Cybersecurity CYSA+ Terms

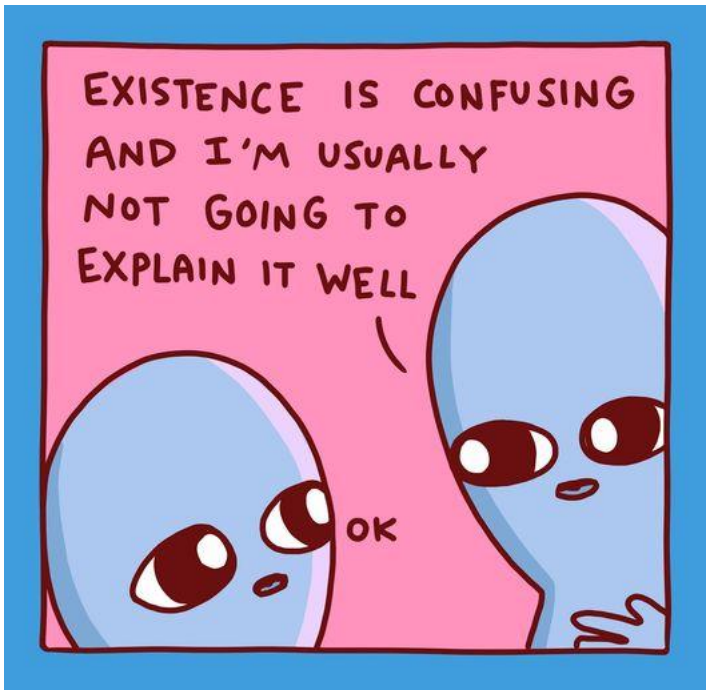
NUCLEAR NOTES©

Rote Memorization as quickly as humanly possible!

Black Tower Academy

ajay Menendez

DRAFT .5



CyberSecurity Terms and Definitions – CYSA+

Domain 1 Security Operations

Log ingestion

Log ingestion refers to the process of collecting and aggregating log data generated by various systems, applications, and devices across an organization's IT infrastructure. This data is typically stored centrally for analysis, monitoring, and troubleshooting purposes. Log ingestion systems gather logs from different sources, normalize them into a common format, and store them in a centralized repository or data store for further analysis.

Time synchronization: In log ingestion, time synchronization ensures that log entries from different sources are accurately timestamped and aligned. It ensures consistency and reliability in log analysis and correlation by synchronizing the clocks of all devices and systems within an organization's network. This synchronization can be achieved using network time protocols such as NTP (Network Time Protocol) or PTP (Precision Time Protocol).

Logging levels: Logging levels categorize log messages based on their severity or importance, allowing administrators and analysts to filter and prioritize log entries during analysis. Common logging levels include DEBUG, INFO, WARN, ERROR, and FATAL. Each level indicates the severity of the event being logged, with DEBUG being the least severe and FATAL indicating critical errors that require immediate attention.

Operating system (OS) concepts

Windows Registry: The Windows Registry is a hierarchical database that stores configuration settings and options for the Windows operating system and installed applications. It contains information about system hardware, software settings, user preferences, and system configurations. The registry is organized into keys, subkeys, and entries, and it is used by the operating system and applications to access and store configuration data.

System hardening: System hardening is the process of securing and reducing the attack surface of an operating system by implementing security best practices and configurations. This includes disabling unnecessary services and features, applying security patches and updates, configuring access controls, enabling firewalls, and implementing security policies to protect against known vulnerabilities and threats.

File structure: The file structure of an operating system refers to the organization and layout of files and directories on disk. It includes the directory hierarchy, file naming conventions, and file system layout used by the operating system to organize and manage data. Understanding the file

structure is essential for navigating and managing files and directories, locating configuration files, and troubleshooting issues.

Configuration file locations: Configuration files are files used by applications and the operating system to store settings and parameters. They are typically stored in specific directories or locations within the file system. Knowing the locations of configuration files is important for system administrators and users to modify settings and customize the behavior of applications and services.

System processes: System processes are programs or tasks running on an operating system that perform various functions and operations. They include both user-level processes initiated by users and system-level processes managed by the operating system kernel. System processes manage system resources, handle user requests, and execute system tasks such as memory management, process scheduling, and I/O operations.

Hardware architecture: Hardware architecture refers to the design and organization of the physical components of a computer system, including the CPU (Central Processing Unit), memory, storage devices, and peripherals. It encompasses the hardware components, their interconnections, and how they interact to execute instructions and process data. Understanding hardware architecture is essential for system administrators and developers to optimize system performance, troubleshoot hardware issues, and design efficient computing systems.

Infrastructure concepts

Serverless: Serverless computing is a cloud computing model in which cloud providers dynamically allocate and manage infrastructure resources to execute code in response to events or requests. In a serverless architecture, developers write and deploy functions or application code without managing underlying servers or infrastructure. Cloud providers handle server provisioning, scaling, and maintenance, allowing developers to focus on writing and deploying code.

Virtualization: Virtualization is the process of creating virtual instances or representations of computing resources such as servers, storage, networks, or operating systems. It enables the abstraction and isolation of physical hardware resources, allowing multiple virtual instances to run on a single physical machine. Virtualization provides flexibility, scalability, and resource efficiency by decoupling software from underlying hardware, making it easier to manage and optimize IT infrastructure.

Containerization: Containerization is a lightweight form of virtualization that encapsulates and isolates application code, dependencies, and runtime environments into self-contained units called containers. Containers package applications with their dependencies, libraries, and configuration files, allowing them to run consistently across different computing environments. Containerization technologies such as Docker and Kubernetes provide efficient deployment, scaling, and management of containerized applications, making it easier to build and deploy cloud-native and microservices-based architectures.

Network architecture

On-premises: On-premises network architecture refers to the traditional model where all network resources and infrastructure are located and managed within an organization's physical premises or data centers. In this model, organizations own and maintain their hardware, servers, and networking equipment, allowing them to have full control over their IT environment but requiring significant upfront investment and ongoing maintenance costs.

Cloud: Cloud network architecture involves deploying and accessing network resources, services, and applications over the internet through cloud service providers such as Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform (GCP). In a cloud architecture, organizations leverage cloud computing services to host, manage, and scale their IT infrastructure dynamically, paying for resources on a consumption basis. Cloud architecture offers scalability, flexibility, and cost-effectiveness but requires a shift in mindset and new skills for managing cloud-based resources.

Hybrid: Hybrid network architecture combines elements of both on-premises and cloud environments, allowing organizations to leverage the benefits of both models. In a hybrid architecture, organizations can deploy certain workloads or services on-premises while using cloud services for others. This approach provides flexibility, scalability, and resilience by allowing organizations to choose the best deployment model for each workload based on factors such as performance, security, and cost.

Network segmentation: Network segmentation involves dividing a network into multiple smaller, isolated segments or subnetworks to improve security, performance, and manageability. Segmentation helps contain network breaches, limit the spread of malware, and control access to sensitive resources by enforcing access policies and isolating critical assets from less secure parts of the network.

Zero trust: Zero trust network architecture is a security model based on the principle of "never trust, always verify." In a zero trust architecture, all users, devices, and network traffic are treated as untrusted, and access to resources is granted based on continuous authentication, authorization, and least privilege principles. Zero trust architectures assume that threats can originate from both inside and outside the network perimeter, requiring strict access controls and verification mechanisms for all network traffic.

