STUDY GUIDE NOTES - PART 2 (CH.11-CH.17)

CHAPTER 11: ENDPOINT SECURITY

OPERATING SYSTEM VULNERABILITIES:

- OS vulnerabilities
- Default passwords
- Configurations
- Misconfigurations

HARDWARE VULNERABILITIES:

- Firmware (many pathways)
- EOL (end of life) AKA End of sales, End of support, legacy

PROTECTING ENDPOINTS:

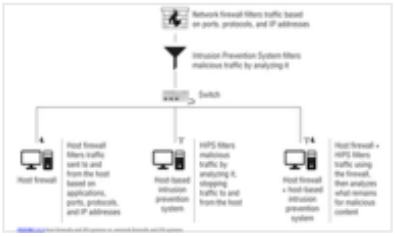
- Endpoint: any device at the endpoint of a network (very broad)
- HSM (Hardware Security Modules): for multiple systems, external devices for creating, storing, and managing digital keys for cryptographic functions
  - FIPS 140 (Federal Information Processing Standards) or Common Criteria (ISO/IEC 15408)
- KMS (Key Management Systems): store and manage keys and certificates while enforcing policies
- TPMs: system security

  - Hardware root of trust options:
    1. UEFI (Unified Extensible Firmware Interface) does secure boot from OEM (original equipment manufacture)
       - replaced originally BIOS (Basic Input/Output System)
    2. Measured boot: TPM (Trusted Platform Module) stores hashed value of secured boot state and compares it to hashed values
  - TPM functions: provides built-in encryption on computer chips
    - Remote attestation
    - Binding —> encrypts data
    - Sealing —> encrypts data + sets state of TPM chip before decryption
  - Alternatives to TPM:
    - Serial Numbers that cannot be modified
    - PUFs (Physically inclinable functions): specific hardware devices
    - Secure Enclave: Apple’s system on a chip (SoC) modules —> isolated from main CPU

- Example: Google's Titan M, Samsung's TrustZone

ENDPOINT SECURITY TOOLS:

- AV (antivirus): AKA antimalware tools
  - Can be installed on any endpoint device
  - Enterprise commonly deploy more than one
- Signature-based detection: hash or pattern-based detection
- Heuristic (behavior) based detection
- AI/ML
- Sandboxing: isolate, test, and document malicious code
- Allow and Deny Lists (AKA whitelist, block list, blacklist): controls what applications can or cannot be installed
  - Allow list stronger than a deny list
  - Takes too much effort for enterprise
- EDR (Endpoint Detection and Response): look for IoCs (Indicators of Compromise) and manual investigation —> useful took for large enterprises
- XDR (Extended Detection and Response): broader than just endpoints —> cloud, security, email, tech stack
- DLP (Data Loss Prevention): classifies data, data labeling/tagging, policy enforcement, monitoring
  - Some encrypt data automatically when its sent outside
  - Tracks sus behavior
- Network Defenses:
  - Host-based firewalls: simple block or allow function on most OSs
  - NIPS: Network-based IPS —> monitors the entire network
  - HIPS (host-based intrusion prevention system): monitors a single host for malicious activity, analyzes traffic before host processes it —> can potentially block legit traffic
  - HIDS (Host-based intrusion detection system): cannot block, only detect, for real-time security, wont cause issues$



HARDENING TECHNIQUES:

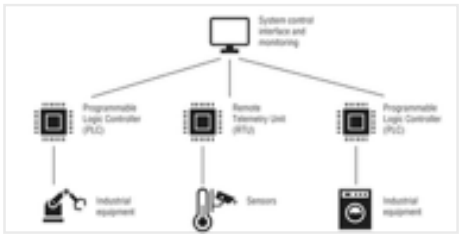
- Hardening: changing settings to increase overall security
  - Disabling ports and protocols: reduces attack surface

        - Example: Windows Services.msc, Linux is service—status-all, Ubuntu is update-rc.d script, RedHat is chkconfig
    - VLAN for network hardening
    - Change default passwords
    - Remove unnecessary software
- CIS (Center for Internet Security) benchmarks for hardening Windows:
    - Setting password history to remember 24 or more passwords
    - Setting maximum password age to "365 days or fewer but not 0"
    - Setting minimum password length
    - Requiring password complexity
    - Disable storage of passwords
- Hardening Windows Registry: configuring permissions, limiting access
- Windows GPO (Group Policy Objects) Hardening: system and domain controls via policy
    - Example: SCT (Security Compliance Toolkit): security baseline config
- Hardening SELinux (Security-Enhanced Linux): SELinux is a linux kernel based security module that provides more capabilities than a traditional Linux
- Configuration Management: make sure they have the right security settings
    - Examples: Jamf Pro (Mac), Configuration Manager (Windows), CFEngine (Open Source)
    1. Baseline Configurations: ideal starting place
        1. Establish baseline
        2. Deploy
        3. Maintain
    2. Configuration Enforcement: monitors and makes changes as needed
- Patch Management:
    - Example: Microsoft's Configuration Manager
    - Most orgs delay installation of a patch a few days after its release
    - Key features of patch management: reporting, ability to choose and block an update
- Encryption:
    - FDE (full disk encryption)
    - Volume encryption (AKA filesystem-level encryption)
    - SED (self-encryption drive): encryption implemented in hardware/firmware
        - Weakness: find a logged-in system or sleep mode. If password is lost, hard to brute force
    - Transparent encryption (AKA on-the-fly, real-time encryption): drive appears unencrypted to user

SECURING EMBEDDED SYSTEMS:

- Embedded system: computers built into other devices (ex: Industrial, appliances, cars, watch)
- RTOS (real-time operating systems)
  - CAN messages: messages with the car
- ICS (Industrial controls systems): industrial automation
- SCADA (supervisory control and data acquisition): large industrial systems
- RTU (remote telemetry units): microprocessors collecting data for SCADA

- Assessing embedded systems:
  - Identity supply chain
  - Trace network activity
  - Identify its services
  - Firmware
  - Document risk plan
  - Document research findings
- Common embedded systems:
  - Medical devices
  - Smart meters
  - Vehicles: cars (controller area network CAN buses), aircrafts, ships
  - Drones and AVs (autonomous vehicles)
  - VoIP
  - MFPs (multifunctions printers): act as reflectors, amplifiers, and pivot points for attackers
  - Surveillance systems
- SCADA and ICS:
  -



SECURING IOT:

- Enumeration: scanning to identify assets

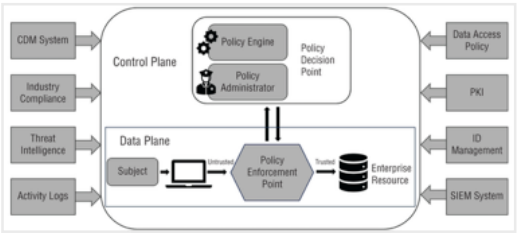
- IoT leverage AI/ML, cloud services to provide “smart services”
- IoT Security Concerns:
  - Poor security practice
  - Short support lifespans —> no patches

    - Vendor data-handling
    - Example: US banned fitness trackers in war zones and sensitive facilities
- Communication Security for IoT:
    - Cellular connectivity: LTE & 5G
    - SIM (Subscriber Identity Module): SIM cloning, physically removing
    - Zigbee: radio frequency
- Security Constraints for Embedded Systems:
    - Low CPU, memory —> no security tools
    - No internet —> inability to patch, secured as independent unit
    - No authentication
    - Hard to replace
    - Embedded systems rely on Implied Trust —> must be reviewed before deploying
- Asset Management Life Cycle:
    1. Inventory
    2. Tracking
    3. Decomissioning: removing device/system from service + inventory + no sensitive data left via sanitizing drives
        - DBAN (Darik's Boot and Nuke): performs multiple passes over a disk
        - FDE and then discard encryption key
        - Certification: certifies proper destruction
        - Banning hand-me-downs
    - Retention: legal or business hold

