



2.0 Security

2.1 Summarize various security measures and their purposes.

- Physical security
 - Bollards
 - Access control vestibule
 - Badge reader
 - Video surveillance
 - Alarm systems
 - Motion sensors
 - Door locks
 - Equipment locks
 - Security guards
 - Fences
- Physical access security
 - Key fobs
 - Smart cards
 - Mobile digital key
 - Keys
- Biometrics
 - Retina scanner
 - Fingerprint scanner
 - Palm print scanner
 - Facial recognition technology (FRT)
 - Voice recognition technology
- Lighting
- Magnetometers
- Logical security
 - Principle of least privilege
 - Zero Trust model
 - Access control lists (ACLs)
 - Multifactor authentication (MFA)
 - Email
 - Hardware token
- Authenticator application
- Short Message Service (SMS)
- Voice call
- Time-based one-time password (TOTP)
- One-time password/passcode (OTP)
- Security Assertions Markup Language (SAML)
- Single sign-on (SSO)
- Just-in-time access
 - Privileged access management (PAM)
- Mobile device management (MDM)
- Data loss prevention (DLP)
- Identity access management (IAM)
- Directory services

2.2 Given a scenario, configure and apply basic Microsoft Windows OS security settings.

- Defender Antivirus
 - Activate/deactivate
 - Update definitions
- Firewall
 - Activate/deactivate
 - Port security
 - Application security
- User and groups
 - Local vs. Microsoft account
 - Standard account
 - Administrator
 - Guest user
 - Power user
- Log-in OS options
 - Username and password
 - Personal identification number (PIN)
 - Fingerprint
 - Facial recognition
 - SSO
 - Passwordless/Windows Hello
- NTFS vs. share permissions
 - File and folder attributes
 - Inheritance
- Run as administrator vs. standard user
- User Account Control (UAC)
- BitLocker
- BitLocker-To-Go
- Encrypting File System (EFS)
- Active Directory
 - Joining domain
 - Assigning log-in script
 - Moving objects within organizational units
 - Assigning home folders
 - Applying Group Policy
 - Selecting security groups
 - Configuring folder redirection



2.3 Compare and contrast wireless security protocols and authentication methods.

- Protocols and encryption
 - Wi-Fi Protected Access 2 (WPA2)
 - WPA3
 - Temporal Key Integrity Protocol (TKIP)
 - Advanced Encryption Standard (AES)
- Authentication
 - Remote Authentication Dial-in User Service (RADIUS)
 - Terminal Access Controller Access-control System (TACACS+)
 - Kerberos
 - Multifactor

2.4 Summarize types of malware and tools/methods for detection, removal, and prevention.

- Malware
 - Trojan
 - Rootkit
 - Virus
 - Spyware
 - Ransomware
 - Keylogger
 - Boot sector virus
 - Cryptominer
 - Stalkerware
 - Fileless
- Adware
 - Potentially unwanted program (PUP)
- Tools and methods
 - Recovery console
 - Endpoint detection and response (EDR)
 - Managed detection and response (MDR)
 - Extended detection and response (XDR)
- Antivirus
- Anti-malware
- Email security gateway
- Software firewalls
- User education regarding common threats
 - Antiphishing training
- OS reinstallation

2.5 Compare and contrast common social engineering attacks, threats, and vulnerabilities.

- Social engineering
 - Phishing
 - Vishing
 - Smishing
 - QR code phishing
 - Spear phishing
 - Whaling
 - Shoulder surfing
 - Tailgating
 - Impersonation
 - Dumpster diving
- Threats
 - Denial of service (DoS)
 - Distributed denial of service (DDoS)
 - Evil twin
 - Zero-day attack
 - Spoofing
 - On-path attack
 - Brute-force attack
 - Dictionary attack
 - Insider threat
 - Structured Query Language (SQL) injection
- Cross-site scripting (XSS)
- Business email compromise (BEC)
- Supply chain/pipeline attack
- Vulnerabilities
 - Non-compliant systems
 - Unpatched systems
 - Unprotected systems (missing antivirus/missing firewall)
 - EOL
 - Bring your own device (BYOD)