Secure access secure edge (SASE): Secure Access Service Edge (SASE) is a network architecture that integrates network security and wide-area networking (WAN) capabilities into a cloud-native service model. SASE converges networking and security functions such as SD-WAN (Software-Defined Wide Area Network), VPN (Virtual Private Network), firewall, secure web gateway, and Zero Trust Network Access (ZTNA) into a unified cloud-based platform. SASE provides secure and scalable access to network resources from any location or device, offering improved performance, flexibility, and cost-efficiency compared to traditional network architectures.

Software-defined networking (SDN): Software-defined networking is an approach to network management and architecture that abstracts network control and forwarding functions from underlying hardware and implements them in software. SDN decouples the control plane from the data plane, allowing administrators to centrally manage and configure network devices and traffic flows through software-based controllers. SDN enables programmability, automation, and dynamic resource allocation, making networks more agile, scalable, and adaptable to changing business requirements.

Identity and access management

Multifactor authentication (MFA): Multifactor authentication is a security mechanism that requires users to provide multiple forms of identification to verify their identity before granting access to resources or systems. MFA typically combines two or more authentication factors, such as passwords, biometric data (fingerprint, facial recognition), security tokens, or mobile devices, to enhance security and reduce the risk of unauthorized access.

Single sign-on (SSO): Single sign-on is an authentication process that allows users to access multiple applications or systems with a single set of credentials (username and password). Instead of requiring users to log in separately to each application, SSO enables seamless and secure access to various resources after an initial authentication. SSO improves user experience, productivity, and security by reducing the need for multiple passwords and centralizing authentication controls.

Federation: Federation is a mechanism that enables identity and access management across multiple domains, organizations, or service providers. In a federated identity model, trusted relationships are established between identity providers (IdPs) and service providers (SPs), allowing users to access resources seamlessly and securely across different domains without the need for separate authentication. Federation standards such as Security Assertion Markup Language (SAML) and OpenID Connect (OIDC) facilitate interoperability and trust between identity providers and service providers, enabling federated identity management and authentication workflows.

Privileged Access Management (PAM): Privileged Access Management (PAM) refers to the practice of controlling and managing access to privileged accounts, which have elevated permissions and access rights within an organization's IT infrastructure. PAM solutions help organizations mitigate the risks associated with unauthorized access to sensitive systems, data, and resources by enforcing strict controls, monitoring privileged user activities, and implementing least privilege principles. PAM solutions typically include features such as password vaulting, session monitoring and recording, privileged user authentication, access control policies, and privileged task automation.

Passwordless: Passwordless authentication is a method of verifying user identities without requiring traditional passwords. Instead of relying solely on passwords, passwordless authentication utilizes alternative authentication factors such as biometrics (fingerprint, facial recognition), hardware tokens, mobile push notifications, or public/private key pairs to verify users' identities. Passwordless authentication enhances security, usability, and user experience by

reducing the risk of password-related attacks (e.g., phishing, credential theft) and eliminating the need for users to remember complex passwords.

Cloud Access Security Broker (CASB): A Cloud Access Security Broker (CASB) is a security technology that acts as an intermediary between an organization's on-premises infrastructure and cloud service providers' platforms, allowing organizations to extend their security policies and controls to cloud environments. CASB solutions provide visibility, governance, and security controls for cloud applications and services by monitoring user activities, enforcing access policies, detecting and preventing threats, and encrypting data. CASB solutions help organizations secure their cloud deployments, ensure compliance with regulations, and protect sensitive data from unauthorized access or exposure.

Encryption:

Public Key Infrastructure (PKI): Public Key Infrastructure (PKI) is a set of cryptographic techniques and protocols used to create, manage, distribute, and validate digital certificates and encryption keys. PKI enables secure communication and authentication in various IT systems and applications by leveraging asymmetric encryption algorithms and digital signatures. PKI components include Certificate Authorities (CAs), Registration Authorities (RAs), Certificate Revocation Lists (CRLs), and digital certificates (e.g., SSL/TLS certificates, code signing certificates) issued to entities such as users, devices, and servers.

Secure Sockets Layer (SSL) inspection: SSL inspection, also known as SSL/TLS interception or SSL decryption, is a process of intercepting and decrypting encrypted SSL/TLS traffic to inspect its contents for security threats or policy violations. SSL inspection is commonly performed by security appliances such as firewalls, proxies, or intrusion detection/prevention systems (IDS/IPS) to enforce security policies, detect malware, and prevent data exfiltration or unauthorized access. SSL inspection involves decrypting SSL/TLS-encrypted traffic, inspecting the decrypted content for malicious activity, and re-encrypting the traffic before forwarding it to its destination.

Sensitive Data Protection:

Data Loss Prevention (DLP): Data Loss Prevention (DLP) is a set of security technologies and policies designed to prevent unauthorized disclosure or leakage of sensitive data from an organization's network, endpoints, and storage systems. DLP solutions monitor, detect, and protect sensitive data (e.g., personally identifiable information, intellectual property, financial data) by classifying data, enforcing data usage policies, monitoring data flows, and blocking or encrypting sensitive information in transit or at rest. DLP solutions help organizations comply with regulations, prevent data breaches, and safeguard their confidential information.

Personally Identifiable Information (PII): Personally Identifiable Information (PII) refers to any information that can be used to identify, contact, or locate an individual, either on its own or in combination with other data elements. PII includes but is not limited to names, addresses, phone numbers, email addresses, Social Security numbers, biometric data, and financial account

numbers. Protecting PII is essential for safeguarding individuals' privacy and preventing identity theft, fraud, or misuse of personal information.

Cardholder Data (CHD): Cardholder Data (CHD) encompasses any sensitive information associated with payment cards (e.g., credit card, debit card) that is processed, transmitted, or stored by merchants, service providers, or payment processors. CHD includes cardholder names, primary account numbers (PANs), expiration dates, and security codes (CVV/CVC). Protecting cardholder data is crucial for complying with payment card industry standards such as the Payment Card Industry Data Security Standard (PCI DSS) and preventing payment card fraud, data breaches, and financial losses.

Network-related:

Bandwidth consumption: Bandwidth consumption refers to the amount of network capacity or data transfer rate utilized by network devices or applications. Unusually high bandwidth consumption may indicate legitimate activities such as large file transfers or streaming media, but it could also be a sign of malicious activities such as distributed denial-of-service (DDoS) attacks, data exfiltration, or unauthorized use of network resources.

Beaconing: Beaconing is a technique used by malware to periodically send signals or "beacons" to command-and-control (C2) servers or remote attackers to establish communication and receive instructions. Beaconing traffic often exhibits regular intervals and unusual patterns, making it detectable through network monitoring and analysis tools.

Irregular peer-to-peer communication: Irregular peer-to-peer communication refers to network traffic generated by peer-to-peer (P2P) file sharing applications or protocols that deviates from normal usage patterns or organizational policies. Such communication may indicate the presence of unauthorized or potentially malicious file sharing activities.

Rogue devices on the network: Rogue devices are unauthorized or unmanaged devices that connect to a network without proper authorization or oversight from network administrators. Rogue devices can include unauthorized wireless access points, switches, routers, or other network-connected devices that pose security risks, such as introducing vulnerabilities, creating unauthorized access points, or bypassing network security controls.