CHAPTER 12: NETWORK SECURITY

DESIGNING SECURE NETWORKS:

- DID (Defense-in-depth): multiple controls to prevent a SPOF
- OSI (Open Systems Interconnection) model: conceptual model on how devices and software operate via networks
    - L1: Physical layer
    - L2: Data link layer
    - L3: Network layer (firewalls, IPSec)
    - L4: Transport layer
    - L5: Session Layer
    - L6: Presentation Layer
    - L7: Application layer

- ZTA (Zero Trust Architecture): control plane + data plane
    - Policy Engine —> Policy Administrator —> Policy Engine
    - 

    - Policy Engines: makes policy decisions
    - Policy Administrator: establish or remove communication between subjects and resources
    - Policy Enforcement Points: communicate with policy admins to forward requests between subjects and receive instructions
    - Subjects: users
- Control Plane:
    1. Adaptive Identity (adaptive authentication): leverages context, may request additional info
    2. Threat scope reduction (AKA limited blast radius)
    3. Policy-driven access control
    4. The Policy Administrator
- Data Plane:
    1. Implicit trust zones: allow movement once authenticated
    2. Subject/system
    3. Policy Enforcement Points
- NAC (Network Access Controls): determines whether or not a system or device should be allowed to connect to a network
    - Agent vs Agentless (agent is better)
    - Pre admission vs post admission
- 802.1X: standard for authenticating devices to wired and wireless networks —> connecting to ports must have 802.1X supplicant
- CAM (content-addressable memory)

- Infrastructure Considerations:
    - Attack surface
    - Device placement: placing them on the correct network/segment
    - Security zones: virtual network segments
    - Connectivity considerations: redundant connections, how fast, what type of connectivity
    - Failure modes: fail-closed vs fail-open
    - Network taps: active or passive
- Network Design Concepts:
    - Physical isolation (AKA air-gapped) —> can be overcome by

removable drives copying itself (ex: Student malware attack)
  - Logical segmentation: done via software/settings
    - Example: VLANs
  - HA (high availability)
  - Implementation of secure protocols: HTTPS (TLS), SSH.
    - Using other obscure ports are not the answer
  - Transport method: choosing secure protocols like TLS
  - Reputation services: tracks and blocks hosts that engage in malicious activity
  - SDN (Software-Defined Networking)
  - SD-WAN (software-defined wide area network): virtual wide area network design that combines many services for organizations
    - Examples: MPLS (Multi-protocol Label Switching) —> SD-WAN, 4G, 5G
  - SASE (Secure Access Service Edge): private networks + SD-WAN + firewalls + CASBs + zero trust networks —> secure access for devices regardless of location

NETWORK SEGMENTATION:

- Network Segmentation: dividing network into logical or physical groupings
  - Example: VLAN (segmented at L2)
  - Broadcast domain: a way to “broadcast” to all machines on the network tho

  - Types of Network Segmentation:
    1. DMZ (demilitarized zones) also called screened subnets: less trusted zones
    2. Intranet: internal network, usually protected from external access
    3. Extranets: external network between partner and customer
    4. ZTA (Zero Trust Architecture): each action is validated when requested
  - Port Security: limits # of MAC addresses on a single port
    - Prevents: MAC address spoofing, CAM (content-addressable memory) table overflows
    - Originally invented by Cisco. Used by many other vendors now too
    - Also prevents: Loop prevention, Broadcast storm prevention (AKA storm control)
    - BPDU (Bridge Protocol Data Unit): protects STP from sending messages it should not
    - DHCP (Dynamic Host Configuration Protocol) snooping: prevents rogue DHCP server from handing out IP addresses

VPNS:

- VPN (Virtual Private Network): virtual network link across a public network

  - Types of VPN Technology:
    1. IPSec VPNs (OSI L3): site-to-site VPNs and for VPNs that need more than web and app traffic
       - Tunnel: entire packet sent to other VPN
       - Transport: IP header not protected but IP payload is
    2. SSL VPNs (technically TLS):
       - Portal-based (HTML 5)
       - Tunnel mode (like IPSec VPN)
       - No client installation required
  - VPN Decision Points:
    - Full-tunnel VPNs: secure network between two channels, always on
    - Site-to-site VPNs: as needed, for remote work
    - Tunneling: Split-tunnel VPN vs full-tunnel VPN
      - Split-tunnel VPN: sends only needed data, less bandwidth
      - Full-tunnel VPN: sends all data

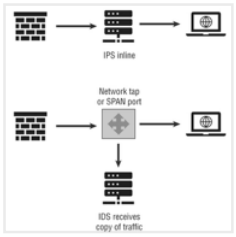
NETWORK APPLIANCES AND SECURITY TOOLS:

- Jump Servers (AKA jump boxes): securely operate in two different security zones via SSH or RDP
- Load Balancing: distribute traffic to multiple systems, provide redundancy, ease of upgrade/patching via VIP (Virtual IP)
- NGFW (next gen firewalls): interact with traffic at OSI L4 and L7 but need more CPU + memory
- Proxy Servers: accept and forward requests
  - Forward proxies: between client —> servers, cancel identity of original client
  - Reverse proxies: between client and servers for load balancing and caching of content
- Web Filters (AKA content filters): centralized proxy servers allowing or blocking traffic based on content rules
- URL (Uniform Resource Locator) scanning: allow or deny lists as well content rules
  - Centralized proxy on a hardware device
  - Content categorization: adult/business/child-friendly —> block rules
- Stateless Firewalls (AKA packet filers): most basic firewall, filters every packet's header
- Stateful Firewalls (AKA dynamic packet filers): track packets, make smart

decisions

- NGFW (Next gen firewalls): all-in-one-network security devices (deep packet inspection, IDS/IPS, AV) —> faster than UTMs because focused but more config time
- UTM (unified threat management): firewall, IDS/IPS, AV, URL/email filtering, DLP, analytics —> “out of the box” solution
  - Deployed at boundaries
  - Many UTMs at once
- WAFs (web application firewalls): database queries, APIs, and other web app tools —> firewall + IPS, blocks attacks in real time
- Screen subnets: connect to Internet, create secured area, create public area (DMZ)
- ACLs (Access Control Lists): allow or deny lists
  - Time-based ACLs
  - Dynamic ACLs

- Network Considerations:
  - Hardware: purpose-built, high-speed traffic
  - Software: virtual machines easily deployed and scaled
  - Cloud appliances: dynamically created, scaled, and used as needed
- Network Security Configuration decisions:
  - Inline: network traffic pass directly through them (fail-open vs fail-close)
  - Taps: replicate traffic for inspection —> monitoring/analysis/security
    1. Active: requires power, direct path
    2. Passive: no power, direct path
    3. SPAN port or mirror port: less secure
- Load Balancer Modes:
  - Active/active: sends to multiple systems at the same time —> ensures a single node won’t be overwhelmed
  - Active/passive: brings backups online when active systems fail —> for DRP
- Load Balancing Algorithms:
  - Round-robin
  - Least connection: sends traffic to the server with fewest active connections
  - Agent-based: adaptive balancing
  - Source IP Hashing: randomization
  - Persistent sessions: client and server communicate throughout the duration of a session
- Weighted Algorithms:
  - Weighted Least connection

