COMPTIA CySA+ STUDY NOTES

Contents

Explaining the Importance of Security Controls and Security Intelligence

Identify Security Control Types

Cybersecurity Roles and Responsibilities:

- Cybersecurity refers to protecting information from unauthorized access, attacks, theft, or data damage over computer systems.
- A cybersecurity analyst is a senior position responsible for protecting sensitive information and preventing unauthorized access.
- Analysts implement security controls, manage security incidents, audit processes, conduct risk assessments, and stay updated on threats.

Security Operations Center (SOC):

- A SOC is where security professionals monitor and protect information assets in an organization.
- SOCs centralize security efforts, supported by organizational policies, motivated professionals, and collaboration.
- SOC principles: balance, staff quality, incident response capabilities, self-protection, awareness, and collaboration.

Security Control Categories:

- Security controls are categorized based on their functions.
- NIST 800-53 identifies controls as belonging to one of 18 families, such as access control, audit and accountability, and risk assessment.
- ISO 27001 framework identifies 14 control categories, including information security policies and physical security.

Security Control Functional Types:

- Security controls can be classified as preventative, detective, or corrective.
- Physical and deterrent controls are separate types.
- Compensating controls serve as substitutes and provide similar or better protection.
- These classifications help map controls to adversary tactics in a Course of Action matrix.

Security Control Selection Based on CIA Requirements:

- Security controls can be classified based on how they uphold the CIA triad (confidentiality, integrity, availability).
- Some technical controls may uphold confidentiality but not integrity or availability.
- An organization needs to define which parameters it needs to uphold to mitigate risk.

Explain the Importance of Threat Data and Intelligence

Threat Intelligence Sources:

- Threat intelligence feeds are essential for cybersecurity.
- There are both proprietary/closed-source and open-source intelligence sources.
- Proprietary sources include paid threat feeds and services, while open-source sources are publicly accessible and include websites, blogs, and forums.

Open-Source Intelligence Sources:

- Open-source threat intelligence includes publicly available sources that provide valuable information about cybersecurity threats.
- Examples of open-source providers include AT&T Security, Malware Information Sharing Project (MISP), Spamhaus, SANS ISC Suspicious Domains, and VirusTotal.
- Blogs and discussions from experienced practitioners offer insights into cybersecurity trends and attitudes.

Information Sharing and Analysis Centers (ISACs):

- ISACs are public/private partnerships that share sector-specific threat intelligence.
- ISACs produce highly industry-specific and relevant data from their members' systems.
- ISAC data is protected by legal measures to encourage information sharing.

Critical Infrastructure ISACs:

- Critical infrastructure sectors like communications, energy, and healthcare have their own ISACs.
- Embedded systems and industrial control systems are crucial areas of focus for cybersecurity in critical infrastructure industries.

Government, Healthcare, Financial, and Aviation ISACs:

- ISACs serve various sectors, including non-federal governments, healthcare, financial, and aviation.
- These sectors face unique cybersecurity challenges, such as election interference, healthcare data protection, and aviation security.

Threat Intelligence Sharing:

- Threat intelligence should be shared with different security functions to enhance risk management, security engineering, incident response, vulnerability management, and detection and monitoring.

- It helps organizations stay updated on threat sources, actors, tactics, and vulnerabilities, allowing them to make informed decisions and improve security.

Utilizing Threat Data and Intelligence

Classify Threats and Threat Actor Types

Threat Classification:

- Threats were historically classified based on "static" known threats like viruses, rootkits, Trojans, and botnets.
- Modern threats require classifying based on behaviors, not just known attack signatures.
- Threat classification is essential for detecting unknown threats, including known unknowns, recycled threats, and unknown unknowns.

Threat Actor Types:

- Threat intelligence includes insights into different types of adversary groups.
- Threat actor types include nation-state actors, organized crime, hacktivists, and insider threats.
- Nation-state actors target both military and commercial objectives and often use advanced persistent threat (APT) tactics.
- Organized crime focuses on activities like financial fraud and blackmail.
- Hacktivists promote political agendas through cyberattacks.
- Insider threats include employees, contractors, and guests who misuse their authorized access.
- Insider threats can be intentional (malicious) or unintentional (lack of awareness or carelessness).
- Threat classification also involves distinguishing commodity malware (general-purpose) from zero-day threats (exploiting newly discovered vulnerabilities).
- APTs are advanced adversary groups with considerable resources and a focus on stealth and persistence in compromised networks.

Utilize Attack Frameworks and Indicator Management

- **IoCs (Indicators of Compromise):**
  - Evidence of a successful attack.
  - May include unauthorized software, suspicious emails, unusual network activity, and more.
- **Behavioral Threat Research:**
  - Correlates IoCs into attack patterns.
  - Analyzes tactics, techniques, and procedures (TTPs) used in attacks.
  - Examples include DDoS, viruses/worms, network reconnaissance, APTs, and data exfiltration.
- **Kill Chain:**
  - Describes the general process of an attack on system security.
  - Phases include reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives.
  - Used to develop defensive strategies at each stage of an attack.
- **MITRE ATT&CK Framework:**
  - Provides a database of known tactics, techniques, and procedures (TTPs) used by attackers.
  - Helps in understanding adversary behavior.
  - Allows comparison of TTPs used by different adversary groups.
- **Diamond Model of Intrusion Analysis:**
  - Analyzes intrusion events by examining relationships between adversary, capability, infrastructure, and victim.
  - Features confidence levels for data accuracy.
  - Allows for the creation of attack graphs and activity threads.
- **Structured Threat Information eXpression (STIX):**
  - Framework for describing CTI (Cyber Threat Intelligence).
  - Uses JSON format for expressing CTI data.
  - Includes elements like Observed Data, Indicators, Attack Patterns, and more.
  - Defines relationships between elements.
- **Trusted Automated eXchange of Indicator Information (TAXII):**
  - A protocol for transmitting CTI data between servers and clients.
  - Supports the sharing of CTI data among security organizations.
  - Uses HTTPS and a REST API for data exchange.
- **OpenIOC and MISP:**
  - OpenIOC provides XML-based threat data sharing using logical detection rules.
  - MISP is a server platform for CTI sharing, supporting STIX, TAXII, and OpenIOC.
  - Facilitates the sharing of threat intelligence among organizations.

Utilize Threat Modeling and Hunting Methodologies

Adversary Capability:

- Start of threat modeling involves identifying threat sources.
- Threat actors can be classified as opportunistic or targeted, and as nation-state, organized crime, or hacktivist.
- Threat intelligence is used to determine the likelihood of attacks from different threat actors.
- Adversary capability refers to a threat actor's ability to create novel exploit techniques and tools.
- MITRE defines different levels of capability: Acquired and augmented, Developed, Advanced, Integrated.

Total Attack Surface:

- The attack surface encompasses all points at which an adversary could interact with a system and compromise it.
- To determine the attack surface, inventory the assets and processes on your network.
- Consider various threat-modeling scenarios, such as corporate data networks, websites/cloud, and bespoke software apps.

Attack Vector:

- The attack vector is a specific means of exploiting a point on the attack surface.
- MITRE identifies three principal categories of attack vectors: Cyber, Human, and Physical.

Threat Modeling Impact and Likelihood:

- Risk assessment is crucial and involves assessing the likelihood and impact of an event.
- Likelihood is measured as a probability or percentage, while impact is expressed as a cost (dollar) value.
- Helps prioritize responses to the most critical threat models.

Proactive Threat Hunting:

- Threat hunting involves proactively searching for evidence of Tactics, Techniques, and Procedures (TTPs) within a network.
- It contrasts with a reactive process triggered by incident reports.
- Utilizes insights from threat research and modeling to discover signs of TTPs.

Establishing a Hypothesis:

- Threat hunting is guided by hypotheses derived from threat modeling.
- Good cases for investigation are threats with high likelihood and high impact.

- Examples include new adversary campaigns or breaches in similar markets.

Profiling Threat Actors and Activities:

- Categorize threat actors and associate them with TTPs.
- Create scenarios showing how attackers might attempt an intrusion and their objectives.

Threat Hunting Tactics:

- Uses tools developed for security monitoring and incident response.
- Often relies on data collected within a security information and event management (SIEM) database.
- Assumptions about attacker objectives help predict tactics and tools used.

Open-Source Intelligence:

- Focus on stages in the kill chain, especially reconnaissance.
- Understanding open-source intelligence (OSINT) helps identify and mitigate risks.
- Sources include publicly available information, social media, HTML code, metadata, and more.

Google Hacking and Search Tools:

- Familiarity with Google search operators and advanced syntax.
- Examples of operators include quotes, NOT, AND/OR, scope modifiers, and URL modifiers.
- Google Hacking Database (GHDB) can identify vulnerable web servers and web applications.

Shodan:

- A search engine for identifying Internet-connected devices.
- Uses banner grabbing to gather device information, firmware, and metadata.
- Useful for finding vulnerable Internet of Things (IoT) and industrial control system (ICS) devices.

Email and Social Media Profiling Techniques:

- Email harvesting and social media profiling to gather information about employees.
- Methods include trading lists, Google searches, and testing for valid email addresses.
- Unwary users may share sensitive information on social media.

DNS and Website Harvesting Techniques:

- DNS harvesting can reveal network configurations and IP addresses.
- Zone transfers may expose the complete DNS records of a domain.
- Website ripping tools cache website code for analysis and potential vulnerabilities.