Scans/sweeps: Scans or sweeps refer to reconnaissance activities conducted by attackers or security professionals to identify and enumerate potential targets, vulnerabilities, or misconfigurations within a network. Scanning activities may include port scans, vulnerability scans, network mapping, or fingerprinting techniques aimed at gathering intelligence for future attacks or security assessments.

Unusual traffic spikes: Unusual traffic spikes are sudden, significant increases in network traffic volume or activity that deviate from normal patterns or baseline levels. Traffic spikes may be caused by legitimate events such as software updates, marketing campaigns, or sudden user activity, but they could also be indicative of malicious activities such as DDoS attacks, malware infections, or network intrusion attempts.

Activity on unexpected ports: Activity on unexpected ports refers to network traffic or communication occurring on ports or protocols that are not typically associated with legitimate services or applications within an organization's network. Such activity may indicate the presence of unauthorized or suspicious activities, such as malware command-and-control communications, backdoor access, or covert data exfiltration channels.

Host-related:

Processor consumption: Processor consumption, also known as CPU utilization, refers to the percentage of a computer's central processing unit (CPU) capacity being used by running processes or applications. Abnormally high CPU consumption may indicate heavy computational tasks, poorly optimized software, or malicious processes such as cryptojacking malware that hijacks CPU resources for cryptocurrency mining.

Memory consumption: Memory consumption refers to the amount of random access memory (RAM) or system memory utilized by running processes, applications, or services on a host system. Excessive memory consumption may result in performance degradation, system instability, or denial-of-service conditions, potentially caused by memory leaks, resource-intensive applications, or memory-resident malware.

Drive capacity consumption: Drive capacity consumption refers to the amount of storage space or disk capacity being used by files, applications, or system components on a storage device (e.g., hard disk drive, solid-state drive). Monitoring drive capacity consumption helps ensure sufficient storage space availability, identify potential storage constraints, and detect abnormal usage patterns or unexpected data growth that may indicate unauthorized file storage or data exfiltration.

Unauthorized software: Unauthorized software refers to applications, programs, or software components installed on a host system without proper authorization, approval, or compliance with organizational policies. Unauthorized software may include unlicensed or pirated software, unsupported or obsolete applications, or potentially unwanted programs (PUPs) that pose security risks, introduce vulnerabilities, or violate software usage policies.

Malicious processes: Malicious processes are unauthorized or malicious software components running on a host system that perform harmful or unauthorized activities without the user's knowledge or consent. Malicious processes may include malware, viruses, worms, ransomware, spyware, or trojan horses designed to compromise system security, steal sensitive information, or disrupt normal operations.

Unauthorized changes: Unauthorized changes refer to modifications, alterations, or updates made to system configurations, settings, files, or registry entries without proper authorization, validation, or change management processes. Unauthorized changes may be caused by human errors, software glitches, or malicious activities such as unauthorized privilege escalation, system tampering, or malware infections attempting to evade detection or maintain persistence.

Unauthorized privileges: Unauthorized privileges refer to excessive or elevated access rights, permissions, or privileges granted to user accounts, processes, or applications beyond what is necessary for performing legitimate tasks or functions. Unauthorized privileges increase the risk of insider threats, privilege abuse, unauthorized data access, or system compromise, potentially leading to security breaches, data leaks, or compliance violations.

Data exfiltration: Data exfiltration, also known as data extrusion or data exfiltration, is the unauthorized transfer, theft, or leakage of sensitive or confidential data from a host system or network to an external destination controlled by an attacker. Data exfiltration techniques may involve covert channels, command-and-control communications, file transfer protocols, or encryption methods to bypass security controls, evade detection, and exfiltrate sensitive information without being detected by security monitoring tools or network defenses.

Abnormal OS process behavior: Abnormal operating system (OS) process behavior refers to anomalous activities, actions, or behaviors exhibited by system-level processes, services, or components that deviate from expected or normal patterns of operation. Abnormal OS process behavior may indicate the presence of malware, rootkits, backdoors, or other malicious software attempting to compromise system integrity, evade detection, or maintain persistence on the host system.

File system changes or anomalies: File system changes or anomalies refer to modifications, additions, deletions, or inconsistencies observed within the file system structure, directories, or file metadata on a host system. File system changes may be caused by legitimate user activities, software installations, updates, or configuration changes, but they could also be indicative of unauthorized file modifications, tampering, or malicious activity attempting to conceal evidence, hide malware payloads, or manipulate system files.

Registry changes or anomalies: Registry changes or anomalies refer to modifications, additions, deletions, or inconsistencies detected within the Windows Registry database, which stores system configurations, settings, and metadata on Microsoft Windows operating systems. Registry changes may be legitimate, such as software installations, updates, or user preferences, but they could also indicate unauthorized changes, registry hijacking, or malware activity attempting to modify critical system settings, execute persistence mechanisms, or evade detection.

Unauthorized scheduled tasks: Unauthorized scheduled tasks refer to automated or recurring processes, scripts, or jobs configured to run at predefined intervals or specific times on a host system without proper authorization, oversight, or change control procedures. Unauthorized scheduled tasks may be used by attackers to execute malicious activities, backdoor commands, or persistence mechanisms, such as malware payloads, data exfiltration routines, or system reconnaissance scripts, to maintain access, evade detection, or escalate privileges.

Application-related:

Anomalous activity: Anomalous activity refers to unusual or abnormal behavior observed within an application's usage patterns, transactions, or operations that deviate from expected or

typical behavior. Anomalous activity may include sudden spikes or drops in user activity, unusual access patterns, unauthorized operations, or abnormal system resource consumption, which could indicate security incidents, software bugs, or operational issues that require investigation and remediation.

Introduction of new accounts: Introduction of new accounts refers to the creation or addition of user accounts, credentials, or access privileges within an application without proper authorization, oversight, or adherence to organizational policies. The introduction of new accounts may result from administrative errors, user provisioning processes, or malicious activities such as unauthorized access, insider threats, or account takeover attempts aimed at gaining unauthorized access to sensitive data or resources.

Unexpected output: Unexpected output refers to unexpected or irregular results, responses, or outputs generated by an application in response to user input, requests, or commands. Unexpected output may indicate software bugs, logic errors, input validation failures, or security vulnerabilities that could lead to data corruption, application crashes, or unintended consequences, posing usability, reliability, or security risks to users or the organization.

Unexpected outbound communication: Unexpected outbound communication refers to unexpected or unauthorized network connections, data transmissions, or communication attempts initiated by an application to external servers, domains, or IP addresses without legitimate reasons or user consent. Unexpected outbound communication may indicate malicious activities such as command-and-control (C2) traffic, data exfiltration, malware infections, or unauthorized access attempts that require investigation and mitigation to prevent security breaches or data leaks.

Service interruption: Service interruption refers to the disruption, degradation, or unavailability of critical services, functions, or features provided by an application due to technical failures, software bugs, infrastructure issues, or malicious attacks. Service interruptions may result in downtime, loss of productivity, financial losses, or reputational damage, highlighting the importance of proactive monitoring, redundancy, and disaster recovery measures to ensure service continuity and reliability.

Application logs: Application logs are records or entries generated by an application to capture and store information about its activities, events, errors, transactions, or interactions with users or other systems. Application logs play a crucial role in troubleshooting, debugging, auditing, compliance, and security incident response by providing visibility into application behavior, performance metrics, security events, and user activities that can be analyzed, monitored, or archived for forensic analysis, compliance reporting, or operational insights.