    - Fixed weighted
    - Weighted response
- IDS + IPS: active vs passive (passive IPS is basically an IDS)
    - Signature-based
    - Anomaly-based AKA behaviors
    - 

- Firewall rules:
    - Source: IP, hostnames, or domains
    - Ports and protocols
    - Allow or deny statements
    - Destination IP addresses
    - Host or hosts
    - Domain with ports and protocols
- Types of Deception/Disruption tools:
    1. Honeypots
    2. Honeyfiles
    3. Honeytokens
    4. Honeynets

NETWORK SECURITY, SERVICES, AND MANAGEMENT:

- Out of band management: remotely access and manage devices and infrastructure
- DNS (domain-name system): only tells WHERE to send traffic —> not inherently secure
- DNSSEC (DNS System Security Extensions): provides authentications of DNS data
- DNS filtering: blocks malicious domains via lists
- DKIM (DomainKeys Identified Mail): signature header to verify email sender
- SPF (Sender Policy Framework): allow list for email domains. If not on the list —> rejected
- DMARC (Domain-based Message Authentication Reporting and Conformance): determine whether you should refuse or accept email message
- Email Security Gateways: phishing protecting, email encryption, attaching sandboxing to counter malware, randomware protection, URL analysis
- Ephemeral Keys: perfect forward key secrecy —> even if key exchange is

compromised, communication will not
- IPv6: relies heavily on ICMP
- SNMP (Simple Network Management Protocol): monitor and manage network devices
  - MIB (management information base): where an MIB is listed
  - SNMP trap (message when device encounters an error) —> SNMP agent —> SNMP manager
- File Integrity monitor: detects changes in files and either reports or restores them
  - Example: Tripwire —> creates digital signature and tracks changes

- Monitoring Systems:
  - Is service port open?
  - What should a valid response look like?
  - Likely failures?
- Hardening Network Devices:
  - CIS (Center for Internet security): provides network device hardening guides for switches and routers
  - Protect management console —> isolated VLAN, jump server, VPN
  - Physical security

USING SECURE PROTOCOLS:
- Insecure protocols: DHCP, NTP, BGP

- Voice, Video, & Videoconferencing:
  - HTTPS
  - SIPS (Session Initiation Protocol [Secured])
  - SRTP ([Secure] Real-time Transport Protocol)
- NTP (Network Time Protocol) —> NTS, relies on TLS, does not protect time data but focuses on authentication
- Email and web:
  - SMTP
  - HTTPS
  - IMAPS
  - POPS
  - DMARC, DKIM, SPF
- FTP has been replaced by HTTPS and SFTP or FTPS
- LDAP —> LDAPS
- Remove access technologies:
  - Telnet —> SSH
  - Microsoft's RDP
- DNS: still a big security issue

    - DNSSEC: digital signatures to provide integrity not confidentiality
    - DNS filtering/reputation lists
- Routing and Switching:
    - BGP (Border Gateway Protocol): lacks built-in features —> susceptible to BGP hijacking
- Network address allocation:
    - DHCPL not secure —> need detection and response
- Subscription services: HTTPS

SECURE PROTOCOLS TO REMEMBER FOR EXAM:

- DNSSEC (Domain Name System Security Extension): provides integrity via digital signatures, not confidentiality
- SNMPv3 (Simple Network Management Protocol version 3): authenticating message sources, message integrity validation, and confidentiality
- SSH (Secure Shell): protocol for remote console access to devices, also a tunneling protocol, also supports other applications, also SSH keys
- HTTPS (Hypertext Transfer Protocol Secure): relies on TLS to provide security
- SRTP (Secure Real-Time Protocol): provides audio and video streams via networks, encryption and authentication
- LDAPS (Secure Lightweight Directory Access Protocols): provides confidentiality and integrity to LDAP
- S/MIME (Secure/Multipurpose Internet Mail Extensions): secure email attachments while providing authentication, integrity, nonrepudiation and confidentiality to S/MIME messages
    - Less frequently used due to needing CA
- FTPS (File Transfer Protocol via TLS)
- SFTP (File Transfer Protocol via SSH): easier to penetrate
- IPSec (Internet Protocol Security): entire suite of security protocols —> used for VPNs
    - AH (Authentication Header): hashing + shared secret key = IP payload is secured
    - ESP (Encapsulating Security Payload): tunnel mode - entire packet secured, transport mode - only payload secured
    - SAs (Security Associations): provides parameters for ESP & AH to operate
        - IKE (Internet Key Exchange): setup using X.509 certificates
        - ISAKMP (Internet Security Association and Key Management Protocol)

NETWORK ATTACKS:

- MITM (man in the middle): on-path attacks
- MITB/MIB (man in the browser): browser-based on-path attack
- Amplified DoS Attack: taking advantage of small query —> large result (ex: DNS query)
- Reflected DoS Attack: spoofing IP address to conduct an attack

- On-Path Attacks (MITM): attacker intercepts traffic
  - SSL Stripping: user sends an HTTP request to a server, attacker responds through communications they control allowing them to take control (common via wireless networks)
    - Normal HTTP request: user sends HTTP request, server responds with HTTPS version, user sends HTTPS request
    - Can be prevented by a CA
    - HSTS (HTTP Strict Transport Security) forces all connections to be HTTPS but only after you visit at least once
  - Browser-based attack (MITB): trojan inserted into browser
- Domain Name System Attacks:
  - Domain Hijacking: changes the registration for a domain
  - DNS poisoning: via on-path attacks, via poisoning cache
  - URL redirection: via inserting alternate IP address
  - DNSSEC + Domain reputation (trusted domain?) = protection
- Malicious code via networks: worms, backdoors via network, viruses, Trojans, ransomware
- Credential Replay Attack: network attack capturing data —> modify, re-send hashes, re-use session IDs
- DDoS Attacks:
  - Network DDoS:
    - UDP floods
    - ICMP Floods (AKA ping floods)
    - SYN floods: attempting handshake but never respond back —> TCP stack resources exhausted
    - Ping of death: ping packet too large to handle
    - Smurf attacks: spoofed sender address via ICMP broadcast messages

---

CHAPTER 13: WIRELESS AND MOBILE SECURITY

BUILDING SECURE WIRELESS NETWORKS:

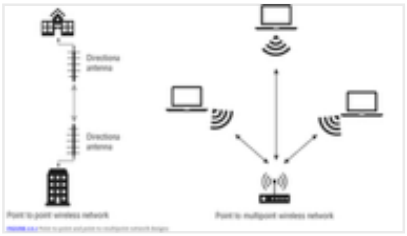
- BYOD (Bring your own device)