Analyzing Security Monitoring Data

Analyze Network Monitoring Output

Wireshark Expert Info:

- Analyst captures traffic for five minutes.
- Analyzes captured data using Wireshark's Expert Info feature.
- Observes a high number of chats and resets.
- Compares this to a summary of "normal" traffic.

Flow Analysis:

- Packet capture generates a large volume of data.
- Full packet capture (FPC) and retrospective network analysis (RNA) capture all network traffic.
- Flow collectors record metadata and statistics about network traffic instead of capturing each frame.
- Flow analysis tools can highlight trends, provide alerts, and visualize network connections.

NetFlow:

- Cisco-developed standard for reporting network flow information.
- Defines traffic flows by shared characteristics (keys) like IP addresses and protocol type.
- Provides valuable information about network traffic.
- Various NetFlow monitoring tools available, including open-source options like SiLK and Argus.

Zeek (Bro):

- Zeek is a passive network monitor that reads packets from a network tap.
- It selectively logs data of interest, reducing storage and processing requirements.
- Customizable data collection and alert settings.

Multi Router Traffic Grapher (MRTG):

- Creates graphs showing traffic flows through network interfaces.
- Polls routers and switches using SNMP.
- Provides visual clues for network traffic patterns.

IP Address and DNS Analysis:

- Analyzing access requests to external hosts, especially for signs of compromise.

- Correlating IP addresses, domains, and URLs in network traffic with reputation tracking whitelists and blacklists.
- Identifying known-bad IP addresses and domains using reputation risk intelligence.

Domain Generation Algorithm Analysis:

- Malware uses dynamically generated domains via a domain generation algorithm (DGA).
- DGAs create a range of possible DNS names.
- Secure recursive DNS resolvers can help detect DGAs.
- Fast flux networks continually change IP addresses.

Uniform Resource Locator (URL) Analysis:

- Analyzing URLs for malicious behavior.
- Identifying flagged URLs on reputation lists.
- Resolving percent encoding, assessing redirection, and showing source code for scripts.

HTTP Methods:

- Understand how HTTP works.
- Common HTTP methods include GET, POST, PUT, HEAD, and DELETE.
- Data can be submitted via URL or in the body of the request.

HTTP Response Codes:

- Response codes indicate the server's response to client requests.
- Categories include success (2xx), redirection (3xx), client errors (4xx), and server errors (5xx).

Percent Encoding:

- Percent encoding allows encoding of safe or unsafe characters in URLs.
- Misused for obfuscation or malicious input.
- Some commonly encoded characters: null, space, +, %, /, , ., ?, ", ', <, >

Analyze Appliance Monitoring Output

Proxy Log Review:

- Forward proxies act on behalf of internal hosts, forwarding their HTTP requests.
- Proxies ensure compliance with administrative and security policies for outbound Internet traffic.
- Proxies can be non-transparent (client configuration required) or transparent (intercept traffic without client reconfiguration).
- Analysis of proxy logs reveals details of HTTP requests, visited websites, and content.
- Proxies may use Common Log Format, recording data in space-delimited fields, including user ID, request method, HTTP status code, resource size, and MIME type.
- Proxies intercepting or blocking traffic can record matched rules, aiding in intent determination.

Reverse Proxy:

- Reverse proxies handle protocol-specific inbound traffic.
- They listen for client requests from the Internet, route requests to internal servers, and send responses back.
- Logs from reverse proxies can help detect attack indicators and anomalous traffic patterns.

Web Application Firewall Log Review:

- Web Application Firewalls (WAFs) apply rules to HTTP traffic, parsing headers and HTML message bodies.
- WAFs address web-based vulnerabilities like SQL injection and cross-site scripting (XSS).
- Logs record source/destination addresses, matched rules, and actions taken.
- Log formats can vary, but useful information includes event time, severity, URL parameters, HTTP methods, and context for the rule.

IDS and IPS Configuration:

- IDS is a packet sniffer that analyzes traffic and generates event logs based on rule matches.
- IDS sensors are placed inside firewalls or near critical servers to identify malicious traffic.
- Spanning ports or TAPs are used for monitoring in switched environments.
- IDS can also function as an Intrusion Prevention System (IPS), taking action to block malicious traffic.
- IDS/IPS solutions include Snort, Zeek, and Security Onion.

IDS and IPS Log Review:

- IDS/IPS creates log entries for rule matches, and rule changes.
- Log entries may contain event time, severity, URL parameters, and more.
- Various output formats include unified, syslog, CSV, and pcap.
- Analysts monitor alerts and decide whether to escalate them to incidents.

IDS and IPS Rule Changes:

- Rule signatures match malicious traffic.
- Rule changes are made to reduce false negatives and improve rule accuracy.
- Rules include action, protocol, source/destination IP, ports, and more.

Port Security Configuration Changes:

- Port security involves physical and MAC filtering.
- MAC filtering allows specifying permitted MAC addresses on a switch port.
- Port security should be implemented to prevent unauthorized device connections.

Network Access Control (NAC) Configuration Changes:

- NAC authenticates users and evaluates device integrity before granting network access.
- IEEE 802.1X provides port-based NAC, requiring authentication for network access.
- NAC policies define health checks, time-based, location-based, role-based, and rule-based access rules.

Analyze Endpoint Monitoring Output

PsExec PowerShell Attack:

- PsExec can exploit the default behavior of launching processes with local SYSTEM account privileges.
- Detection of suspicious PowerShell parameters should be done using host-based EDR or protection suites with behavioral analysis routines.
- Post-exploitation allows an attacker to manipulate files with SYSTEM account privileges and open a reverse shell connection for further actions.

Injecting a Keylogger:

- A keylogger can capture user activity, and any suspicious behavior should alert both attackers and defenders.
- Discovering modern malware with administrative privileges can be challenging; check for network communication to its handler.

Anomalous Behavior Analysis:

- Process Monitor records process interactions with the system, including Registry key usage, and helps analyze operations.
- Autoruns shows autostart processes and their configurations in the Registry and file system.
- System Monitor (sysmon) logs security-relevant event types.
- EDR configurations need tuning to reduce false positives and to share threat intelligence.
- Custom malware signatures can be developed and shared through industry portals or with security vendors.

Blacklisting and Whitelisting:

- Blacklisting blocks known threats but risks false positives and may not cover all threats.
- Whitelisting allows only trusted elements but can be restrictive and requires constant fine-tuning.
- Execution control enforces what software can be installed beyond a baseline and can use whitelisting or blacklisting.

Configuration Changes:

- Maintain and update blacklists and whitelists in response to incidents and threat monitoring.
- Consider strategic changes like adopting a "least privileges" model for increased security but assess the potential impact.

Analyze Email Monitoring Output

Email Message Internet Header Analysis:

- Internet email headers contain sender and recipient addresses, plus details about the servers handling email transmission.
- Multiple servers are involved in the email's journey from sender to recipient, and each adds information to the header.
- Headers consist of three "sender" address fields: Display from, Envelope from, and Received from/by.

- Analyzing these headers can reveal the true origin of an email, especially in cases of spoofing.

Email Malicious Content Analysis:

- Emails can carry malicious payloads, including exploits targeting vulnerabilities in email clients or file attachments designed to trick users.
- Attackers also use embedded links in emails, which may lead to malicious sites.
- Analyzing the email's body content, MIME format, and embedded links can help detect malicious content.

Email Signature Block:

- A missing or poorly formatted email signature block is a sign of a phishing message.
- Attackers may impersonate an organization's signature block to embed malicious links or incorrect contact details.

Email Server Security:

- Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) authenticate email senders.
- Domain-Based Message Authentication, Reporting, and Conformance (DMARC) helps ensure the effective use of SPF and DKIM.
- These mechanisms can be used to identify authorized email servers and prevent email spoofing.

SMTP Log Analysis:

- SMTP logs record the exchange of requests and responses between local and remote email servers.
- Status codes in SMTP logs indicate the success or failure of email transmission.
- Analyzing SMTP logs helps identify email issues and potential security concerns.

Email Message Security and Digital Signatures:

- S/MIME (Secure/Multipurpose Internet Mail Extensions) provides message authentication and confidentiality.
- Users are issued digital certificates containing public keys to validate their identities.
- Digital signatures and encryption are used to secure email messages.

Collecting and Querying Security Monitoring Data

Configure Log Review and SIEM Tools

1. **SIEM Overview:**
   - SIEM stands for Security Information and Event Management.
   - It's a critical tool for collecting, analyzing, and responding to security-related data.
   - SIEM tools assist in monitoring security events and ensuring compliance with regulations.
2. **SIEM Tools:**
   - Prominent SIEM tools include Splunk, ELK/Elastic Stack, ArcSight, QRadar, AlienVault/OSSIM, and Graylog.
   - These tools vary in features and capabilities and can be deployed as enterprise software or cloud solutions.
3. **Security Data Collection:**
   - SIEMs collect data from various sources using agents, listeners/collectors, and sensors.
   - Data normalization ensures that diverse data formats and timestamps are standardized for analysis.
   - Secure channels and sufficient IT resources are necessary for logging and data storage.
4. **Event Log:**
   - Event logs from systems like Windows categorize events into different log categories such as Application, Security, System, Setup, and Forwarded Events.
   - Severity levels indicate the impact of an event (Information, Warning, Error).
   - Event subscriptions in modern Windows versions enable centralized event logging.
5. **Syslog:**
   - Syslog is a protocol for centralized event collection from multiple sources using UDP (port 514).
   - It uses PRI codes, facility, and severity levels to classify and route events.
   - Secure syslog implementations introduce security features like TCP delivery, TLS encryption, and message integrity protection.
6. **Beyond OS Event Logs:**
   - Various log formats are used for exchanging event data between security tools and SIEMs.
   - These formats help in the structured exchange of data, especially from intrusion detection systems (IDS) and firewalls.