Other:

Social engineering attacks: Social engineering attacks are manipulation tactics used by attackers to deceive, manipulate, or exploit human psychology, trust, or emotions to trick individuals into disclosing sensitive information, performing actions, or bypassing security controls. Social engineering attacks may involve impersonation, pretexting, phishing, spear

phishing, baiting, or other techniques aimed at exploiting human vulnerabilities to gain unauthorized access, steal credentials, or compromise security defenses.

Obfuscated links: Obfuscated links are web links or URLs that have been deliberately obscured, disguised, or encoded to conceal their true destination or purpose from users or security tools. Obfuscated links may use URL shortening services, URL redirection techniques, or character encoding schemes to obfuscate malicious URLs, phishing links, or malware download links embedded in emails, messages, or web pages, making them harder to detect or identify by users or automated security controls.

Tools:

Packet capture:

> **Wireshark**: Wireshark is a popular open-source network protocol analyzer that allows users to capture and interactively browse the traffic running on a computer network in real-time. It is widely used for network troubleshooting, analysis, protocol development, and education. Wireshark supports hundreds of protocols and provides detailed packet inspection, filtering, and analysis capabilities.
>
> **tcpdump**: tcpdump is a command-line packet analyzer available for Unix-like operating systems. It captures network packets and displays them in a human-readable format or saves them to a file for offline analysis. tcpdump is commonly used for network traffic monitoring, troubleshooting, security analysis, and protocol debugging tasks.

Log analysis/correlation:

> **Security Information and Event Management (SIEM)**: SIEM is a software solution that aggregates, correlates, and analyzes log data and security events from various sources across an organization's IT infrastructure. SIEM platforms provide real-time threat detection, incident response, compliance reporting, and security monitoring capabilities by centralizing and correlating log data from networks, servers, applications, and security devices.
>
> **Security Orchestration, Automation, and Response (SOAR)**: SOAR platforms integrate security tools, technologies, and processes to automate incident response, threat hunting, and security operations workflows. SOAR solutions orchestrate and streamline security tasks, playbooks, and workflows by integrating with existing security tools, enriching threat intelligence, and automating response actions to improve operational efficiency, incident response times, and security posture.

Endpoint security:

> **Endpoint Detection and Response (EDR)**: EDR solutions provide advanced threat detection, visibility, and response capabilities on endpoints such as desktops, laptops, servers, and mobile devices. EDR platforms continuously monitor endpoint activity,

detect suspicious behavior, analyze threats in real-time, and respond to security incidents by blocking, isolating, or remediating threats to prevent data breaches and unauthorized access.

Domain name service (DNS) and Internet Protocol (IP) reputation:

WHOIS: WHOIS is a protocol and database query tool used to look up registration and ownership information of domain names, IP addresses, and autonomous system numbers (ASNs). WHOIS provides details about domain registrants, domain status, registration dates, and contact information, helping organizations investigate domain ownership, identify malicious domains, and assess IP reputation.

AbuseIPDB: AbuseIPDB is a free online service and database that collects and analyzes reports of malicious IP addresses engaged in abusive behavior such as spamming, hacking, scanning, or distributing malware. AbuseIPDB allows users to check the reputation of IP addresses, report abusive activity, and contribute to a community-driven platform for tracking and mitigating cyber threats.

File analysis:

Strings: Strings is a command-line utility that extracts human-readable strings of text from binary files, executables, libraries, and other data files. It is commonly used for reverse engineering, malware analysis, and forensic investigations to extract plaintext strings, URLs, file paths, API calls, and other valuable information embedded within files.

VirusTotal: VirusTotal is a free online service and malware analysis platform that aggregates antivirus scan engines, file analysis tools, and threat intelligence feeds to analyze and detect suspicious files, URLs, and domains. VirusTotal allows users to upload files or submit URLs for analysis, check for malware infections, and obtain detailed reports and verdicts from multiple antivirus engines and security vendors.

Sandboxing:

Joe Sandbox: Joe Sandbox is a commercial malware analysis platform that provides automated dynamic analysis, behavior monitoring, and sandboxing capabilities to analyze and detect malware threats. Joe Sandbox executes suspicious files in a controlled environment, monitors their behavior, captures system activities, and generates detailed analysis reports to identify malicious behavior, techniques, and indicators of compromise (IOCs).

Cuckoo Sandbox: Cuckoo Sandbox is an open-source malware analysis system that allows users to analyze and detect malware threats by running suspicious files in an isolated virtual environment. Cuckoo Sandbox monitors and analyzes the behavior of malware samples, captures network traffic, system calls, and changes to file system and

registry, and generates detailed reports with behavioral analysis, signatures, and IOCs to aid in malware detection and remediation.

Common techniques:

Pattern recognition:

Command and control: Identifying patterns associated with command-and-control (C2) communications, which are used by attackers to control compromised systems remotely. By analyzing network traffic or logs, security analysts can detect communication patterns indicative of malware or malicious activity, such as beaconing or periodic connections to external servers.

Interpreting suspicious commands: Analyzing commands issued on systems or networks to identify suspicious or potentially malicious activity. This involves monitoring command-line activity, processes, and system logs for unusual or unauthorized commands that may indicate unauthorized access, lateral movement, or exploitation attempts by threat actors.

Email analysis:

Header analysis: Inspecting email headers to extract metadata and trace the path of email messages through the internet. Email header analysis can reveal valuable information about the sender, recipient, mail servers, routing, and delivery timestamps, helping to identify spoofed or malicious emails, trace their origins, and investigate email-based threats.

Impersonation: Detecting email impersonation attempts or spoofed sender identities used in phishing, business email compromise (BEC), or email fraud attacks. By analyzing sender information, domain names, and email content, security analysts can identify signs of impersonation and validate the authenticity of email communications.

DomainKeys Identified Mail (DKIM): DKIM is an email authentication technique that allows senders to digitally sign outgoing emails with cryptographic signatures, which can be verified by recipient mail servers to confirm the sender's identity and ensure message integrity. DKIM helps prevent email spoofing, tampering, and phishing attacks by enabling domain-based email authentication and validation.

Domain-based Message Authentication, Reporting, and Conformance (DMARC): DMARC is an email authentication protocol that enables domain owners to specify email authentication policies and receive feedback reports on email authentication failures. DMARC helps prevent email spoofing, domain impersonation, and phishing attacks by enforcing sender authentication checks, specifying handling instructions for unauthenticated emails, and providing visibility into email delivery and authentication status.

Sender Policy Framework (SPF): SPF is an email authentication mechanism that allows domain owners to publish DNS records containing a list of authorized email servers and IP addresses allowed to send emails on behalf of their domain. SPF helps prevent email spoofing, phishing, and domain impersonation attacks by enabling recipient mail servers to verify the sender's identity and reject unauthorized emails from spoofed domains.

Embedded links: Analyzing URLs embedded within email messages to identify malicious or suspicious links used in phishing, malware distribution, or drive-by download attacks. Security analysts inspect email content, hyperlinks, and URL redirections to assess the legitimacy of embedded links, verify sender reputation, and detect phishing attempts targeting email recipients.

File analysis:

Hashing: Calculating cryptographic hash values (e.g., MD5, SHA-256) of files or data to generate unique digital fingerprints or checksums used for file integrity verification, data deduplication, and malware detection. File hashing enables security analysts to compare file signatures, identify known malware variants, and detect unauthorized changes or tampering in files or data.