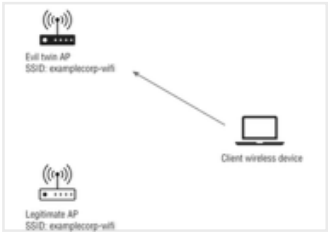
- CYOD (Choose your own device)
- COPE (corporate-owned, personally enabled)
- Cellular: divides geographic areas into “cells”
  - LTE (long-term evolution) current is 4G & 5G
- Wi-Fi (wireless fidelity): 2.4 GHz and 5 GHz
  - WPA2/WPA3: encryption options, protection for network frames, authentication options
- Bluetooth: 2.4 GHz, 5-30 meters, point-to-point pairing, no encryption but has PIN
  - Security Mode 1: No-security
  - Security Mode 2: service-level enforced security
  - Security Mode 3: Link-level enforced security
  - Security Mode 4: Standard pairing with Security Simple Pairing (SSP)
- RFID (Radio frequency identification): uses a tag and receiver —> active tags vs. Sem-active tags vs. passive tags
  - Low frequency RFIDs: short-range, low power
  - High frequency RFIDs: longer readable range —> used for NFCs
  - Ultra-high frequencies: fastest to read + longest range
- GPS (Global Positioning System): uses satellite network (ex: U.S. GPS system, Russian GLONASS) —> used for Geolocation authentication, geofencing
- NFC (near-field communication): very short-range communication (4 inches) between devices (ex: Apply Pay, Google Pay)
- IR (Infrared): only work in line-of-sight (speeds from 115 Kbit/s to 1 Gbit/s)

- Other types of wireless networks: Bluetooth, Cellular, Zigabee
- Wireless Network Models:
  - Point-to-point: connects two nodes
  - Point-to-multipoint: Wi-Fi, many nodes receiving information sent by a single node
  - Mesh
  - Broadcast: send out information and do not care about receiving a response (ex: GPS, radio)

WI-FI STANDARD	GENERATION NAME	MAXIMUM SPEED	FREQUENCIES
802.11b		11 Mbit/s	2.4 GHz
802.11a		54 Mbit/s	5 GHz
802.11g		54 Mbit/s	2.4 GHz

802.11n	Wi-Fi 4	600 Mbit/s	2.4 GHz and 5 GHz
802.11ac	Wi-Fi 5	6.9 Gbit/s	5 GHz
802.11ax	Wi-Fi 6 and Wi-Fi 6E	9.6 Gbit/s	2.4 GHz, 5 GHz, 6 GHz
802.11be	Wi-Fi 7	40+ Gbit/s	2.4 GHz, 5 GHz, 6 GHz





ATTACKS AGAINST WIRELESS NETWORKS AND DEVICES:

- Evil twin: malicious access point trying to appear legitimate
- Rogue access points: Ads added to network either intentionally or unintentionally
- Disassociation: device disconnects from access point by sending an AP a deauthentication frame by spoofing victim's MAC address
  - Wi-Fi deauthers: sneds deauthentication frames
- Jamming: block traffic in range or frequency
  - Jammers: drown out signal
- Sideloading: process of transferring files to a mobile device via USB connection/MicroSD card/Bluetooth OUTSIDE of App Store
- Jailbreaking: privilege escalation, root access, installing apps/custom elements to OS

- Bluetooth Attacks: best security is to turn off bluetooth
  - Bluejacking: sending unsolicited messages
  - Bluesnarfing: unauthorized access to a bluetooth device to gather info
  - BIA (Bluetooth Impersonation attacks): exploit mutual authentication

DESIGNING A NETWORK:

- Careful WAP placement
- Site Surveys
- Heatmap: how strong a signal is
- WLAN (Wireless local area network): manage access points and the organization's wireless network
    - Hardware/cloud service/virtual machine/software package
    - Advanced WLAN features: security features, threat intelligence, intrusion prevention
- RADIUS (Remote Authentication Dial-In User Service): allows servers to be federated
    - Example: Eduroam is a federated higher education institution

- 2.4 GHz Band:
    - Each channel is 20 MHz wide
    - 5 MHz space in between
    - 11 channels in 2.4 GHz Wi-Fi deployment
- WPA2:
    - WPA2-Personal (WPA2-PSK): pre-shared key, allows client to authenticate with a server infrastructure
    - WPA2-Enterprise: relies on RADIUS as part of 802.1X
    - CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol): uses AES to provide confidentiality
        - Provides authentication for user and access control capabilities
- WPA3: replacement fro WPA2 since 2020
    - SAE (Simultaneous Authentication of Equals): requires client/network to validate both sides
    - Perfect forward secrecy: changes encryption keys on ongoing basis, ensures traffic is secure even if keys change
    - Optional 192-bit security mode
    - Continues to use RADIUS
    - OWE (Opportunistic wireless encryption): provide encrypted Wi-Fi on open networks when possible

WIRELESS AUTHENTICATION:

- 802.1X: IEEE standard for access control for wired/wireless networks
    - Captive Portal: redirects traffic to a website/registration before allowing access (ex: airport, hotel wifi)
    - 802.1X integrated with RADIUS servers —> allows enterprise to authenticate and gain access to network
    - Wireless enterprise networks relies on IEEE 802.1X + EAP when

authenticating to RADIUS server
- EAP variants:
  - PEAP (protected EAP): authenticates servers using certificates and wraps EAP using TLS tunnel
  - EAP-FAST (Flexible Authentication via Secure Tunneling): improves on vulnerabilities in LEAP. FAST provides faster authentication while roaming
  - EAP-TLS (Transport Layer Security): implements certificate-based authentication as well as mutual authentication
    - Used less frequently
  - EAP-TTLS (Tunneled Transport Layer Security): does not require client devices have a certificate to create a secure session bye requiring software

MANAGING SECURE MOBILE DEVICES:
- BYOD (bring your own device)
- CYOD (choose your own device)
- COPE (Corporate owned personally enabled): allows for reasonable personal use since users dont want to carry two phones
- COBO (Corporate Owned Business Only):
- Corporate-owned
- VDI
- Containerization

- Hardening Mobile Devices: patching OS, enabling remote wipe, requiring passcodes, setting automatic screen lock
  - CIS (Center for Internet Security): has benchmarks for iOS and Android hardening
- MDM (Mobile Device Management):
    - Example: DOD bans cell phone use with cameras automatically in their facilities
    - Example 2: Limiting SMS, MMS, or RCS (rich communication services), On-the-go (OTG)
  - UEM (Unified Endpoint Management): combines mobile, devices, desktops, laptops
  - MAM (Mobile Application Management)
  - VPN may be used for BYOD devices
  - Application management: limiting apps, remotely adding, removing, changing applications, monitoring applications
  - Content management (MCM): document/media on mobile devices
  - Remote-wipe capabilities: used when a device is lost/stolen/owner is no longer employed by organization

- Geolocation & geofencing
- Screen locks, passwords, PINs
- Containerization
- Storage segmentation
- FDE (Full-device encryption)
- Push notifications
- OTA (over-the-air)

CHAPTER 14: MONITORING AND INCIDENT RESPONSE

INCIDENT RESPONSE:

- IR (Incident Response): plan, process, team, technology, skills, and training to respond appropriately (ongoing process)
- Incident: violation of organizations policies
- Events: observable occurrence