Analyze and Query Logs and SIEM Data

Analysis and Detection Methods:

- Security Information and Event Management (SIEM) systems apply rules to data inputs and generate alerts for analysts to investigate.
- SIEMs often produce false negatives, making it crucial to understand how alerts are generated.
- Simple correlation methods in SIEM include signature detection and rules-based policies, but they tend to produce many false positives and are blind to new threats.
- Heuristic analysis and machine learning enhance simple correlation methods by analyzing data points and context to generate alerts.
- Human analysts are slow compared to automated systems and cannot handle the volume of data.
- Machine learning allows systems to adapt and respond to evolving threats.

Behavioral Analysis:

- Behavioral analysis, or behavior-based detection, recognizes baseline network or user account behavior.
- It generates alerts when deviations from these baselines occur.
- The engine uses heuristics to create statistical models of baseline behavior, leading to initial false positives and negatives.
- Over time, the system improves its statistical models.

Anomaly Analysis:

- Anomaly analysis identifies events that don't conform to expected patterns or rules.
- It doesn't rely on known malicious signatures, reducing false negatives.
- It can check network traffic or host-based events against established standards and raise alerts if deviations occur.

Trend Analysis:

- Trend analysis identifies patterns within datasets over time to predict future events and detect relationships between events.
- It can help in predicting attacks and understanding the nature of incidents.
- Trend analysis involves frequency-based, volume-based, and statistical deviation analysis.

- Metrics for trend analysis include the number of alerts and incidents, network and host metrics, threat awareness education, compliance, and externally measured threat levels.

Rule and Query Writing:

- Correlation rules interpret relationships between data points and diagnose significant incidents.
- Correlation rules use logical expressions and operators to match conditions.
- Queries extract records based on conditions from stored data.
- Regular expressions are used to search for patterns in string data.
- The "grep" command in Unix-like systems and "findstr" in Windows support string searches using regular expressions.

Scripting Tools:

- Bash and PowerShell are scripting languages used to automate data analysis tasks.
- Awk is a scripting engine used to modify and extract data.
- WMIC (Windows Management Instrumentation Command-line) is used to review logs in remote Windows machines.
- PowerShell offers advanced functionality, cmdlets, and the ability to execute scripts for managing Windows systems.

Utilizing Digital Forensics and Indicato Analysis Techniques

Identify Digital Forensics Techniques

1. **Workstation Requirements**: Digital forensics workstations require specific hardware specifications, such as a multiprocessor system with at least 32 GB of main memory. They should support a variety of drive host bus adapter types, including EIDE, SATA, SCSI, SAS, USB, Firewire, Thunderbolt, etc. Other useful components include an optical drive and memory card reader. Additionally, high-capacity disk subsystems or access to a storage area network (SAN) are essential for storing acquired images.
2. **System Memory Image Acquisition**: System memory contains volatile data. Various methods can be used to collect data from system memory, including live acquisition, crash dumps, hibernation files, and pagefiles. Live acquisition captures memory contents while the computer is running, but it can be risky as it might change the source system.

3. **Disk Image Acquisition**: This refers to acquiring data from non-volatile storage media like hard disk drives (HDDs) and solid-state drives (SSDs). There are different methods for acquisition, such as live acquisition (while the computer is running), static acquisition by shutting down the computer, or static acquisition by pulling the plug. It's crucial to document the acquisition process.
4. **Write Blockers**: Write blockers ensure that the image acquisition tools do not change the source disk's data. These can be hardware devices or software running on the forensics workstation.
5. **Imaging Utilities**: Once the target disk is connected, imaging utilities are used to create a cryptographic hash of the data and obtain a bit-by-bit copy of the disk contents. Different tools and formats are mentioned, including vendor-specific file formats like .e01.
6. **Hashing**: Creating cryptographic hashes of disk contents is essential for proving that the data has not been tampered with. Secure Hash Algorithm (SHA) and Message Digest Algorithm (MD5) are mentioned as common methods for hashing.
7. **File Integrity and Changes to Binaries**: Hash values can be used to check the integrity of files, especially for operating system and application binaries. Differences in hash values might indicate changes, which can be investigated for potential malware.
8. **Timeline Generation and Analysis**: Timelines are constructed to establish a chronological order of events, helping in forensic investigations. The timeline can provide insights into how an adversary gained access, installed tools, made changes, retrieved data, and potentially exfiltrated data.
9. **Carving**: File carving involves extracting data from an image when there's no associated file system metadata. This process is based on file signatures and is used to reconstruct deleted files or data fragments from unallocated and slack space.
10. **Chain of Custody**: The chain of custody refers to documenting the handling of evidence from collection to presentation in court. It ensures the integrity and proper custody of evidence. Physical devices need to be properly identified, labeled, and stored, and metadata should be created to describe evidence characteristics. Adequate physical security measures are also crucial for preserving evidence.

Analyze Network-related IoCs

1. **Binary Upload and ARP Spoofing:**
   - Binary uploads with non-standard SMB traffic and ports can indicate malicious activity.
   - ARP spoofing redirects IP addresses to unintended MAC addresses, and Snort can help detect this.
   - Monitor ARP cache with 'arp -a' to compare MAC addresses to known server machines.
2. **Rogue Devices:**
   - Unauthorized devices on a network are rogue devices, such as USB drives, additional NICs, or personal smartphones.
   - Maintain an inventory of all devices in your organization to detect rogue devices.

3. **Rogue Machine Detection Techniques:**
   - Visual inspection, network mapping, wireless monitoring, packet sniffing, NAC, and intrusion detection can be used to detect rogue devices.
4. **Scan/Sweep Intrusion Indicators:**
   - Rogue devices are used for scanning and sweeping to identify vulnerable hosts.
   - Scanning activity can be detected through intrusion detection systems.
5. **Common Protocol and Nonstandard Port Usage Indicators:**
   - Malicious traffic often uses non-standard ports; attackers adapt to different port usages.
   - Mitigate non-standard port use by configuring firewalls with whitelisted ports.
6. **Shell and Reverse Shell:**
   - Attackers use remote access tools to obtain a shell on compromised systems.
   - Reverse shells can be used to exploit systems without outbound traffic filtering.
7. **Data Exfiltration Indicators:**
   - Data exfiltration occurs when attackers steal sensitive data from an organization.
   - Indicators include unusual HTTP transfers, DNS queries, explicit tunnels, and more.
8. **Covert Channels:**
   - Covert channels allow stealthy data transmission and can evade intrusion detection.
   - They can be categorized as storage or timing channels.
9. **Steganography:**
   - Steganography hides data within images or videos to evade detection.
   - It conceals information so well that it's difficult to detect without specialized tools.

Analyze Host-related IoCs

Performance Monitoring and Diagnosing Problems:

- Monitor processor usage to identify the cause of performance issues.
- Memory consumption can be an indicator; excessive memory use can suggest malware.
- Tools like Task Manager and Performance Monitor (Windows) and free/top (Linux) can assist.

Memory Overflow:

- Memory overflow, or buffer overflow, can be used by attackers to execute arbitrary code.
- A memory leak may indicate an attempt at a buffer overflow.

Disk and File System Indicators of Compromise (IoCs):

- Analyze file system changes and anomalies, even if malware isn't saved to disk.
- Metadata about file creation, access, and modification can help establish timelines.

Staging Areas and Data Exfiltration:

- Attackers often aim to exfiltrate data; their motives may evolve as they gain access.
- Data staging techniques include temporary files, user profiles, alternate data streams, etc.
- Data may be compressed and encrypted for exfiltration.

File and File System Viewers:

- File system viewers help reconstruct timelines of computer events.
- Tools to analyze file metadata and view different file types are available.
- Visualization tools can create graphs of file activities.

Cryptography Tools:

- Cryptography analysis tools help determine encryption types and key strength.
- In some cases, decryption keys can be recovered from system memory.

Unauthorized Privilege Indicators:

- Attackers often attempt privilege escalation to gain extensive access.
- Monitoring authentication and authorization systems can reveal valuable information.
- Indicators include unauthorized sessions, failed log-ons, new accounts, and off-hours usage.

Unauthorized Software Indicators:

- Presence of known malicious software or attack tools can be indicators.
- Unauthorized changes to existing files or software can be used for attacks.
- Application viewers and analysis tools help assess application usage and history.

Persistence Indicators:

- Persistence mechanisms include the Registry and scheduled tasks.
- Changes or anomalies in the Registry can indicate malicious activity.
- Scheduled tasks can be used to run malicious code persistently.

Analyze Application-Related IoCs

Service Defacement:

- Website defacement is a clear sign of compromise.
- Attackers exploit vulnerabilities, like SQL injection, to alter a website's presentation.
- Defacements can be blatant or subtle, with attackers sometimes making subtle modifications.
- Subtle defacements can mislead users into thinking the organization is responsible.

Service Interruption IoCs:

- Application services may fail to start or stop unexpectedly for various reasons.
- Service interruption may lead to suspicions of cybersecurity issues.
- Causes can include adversaries preventing security services from running, compromised service processes, DoS/DDoS attacks, or excessive bandwidth usage.

Service Analysis Tools for Windows:

- Tools to monitor running services in Windows include Task Manager, Services.msc, net start, and the Get-Service PowerShell cmdlet.