User behavior analysis:

Abnormal account activity: Monitoring user accounts, login events, and access patterns to identify abnormal or suspicious behavior indicative of account compromise, insider threats, or unauthorized access attempts. User behavior analysis involves profiling user activity, setting baseline behavior metrics, and detecting deviations or anomalies in user behavior, such as unusual login times, locations, or access to sensitive resources.

Impossible travel: Detecting and alerting on user login events or access attempts from geographically distant locations within a short time frame, which may indicate account compromise, credential theft, or unauthorized access by threat actors. Impossible travel analysis relies on geolocation data, IP addresses, and user login history to identify suspicious login patterns and potential security incidents requiring investigation.

JavaScript Object Notation (JSON): JSON is a lightweight data-interchange format commonly used for transmitting data between a server and a web application. It is human-readable and easy for both humans and machines to understand. JSON consists of key-value pairs and arrays, making it suitable for representing structured data such as configuration settings, application state, or API responses.

Extensible Markup Language (XML): XML is a markup language used for encoding structured data in a human-readable and machine-readable format. It defines a set of rules for structuring documents using tags and attributes, similar to HTML. XML is widely used for data exchange, configuration files, and representing hierarchical data structures in various applications and industries.

Python: Python is a high-level, interpreted programming language known for its simplicity, readability, and versatility. It supports multiple programming paradigms, including procedural, object-oriented, and functional programming. Python is widely used for web development, data analysis, scientific computing, automation, machine learning, and scripting tasks due to its extensive standard library, rich ecosystem of third-party libraries, and developer-friendly syntax.

PowerShell: PowerShell is a task automation and configuration management framework developed by Microsoft for Windows operating systems. It provides a command-line shell and scripting language specifically designed for system administration, automation, and management of Windows-based environments. PowerShell supports object-oriented programming, pipeline processing, and integration with .NET Framework, making it a powerful tool for system administrators and developers.

Shell script: Shell scripting refers to writing scripts or programs in shell languages such as Bash (Bourne Again Shell) on Unix-like operating systems (e.g., Linux, macOS). Shell scripts are used for automating system tasks, file manipulation, process management, and system administration tasks. They are executed directly by the shell interpreter and can interact with the underlying operating system's command-line interface and utilities.

Regular expressions: Regular expressions (regex) are patterns used for matching and manipulating text based on specific search criteria. They are widely used in programming, text processing, and data validation tasks to find, extract, or replace patterns of characters within strings. Regular expressions provide a powerful and flexible mechanism for performing text manipulation operations, such as pattern matching, string splitting, and data extraction, using a concise and expressive syntax.

Threat actors: These are entities or individuals who pose a threat to an organization's cybersecurity. They can range from sophisticated state-sponsored attackers to individuals with limited technical skills. Understanding the motivations, capabilities, and tactics of threat actors is crucial for developing effective cybersecurity defenses.

Advanced Persistent Threat (APT): A sophisticated and targeted cyberattack conducted by well-funded and organized threat actors, often with the backing of nation-states. APT attacks are characterized by their stealthy nature, long-term persistence, and use of advanced techniques to breach and maintain unauthorized access to target systems.

Hacktivists: These are individuals or groups who use hacking techniques to promote social or political causes, often through website defacements, data breaches, or distributed denial-of-service (DDoS) attacks. Hacktivism aims to raise awareness or protest against perceived injustices or issues.

Organized crime: Criminal syndicates or groups that engage in cybercrime activities such as financial fraud, identity theft, ransomware attacks, and illegal trafficking of stolen data or goods for financial gain. Organized cybercrime operations often have sophisticated infrastructure and operate across multiple jurisdictions.

Nation-state: Government-sponsored threat actors or intelligence agencies that conduct cyber espionage, cyber warfare, or sabotage operations against other nations, organizations, or critical infrastructure. Nation-state attacks can have geopolitical motives, such as stealing intellectual property, disrupting critical services, or undermining rival nations' security.

Script kiddie: An individual with limited technical skills who uses pre-written scripts or tools to launch basic cyberattacks without fully understanding the underlying technology or techniques. Script kiddies typically target vulnerable systems for fun, vandalism, or to gain notoriety within online communities.

Insider threat: Any individual within an organization who poses a risk to the confidentiality, integrity, or availability of sensitive information or systems. Insider threats can be intentional (malicious insiders) or unintentional (negligent employees or contractors) and may result from disgruntlement, financial incentives, or lack of awareness about cybersecurity best practices.

Supply chain: Threat actors targeting the supply chain seek to compromise or exploit vulnerabilities in third-party vendors, partners, or service providers to gain unauthorized access to target organizations' networks, systems, or data. Supply chain attacks can have far-reaching consequences and are increasingly common in today's interconnected business ecosystem.

Tactics, techniques, and procedures (TTP): These refer to the methods, strategies, and behaviors employed by threat actors to achieve their objectives during cyberattacks. TTPs encompass a wide range of activities, including reconnaissance, initial access, privilege escalation, lateral movement, data exfiltration, and covering tracks. Understanding the TTPs used by threat actors helps organizations detect, prevent, and respond to cyber threats effectively.

Confidence levels: These represent the degree of certainty or trustworthiness associated with cybersecurity intelligence, alerts, or threat information. Confidence levels are influenced by factors such as the reliability of the data source, the accuracy of threat indicators, the timeliness of information, and the relevance to the organization's security posture.

Timeliness: Refers to how quickly cybersecurity intelligence or threat information is delivered to stakeholders, enabling them to take timely action to mitigate risks or respond to incidents.

Relevancy: Indicates the degree to which cybersecurity intelligence or threat information is pertinent or applicable to an organization's assets, systems, or operations. Relevant threat intelligence helps organizations prioritize security efforts and allocate resources effectively.

Accuracy: Reflects the reliability and correctness of cybersecurity intelligence or threat information, including the precision of threat indicators, the quality of analysis, and the absence of false positives or misleading data. Accurate threat intelligence enables

organizations to make informed decisions and avoid unnecessary disruptions or false alarms.

Collection methods and sources: These refer to the techniques and channels through which organizations gather cybersecurity intelligence and threat information to enhance their security posture and defend against potential cyber threats.

Open source: Information publicly available on the internet, including social media platforms, blogs, forums, government bulletins, computer emergency response teams (CERTs), and cybersecurity incident response teams (CSIRTs). Open-source intelligence (OSINT) provides valuable insights into emerging threats, vulnerabilities, and attacker tactics.

Social media: Platforms like Twitter, LinkedIn, and Reddit can be sources of real-time information about security incidents, threat actors' activities, and cybersecurity trends.

Blogs/forums: Security blogs, online forums, and discussion boards hosted by cybersecurity professionals, researchers, and industry experts often share insights, analysis, and threat intelligence.

Government bulletins: Government agencies, such as the Department of Homeland Security (DHS), publish security advisories, alerts, and bulletins to inform the public about cybersecurity threats, vulnerabilities, and recommended mitigation measures.

Computer Emergency Response Team (CERT): CERTs, such as CERT Coordination Center (CERT/CC), provide incident response support, vulnerability coordination, and threat intelligence sharing services to organizations and the cybersecurity community.

Cybersecurity Incident Response Team (CSIRT): CSIRTs within organizations or industry sectors focus on coordinating incident response activities, analyzing security incidents, and sharing threat intelligence with relevant stakeholders.