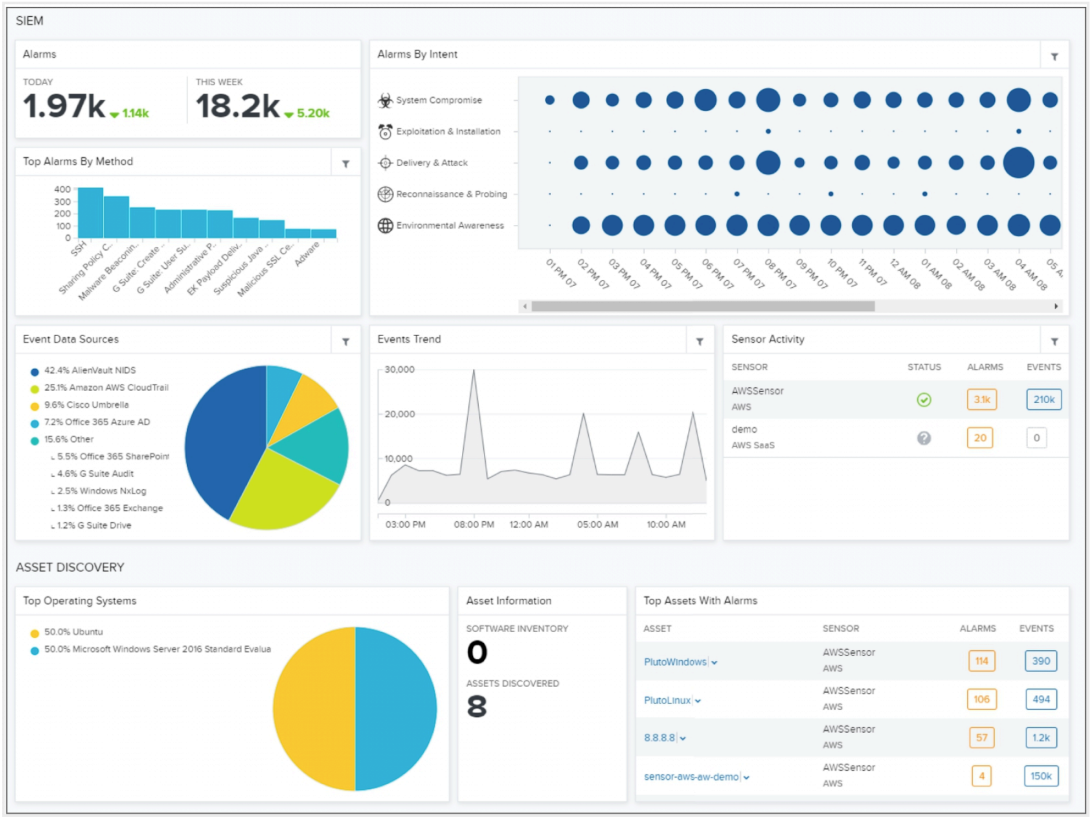
- Incident Response Process (by SANS): PICERL
  1. Preparation: build the tools, processes, procedures to an incident
  2. Identification: IoC, log analysis, security monitoring capabilities
  3. Containment: Quarantine, placing system/device in an isolated network zone
  4. Eradication: removing artifacts from the incident
  5. Recovery: restoration to normal
  6. Lessons Learned
- Incident Response Process (by NIST):
  1. Preparation
  2. Detection and Analysis
  3. Containment, Eradication, and Recovery
  4. Post-incident Activity
- Incident Response Team:
  - Management or leadership
  - Info sec staff are the core
  - Technical experts (sys admin, devs, etc)
  - PR team for internal and external communication
  - Legal and HR
  - Law enforcement
- Exercises:
  - Tabletop exercises
  - Simulations

- Building Incident Response Subplots:
  - Communications plans
  - Stakeholder management plan
  - BC (Business Continuity) plans: making sure business can continue despite the incident, important for larger incidents
  - DR (Disaster Recovery): focuses on natural and human-made disasters that destroys facilities/infrastructure

TRAINING:

- CISA (Cybersecurity & Infrastructure Security Agency): offers IR training for preventing attacks, IoC, managing logs
- IoCs (Indicators of Compromise)
- MITRE ATT&CK: Adversarial Tactics, Techniques, and Common Knowledge (MITRE is a corporation)
  - Pre-attack
  - Enterprise
  - Data sources
  - Threat actor groups/software/host

- Common IoCs:
  - Account lockout: due to brute-force login attempts
  - Concurrent session usage: two locations at once
  - Blocked Content: DNS filter prohibits domains, IP addresses trigger it
  - Impossible travel
  - Resource consumption
  - Resource inaccessibility
  - Out-of-cycle logging: logging in at 2am
  - Missing logs: someone trying to hide their actions
  - Published/documented: IoC that has been published/documented



SIEM:

- SIEM (Security Information and Event Management): the central security monitoring tool.
    - Collects and aggregates log data —> correlation and analysis
    - Review user behavior
    - Older versions: SIM and SEM
- NetFlow Protocol (AKA sFlow): collect IP traffic as it enters or exits interface, developed by Cisco in 1996 —> tracks bandwidth utilization
    - IPFIX: another example of NetFlow v9
    - May lose some resolution in the detail of the flow analysis
- Syslog: logs all activity on a system

- SIEM Dashboards: shows most critical information (ex: AlienVault SIEM)
    - Sensor activity
    - Alarms
    - Events trend

    - Correlation engines and rules
    - Sensitivity
- Sensors: can be software agents, virtual machine, or dedicated device
    - Location: where unique data is being generated (big decision)
    - Must be secured like anything else
- Sensitivity and Thresholds: alerts only activate after a certain amount of times
- Trends: new problem cropping up, detected frequently
- Alerts & Alarms: malware beaconing, infection
    - Alert tuning: modifying alerts to only alarm on important events
    - Alert fatigue: BIGGEST threat to SIEM
- Log Aggregation, Correlation, and Analysis
- Rules: SIEM vendors have default rules but also allow custom-built rules for organizations
    - Follow data for entire life cycle
- Integrations: built-in services like Google, ServiceNow, Office 365, Okta, Sophos
- Log Files: target for attacks, IR watch to make sure log files haven't been tampered
    - Firewall logs: blocked or allowed traffic (NGFW, UTM, IDS/IPS)
    - Application logs: IIS (Internet Information Services) track web server and related events —> helps identify SQL injection
    - Endpoint logs: application logs, system/service logs, endpoint devices
    - OS-specific security logs: failed/successful logins,
- IDS/IPS logs: insight into traffic that was detected/blocked
- Network logs: routers, switches, traffic information, network flows, packet analyzers like Wireshark
- Bandwidth usage
- Logging Protocols and Tools:
    - syslog —> replaced rsyslog (rocket-fast system for log processing)
    - Syslog-ng: enhanced filtering
    - NXLog: open source log system
    - Systemd's Journal in Linux: journlctl —> display journal entries, initrd —> messages
- Retention: logs kept for 30-180 days depending
- Metadata Types:
    - Email metadata: sender, recipient, date/time, attachment, systems, antispam
    - Mobile metadata: call logs, SMS, data usage, GPS location tracking, cellular tower
    - Web metadata: metatarsi, headers, cookies, website functionality
    - File metadata: creation date, how it was created, modified, GPS

location
    - Example: ExifTool —> shows all metadata about photos
- Other data sources:
    - Agents
    - Vulnerability scans
    - Automated reports
    - Dashboards
- Benchmarks and Logging: requires central logging, configuration logs, alerting levels
- Reporting and archiving:
    - Reporting: identifying trends, providing visibility
    - Archiving logs: data retention life cycle

MITIGATION AND RECOVERY:

- SOAR (Security Orchestration, Automation, And Response): quick assess attack surface, state of systems, where issues are
- RCA (Root Cause Analysis):
    - Ask five why's
    - Event analysis
    - Diagramming cause and effect