Service Analysis Tools for Linux:

- Linux offers commands like who, w, and rwho to monitor user sessions.
- The lastlog command provides log-on history.
- User account creation and authentication attempts are logged in /var/log/auth.log or /var/log/secure.

Application Log IoCs:

- Many applications log events, including web servers.
- DNS event logs can provide information about queries and suspicious site communication.
- HTTP access logs include status codes, HTTP headers, and User-Agent information.

SQL Event Logs:

- SQL databases log events, startup, shutdown, and access attempts.
- SQL servers can also log individual query strings, providing intelligence on SQL injection attacks or unauthorized data modification.

Introduction of New Account IoCs:

- The creation of rogue accounts is a way for attackers to maintain access.
- Rogue accounts are often overlooked among numerous accounts.
- A rogue account might be created or modified to gain privileges and remain dormant.

Digital Forensics for Virtualization:

- Virtualization adds complexity to digital forensics.
- VM introspection (VMI) and saved state files can be analyzed.
- Lost system logs on elastic VMs make incident analysis difficult.

Digital Forensics for Mobiles:

- Mobile forensics involve data collection and extraction.
- Encrypted data on modern mobile devices is challenging to recover without unlocking.
- Different extraction methods like manual, logical, file system, and call data extraction can be used.
- Notable mobile device forensics software includes Cellebrite, AccessData, EnCase, Oxygen Forensics, and Micro Systemation AB.

Carrier Provider Logs:

- Carrier providers may keep records of device activity.
- Records can include call details, voicemail, text messages, images sent over MMS, IP addresses, and geolocation data.

Analyze Lateral Movement and Pivot IoCs

1. **Pass-the-Hash Attack**
   - Attackers use stolen credential hashes to gain access to other systems.
   - To defend against this, limit the use of domain admin accounts and monitor Windows Event Logs for PtH attempts.
2. **Golden Ticket Attack**
   - Attackers create golden tickets from the krbtgt hash, potentially gaining administrative access to a domain.
   - Change krbtgt account password periodically and restart application services if a breach is suspected.
3. **Other Lateral Movement Techniques**
   - Attackers exploit cleartext credentials and remote access protocols.
   - Vulnerabilities arise when users reuse weak passwords.
4. **Remote Access Services**
   - Attackers utilize services like Telnet, RDP, and VNC to move between hosts.
   - Remote desktop protocols provide normal user access to target machines.

5. **Windows Management Instrumentation Command-Line (WMIC)**
    - Administrators use WMIC for remote host management.
    - Attackers can misuse WMIC for lateral movement.
6. **PsExec**
    - PsExec allows attackers to execute processes on remote machines without installing services.
    - Attackers can elevate privileges using PsExec.
7. **Windows PowerShell**
    - PowerShell can be abused for lateral movement and post-exploitation.
    - Attack modules in tools like PowerShell Empire facilitate attacks.
8. **Pivoting Techniques**
    - Pivoting is similar to lateral movement but involves compromising a central host (pivot) to access other hosts.
    - Port forwarding and SSH tunnels are common pivoting methods.

Applying Incident Response Procedures

Explain Incident Response Processes

1. **Public Relations (PR)**
    - PR plays a crucial role in managing negative publicity during and after a serious incident.
    - Controlling the release of incident information is essential.
    - Regulations may require specific communications to customers, partners, and agencies.
2. **Incident Response Training**
    - Staff actions following incident detection are critical.
    - Clear policies and effective training are essential for incident detection and reporting.
    - Encouraging employees to report suspicions securely aids in detecting insider threats.
    - Cross-departmental training helps enhance communication among different sections.
3. **Security Awareness and Compliance Training**
    - Lessons learned from incidents may reveal the need for added security awareness and compliance training for specific employees or job roles.
    - Such training equips employees with knowledge to resist similar attacks.
4. **Testing Incident Response**

- Testing is crucial to ensure the robustness of incident-handling procedures.
- Penetration testing (pen testing) is an effective way to simulate incidents and test response procedures.
- Penetration testing may involve a red team attempting an intrusion, while a blue team uses established procedures to detect and repel the attack.

5. **Methodology and Rules of Engagement**
    - Clear methodologies and rules of engagement are essential for penetration testing.
    - NIST's SP 800-115 provides guidance on penetration testing.
    - Various toolkits, such as Rapid7's Metasploit, Cobalt Strike, and pen test distributions like KALI, are used for crafting and launching attacks during testing.

Apply Detection and Containment Processes

OODA Loop in Incident Response:

- In incident response, the OODA loop (Observe, Orient, Decide, Act) model is used to make tactical decisions in analyzing and responding to specific incidents.
- It helps in maintaining clarity and decisiveness when responding to stressful and intense situations, such as cybersecurity incidents.

Defensive Capabilities and Courses of Action:

- Defensive capabilities are categorized in the courses of action (CoA) matrix, mapping to each stage of an adversary's kill chain.
- Defensive capabilities include Detect, Destroy, Degrade, Disrupt, Deny, and Deceive.
- These capabilities are used to address various stages of an adversary's attack.

Incident Detection and Analysis:

- Incident detection and analysis rely on both manual and automated detection mechanisms.
- Identifying indicators of compromise (IoCs) from various sources is crucial.
- Accurate analysis is needed to distinguish between false positives and real incidents.
- Using security information and event management (SIEM) tools helps aggregate and analyze data.

Impact Analysis:

- Impact analysis assesses the costs and implications of an incident.

- Factors affecting impact analysis include data integrity, system process criticality, downtime, economic consequences, and data correlation.
- Incident security level classification helps categorize incidents based on their impact.

Containment:

- Containment techniques aim to prevent the ongoing intrusion or data breach.
- Isolation-based containment involves removing an affected component from its environment.
- Segmentation-based containment uses network technologies, such as VLANs, routing, and firewall ACLs, to prevent communication between the affected component and the rest of the network.

Apply Eradication, Recovery, and Post-Incident Processes

Eradication:

- Eradication involves mitigating and eliminating an incident from affected systems.
- Identification of affected hosts and devices is necessary to understand the scope of the incident.
- Sanitization and secure disposal methods are discussed, including cryptographic erasure (CE) and zero-fill-based methods.
- Special considerations for SSDs and hybrid drives are mentioned.
- When secure disposal is needed for highly confidential or top-secret information, physical destruction methods like shredding, incineration, or degaussing (for magnetic media) may be applied.
- The goal of eradication is to remove the incident and prevent its recurrence.

Reconstruction/Reimaging:

- Restoring the host software and settings through reimaging using clean backups or templates.
- Reconstructing a system using a configuration template or scripted install from trusted media.
- Ensuring that a sanitized system is free from infection.

Reconstitution of Resources:

- Steps for manually reconstituting a resource when reimaging is not possible, focusing on malware removal and system cleanup.
- Disabling autostart locations to prevent malicious processes from executing.
- Replacing contaminated OS and application processes with clean versions.
- Continuing to monitor the system after reconstitution.

Recovery:

- Recovery aims to restore capabilities and services, depending on the nature of the incident.
- Examples of recovery scenarios include data restoration, rebooting servers, and malware removal.
- Patching vulnerable systems is crucial to prevent future incidents.
- Restoration of permissions, verification of logging and communication to security monitoring, and vulnerability mitigation through system hardening are discussed.

Post-Incident Activities:

- Post-incident activities include report writing, evidence retention, lessons learned, and incident response plan updates.
- Report writing should convey technical information to non-technical executives, emphasizing the impact, security policy changes, and recommendations.
- Evidence must be preserved for legal or regulatory purposes.
- Lessons learned meetings are conducted to analyze incidents, determine root causes, and improve procedures.
- Lessons learned reports serve as the basis for incident summary reporting.
- Indicator of Compromise (IoC) generation and monitoring for improved detection is emphasized.
- Corrective actions and controls should follow the change control process, ensuring minimal impact on business functions.

Applying Risk Mitigation and Security Frameworks

Apply Risk Identification, Calculation,and Prioritization Processes

Risk Prioritization:

- Risk mitigation involves reducing exposure to risk factors.
- Risk deterrence and risk reduction are methods to mitigate risk.
- Risk avoidance means stopping a risky activity, while risk transference shares risk with a third party.
- Risk acceptance means acknowledging a risk and monitoring it.

Security Control Prioritization:

- The selection of security controls depends on various factors, including regulations, cost, and risk impact.
- The Return on Security Investment (ROSI) helps evaluate the cost-effectiveness of security controls.

Engineering Tradeoffs:

- Risk cannot be completely eliminated; it must be managed to balance security and functionality.
- Tradeoffs occur when implementing security measures with potential added costs or complexity.

Communication of Risk Factors:

- Risk scenarios must be articulated in plain language, explaining the cause, effect, and business impact.
- Effective communication ensures that stakeholders understand the risks associated with their workflows.

Risk Register:

- A risk register documents the results of risk assessments, including risk ratings, descriptions, and countermeasures.
- It should be shared among stakeholders to enhance risk visibility.

Documented Compensating Controls:

- Compensating controls are used when a standard control cannot be implemented due to business or technical reasons.
- They require documentation to demonstrate their effectiveness and consistent use.

Exception Management:

- Exception management is used to document cases where policies or procedures cannot be followed due to practical constraints.
- It includes details about the exception, the risk assessment, and compensating controls.

Training and Exercises:

- Training and exercises are essential for ongoing risk management and security control validation.
- Tabletop exercises are facilitated training events where participants respond to risk scenarios.
- Penetration testing involves actively trying to exploit vulnerabilities to test security controls.
- Red and blue team exercises simulate adversarial attacks and defense, with a white team overseeing and reporting the results.