Deep/dark web: Hidden parts of the internet not indexed by traditional search engines, where threat actors may operate underground markets, forums, or communities to buy, sell, or exchange cybercriminal tools, services, and stolen data.

Closed source: Proprietary or restricted-access intelligence sources obtained through paid subscriptions, information sharing organizations, or internal sources.

Paid feeds: Commercial threat intelligence providers offer subscription-based services that deliver curated threat intelligence feeds, reports, and analysis tailored to specific industries, regions, or threat actors.

Information sharing organizations: Industry-specific information sharing and analysis centers (ISACs), sectorial threat intelligence sharing communities, or private-sector consortia facilitate collaboration and sharing of threat intelligence among member organizations to enhance collective defense against cyber threats.

Internal sources: Data generated and collected within an organization's own infrastructure, including security logs, network traffic, endpoint telemetry, incident reports, and threat intelligence generated from internal security operations.

Threat intelligence sharing: The practice of exchanging cybersecurity intelligence and threat information among organizations, industry sectors, government agencies, and security communities to improve collective defense, incident response, vulnerability management, risk management, security engineering, and detection and monitoring capabilities.

Incident response: Sharing threat intelligence related to security incidents, breaches, and compromises to assist in incident detection, analysis, containment, eradication, and recovery efforts.

Vulnerability management: Sharing information about software vulnerabilities, exploits, patches, and mitigation techniques to prioritize remediation efforts and reduce exposure to cyber threats.

Risk management: Sharing insights into emerging threats, threat actors' tactics, and potential impacts to help organizations assess and manage cyber risks effectively.

Security engineering: Sharing knowledge, best practices, and lessons learned from security incidents to improve the design, development, and deployment of secure systems, applications, and infrastructure.

Detection and monitoring: Sharing threat intelligence indicators, signatures, and behavioral patterns to enhance detection capabilities and identify anomalous activities indicative of cyber threats or attacks.

Threat hunting: This is a proactive cybersecurity practice aimed at identifying and mitigating potential threats and security weaknesses within an organization's network and systems. Threat hunters use a combination of tools, techniques, and expertise to search for signs of malicious activity that may have evaded traditional security measures.

Indicators of Compromise (IoC): These are pieces of evidence or artifacts that indicate an ongoing or past security incident. Threat hunters leverage IoCs to identify and investigate potential threats. IoCs can include IP addresses, domain names, file hashes, registry keys, network traffic patterns, and behavioral anomalies.

Collection: Gathering IoCs from various sources such as threat intelligence feeds, security logs, network traffic, endpoint telemetry, and open-source intelligence (OSINT).

Analysis: Analyzing collected IoCs to determine their relevance, significance, and potential impact on the organization's security posture. This involves correlating IoCs with known threat actor tactics, techniques, and procedures (TTPs) and assessing the level of risk posed.

Application: Using IoCs to proactively search for signs of compromise within the organization's environment. Threat hunters employ advanced detection techniques, including data mining, anomaly detection, and behavioral analysis, to uncover hidden threats and security vulnerabilities.

Focus areas: These are specific areas of interest or concern that threat hunters prioritize during their investigations to maximize the effectiveness of their efforts.

Configurations/misconfigurations: Investigating system configurations and potential misconfigurations that could expose the organization to security risks, such as open ports, weak access controls, or outdated software.

Isolated networks: Examining isolated or less monitored network segments that may be more susceptible to intrusions or unauthorized access due to limited visibility and security controls.

Business-critical assets and processes: Focusing on protecting assets and processes critical to the organization's operations, reputation, and financial well-being. Threat hunters prioritize identifying and mitigating threats that could disrupt essential business functions or compromise sensitive data.

Active defense: This involves taking proactive measures to disrupt and mitigate potential threats before they can cause harm to the organization. Active defense techniques may include threat hunting, threat intelligence sharing, deception tactics, and countermeasures designed to deter or thwart attackers.

Honeypot: A honeypot is a decoy system or network designed to attract and deceive attackers, allowing security teams to monitor and analyze their behavior. Threat hunters deploy honeypots to gather intelligence about attacker tactics, techniques, and tools, which can inform defensive strategies and enhance threat detection capabilities.

Standardize processes: This involves establishing uniform procedures and workflows across the organization to improve efficiency, consistency, and reliability.

Identification of tasks suitable for automation: Teams assess tasks that are repetitive, rule-based, and do not require human judgment or intervention. These tasks are prime candidates for automation to reduce manual effort and human error.

Team coordination to manage and facilitate automation: Collaboration among team members is essential to identify automation opportunities, prioritize tasks, develop

automation scripts or workflows, and ensure successful implementation and maintenance of automated processes.

Streamline operations: The goal here is to optimize processes and workflows to achieve greater efficiency and effectiveness in managing security operations.

Automation and orchestration: Organizations leverage automation and orchestration solutions, such as Security Orchestration, Automation, and Response (SOAR) platforms, to automate routine security tasks, coordinate incident response activities, and streamline workflow management.

Orchestrating threat intelligence data: By automating the ingestion, analysis, and dissemination of threat intelligence data, organizations can enrich their security posture and improve their ability to detect, respond to, and mitigate cyber threats.

Data enrichment: Automated processes can enhance threat intelligence data by adding context, such as geolocation, threat actor attribution, or malware analysis results, to facilitate more informed decision-making.

Threat feed combination: Automation can consolidate multiple threat intelligence feeds from different sources, normalize the data, and integrate it into security tools and processes for comprehensive threat visibility and analysis.

Minimize human engagement: Automation aims to reduce manual intervention in security operations, allowing security teams to focus on higher-value tasks, such as threat hunting, incident investigation, and strategic decision-making.

Technology and tool integration: Integration of security technologies and tools enables seamless communication and interoperability, enhancing overall security posture and operational efficiency.

Application programming interface (API): APIs facilitate the integration of disparate security solutions by enabling them to exchange data and interact with each other programmatically. This interoperability streamlines workflows and enables automation across the security stack.

Webhooks: Webhooks provide a lightweight mechanism for real-time communication between applications and systems. Security tools can use webhooks to trigger actions or events automatically based on predefined conditions or alerts.

Plugins: Many security tools and platforms support plugin architectures that allow users to extend functionality by integrating additional modules or components. Plugins enable customization and integration with third-party systems, enabling organizations to tailor their security infrastructure to their specific needs.

Single pane of glass: This concept refers to a unified, centralized interface that provides comprehensive visibility and control over an organization's security posture and operations.

A single pane of glass dashboard aggregates data from multiple security tools and sources, presenting it in a consolidated view for easier monitoring, analysis, and decision-making.

This approach reduces the complexity of managing disparate security solutions and enables security teams to quickly identify threats, prioritize responses, and take appropriate actions from a single interface.

Domain 2 Vulnerability Management

Asset discovery: The process of identifying and cataloging all devices, systems, applications, and resources connected to an organization's network.

> **Map scans**: Conducting scans of the network to create visual representations, or maps, of the network topology and identify active hosts, services, and relationships between them.
>
> **Device fingerprinting**: Collecting information about devices on the network, such as operating system versions, open ports, installed software, and hardware characteristics, to uniquely identify and classify them.

Special considerations: Factors to take into account when planning and executing asset discovery activities.