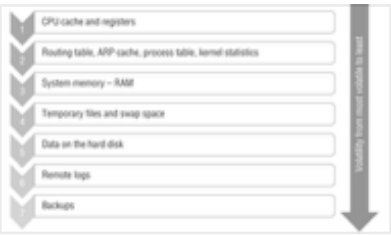
- Mitigation techniques:
    - Application allow lists (AKA whitelisting): application or files that are allowed on the system
    - Application deny lists (AKA blacklists): application or files not allowed on a system
    - Isolation or Quarantine
    - Monitoring
- Configuration Changes: common remediation technique
    - Firewall rule changes
    - MDM changes
    - DLP tool changes
    - Content/URL filtering
    - Updating or revoking certificates
- Incident Response actions:
    - Isolation
    - Containment: leaves system in place but prevents further actions
    - Segmentation

CHAPTER 15: DIGITAL FORENSICS

DIGITAL FORENSIC CONCEPTS:

- DFIR (Digital Forensics and Incident Response): finding evidence, removing attacker, assessing damage, lessons learned
  - Computer Forensics is a subfield of Digital Forensics
- Artifacts: pieces of evidence that point to an activity on a system
- E-discovery: electronic discovery
- Legal hold: notice that informs organizations that they preserve data and records
- Spoliation of evidence: intentionally, recklessly, or negligently altering/destroying/fabricating/hiding/withholding evidence

- DFIR Tools:
  - Eric Zimmerman's Tools
  - KAPE (Knoll Artifact Parser and Extractor): automates artifact collection, creates timeline
  - Autopsy: open source forensic platform
  - Volatility: memory analysis
  - Redline: collecting forensic information
  - Velociraptor: open-source advanced endpoint-monitoring, forensics, and response platform
- Elements Digital Forensics:
  - Acquiring and analyzing digital forensic data
  - Documenting the process
  - Human side - interview with individuals
  - Example: Google's Vault
- EDRM (Electronic Discovery Reference Model) Reference Model:
  1. Information governance to scope and control data provided
  2. Identification of electronically stored information
  3. Preservation
  4. Collection
  5. Processing of data to remove unwanted information
  6. Review data to contain only what its supposed to
  7. Analysis of key elements
  8. Production of data
  9. Presentation of data



CONDUCTING DIGITAL FORENSICS:

- Venue: location where a case is heard
- Nexus: concept of connection
- Evidence Preservation: since forensic analysis containments evidence, evidence is first collected and then write-protected
- Chain-of-custody: documentation if the forensic case may result in legal case
- FTK Imager: free forensic image tool
- WinHex: disk editing tool —> directly reading/modifying data, memory, RAID arrays, and other filesystems
- Logical copy: simply copying a file/folder/drive
- Forensic Copies: bit-by-bit
- Checksum: small-sized block of data derived from another block of data data for there purpose of detecting errors
- Provenance: chronology of the ownership
- Write blocker: allows a read to read & accessed by not written to
- Order of Volatility: prioritize preserving RAM before hard drive

  - Order of Volatility: what data is most likely to be lost to due normal processes
    - CPU cache and registers
    - Ephemera data: kernel statistics, ARP cache, process table
    - System memory - RAM
    - Temporary files and swap space
    - Data on the disk
    - OS
    - Devices, IoT devices
    - Firmware
    - Snapshots from VMs
    - Remote logs
    - Backups
  - FTK Imager: free forensic image tool —> physical/logical/image/CD/DVD all supported by FTK Imager
    - supports raw (dd)-style format
    - SMART (ASR Data's format for their SMART forensic tool)

    - E01 (EnCase)
    - AFF (Advanced Forensics Format)
    - Can capture live memory on a system too
- Cloud Forensics:
    - Right-to-audit clauses: ability to directly audit cloud or use third-party
    - Regulatory and jurisdiction concerns
    - Data breach notification laws: vary location to location
- Forensics tools missing from Sec+ Exam:
    - EnCase
    - SANS SIFT distribution
- Acquiring Network Forensic Data:
    - Capturing logs (firewalls, IDS/IPS, email server, authentication logs)
    - Wireshark for packet analyzing
    - Taps and ports aren't as useful —> too much info
- Acquiring Forensic Information from Other Sources:
    - VMs: snapshots. Cannot remove hardware
    - Containers: hard to do forensics —> requires additional planning
- Validating Forensic Data Integrity:
    - Hashing original and copy verifies their identity (MD5/SHA1) —> hash values are part of chain of custody

DATA RECOVERY:

- Wear Leveling: extends life of SSDs by moving data from less worn cells as needed
    - Can still use FDE
- Forensic Suites: complete forensic solutions

- Deleting Data:
    - Deleting files doesn't erase data —> removes its index for re-use
    - Same for quick formatting —> affects the index
- Recovery Tools:
    - Search for matching file headers/metadata to locate deleted data
    - Partial overwrites: still can recover some
    - Data stored in blocks —> not all blocks erased at once
        - Example: if 100MB is deleted by a 25MB file, 75MB is still recoverable
- Anti-forensic techniques: delete securely and overwrite
- Forensic Suites:
    - FTK: major Commerical option
    - EnCase: major Commerical option
    - Autopsy: open source forensic suite

REPORTING:

- Forensic Report includes:
  - Summary of findings
  - Outline of process
  - Sections
  - Conclusion/recommendations
- Digital Forensic Use Cases:
  - Legal cases
  - Internal investigations
  - Incident response
  - Learning/gaining intel

1. C
2. C
3. A
4. B? ~~D?~~
5. C
6. B
7. ~~C?~~ D?
8. D
9. ~~C B —> INCORRECT TIME ZONE~~
10. C
11. ~~? B? A —> MEMORY FORENSIC TECHNIQUES~~
12. ~~A C —> INTERVIEW FIRST~~
13. B
14. ~~D? B —> QUICK FORMATTING REMOVES FILE INDEXES BUT LEAVES FILE CONTENT ON DRIVE~~
15. ~~C? B —> FORENSICALLY EXAMINE DRIVES IS NOT USUALLY INCLUDED~~
16. ~~C? D —> CHAIN OF CUSTODY DOES NOT INCLUDE HOW THE ITEMS WERE TRANSPORTED~~
17. C?
18. C
19. C
20. A?

Dd?
PED address

CHAPTER 16: SECURITY GOVERNANCE AND COMPLIANCE

SECURITY GOVERNANCE:

- Governance programs: set of procedures and controls put in place to allow an organization to effectively direct its work
- GRC: Governance, risk, and compliance

  - Public Corporate Governance: Shareholders —> Board of Directors —> CEO —> management
    - SEC has min requirement for independent directors on board
  - Private Corporate Governance: “self-perpetuating” model --> current board elects new members
    - CEO can also be board member
  - Types of Governance Structures:
    - Centralized governance models: top-down approach
    - Decentralized governance models: bottom-up approach —> individual units are delegated authority
    - SMEs (Subject Matter Experts)
    - Government entities
    - Regulatory agencies

UNDERSTANDING POLICY DOCUMENTS:

- Information Security Policy Framework: series of documents designed to describe the organizations cybersecurity program
  - Policies: high-level statements of management intent. Compliance is mandatory
  - Standards: mandatory requirement for how an organization will carry out its information security policies
  - Procedures: step-by-step process that individuals and organizations must follow
  - Guidelines: best practices and recommendations related to a concept or task

  - Policies contain:
    - State of importance of cybersecurity
    - Requirement of staff to protect CIA
    - Statement of ownership by org
    - Designation of the CISO for security issues
    - Delegating CISO to create standards, procedures, and guidelines for company