Explain Frameworks, Policies, and Procedures

1. **Framework:**
    - A framework is a structured approach or set of guidelines that organizations use to manage and implement IT and cybersecurity practices.
    - It helps ensure that IT services align with the organization's overall business strategies and objectives, creating value for the business.
    - Frameworks provide a structured list of activities and objectives designed to mitigate risks in various areas, including cybersecurity.
    - They may include best practice guides, checklists, and recommended activities and technologies.
    - Frameworks enable organizations to assess their current cybersecurity capabilities objectively, define target levels of capability, and prioritize investments to achieve those targets.
    - These frameworks can be crucial for demonstrating regulatory compliance and enhancing internal risk management procedures.
2. **Policies:**
    - Policies are high-level statements or rules that guide an organization's behavior and decision-making processes.
    - In the context of cybersecurity, policies establish what is allowed and what is not in terms of security practices.
    - They define the organization's stance on various security-related issues, such as data protection, access control, and incident response.
    - Policies provide a foundation for creating detailed procedures and controls.
    - These policies help ensure that everyone in the organization understands the expectations and requirements for maintaining a secure environment.
3. **Procedures:**

- Procedures are detailed, step-by-step instructions that specify how to implement the policies.
- They provide practical guidance on how to carry out security-related tasks or respond to security incidents.
- Procedures are specific and actionable, outlining the exact actions to take in various scenarios.
- These detailed procedures ensure that security practices are carried out consistently and correctly.
- They are often tailored to the organization's specific needs and technologies, helping employees follow best practices and maintain a secure environment.

Performing Vulnerability Management

Analyze Output from Enumeration Tools

1. **Nmap**: Nmap is a popular network scanning tool used for host discovery, port scanning, service discovery, and OS fingerprinting. It can be used for both legitimate network mapping and potentially malicious purposes. Nmap has various scanning techniques, including TCP SYN scans and UDP scans, and provides information about open, closed, and filtered ports.
2. **Nmap Port Scans**: The text mentions different types of port scans, such as TCP SYN scans, TCP connect scans, and TCP flag manipulation scans. These scans help identify the state of ports on target hosts.
3. **Nmap Fingerprinting**: Nmap can perform service discovery and fingerprinting to identify operating systems, application versions, device types, and other details about the target hosts. It can use scripts to gather additional information.
4. **hping**: hping is a tool used for crafting and sending network packets, making it useful for various network testing purposes. It can be used for host and port detection, as well as traceroute functionality. hping can also be used for spoofing and packet fragmentation.
5. **Responder**: Responder is a man-in-the-middle tool that exploits name resolution on Windows networks. It intercepts LLMNR and NBT-NS requests to gain access to network services. It can be used to retrieve password hashes and other information from victim hosts.
6. **Wireless Assessment Tools**: The text briefly mentions tools for assessing wireless networks.
    - **Aircrack-ng**: Aircrack-ng is a suite of tools used to assess the security of wireless networks. It can capture frames, perform deauthentication attacks, and

crack WEP encryption. However, it's mostly effective against outdated WEP security.

- **Reaver**: Reaver targets Wi-Fi Protected Setup (WPS) vulnerabilities to gain unauthorized access to wireless networks. It can crack WPS PINs through brute force attacks, but it's not effective against networks with strong security measures.

Configure Infrastructure Vulnerability Scanning Parameters

- Assessment Scan Workflow:
  - Who conducts scans?
  - When are scans conducted?
  - Which systems are scanned?
  - How do scans impact systems?
  - Is isolation needed during scans?
  - Contact for assistance.
- Workflow:
  - Install software on target systems.
  - Perform an initial assessment.
  - Analyze reports against a baseline.
  - Take corrective actions based on findings.
  - Repeat the assessment.
  - Document findings and prepare reports.
  - Perform ongoing assessments for improvements.
- Mapping/Enumeration and Assessment Scope:
  - Types of scanners: Infrastructure, web application, cloud infrastructure.
  - Scanners identify vulnerabilities, suggest remediation options.
- Internal vs. External Scans:
  - Internal scans are local.
  - External scans are from different networks.
- Scanner Types:
  - Infrastructure scanners in active vs. passive, credentialed vs. non-credentialed modes.
  - Passive scanning for indirect evidence.
  - Active scanning with network connection.
  - Credentialed scans for detailed analysis.
  - Non-credentialed scans for external assessment.
- Server-Based vs. Agent-Based Scanning:
  - Scans from servers, managed by administration server.
  - Agent-based scans for reduced impact on network.
  - Agent range may be OS-specific.
- Special Considerations for Scanning Parameters:
  - Consider segmentation for network zones.
  - Intrusion prevention, firewall settings.

    - Scanning bandwidth impacts.
    - Scanning parameters vary by data sensitivity.
- Assessment Scan Scheduling and Constraints:
    - Scan frequency based on risk, new vulnerabilities, breaches, audits, compliance.
    - Technical constraints and service disruption risks.
- Vulnerability Feed Configuration:
    - Vulnerability feeds with known vulnerabilities.
    - Use of SCAP for compliance checks.
- Assessment Scan Sensitivity Levels:
    - Discovery scans for enumeration.
    - Fast/basic assessment scans for common vulnerabilities.
    - Full/deep assessment scans for comprehensive checks.
    - Compliance scans for regulatory requirements.
- Assessment Scanning Risks:
    - Disruption to hosts and network traffic.
    - Confidentiality of scan results.
    - Security risks from open network ports.

Analyze Output from Infrastructure Vulnerability Scanners

Vulnerability Scan Reports:

- Vulnerability assessment tools generate summary reports after scans.
- Reports categorize vulnerabilities by their criticality, often using color-coding (e.g., red for critical).
- Reports can be viewed by scope (across all hosts) or by specific hosts.
- Each vulnerability should be detailed, with information on how to remediate issues.

Report Confidentiality:

- Vulnerability scan reports are logged and should be treated as highly confidential.
- Access to these reports should be limited to authorized administrators.

Automated Report Distribution:

- Some tools allow for automated distribution of reports via email or alerts for non-compliance.

- Automated distribution may risk confidentiality and misinterpretation, so manual distribution can be preferable.

Common Identifiers:

- Vulnerability scanners use common identifiers to share intelligence data across platforms.
- These identifiers include:
  - Common Vulnerabilities and Exposures (CVE).
  - Common Weakness Enumeration (CWE).
  - Common Attack Pattern Enumeration and Classification (CAPEC).
  - Common Platform Enumeration (CPE).
  - Common Configuration Enumeration (CCE).

Common Vulnerability Scoring System (CVSS) Metrics:

- Vulnerability scan reports often use CVSS metrics to rate the severity of vulnerabilities.
- The CVSS scores vulnerabilities from 0 (none) to 10 (critical).
- These scores are based on various metrics, including access vector, access complexity, privileges required, user interaction, scope, and confidentiality, integrity, and availability impacts.

False Positives and False Negatives:

- Vulnerability scans can produce false positives (incorrectly identifying issues that don't exist) and false negatives (missing real issues).
- Addressing false positives may involve adjusting scan scopes, updating baselines, or adding exceptions.
- Monitoring false negatives can be mitigated through repeated scans, different scan types, and using multiple scanners or databases.

Report Validation Techniques:

- Validating scan results involves reconciling them with your knowledge of the environment.
- This can include reconciling results, correlating results with other data sources, comparing to best practices, and identifying exceptions.

Scanner Examples:

- Notable vulnerability scanners include Nessus, OpenVAS, and Qualys.
- Nessus is available in various versions (on-premises and cloud) and uses CVE and CVSS metrics for scoring.
- OpenVAS is open-source software derived from Nessus and is available for Linux.
- Qualys is a cloud-based solution with sensors and agents for vulnerability management.

Mitigate Vulnerability Issues

1. **Interpreting Vulnerability Scan Results:** Vulnerability scan reports are not always straightforward. They require careful analysis and judgment to determine the nature and validity of vulnerabilities.
2. **Remediation/Mitigation Plans:** After identifying vulnerabilities, you need to prioritize your response based on factors like the criticality of the system and the difficulty of implementing the fix. Scanner reports often provide suggestions for fixing issues.
3. **Risk Acceptance:** Sometimes, due to cost or unavoidable delays, organizations may accept certain risks. This means no countermeasures are put in place, but the risk is continuously monitored.
4. **Verification of Mitigation:** Remediation actions should be validated to ensure they effectively mitigate vulnerabilities. This can involve rescanning systems or performing more advanced assessments like penetration testing.
5. **Configuration Baselines:** Comparing vulnerability assessment results to established configuration baselines helps identify vulnerabilities. Deviations from these baselines should be addressed.
6. **Center for Internet Security (CIS):** CIS provides security benchmarks and best practices for various systems and frameworks, helping organizations secure their environments.
7. **Compensating Controls:** Compensating controls are used when it's not possible to implement recommended controls. They must provide the same level of security assurance as the recommended controls.
8. **System Hardening and Patching:** System hardening involves securing a system, ensuring it only runs necessary services, and reducing the attack surface. Regular patching is crucial to fix known vulnerabilities.
9. **Inhibitors to Remediation:** Remediation efforts can face various challenges, including legacy systems, proprietary systems, organizational governance, business process interruption, degrading functionality, and impacts on agreements such as SLAs and MoUs.