> **Scheduling**: Determining the frequency and timing of asset discovery scans to minimize disruption to normal business operations while ensuring comprehensive coverage and accuracy.
>
> **Operations**: Ensuring that asset discovery processes align with organizational policies, procedures, and objectives, and integrating them seamlessly into existing workflows and systems.
>
> **Performance**: Optimizing asset discovery tools and techniques to maximize efficiency and minimize resource consumption, such as network bandwidth and system resources.
>
> **Sensitivity levels**: Tailoring asset discovery activities to account for the sensitivity of data and systems being scanned, ensuring compliance with privacy and security requirements.
>
> **Segmentation**: Considering network segmentation and access controls to ensure that asset discovery scans are limited to authorized areas and do not inadvertently expose sensitive information or disrupt critical systems.
>
> **Regulatory requirements**: Adhering to relevant laws, regulations, and industry standards governing asset discovery activities, such as data protection and privacy regulations.

Internal vs. external scanning: Distinguishing between asset discovery activities conducted within an organization's internal network and those performed from an external perspective, such as from the internet or a third-party service.

Agent vs. agentless: Choosing between using software agents installed on target devices and agentless methods that rely on network-based scanning techniques to discover assets.

Credentialed vs. non-credentialed: Deciding whether to conduct asset discovery scans with privileged credentials to gather detailed information from target systems or using non-privileged access methods.

Passive vs. active: Contrasting approaches that involve monitoring network traffic passively to identify assets and their characteristics versus actively probing devices and services to collect information.

Static vs. dynamic: Comparing techniques that analyze static configurations and data versus those that involve real-time interaction and testing of systems and applications.

> **Reverse engineering**: Analyzing software binaries or firmware to understand their functionality, behavior, and vulnerabilities.
>
> **Fuzzing**: Sending invalid, unexpected, or random data inputs to applications to identify vulnerabilities, software bugs, and security weaknesses.

Critical infrastructure refers to systems and assets that are essential for the functioning of a society and economy. This includes various sectors such as energy, transportation, water, telecommunications, healthcare, and finance. Protecting critical infrastructure from cyber threats is crucial to ensure the continued operation of essential services and prevent disruptions that could have significant societal and economic impacts.

Operational technology (OT): The hardware and software used to monitor and control physical devices, processes, and industrial operations. OT systems are commonly found in industrial environments such as manufacturing plants, power plants, and transportation systems.

Industrial control systems (ICS): A type of OT that manages and controls industrial processes and machinery. ICS includes components such as programmable logic controllers (PLCs), human-machine interfaces (HMIs), and supervisory control and data acquisition (SCADA) systems.

Supervisory control and data acquisition (SCADA): A type of control system used to monitor and control industrial processes in real-time. SCADA systems are commonly used in industries such as energy, water treatment, and manufacturing.

Security baseline scanning: The process of assessing the security configuration of systems and devices against established security baselines or standards. Baseline scanning helps organizations identify and remediate security vulnerabilities and misconfigurations to improve overall security posture.

Industry frameworks: Established guidelines and best practices for improving cybersecurity within specific industries or sectors.

> **Payment Card Industry Data Security Standard (PCI DSS)**: A set of security standards designed to protect payment card data and ensure secure payment transactions.

Center for Internet Security (CIS) benchmarks: Industry-accepted best practices for securing various IT systems and infrastructure components, including operating systems, network devices, and applications.

Open Web Application Security Project (OWASP): A community-driven organization that provides resources, tools, and guidelines for improving the security of web applications.

International Organization for Standardization (ISO) 27000 series: A series of standards and guidelines developed by the ISO for implementing and managing information security management systems (ISMS). ISO 27001 specifically addresses the requirements for establishing, implementing, maintaining, and continually improving an ISMS.

Network scanning and mapping:

Angry IP Scanner: A lightweight and cross-platform network scanner that scans IP addresses and ports.

Maltego: A data visualization tool used for link analysis and mapping of relationships between entities on networks.

Web application scanners:

Burp Suite: A comprehensive platform for web application security testing, including scanning for vulnerabilities, testing for CSRF, and more.

Zed Attack Proxy (ZAP): An open-source web application security scanner and proxy that helps identify security vulnerabilities in web applications.

Arachni: A feature-rich web application security scanner with support for various attack types and comprehensive reporting capabilities.

Nikto: A web server scanner that performs comprehensive tests against web servers for multiple known vulnerabilities.

Vulnerability scanners:

Nessus: A widely-used vulnerability scanner that identifies security vulnerabilities, misconfigurations, and compliance issues in networks, systems, and applications.

OpenVAS: An open-source vulnerability scanner that detects and reports security issues in networks and hosts.

Debuggers:

Immunity debugger: A powerful debugger used for analyzing and reverse engineering binary files and malware.

GNU debugger (GDB): A versatile command-line debugger for debugging programs written in C, C++, and other programming languages.

Multipurpose:

Nmap: A versatile network scanning tool used for network discovery, port scanning, service enumeration, and vulnerability detection.

Metasploit framework (MSF): A popular penetration testing framework that provides various tools and modules for exploiting vulnerabilities and conducting security assessments.

Recon-ng: A reconnaissance framework that automates the process of gathering information about targets from various online sources.

Cloud infrastructure assessment tools:

Scout Suite: A security auditing tool for AWS environments that assesses security configurations, permissions, and compliance.

Prowler: A security tool for AWS that performs automated checks against AWS security best practices, compliance standards, and security controls.

Pacu: An AWS exploitation framework that helps security professionals assess the security posture of AWS environments and automate security assessments.

The Common Vulnerability Scoring System (CVSS) provides a standardized framework for assessing and rating the severity of vulnerabilities. Here's how various components of CVSS can be interpreted:

Attack vectors: This metric evaluates how an attacker can exploit the vulnerability. It could be through the network (N), adjacent (A), local (L), or physical (P) access.

Attack complexity: It measures how difficult it is for an attacker to exploit the vulnerability. It ranges from low to high.

Privileges required: This metric indicates the level of privileges an attacker needs to exploit the vulnerability, ranging from none (N) to high (H).

User interaction: It assesses whether user interaction is required to exploit the vulnerability. It could be none (N), required (R), or necessary (A).

Scope: Scope describes the extent of the vulnerability's impact on the affected system or environment. It can be either unchanged (U), changed (C), or changed and unrelated (CI).

Impact:

Confidentiality: This evaluates the impact on data confidentiality if the vulnerability is exploited.

Integrity: It measures the impact on data integrity.

Availability: It assesses the impact on system availability.

Validation:

True/false positives: Indicates whether the identified vulnerability is valid or a false positive.

True/false negatives: Determines if the vulnerability assessment correctly identifies the absence or presence of vulnerabilities.

Context awareness:

Internal: The vulnerability exists within the organization's internal network.

External: The vulnerability is external-facing, accessible from outside the organization.

Isolated: Indicates whether the vulnerability is isolated or interconnected with other systems.

Exploitability/weaponization: It evaluates the likelihood of the vulnerability being exploited or weaponized by attackers.

Asset value: Determines the value of the asset affected by the vulnerability, such as critical systems, sensitive data, etc.

Zero-day: Refers to vulnerabilities that are unknown to the software vendor and have no available patches or fixes at the time of discovery.

Cross-site scripting (XSS):

Reflected XSS: Occurs when an attacker injects malicious scripts into a web application, which are then reflected off a vulnerable web server to the victim's browser.

Persistent XSS: Involves injecting malicious scripts into a web application's database, allowing the attacker to target multiple users who access the same data.

Overflow vulnerabilities:

Buffer overflow: Results from writing more data to a buffer than it can hold, potentially leading to code execution or system crashes.