2.6 Given a scenario, implement procedures for basic small office/home office (SOHO) malware removal.

- | | | |
|---|--|---|
| <ol style="list-style-type: none"> 1. Investigate and verify malware symptoms. 2. Quarantine infected system. 3. Disable System Restore in Windows Home. | <ol style="list-style-type: none"> 4. Remediate infected systems. 5. Update anti-malware software. 6. Scan and removal techniques (e.g., safe mode, preinstallation environment) 7. Reimage/reinstall. | <ol style="list-style-type: none"> 8. Schedule scans and run updates. 9. Enable System Restore and create a restore point in Windows Home. 10. Educate the end user. |
|---|--|---|

2.7 Given a scenario, apply workstation security options and hardening techniques.

- | | | |
|--|---|--|
| <ul style="list-style-type: none"> • Data-at-rest encryption • Password considerations <ul style="list-style-type: none"> – Length – Character types – Uniqueness – Complexity – Expiration • Basic input/output system (BIOS)/Unified Extensible Firmware Interface (UEFI) passwords | <ul style="list-style-type: none"> • End-user best practices <ul style="list-style-type: none"> – Use screensaver locks – Log off when not in use – Secure/protect critical hardware (e.g., laptops) – Secure personally identifiable information (PII) and passwords – Use password managers • Account management <ul style="list-style-type: none"> – Restrict user permissions | <ul style="list-style-type: none"> – Restrict log-in times – Disable guest account – Use failed attempts lockout – Use timeout/screen lock – Apply account expiration dates • Change default administrator's user account/password • Disable AutoRun • Disable unused services |
|--|---|--|

2.8 Given a scenario, apply common methods for securing mobile devices.

- | | | |
|---|---|--|
| <ul style="list-style-type: none"> • Hardening techniques <ul style="list-style-type: none"> – Device encryption – Screen locks <ul style="list-style-type: none"> ◦ Facial recognition ◦ PIN codes ◦ Fingerprint ◦ Pattern ◦ Swipe – Configuration profiles | <ul style="list-style-type: none"> • Patch management <ul style="list-style-type: none"> – OS updates – Application updates • Endpoint security software <ul style="list-style-type: none"> – Antivirus – Anti-malware – Content filtering | <ul style="list-style-type: none"> • Locator applications • Remote wipes • Remote backup applications • Failed log-in attempts restrictions • Policies and procedures <ul style="list-style-type: none"> – MDM – BYOD vs. corporate-owned devices – Profile security requirements |
|---|---|--|

2.9 Compare and contrast common data destruction and disposal methods.

- | | | |
|--|--|---|
| <ul style="list-style-type: none"> • Physical destruction of hard drives <ul style="list-style-type: none"> – Drilling – Shredding – Degaussing – Incineration | <ul style="list-style-type: none"> • Recycling or repurposing best practices <ul style="list-style-type: none"> – Erasing/wiping – Low-level formatting – Standard formatting | <ul style="list-style-type: none"> • Outsourcing concepts <ul style="list-style-type: none"> – Third-party vendor – Certification of destruction/recycling • Regulatory and environmental requirements |
|--|--|---|

**2.10** Given a scenario, apply security settings on SOHO wireless and wired networks.

- Router settings
 - Change default passwords
 - IP filtering
 - Firmware updates
 - Content filtering
 - Physical placement/secure locations
 - Universal Plug and Play (UPnP)
- Screened subnet
- Configure secure management access
- Disabling SSID broadcast
- Encryption settings
- Configuring guest access
- Wireless specific
 - Changing the service set identifier (SSID)
- Firewall settings
 - Disabling unused ports
 - Port forwarding/mapping

2.11 Given a scenario, configure relevant security settings in a browser.

- Browser download/installation
 - Trusted sources
 - Hashing
 - Untrusted sources
- Browser patching
- Extensions and plug-ins
 - Trusted sources
 - Untrusted sources
- Password managers
- Secure connections/sites–valid certificates
- Settings
 - Pop-up blocker
 - Clearing browsing data
 - Clearing cache
 - Private-browsing mode
 - Sign-in/browser data synchronization
- Ad blockers
- Proxy
- Secure DNS
- Browser feature management
 - Enable/disable
 - Plug-ins
 - Extensions
 - Features