Applying Security Solutions for Infrastructure Management

Apply Identity and Access Management Security Solutions

Password Policies:

- Password policies are essential for proper credential management.
- They instruct users on choosing and maintaining secure passwords.
- NIST guidance suggests simplicity in password rules, avoiding complexity.
- Aging policies should allow users to choose when to change passwords.
- Password hints should be avoided to prevent the risk of account recovery.
- Password managers can generate and securely store complex passwords.
- Organizations should consider allowing or prohibiting the use of password managers.

Single Sign-On (SSO) and Multifactor Authentication (MFA):

- SSO allows users to authenticate once for access to multiple resources.
- MFA enhances password security by adding extra verification steps.
- MFA methods include two-step verification, biometrics, certificates, and location-based access.

Certificate Management:

- Digital certificates are crucial for machine and user identity assurance.
- Root certificates are vital, and their compromise can be a high-value target.
- Certificates are used for authentication, encryption, and digital signatures.
- OpenSSL and certutil are tools for creating and managing certificates.
- SSH key management is essential to prevent data breaches.

Federation:

- Identity federation allows shared sign-on across multiple systems.
- It connects the identity management services of various networks.
- Trust relationships and communication links between networks are established.
- Federation simplifies access across different systems.

Privilege Management:

- Privilege management involves defining user access rights and policies.
- Least privilege and separation of duties are fundamental principles.
- MAC, RBAC, and ABAC are access control models used to enforce policies.
- Role-based access control (RBAC) grants rights based on roles.
- Attribute-based access control (ABAC) allows fine-grained access decisions.

IAM Auditing, Monitoring, and Logging:

- Auditing and monitoring are critical to detect insider threats and unauthorized access.
- Logs should include access attempts and changes to system configuration.
- SIEM systems and rule-based monitoring can automate log analysis.
- Manual review ensures proper account and privilege management.

Conduct and Use Policies:

- A code of conduct and privileged user agreement (PUA) sets ethical behavior expectations.
- Acceptable use policies (AUP) govern the proper use of equipment and services.
- AUPs prevent misuse of equipment and protect organizations from legal issues.

Apply Network Architecture and Segmentation Security Solutions

Asset and Change Management:

- Organizations need well-documented inventories of tangible and intangible assets, including network appliances, servers, workstations, and infrastructure components.
- Asset tagging using methods like barcodes or RFID tags can help track asset location and prevent theft.
- Asset management databases should store information about asset type, model, serial number, asset ID, location, user(s), value, and service details, along with vendor documentation.
- Change management processes should document all changes to network components, including configuration changes, patches, backup records, and suspected breaches.
- Every change should have a rollback plan for potential reversals.
- Changes should be assessed post-implementation for impact and documentation of outcomes.

Network Architecture:

- The design of network architecture is crucial for implementing a defense-in-depth strategy.

- Physical network architecture refers to cabling, switch ports, router ports, and wireless access points, which can introduce vulnerabilities if not secured.
- Security controls such as physical security measures, authentication, and endpoint security help protect physical network components.
- Adversaries may attempt to exploit physical access points using devices like Wi-Fi Pineapple.
- VPNs (Virtual Private Networks) are used to secure remote access to internal network resources.
- Software-Defined Networking (SDN) abstracts network functions into control, data, and management planes, simplifying network configuration and enhancing security.

Segmentation:

- Network segmentation divides the network into distinct subnetworks to limit the spread of compromises.
- Segmentation creates secure zones, such as DMZs, management interfaces, and audit and logging zones.
- VLANs (Virtual LANs) and firewalls are commonly used for segmentation.
- System isolation or "air gap" physically separates networks or hosts with special security requirements from others.
- Logical isolation via firewalls or VPNs may also be used to protect sensitive hosts.
- Physical segmentation uses separate switches and routers for network segments.
- Virtual segmentation leverages VLANs and is more cost-effective and flexible.

Explain Hardware Assurance Best Practices

Supply Chain Assessment:

- Many organizations use commercial off-the-shelf products and services, relying on vendor claims for security.
- Organizations with more control can establish a trusted computing environment where every element, including hardware, is tamper-resistant.

Vendor Due Diligence:

- When onboarding new vendors, suppliers, or partners, due diligence should confirm that they meet minimum standards for cybersecurity risk management, security assurance, product support lifecycle, and more.

Hardware Source Authenticity and Trusted Foundry:

- For high-value data processing, it's essential to verify every stage of the supply chain, including electronics manufacturing, to ensure no backdoors or monitoring mechanisms are present.
- The US Department of Defense (DoD) operates the Trusted Foundry Program to ensure secure supply chain operations.
- Organizations should purchase hardware from reputable suppliers to avoid counterfeit or compromised devices.

Hardware Root of Trust:

- A hardware root of trust (RoT) or trust anchor is a secure subsystem that provides attestation for system integrity.
- Trusted Platform Module (TPM) is a common RoT, often found in computers, and used to verify system integrity.
- TPM helps verify and secure the boot process and system integrity.

Hardware Security Module (HSM):

- HSM is used for secure key management, especially in cases where multiple entities require secure key pairs for encryption.
- HSMs automate key management processes and minimize the risk of human compromise.
- HSMs come in various form factors and can be used for enterprise key management.

Anti-Tamper:

- Anti-tamper mechanisms use FPGA and physically unclonable functions (PUF) to detect tampering with hardware.
- These mechanisms can automatically take remedial actions like zero-filling cryptographic keys.

Trusted Firmware:

- Firmware exploits can be mitigated by deploying encryption technologies at the firmware level.
- Unified Extensible Firmware Interface (UEFI) offers security features like secure boot and measured boot to protect against malicious OS or firmware alterations.

eFUSE:

- eFUSE is used for firmware protection, preventing downgrades, and sealing cryptographic keys during firmware development.

Secure Processing:

- Secure processing is designed to protect sensitive data in memory from malicious code.

- Processor security extensions enable secure processing, and trusted execution ensures a trusted OS is running.
- Secure enclaves secure sensitive data in an encrypted container, preventing attacks like buffer overflows.

Explain Vulnerabilities Associated with Specialized Technology

1. **Mobile Devices:**
    - **BYOD (Bring Your Own Device):** When employees bring their own mobile devices to work, it introduces security concerns. These devices may not be under the organization's full control, making it challenging to manage risks associated with them.
    - **Deperimeterization:** With BYOD, sensitive data might leave the organization's security perimeter. Employees who don't secure their personal devices risk data exposure.
    - **Unpatched and Unsecure Devices:** Mobile devices may be difficult to patch, running outdated software, and lacking built-in anti-malware. This can lead to vulnerabilities and malware spread.
    - **Strained Infrastructure:** Multiple devices can strain the network, leading to reduced performance and potential Denial of Service (DoS) attacks.
    - **Forensics Complications:** Investigating incidents involving employee-owned devices can be challenging, compromising forensics investigations.
2. **Specific Mobile Platform Threats and Vulnerabilities:**
    - **Android:** Android devices are more susceptible to malware due to factors like a larger market share, outdated software, and the open nature of the operating system.
    - **iOS:** Jailbroken iOS devices can be targeted, allowing attackers to steal user credentials or gain root access.
    - **Zero-Day Exploits:** Nation-state actors and Advanced Persistent Threats (APTs) may exploit zero-day vulnerabilities in mobile platforms, especially when targeting high-value individuals.
3. **Mobile Device Management (MDM) and Enterprise Mobility Management (EMM):**
    - MDM and EMM solutions help manage mobile devices, offering features like remote wipe, locating devices, and enforcing security policies.
4. **Vulnerabilities Associated with Internet of Things (IoT):**
    - IoT devices can be vulnerable due to poor patch management, use of vendor-specific software, and inadequate security documentation.
    - Smart devices are at risk of compromise, including surveillance through integrated peripherals like cameras and microphones.
5. **Vulnerabilities Associated with Embedded Systems:**

  - Embedded systems are static environments that are ideal for security but can be black boxes to security administrators.
  - Updates for embedded systems are possible but should be carefully controlled.
6. **Vulnerabilities Associated with Controller Systems:**
   - Industrial systems prioritize safety, availability, and integrity over confidentiality.
   - Workflow and process automation systems are often used to control critical infrastructure, and vulnerabilities can have significant consequences.
7. **Mitigation for Vulnerabilities in Specialized Systems:**
   - Recommendations include hiring staff with expertise in operational technology (OT) networks, minimizing connections to OT networks, developing and testing a patch management program, and regularly auditing logical and physical access to OT systems.
8. **Vulnerabilities Associated with Premises and Vehicular Systems:**
   - Building automation and physical access control systems can have vulnerabilities related to PLCs, plaintext credentials, and code injection.
   - Gaining physical access to these systems may lead to further attacks.
   - Vehicles and drones with CAN bus systems may be vulnerable to attacks due to the lack of source addressing and message authentication in the CAN bus protocol. Remote access to these systems can also pose risks.

Understanding Data Privacy and Protection

Identify Non-Technical Data and Privacy Controls

1. **Data Classification and Confidentiality**: The text discusses the classification of data into different levels based on confidentiality. It includes unclassified, classified, confidential, secret, and top-secret categories. This is a non-technical control used to label and protect data based on its sensitivity.
2. **Data Types and Privacy**: The text mentions classifying data into different types, such as personally identifiable information (PII), sensitive personal information (SPI), personal health information (PHI), and financial information. This classification helps in understanding privacy and security requirements for different data types.
3. **Privacy versus Security**: The text distinguishes between privacy and security, emphasizing that privacy is focused on data governance when collecting and processing personal data. It discusses the need for policies to protect personal data and the rights of data subjects.
4. **Legal Requirements**: The text discusses various legal requirements related to data privacy, such as the EU's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), the Sarbanes-Oxley Act (SOX), the Gramm-Leach-Bliley

Act (GLBA), the Federal Information Security Management Act (FISMA), and more. These legal requirements are non-technical controls that organizations must adhere to.

