

Documented compensating controls

Training and exercises

- Red team
- Blue team
- White team
- Tabletop exercise

Supply chain assessment

- Vendor due diligence
- Hardware source authenticity

5.3 Explain the importance of frameworks, policies, procedures, and controls

Frameworks

- Risk-based
- Prescriptive

Policies and procedures

- Code of conduct/ethics
- Acceptable use policy (AUP)
- Password policy
- Data Ownership
- Data retention
- Account management
- Continuous monitoring
- Work product retention

Category

- Managerial
- Operational
- Technical

Control type

- Preventative
- Detective
- Corrective
- Deterrent
- Compensating
- Physical

Audits and assessments

- Regulatory
- Compliance