- Security Policy Library:
  - Information security policy
  - Incident response policy
  - AUP (Acceptable use policy)
  - Business continuity and disaster recovery policies
  - SDLC (Software development life cycle)
  - Change management and change control policies
- Standards:
  - Password standards: password length, complexity, reuse, similar issues
  - Access control standards: amount of life cycle from provisioning through active use and decommissioning
  - Physical security standards: guidelines for securing physical premises and assets of organization
  - Encryption standards: transit and at rest
- Procedures:
  - Example #1: Payment Card Industry Forensic Investigator (PFIs):
    - Engage a PFI within 5 business days
    - Provide Visa with the initial forensics within in 10 days
    - Provide Visa with final forensic report
  - Example #2: policy frameworks
    - Change management procedures: how organization will perform change management
    - Onboarding and off boarding procedures: how will add and remove accounts
    - Playbooks: describe IR response
- Guidelines:

EXCEPTIONS AND COMPENSATING CONTROLS:

- Compensating Controls: internal control that can be used in place of a recommended security control
  - Balances the fact that it isn't possible to implement every possible security control
    - Ex: PCI DSS
- Change Management: ensuring changes do not cause outages
  - Weighs usability against risk of weakening security
- Impact analysis
- Maintenance Window: preplanned and announced times when all non-emergency changes will take place
- Version Control: ensures developers and users have the latest version of software

- Exception Process:
  - Standard/requirement that requires exception
  - Reasons for noncompliance with requirement
  - Business and/or technical justification for the execution
  - Scope, duration of the exception
  - Risks associated with the exception
  - Description of any supplemental controls that mitigate the risk of the exception
  - Plan for achieving compliance
  - Identification of any unmitigated risks
- Five Criteria for a compensating control:
  1. Control must meet intent and rigor of original requirement
  2. Control must provide similar level of dense as original requirement
  3. Control must be above and beyond other PCI DSS requirements
  4. Control must address additional risk imposed by not adhering to PCI DSS requirement
  5. Control must address the requirement currently and in the future
- Change Management Processes and Controls:
  1. Request the change: usually internal logs that allow anyone to see
  2. Review the change: may require a formal CAB (change review board)
  3. Approve/reject the change
  4. Test the change
  5. Schedule and implement the change: have a blackout plan though
  6. Document the change
     - Always must document before closing out change management

PERSONNEL MANAGEMENT:

- Least privilege: individuals only granted minimum set of permissions necessary to carry out their job functions
- Privilege creep: when employee moves from to job and accumulates privileges
- Separate of duties: no single person may have the privileges required to perform both tasks
- Two-person control: requires the participation of two people to perform a single sensitive action
- Job rotation: moves employees with sensitive roles to another position in the organization
- Mandatory vacations: forcing employees to take a vacation and revoking their permissions during that time
- Clean Desk policies: limit amount of paper left exposed on unattended employees desk to protect confidentiality

- Onboarding and off boarding: standard operating procedures, should include background checks
- NDA (Nondisclosure agreements): new employees should sign

THIRD-PARTY RISK MANAGEMENT (TPRM):

- Due diligence: vetting potential vendors to ensure they meet the organization's standards
- Conflicts of interest: when a vendor has a competing interest that could influence their behavior
- Vendor assessment: after initial selection process, organizations continuously assess chosen vendors
  - Penetration testing: simulated attacks carried out to identify vulnerabilities
  - Right-to-audit clause: allows customers to audit vendor's operations
  - ISO 27001 or SOC reports: independent 3rd-party experts to evaluate a vendor
  - Supply chain analysis: risks of vendor's supply chain
  - Questionnaires: collecting information on vendor's practices and performance regularly
- Vendor monitoring: includes security monitoring, vendor's security posture, data breaches, compliance, financial monitoring (important for long-term contracts)
- Rules of engagement: rules that define the boundaries which vendors should operate
- KPIs (key performance indicators): quantitative measurements of the vendor's performance

- Vendor Agreements:
  - MSAs (Master Service Agreements): umbrella contract for the work that a vendor does
  - WO (work order) or SOW (statement of work): project-specific details and references to MSAs
  - SLAs (Service level agreements): contracts that specify conditions of service will be provided by vendor
  - MOU (Memorandum of Understanding): informal document laying out relationship with vendor
  - MOA (memorandum of agreement): formal document outlining the terms between parties, establishing roles and responsibilities. More detailed than MOUs
  - BPAs (Business partner agreements): when two organizations agree to do business together, could potentially specify responsibilities and division of profits

- Winding Down:
  - EOL (end of life)
  - EOSL (end of service life)

COMPLYING WITH LAWS AND REGULATIONS:

- HIPAA (Health Insurance Portability and Accountability Act): privacy rules for medical industry in US
- PCI DSS (Payment Card Industry Data Security Standard): not a law but contractual obligation with merchants
- GLBA (Gramm-Leach-Bliley Act): US financial institutions must have security program
- SOX (Sarbanes-Oxley) Act: strong security for publicly traded companies' financials records
- GDPR (General Data Protection Regulation): security and privacy requirements for PII in the EU
- FERPA (Family Educational Rights and Privacy Act): US student educational records privacy
- Due diligence: continuously researching and understanding the legal and regulatory requirements that pertain to the organization
- Due care: ongoing efforts to ensure implemented policies and controls are effective and continuously maintained
- Acknowledgment: ensuring employees and business partners are aware of compliance requirements
- Attestation: aware of requirements and have confirmed they are practicing these policies
- Internal monitoring: internal audits, review, and checks to ensure meeting legal requirements
- External monitoring: third-party audits and assessments

- Compliance Reporting:
  - Internal compliance reporting: regular reports to management or board about state of compliance
  - External compliance reporting: mandated by regulatory or contractual obligations, must submit documentation
- Consequences of noncompliance:
  - Fines/sanctions (ex: GPDR is 4% of revenue or 20million, whichever is higher)
  - Restrictions on business operations
  - Reputational damage
  - Loss of business: contract termination

ADOPTING STANDARD FRAMEWORKS:

- CSF (Cybersecurity Framework): broad structure for cybersecurity controls
  - Commonly used in private sector
- RMF (Risk Management Framework): formal process for implementing security controls and authorizing system use
- ISO (International Organization for Standardization) Standards:
  - ISO 27001: Information *security* management systems
  - ISO 27002: controls implemented to meet cybersecurity objectives
  - ISO 27701: standard guidance for managing *privacy* controls
  - ISO 31000: guidelines for risk management

- NIST Cybersecurity Framework: CSF (Cybersecurity Framework) version 1.1 released in 2018. New framework coming in 2024
  1. Describe current cybersecurity posture
  2. Describe target state for cybersecurity
  3. Identify and prioritize opportunities for improvement in a repeatable process
  4. Asses progress towards the target state
  5. Communicate among internal and external stakeholders
- NIST Framework Components:
  1. The Framework Core: set of five security functions that apply across all industries and sectors

        1. Identify
        2. Protect
        3. Detect
        4. Respond
        5. Recover
    2. The Framework Implementation Tiers: assessing how an organization is positioned to meet cybersecurity objectives.
        - Maturity Model: describes the current and desired positioning of an organization along a continuum of progress
    3. The Framework Profile: describe its current state and separate profile into described future state
- NIST Cybersecurity Framework Implementation tiers:
    - Tier 1: Partial
    - Tier 2: Risk Informed
    - Tier 3: Repeatable
    - Tier 4: Adaptive
- NIST Risk Management Framework