5. **Personal Data Processing Policies**: The text outlines privacy principles and policies, including purpose limitation, data minimization, data sovereignty, and data retention. These policies are non-technical controls aimed at ensuring the proper handling of personal data.
6. **Data Ownership Policies and Roles**: The text defines various roles within an organization related to data ownership and stewardship, such as data owner, data steward, data custodian, and privacy officer. These roles are responsible for managing and protecting data, and they represent non-technical controls.
7. **Data Sharing and Privacy Agreements**: The text discusses legal agreements like Service Level Agreements (SLAs), Interconnection Security Agreements (ISAs), Non-Disclosure Agreements (NDAs), and Data Sharing and Use Agreements. These agreements are non-technical controls used to formalize the responsibilities and expectations related to data sharing and privacy.

Identify Technical Data and Privacy Controls

Access Controls:

- Access control models apply to data security, often used in network, file system, and database security.
- File systems use Access Control Lists (ACLs) to specify permissions for objects, such as files and directories.
- Database security involves securing various database objects like tables, views, rows, and columns.
- Geographic access requirements involve data sovereignty and controlling access from different locations.

File System Permissions Configuration Changes:

- Data breaches often result from incorrect permissions, which can be identified through audits.
- Tools like 'icacls' (Windows) and 'chmod' (Linux) allow configuration and modification of file permissions.
- Linux permissions consist of read, write, and execute, with settings for owner, group, and others.
- Absolute mode uses octal notation (r=4, w=2, x=1) to set permissions.
- More advanced permission configurations can be configured using special permissions and ACLs.

Encryption:

- Encryption safeguards data against unauthorized access and is used for data at rest, data in transit, and data in use.
- Data at rest is stored on persistent media, which can be encrypted using whole disk encryption, database encryption, etc.
- Data in transit is protected using transport encryption protocols like TLS or IPsec.
- Data in use is stored in volatile memory and can be encrypted to prevent unauthorized access.

Data Loss Prevention (DLP) Configuration Changes:

- DLP products automate data discovery, classification, and policy enforcement to prevent unauthorized data access or transfer.
- Components include a policy server, endpoint agents, and network agents.
- DLP agents scan structured and unstructured data, preventing data leakage through various means.
- Remediation actions include alerting, blocking, quarantining, or using tombstone techniques.

DLP Data Discovery and Classification:

- DLP uses methods like classification, dictionaries, policy templates, exact data match, document matching, and statistical analysis.
- DLP helps to protect data with confidentiality classifications or sensitive data types.

Deidentification Controls:

- Deidentification methods are used to remove or generalize personal information from datasets.
- Techniques include data masking, tokenization, aggregation, and banded data.
- Care must be taken, as reidentification is possible with sufficient contextual information.
- K-anonymous data refers to data linked to at least two individuals within a dataset.

Digital Rights Management (DRM) and Watermarking:

- DRM technologies are used to prevent unauthorized distribution of digital content.
- Authorized players and viewers may use cryptographic keys or specific software for playback.
- Watermarking can be used for content protection, including visible and digital (forensic) watermarks.
- Watermarks help track and protect content in case of misuse.

Applying Security Solutions for Software Assurance

Mitigate Software Vulnerabilities and Attacks

Waterfall vs. Agile Software Development Life Cycles:

- Waterfall and Agile are two different approaches to software development.
- Waterfall is a linear and sequential process with distinct phases like requirements, design, coding, testing, and maintenance.
- Agile is an iterative and flexible approach that emphasizes collaboration, customer feedback, and adapting to changes.
- Waterfall is suited for well-defined projects, while Agile is suitable for projects with evolving requirements.

Security Development Life Cycle (SDL):

- SDL runs parallel or integrated with the focus on software functionality and usability.
- SDL incorporates threat, vulnerability, and risk-related controls within the life cycle to produce systems that are secure by design.
- Examples of SDL frameworks include Microsoft's SDL and the OWASP Software Security Assurance Process.

Secure Development Phases in SDL:

- Planning phase involves training developers and testers in security, acquiring security analysis tools, and ensuring a secure development environment.
- Requirements phase determines security and privacy needs regarding data processing and access controls.
- Design phase identifies threats, controls, and secure coding practices to meet requirements.
- Implementation phase includes white-box source code analysis and code review to identify and resolve vulnerabilities.
- Testing phase involves black-box or grey-box analysis to test for vulnerabilities in the published application.
- Deployment phase includes source authenticity verification of installer packages and best practice configuration.

- Maintenance phase covers ongoing security monitoring, incident response, patch development and management, and other security controls.

Secure Coding Best Practices:

- Secure coding standards provide rules and guidelines for developing secure software systems.
- Open Web Application Security Project (OWASP) provides resources on secure programming, web app vulnerabilities, and best practices.
- SysAdmin, Network, and Security (SANS) Institute offers research, white papers, and best practice guidance on secure coding.

Execution and Escalation Attacks:

- Attacks against software code aim to run the attacker's code on the system.
- Arbitrary code execution allows attackers to run their code on the system.
- Privilege escalation occurs when a user gains access to additional resources or functionality they are not normally allowed to access.
- Types of privilege escalation include vertical and horizontal privilege escalation.

Rootkits:

- Rootkits are tools with root-level access to the computing device, allowing unrestricted access.
- Kernel mode rootkits can gain complete control over the system and require low-level access.
- User mode rootkits work within the user-level processes and are less privileged.

Overflow Attack Types and Vulnerabilities:

- Buffer overflow attacks target the stack or heap, potentially allowing arbitrary code execution.
- Integer overflow attacks can cause unexpected behavior in software, like changing a debit to a credit or altering buffer sizes.
- Memory layout, languages used, and security measures can mitigate overflow issues.

Race Condition Vulnerabilities:

- Race conditions occur when the order and timing of events affect the outcome of execution processes.
- Null pointer dereference is a common exploit that can trigger race conditions.
- Time of check to time of use (TOCTTOU) race conditions can lead to exploits in which a resource is changed between checking and using it.

Improper Error Handling Vulnerabilities:

- Error handling is crucial in software development to gracefully handle errors and exceptions.
- Poorly written error handlers can lead to vulnerabilities, leakage of sensitive information, and even attacks.
- Custom error handlers should be used, and logging should be carefully configured to prevent information leakage.

Software Design Vulnerabilities:

- Insecure components, insufficient logging, and weak or default configurations can introduce vulnerabilities in the software.
- Best practices should be followed for each type of platform, whether it's client/server, web, mobile, embedded, firmware, SoC, or any other type of development.

Mitigate Web Application Vulnerabilities and Attacks

Remote File Inclusion (RFI):

- RFI involves injecting a remote file into a web app or website.
- Attackers manipulate parameters to execute scripts from external malicious links.
- Example: Injecting a malicious PHP file via a parameter in a PHP page.

Local File Inclusion (LFI):

- Attackers add files to a web app from the hosting server.
- Exploits vulnerabilities like directory traversal.
- Attacker may gain control of the server, e.g., opening a command prompt.
- Techniques like null characters (%00) can bypass security mechanisms.

Cross-Site Scripting Attacks (XSS):

- XSS is a powerful input validation exploit.
- It involves a trusted site, a client, and an attacker's site.
- Attackers inject malicious code via links, email messages, or form posts.
- Malicious code runs in the client's browser with trusted site permissions.
- Effective due to breaking browser's security model and relying on scripting.

Persistent XSS:

- Involves inserting code into a back-end database.

- Attacker submits a post with a malicious script, which executes when other users view the message.
- Exploits server-side scripts.

Document Object Model (DOM) XSS:

- Exploits vulnerabilities in client-side scripts using DOM.
- Allows modifying content and layout of a web page.
- Can run with the user's local system privileges.

SQL Injection:

- Attackers modify SQL queries using input within web apps.
- Input sources include URL parameters, form fields, cookies, etc.
- Common method: Testing with single and double apostrophes.
- Attackers may use SQL wildcard characters (%) or mathematical expressions.
- Example of a SQL injection exploit.

Insecure Object Reference:

- Involves manipulating parameters to grant unauthorized access.
- Example: Changing an account name parameter to access other accounts.
- Important to implement access control techniques.

Extensible Markup Language (XML) Attacks:

- XML used for authentication, data exchange, and uploading in web apps.
- Vulnerable to spoofing, request forgery, arbitrary data/code injection.
- Types of attacks: XML bomb (Billion Laughs), XML External Entity (XXE).

Secure Coding Best Practices:

- Input validation is crucial.
- Validate input locally and remotely.
- Use normalization or sanitization procedures.
- Beware of canonicalization attacks.
- Implement output encoding to prevent malicious code execution.
- Use parameterized queries to defend against code injection.

Authentication Attack Types and Best Practices:

- Impersonation attacks target obtaining user accounts fraudulently.
- Spoofing is software-based attack to assume another identity.
- Man-in-the-Middle (MitM) and man-in-the-browser (MitB) attacks.
- Password spraying, credential stuffing, and best practices for defense.

Session Hijacking Attack Types:

- Session management is vital for web applications.
- Session hijacking exploits cookies, session tokens, and browser security.
- Attack types: XSRF/CSRF, cookie poisoning, and data protection.
- Prevention techniques: User-specific tokens, encryption, and secure cookies.

