CompTIA CySA+: Analisi e Risposta alle Minacce Informatiche

IN-FORMAZIONE SRL - Via Riccardo Grazioli Lante, 9 - 00195 Roma
P.IVA 07252070722 - Tel. : 0687153208 - info@musaformazione.it

COMPTIA CYSA+: ANALISI E RISPOSTA ALLE MINACCE INFORMATICHE

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.

1.4 COMPARE AND CONTRAST THREAT-INTELLIGENCE AND THREAT-HUNTING CONCEPTS.

- Threat actors
  - 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, CERT, 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
  - Team coordination to manage and facilitate automation
- Streamline operations
  - Automation and orchestration (SOAR)
  - Orchestrating threat intelligence data
  - Data enrichment
  - Threat feed combination
  - Minimize human engagement
- Technology and tool integration
  - API
  - Webhooks
  - Plugins

- Single pane of glass

2.0 VULNERABILITY MANAGEMENT

2.1 GIVEN A SCENARIO, IMPLEMENT VULNERABILITY SCANNING METHODS AND CONCEPTS.

- Asset discovery
  - Map scans
  - Device fingerprinting
- Special considerations
  - Scheduling
  - Operations
  - Performance
  - Sensitivity levels
  - Segmentation
  - Regulatory requirements
- Internal vs. external scanning
- Agent vs. agentless
- Credentialed vs. non-credentialed
- Passive vs. active
- Static vs. dynamic: Reverse engineering, Fuzzing
- Critical infrastructure
  - OT
  - ICS

- SCADA

- Security baseline scanning
- Industry frameworks
  - PCI DSS
  - CIS benchmarks
  - OWASP
  - ISO 27000 series

2.2 GIVEN A SCENARIO, ANALYZE OUTPUT FROM VULNERABILITY ASSESSMENT TOOLS.

- Tools
  - Network scanning/mapping: Angry IP Scanner, Maltego
  - Web app scanners: Burp Suite, ZAP, Arachni, Nikto
  - Vulnerability scanners: Nessus, OpenVAS
  - Debuggers: Immunity debugger, GDB
  - Multipurpose: Nmap, Metasploit, Recon-ng
  - Cloud assessment: Scout Suite, Prowler, Pacu

2.3 GIVEN A SCENARIO, ANALYZE DATA TO PRIORITIZE VULNERABILITIES.

- CVSS interpretation
  - Attack vectors
  - Attack complexity
  - Privileges required
  - User interaction
  - Scope

- Impact: Confidentiality, Integrity, Availability

- Validation
  - True/false positives
  - True/false negatives
- Context awareness
  - Internal
  - External
  - Isolated
- Exploitability/weaponization
- Asset value
- Zero-day

2.4 GIVEN A SCENARIO, RECOMMEND CONTROLS TO MITIGATE ATTACKS AND SOFTWARE VULNERABILITIES.

- Cross-site scripting: Reflected, Persistent
- Overflow vulnerabilities: Buffer, Integer, Heap, Stack
- Data poisoning
- Broken access control
- Cryptographic failures
- Injection flaws
- Cross-site request forgery
- Directory traversal
- Insecure design
- Security misconfiguration
- End-of-life or outdated components
- Identification/authentication failures

- Server-side request forgery
- Remote code execution
- Privilege escalation
- LFI/RFI

2.5 EXPLAIN CONCEPTS RELATED TO VULNERABILITY RESPONSE, HANDLING, AND MANAGEMENT.

- Control types
  - Managerial
  - Operational
  - Technical
  - Preventative
  - Detective
  - Responsive
  - Corrective
- Patching/configuration management
  - Testing
  - Implementation
  - Rollback
  - Validation
- Maintenance windows
- Exceptions
- Risk management principles
  - Accept
  - Transfer
  - Avoid

- Mitigate

- Policies, governance, and SLOs
- Prioritization and escalation
- Attack surface management
  - Edge discovery
  - Passive discovery
  - Security controls testing
  - Penetration testing
  - Bug bounty
  - Attack surface reduction
- Secure coding best practices
  - Input validation
  - Output encoding
  - Session management
  - Authentication
  - Data protection
  - Parameterized queries
- Secure SDLC
- Threat modeling
-

3.0 INCIDENT RESPONSE AND MANAGEMENT

3.1 EXPLAIN CONCEPTS RELATED TO ATTACK METHODOLOGY FRAMEWORKS.

- Cyber kill chains
- Diamond Model of Intrusion Analysis

- MITRE ATT&CK
- OSS TMM
- OWASP Testing Guide

3.2 GIVEN A SCENARIO, PERFORM INCIDENT RESPONSE ACTIVITIES.

- Detection and analysis
  - IoC
  - Evidence acquisitions: Chain of custody, Validating data integrity, Preservation, Legal hold
  - Data and log analysis
- Containment, eradication, and recovery
  - Scope
  - Impact
  - Isolation
  - Remediation
  - Re-imaging
  - Compensating controls

3.3 EXPLAIN THE PREPARATION AND POST-INCIDENT ACTIVITY PHASES OF THE INCIDENT MANAGEMENT LIFE CYCLE.

- Preparation
  - Incident response plan
  - Tools
  - Playbooks
  - Tabletop
  - Training

- BC/DR

- Post-incident activity
  - Forensic analysis
  - Root cause analysis
  - Lessons learned

4.0 REPORTING AND COMMUNICATION

4.1 EXPLAIN THE IMPORTANCE OF VULNERABILITY MANAGEMENT REPORTING AND COMMUNICATION.

- Vulnerability management reporting
  - Vulnerabilities
  - Affected hosts
  - Risk score
  - Mitigation
  - Recurrence
  - Prioritization
- Compliance reports
- Action plans
  - Configuration management
  - Patching
  - Compensating controls
  - Awareness, education, and training
  - Changing business requirements
- Inhibitors to remediation

- MOU
- SLA
- Organizational governance
- Business process interruption
- Degrading functionality
- Legacy systems
- Proprietary systems

- Metrics and KPIs
  - Trends
  - Top 10
  - Critical vulnerabilities and zero-days
  - SLOs

- Stakeholder identification and communication

4.2 EXPLAIN THE IMPORTANCE OF INCIDENT RESPONSE REPORTING AND COMMUNICATION.

- Stakeholder identification and communication
- Incident declaration and escalation
- Incident response reporting
  - Executive summary
  - Who, what, when, where, and why
  - Recommendations
  - Timeline
  - Impact
  - Scope
  - Evidence

- Communications
    - Legal
    - Public relations: Customer communication, Media
    - Regulatory reporting
    - Law enforcement
- Root cause analysis
- Lessons learned
- Metrics and KPIs
    - Mean time to detect
    - Mean time to respond
    - Mean time to remediate
    - Alert volume