- ISO 27001:
    1. Information security policies
    2. Organization of information security
    3. Human resource security
    4. Asset management
    5. Access control
    6. Cryptography
    7. Physical and environmental security
    8. Operations security
    9. Communications security
    10. System acquisition, development, and maintenance
    11. Supplier relationships
    12. Information security incident management
    13. Information security aspects of business continuity management
    14. Compliance with internal requirements
- ISO 27002:
    1. Select information security controls
    2. Implement information security controls
    3. Develop informations Security management guidelines
- ISO 27701: ISO 27001 + ISO 27002

SECURITY AWARENESS AND TRAINING:

- CBT (Computer Based Training): part of a diversity of a strong security training program

- Role-Based Training
- Phishing simulations: sending users fake phishing messages to test their skills
- Anomalous behavior recognition: employees should recognize risk, unexpected, or unintended behavior takes place
    - I.E.: Insider Threat
- Security Awareness : less formal efforts designed to remind employees about the security lessons they've learned

- User Guidance and Training:
    - Security Policies and Handbooks
    - Situational Awareness
    - Insider Threats
    - Password Management
    - Removable Media and Cables
    - Social Engineering
    - Operational Security
    - Hybrid/Remote Work Environments
- User Training Considerations:
    - Training Frequency: whenever someone joins + annual training
    - Development and Execution: assessing org's security landscape, IDing risks, include real-world examples, workshops, e-learning, simulations
    - Reporting and Monitoring: collect feedback from employees, provide management with reports, keep content relevant

1. B
2. A
3. C
4. B
5. C
6. D
7. C
8. B?
9. C
10. B
11. C
12. B
13. D
14. B
15. ~~B? D —> MANDATORY VACATIONS DESINGED TO LET FRAUD ACTIIVITES COME TO LIGHT~~

16. D
17. A
18. B
19. D
20. C

CIS?

CHAPTER 17: RISK MANAGEMENT AND PRIVACY

ANALYZING RISK:

- Risk management: seeks to bring order to the process of identifying and addressing risks
- ERM (Enterprise Risk Management): formal org approach to risk analysis. Identify risks, determine severity
- Threats: any possible event that might have a negative effect on CIA triad
- Vulnerabilities: weaknesses that can be exploited
- Risks: threat + vulnerability
- Risk severity: likelihood * impact (ex: PII data breach in the EU gets a huge fine)
- Risk analysis: formalized approach to conduct their review in a structured manner
- AV (asset value): express in dollars
- RAO (annualized rate of occurrence): ARO 2.0 means 2x per year
- EF (Exposure Factor): percentage of expected damage (ex: EF 90%)
- SLE (Single loss expectancy): AV * EF, amount of financial damage expected each time a risk materializes

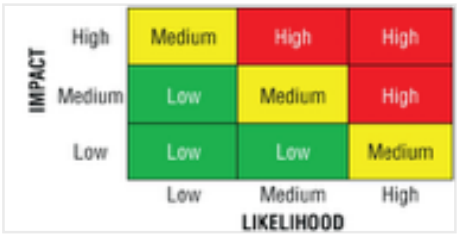
    - Example: AV $3,000 * EF 90% = SLE of $2,700
- ALE (annualized loss expectancy): SLE * ARO amount of damage expected each year

- Examples of Risk:
  - External risk
  - Internal risk
  - Multiparty risks: impacts more than one org
  - Legacy systems
  - Intellectual Property (IP) theft
  - Software compliance/licensing risks: software licensing that runs afoul
- Risk Assessments:
  - One-time risk assessments: current risk state at a specific point in time
  - Ad hoc risk assessments: in response to something (ex: new event, technology implementation, significant change)
  - Recurring risk assessment: regular intervals (ex: annually, quarterly)
  - Continuous risk assessment: ongoing monitoring and analysis of risks (ex: automated)
- Supply Chain Assessment:
  - 3rd Party and supply chain have high risks
- Risk Assessments methods: repeated for each vulnerability/risk
  1. Quantitative risk analysis
  2. Qualitative risk analysis
- Quantitative Risk Analysis:
  1. Determine the asset value (AV) of the asset affect by the risk
  2. Determine the likelihood that the risk will occur
  3. Determine the amount of damage that will occur to the asset if the materializes
  4. Calculate the single loss expectancy
  5. Calculate the annualized loss expectancy
- Qualitative Risk Analysis: used in conjunction with quantitive risk

MANAGING RISK:

- Risk management: systematically addressing the risks facing an organization
- Risk mitigation: applying security controls to reduce the probability and/or magnitude of risk
    - Ex: tamperproof tags, DDoS prevention
- Risk avoidance: completely eliminate the potential risk completely
- Risk transference: shifts the impact of a risk to another entity

    - Ex: cyber insurance
- Risk acceptance: purposely accepting risk to continue operations
    - Exception: acknowledging the risk but accepting it
    - Exemptions: higher lever of approval, often short-term



RISK TRACKING:

- Inherent risks: original level of risk before implementing any controls
- Residual risks: risk that remains after implementing controls
- Risk appetite: level of risk will to accept
    - Expansionary risk appetites: high risk, high reward mentality
    - Neutral risk appetites
    - Conservative risk appetites: focused on maintaining
- Risk threshold: specific level at which risk becomes unacceptable —> will trigger some action
- Risk tolerance: withstand risks and continue operations without any significant impact
- KRIs (Key Risk Indicators): metrics used to measure and provide early warning signals of risk
- Risk owner: entity responsible for managing and monitoring risks
- Risk register: tool for tracking risks
    - Risk owner
    - Risk threshold
    - KRIs
- Risk matrix (AKA heat map): quick summary of risk register
- Risk reporting: communicating status and evolution of risk to stakeholders
- DRP (disaster recovery planning): developing plans to recover as quickly as possible
- BIA (Business impact analysis): identifying the mission-essential functions and the critical system that support those functions

- MTBF (Mean time between failures): expected time between failures, measures reliability of a system
- MTTR (mean time to repair): average amount of time to restore
- RTO (Recovery Time objective): amount of time an organization can tolerate being down
- RPO (recovery point objective): amount of data an org can tolerate losing during an outage

- Types of risk reporting:
  - Regular updates: routine
  - Dashboard Reporting: dashboard that updates in real-time
  - Ad Hoc Reports: produced as needed
  - Risk Trend Analysis: using historical data
  - Risk Event Reports: documenting specific risks

PRIVACY:

- PII (personal identifiable information)
- PHI (protected health information): subject to HIPAA
- Data subjects: individuals whose personal data is being processed
- Data controllers: entity determines the reason for processing personal information
- Data stewards: individuals who carry out the intent of data controller
- Data custodians: only responsible for safeguarding information
- Data processors: service providers who process PII on behalf of data controller
- DPO (data protection officer): formal role required by GDPR, called Chief Privacy Officer in US
- Data minimization: collecting the smallest possible amount of information necessary
  - Purpose limitation: data should only be used by org for the exact purpose it was collected for
- Right to be forgotten (AKA right to erasure): allows user to request deletion of personal data via GPDR
- Deidentification: removes ability to link data back to an individual
- Data Obfuscation: obscuring data
  - Hashing: one-way function
  - Tokenization: unique identifier using a lookup table
  - Data masking: hides sensitive information

- Types of data: whether binary or human-readable
  - PII
  - Protected health information

    - Financial information
    - Intellectual property
    - Legal information
    - Regulated information
- Information classification:
    - Top secret: highest degree of protection, could cause grave damage to NS
    - Secret: substantial degree of protection, serious damage to NS
    - Confidential: some protection, damage to NS
    - Unclassified: still not publicly released without authorization
- Business classifications:
    - Highly sensitive
    - Sensitive
    - Internal
    - Public