Clickjacking:

- Clickjacking tricks users into clicking unintended links.
- Commonly achieved through framing using iframes.
- Frame busting and X-Frame-Options defense are countermeasures.

Analyze Output from Application Assessments

Formal Methods for Verification:

- Formal methods are used for critical software where corner cases must be eliminated.
- They require a formal system specification, which can be complex.
- They are valuable in verifying the security of systems.
- Byron Cook's article on formal reasoning about Amazon Web Services is a case study.

User Acceptance Testing (UAT):

- UAT is the beta testing phase of software.
- It involves limited users testing the software to ensure it meets requirements, including security.
- UAT gathers feedback from the target audience.
- It assesses whether users accept the product, focusing on security.

Security Regression Testing:

- Regression testing verifies that code changes haven't caused existing functionality to fail.
- Security regression testing focuses on input validation, data processing, and control logic.
- It identifies broken security mechanisms after code changes.

Reverse Engineering Tools:

- Reverse engineering extracts code from a binary executable.
- Three principal means: machine code, assembly code, high-level code.
- Disassemblers and decompilers are used to analyze code.
- Bytecode is used in virtual machine environments.

Dynamic Analysis Tools:

- Dynamic analysis involves executing the compiled program.
- Debugger is the primary means for dynamic analysis.
- Stress tests evaluate app performance under extreme loads.
- Fuzzing tests software for bugs and vulnerabilities.

Web Application Scanner Output Analysis:

- Web application scanners identify vulnerabilities.
- Nikto and Arachni are common web application scanners.
- They examine vulnerabilities like XSS, SQL injection, and more.
- Web proxies like Burp Suite and OWASP ZAP analyze communication between apps and servers.

Applying Security Solutions for Cloud and Automation

Identify Cloud Service and Deployment Model Vulnerabilities

Public Cloud Deployment Model Threats and Vulnerabilities:

- Public clouds are shared by multiple consumers.
- Risk to the security and privacy of data from other tenants.
- CSP (Cloud Service Provider) is responsible for the integrity and availability of the platform.
- Consumers are responsible for instances within the cloud, client authorization, and management.
- Data should be encrypted to and from the public cloud.

Community Cloud Deployment Model:

- Multiple organizations share ownership.
- Pool resources for common concerns like standardization and security policies.
- Security responsibilities should be clearly defined among cooperating organizations.

Multicloud:

- Organization uses services from multiple CSPs.
- Requires due diligence and risk assessment.
- Ensuring integration and communication components work securely is important.

Private Cloud Deployment Model Threats and Vulnerabilities:

- Operated by a single company.
- More control over cloud infrastructure.
- Greater responsibility for security.
- Management of security of host platforms, hypervisors, and automation management platforms.

Hybrid Clouds:

- Composed of public cloud, private cloud, and on-premises infrastructure.
- Greater complexity and decentralized nature.
- Demonstrating compliance can be challenging.
- Security management across both public and private cloud components.

Cloud Service Model Threats and Vulnerabilities:

- Software as a Service (SaaS): CSP handles platform and infrastructure security, consumer is responsible for application security.
- Infrastructure as a Service (IaaS): CSP is responsible for the resource pool's security, while consumers have responsibilities for instances' security.
- Platform as a Service (PaaS): CSP handles platform components' security, while consumers are responsible for application security.

Cloud-Based Infrastructure Management:

- Virtual Private Cloud (VPC) provides a virtual network within a public cloud.
- Consumers are responsible for configuring and securing network components.

Cloud versus On-Premises:

- Security solutions can be deployed on-premises or in the cloud.
- Cloud-based solutions can be cost-effective and provide additional security.
- Compliance and vendor lock-in can be concerns.

Cloud Access Security Broker (CASB):

- CASB mediates access to cloud services by users across devices.
- Functions include single sign-on authentication, malware scanning, monitoring, and DLP.
- CASBs function in forward proxy, reverse proxy, and API modes for different security management purposes.

Explain Service-Oriented Architecture

- **Service-Oriented Architecture (SOA) and Microservices**:
  - In the context of cloud and automation, traditional network applications and infrastructure are transitioning to service-oriented architecture (SOA) and microservices architecture.
  - SOA and microservices focus on efficiently mapping business workflows to IT systems that support them, offering more flexibility.
- **Service-Oriented Architecture (SOA)**:
  - SOA involves atomic services closely aligned with business workflows, each with well-defined inputs and outputs.
  - Services are self-contained and do not rely on the state of other services, making interoperability easier.
  - Loose coupling allows services and clients to work independently of each other, promoting flexibility and sustainability.
- **Microservices**:
  - Microservices are a design paradigm applied to application development, emphasizing self-contained service modules that perform single functions.
  - Microservices are highly decoupled, allowing for independent development, testing, and deployment.
  - They are more easily scalable compared to monolithic applications.
- **Simple Object Access Protocol (SOAP)**:
  - SOAP is used in SOA for accessing data from various sources through a well-defined interface.
  - SOAP uses XML-format messaging and includes features like authentication, transport security, and error handling.
- **Security Assertions Markup Language (SAML)**:
  - SAML is an XML-based framework used for exchanging security-related information like user authentication and entitlement.
  - It enables single sign-on (SSO) and federated identity management.
  - SAML communicates information in the form of assertions and relies on an identity provider (IdP) and a service provider (SP).
- **Representational State Transfer (REST)**:
  - RESTful APIs are commonly used in public clouds, offering a more flexible and loosely defined architectural framework compared to SOAP.

  - REST requests can be submitted as HTTP operations, with each resource having a single URL.
  - REST responses can use various formats, including JSON.
- **OAuth (Open Authorization)**:
  - OAuth 2 is a protocol that enables the sharing of user profile information between sites without revealing the user's password.
  - It involves clients, identity providers, and resource servers, allowing access to user accounts with authorization tokens.
- **JSON Web Tokens (JWTs)**:
  - JWTs are used to format tokens and contain a header, payload (claims fields), and a signature.
  - They are often used for authentication and authorization purposes.
- **OpenID Connect (OIDC)**:
  - OIDC is an authentication protocol that builds on OAuth and defines specific token fields.
- **Application Programming Interface (API)**:
  - Cloud Service Providers (CSPs) offer APIs for automated administration, management, and monitoring of their services.
  - APIs are used for provisioning resources, configuring services, and exchanging data between client applications.
- **Scripting**:
  - Scripting languages like Python, Ruby, and JavaScript are used for automating cloud-related administrative tasks.
  - Scripts include parameters, logic statements, validation, error handlers, and unit tests.
- **Workflow Orchestration**:
  - Orchestration automates sequences of tasks and entire processes, including resource provisioning, workload management, and service deployment.
  - Tools like Chef, Puppet, Ansible, Docker, and Kubernetes are used for orchestration.

Analyze Output from Cloud Infrastructure Assessment Tools

API Key Management:

- Avoid embedding API keys in source code; use environment variables.

- Allocate only necessary authorizations and actions to a single key.
- Delete unused keys and periodically regenerate keys.
- Apply strict hardening policies to client hosts and development workstations.

Logging and Monitoring:

- Ensure sufficient logging and monitoring for API security.
- Monitor for potential DoS attacks and authentication errors.
- Establish logging and monitoring requirements in the service level agreement (SLA).

Unprotected Storage:

- Cloud storage containers (buckets or blobs) have customizable metadata attributes.
- Misconfigurations like incorrect permissions and origin settings can expose data to risks.
- Vulnerabilities can lead to data breaches, destruction, or integrity issues.

Cloud Infrastructure Assessment Tools:

- Managing vulnerabilities in hosted public cloud can be complex due to reliance on service providers.
- Use tools like ScoutSuite, Prowler, and Pacu for automated vulnerability and penetration testing assessment.
- Cloud service providers' acceptable use policies should be consulted before scanning hosts and services.

Digital Forensics for Cloud:

- Forensic analysis in the cloud can be challenging due to virtualized resources and dispersed data.
- On-demand cloud services make data recovery difficult.
- Chain of custody issues can arise, and reliance on cloud service providers may be required.

Compare Automation Concepts and Technologies

Continuous Integration and Deployment:

- Continuous Integration (CI) emphasizes frequent code commits and automated testing to detect and resolve conflicts early in development.

- Continuous Delivery (CD) involves testing all infrastructure components supporting the app.
- Continuous Deployment is the process of making changes to the production environment to support a new app version.

DevSecOps:

- DevOps promotes collaboration between developers and system administrators to build, test, and release software faster.
- DevSecOps extends collaboration to include security specialists, making security a primary consideration at every stage.

Infrastructure as Code (IaC):

- IaC replaces manual configuration with automation and orchestration, leading to consistent builds and lower IT costs.
- IaC ensures idempotence, where the same input parameters always produce the same result.

Machine Learning:

- Machine learning uses algorithms and data to develop strategies for tasks such as identifying objects or detecting patterns.
- Deep learning involves neural networks with multiple hidden layers to make more informed determinations about complex concepts.

Data Enrichment and Malware Signature Creation:

- Data enrichment enhances SIEM analysis by providing contextual information, reducing false positives, and improving threat intelligence.
- Automated malware signature creation uses machine learning to detect obfuscated malware by analyzing features in executables.

Security Orchestration, Automation, and Response (SOAR):

- SOAR combines automation and orchestration to streamline incident response and threat hunting.
- Playbooks and runbooks guide specific incident response actions, leveraging automation while allowing human analysts to make informed decisions.