Cybersecurity

Candidates for this exam are preparing for a job as an entry-level cybersecurity technician or junior analyst. This exam assesses their understanding of key security principles, frameworks, and mindset. Successful candidates will have a keen awareness of how vulnerabilities open a company to security incidents, and how adhering to security principles and implementing benchmarks can help to mitigate the risk of attack. They are developing the investigation and interpretation skills necessary to succeed in the field and have an aptitude and desire to learn more. They are familiar with the toolset used to monitor an endpoint device and network for indications of an incident and can analyze logs to determine whether an escalation should occur. Candidates should have at least 150 hours of instruction or hands-on experience with cybersecurity.

1. Security Principles

1.1 Explain common security principles

- Hardening; defense-in-depth; confidentiality, integrity, and availability (CIA); code of ethics; Zero Trust security; privacy (including AI use cases); data classification and retention policies; security governance

1.2 Explain cybersecurity frameworks and industry-accepted best practices

- NIST Cybersecurity Framework, ISO/IEC 2700, CIS Critical Security Controls

1.3 Explain vulnerabilities, threats, and common attacks

- Vulnerabilities, threats, exploits, and risks; types of attackers; reasons for attacks; attack vectors
- Types of attacks: Malware, brute force, website, application, and adversarial attacks (SQL injection, input data manipulation, and buffer overflow), privilege escalation, ransomware, denial of service/DDoS, botnets, physical attacks, man-in-the-middle, IoT vulnerabilities, insider threats, Advanced Persistent Threat (APT), spoofing

1.4 Recognize social engineering attacks

- Tailgating and impersonation
- Spear phishing, phishing, vishing, smishing, whaling, watering holes, pharming, etc.
- Malicious redirection (QR codes, shortened URLs, and fake websites)
- Increased attack sophistication due to the use of AI and bots

1.5 Explain access management principles and procedures

- Authentication, authorization, and accounting (AAA); RADIUS; methods of multifactor authentication (MFA); password policies; biometric authentication; cloud-based resource sharing

1.6 Explain how encryption protects the confidentiality and integrity of data

- Asymmetric and symmetric encryption, hashing; certificates; public key infrastructure (PKI); strong vs. weak encryption algorithms; encryption used for data in transit, data at rest, and data in use

2. Securing the Network

2.1 Identify vulnerabilities associated with commonly used protocols

- TCP, ARP, ICMP, DHCP, DNS, SMTP, ND, CDP/LLDP, SNMP, syslog
- HTTP/HTTPS, FTP/SFTP, Telnet/SSH

2.2 Describe the role of addressing in network security

- Network segmentation (DMZ, VLANs),
- NAT; public vs. private networks; internal, external, and trusted networks

2.3 Describe the purpose and function of network security technologies

- Honeypot, proxy server, IDS, IPS, captive portal, types of firewalls (stateful, stateless), ACLs
- VPN, NAC, remote desktop tools
- Cloud security infrastructure (VPC and security groups)
- Input validation, malware detection, spam filtering, adversarial training, data sanitization

2.4 Validate the security of wireless networks

- MAC address filtering; wireless encryption standards and protocols, SSID

2.5 Examine network security logs to identify anomalies

- firewall logs, IDS/IPS logs

3. Securing Endpoint Devices

3.1 Apply security settings to harden operating systems

- Operating Systems: Windows, macOS, and Linux
- Windows Defender, file and directory permissions, privilege escalation, file and drive encryption, using CIS benchmarks

3.2 Use endpoint tools to gather security assessment information

- netstat, nslookup, nmap, zenmap, ss

3.3 Use packet capture utilities to identify anomalies

- Wireshark, tcpdump

3.4 Demonstrate familiarity with endpoint security policies and standards

- Regulatory compliance (PCI DSS, HIPAA, GDPR), BYOD, device management (verify status of Windows Updates, application updates, device drivers, firmware, and patches), configuration management

3.5 Interpret system logs to identify anomalies

- Event Viewer, console, audit logs, system and application logs, syslog
- Server and end user devices

3.6 Perform malware removal

- Scanning systems, reviewing scan logs, malware remediation, understanding that malware can infect restore points and backups, malware incident response (containment, quarantine, treatment, and inoculation)

INFORMATION TECHNOLOGY
SPECIALIST

4. Vulnerability Assessment and Risk Management

4.1 Use threat intelligence sources to identify potential network vulnerabilities

- Uses and limitations of vulnerability databases; Common Vulnerabilities and Exposures (CVEs), cybersecurity reports, cybersecurity news, subscription services, and collective intelligence; ad hoc and automated threat intelligence; the importance of updating documentation and other forms of communication proactively before, during, and after cybersecurity incidents; how to secure, share, and update documentation

4.2 Explain risk management

- Vulnerability vs. risk, approaches to risk management, risk mitigation strategies, levels of risk severity (low, medium, high, extremely high), likelihood of occurrence, risks associated with specific types of data and data classifications, security assessments of IT systems (information security, change management, computer operations, information assurance)

4.3 Explain the penetration testing process

- Vulnerability identification, reporting results to stakeholders, and making recommendations for mitigation; active and passive reconnaissance; testing (port scanning and automation);
- Testing an application for vulnerabilities before deployment (Dynamic Application Security Testing (DAST) and Static Application Security Testing (SAST))

5. Incident Handling

5.1 Monitor security events to determine if escalation is required

- Role of SIEM and SOAR, identifying suspicious events as they occur, differentiating between a true or false positive, differentiating between a true or false negative

5.2 Explain the digital forensics process and attack frameworks

- Sources of evidence (artifacts); evidence handling (preserving digital evidence, chain of custody)
- Cyber Kill Chain, MITRE ATT&CK Matrix, Diamond Model; Tactics, Techniques, and Procedures (TTP); Pyramid of Pain

5.3 Explain the elements of cybersecurity incident response

- Policy, plan, and procedure elements; incident response lifecycle stages (NIST Special Publication 800-61 sections 2.3, 3.1-3.4)
- Impact of compliance frameworks (GDPR, HIPAA, PCI-DSS, FERPA, FISMA) on notification and reporting requirements

5.4 Explain the importance of disaster recovery and business continuity planning

- Natural and human-caused disasters, features of disaster recovery plans (DRP) and business continuity plans (BCP), all types of data backups, hot and cold spares, disaster recovery controls (detective, preventive, and corrective)

5.5 Assist users in restoring data after an incident

- Restore points, restoring from cloud storage, Recovery Point Objective, Recovery Time Objective, hot, warm, and cold standby