Integer overflow: Occurs when arithmetic operations cause an integer value to exceed its maximum limit, leading to unexpected behavior or security vulnerabilities.

Heap overflow: Involves writing data beyond the allocated memory space of the heap, which can lead to system crashes or code execution.

Stack overflow: Happens when a program's call stack exceeds its memory allocation, often due to recursive function calls or excessively large data structures.

Data poisoning: Refers to the manipulation of data inputs to deceive or disrupt the functionality of a system, potentially leading to unauthorized access, data corruption, or system compromise.

Broken access control: Occurs when a system fails to properly enforce access controls, allowing unauthorized users to gain access to resources or perform actions they shouldn't have permissions for.

Cryptographic failures: Encompasses various weaknesses in cryptographic implementations, such as using weak algorithms, improper key management, or insecure encryption protocols, which can lead to data exposure or compromise.

Injection flaws: Include vulnerabilities such as SQL injection, LDAP injection, or OS command injection, where an attacker can inject malicious code or commands into an application's input fields to manipulate the application's behavior or access unauthorized data.

Cross-site request forgery (CSRF): Occurs when an attacker tricks a user into performing unintended actions on a web application where they are authenticated. This is often achieved by exploiting the user's session credentials to submit forged requests to the application on behalf of the user.

Directory traversal: Also known as path traversal, it's a vulnerability that allows an attacker to access files and directories outside the web server's root directory. This can lead to unauthorized access to sensitive files, such as configuration files, user data, or even system files.

Insecure design: Occurs when a system or application is designed with security vulnerabilities, such as weak authentication mechanisms, lack of input validation, or improper data handling. This can result in various security risks, including unauthorized access, data breaches, or system compromise.

Security misconfiguration: Refers to the improper configuration of system components, such as web servers, databases, or cloud services, leading to security vulnerabilities. Examples include default passwords, unnecessary services enabled, or insecure access controls.

End-of-life or outdated components: Using outdated or unsupported software components can expose systems to known security vulnerabilities that have been patched in newer versions. Attackers often target systems running outdated software with known vulnerabilities to exploit them.

Identification and authentication failures: Weak or inadequate identification and authentication mechanisms can lead to unauthorized access to systems or sensitive data. This includes weak passwords, lack of multi-factor authentication, or improper credential management.

Server-side request forgery (SSRF): SSRF is a vulnerability that allows an attacker to manipulate server-side requests initiated by the web application, potentially leading to unauthorized access to internal systems, data exfiltration, or server-side attacks.

Remote code execution (RCE): RCE occurs when an attacker is able to execute arbitrary code on a remote server or application, often resulting from vulnerabilities such as buffer overflows, injection flaws, or insecure deserialization. RCE can lead to complete compromise of the target system.

Privilege escalation: Involves exploiting vulnerabilities to elevate privileges and gain unauthorized access to resources or functionality that would normally be restricted. This can include escalating privileges from a regular user to an administrator or gaining access to sensitive data.

Local file inclusion (LFI)/remote file inclusion (RFI): LFI and RFI vulnerabilities allow attackers to include and execute arbitrary files on a server. LFI occurs when an attacker can include local files, while RFI occurs when an attacker can include remote files hosted on external servers. These vulnerabilities can lead to data disclosure, server compromise, or remote code execution.

A compensating control is a security measure put in place to mitigate or compensate for a weakness or deficiency in an organization's primary control environment. It helps to reduce the risk associated with the identified vulnerability. Here's a breakdown:

Control types:

Managerial: Policies, procedures, and guidelines established by management to guide security efforts and ensure compliance with regulatory requirements.

Operational: Controls related to the day-to-day functioning of an organization's security program, such as access control procedures, security awareness training, and incident response processes.

Technical: Controls implemented through technology solutions, such as firewalls, intrusion detection systems, encryption, and antivirus software.

Preventative: Controls designed to prevent security incidents from occurring, such as access controls, authentication mechanisms, and encryption.

Detective: Controls aimed at detecting security incidents or breaches that have occurred, including log monitoring, intrusion detection systems, and security event correlation.

Responsive: Controls that respond to security incidents or breaches in real-time, such as automated alerting systems, incident response plans, and emergency procedures.

Corrective: Controls implemented to correct the effects of a security incident or breach and restore normal operations, such as system restoration procedures, data recovery processes, and incident post-mortems.

Patching and configuration management:

Testing: Compensating controls may involve thorough testing of software patches, configurations, or changes before implementation to ensure they do not introduce new vulnerabilities or disrupt critical systems.

Implementation: Once tested, patches and configuration changes are implemented following established change management procedures to minimize risks to production systems.

Rollback: In the event that a patch or configuration change causes unforeseen issues, compensating controls may include rollback procedures to revert systems to a previous state until the issue can be addressed.

Validation: After implementation, compensating controls may involve validation steps to ensure that patches or configuration changes were successfully applied and that systems are functioning as intended.

Maintenance windows:

Compensating controls may include scheduling maintenance windows during off-peak hours to minimize disruption to business operations while implementing patches or making configuration changes. These windows provide a structured timeframe for performing maintenance activities, reducing the likelihood of conflicts or interruptions.

Exceptions in the context of cybersecurity refer to deviations from established policies, standards, or procedures due to specific circumstances or requirements. Here's how exceptions relate to various aspects of risk management, policies, governance, service-level objectives (SLOs), prioritization, escalation, and attack surface management:

Risk management principles:

Accept: Sometimes, organizations may accept certain risks due to cost or resource constraints, regulatory requirements, or business needs. In such cases, exceptions may be granted to allow deviations from standard security controls.

Transfer: Organizations may transfer risks to third parties through contracts, insurance, or other arrangements. Exceptions may be necessary to accommodate the specific terms of risk transfer agreements.

Avoid: When risks are deemed too high or unacceptable, organizations may choose to avoid them altogether. Exceptions may be granted for situations where risk avoidance is not feasible or practical.

Mitigate: Organizations often implement controls to mitigate risks to an acceptable level. Exceptions may arise when existing controls cannot be implemented due to technical constraints, budget limitations, or other factors.

Policies, governance, and service-level objectives (SLOs):

Exceptions to established policies and governance frameworks may be granted under certain circumstances, such as when adherence to the policy would result in significant operational disruption or when a specific business need requires flexibility.

Service-level objectives (SLOs) define the level of service expected by customers. Exceptions to SLOs may be granted if meeting the defined objectives is not feasible due to unforeseen circumstances or resource constraints.

Prioritization and escalation:

In the context of incident response and vulnerability management, exceptions may be granted to adjust the prioritization of security incidents or vulnerabilities based on their severity, potential impact, or other factors.

Escalation procedures may include exceptions that allow deviations from standard escalation paths in urgent or critical situations to ensure timely resolution and mitigation of security threats.

Attack surface management:

Edge discovery involves identifying and assessing assets and vulnerabilities at the network perimeter. Exceptions may be necessary to accommodate unique network configurations or legacy systems that cannot be scanned using standard methods.

Passive discovery techniques, such as monitoring network traffic for signs of suspicious activity, may require exceptions to privacy or data protection policies to allow the collection and analysis of network data.

Security controls testing, penetration testing, adversary emulation, and bug bounty programs may involve exceptions to normal operating procedures to facilitate ethical hacking activities and identify vulnerabilities before they can be exploited by malicious actors.

Attack surface reduction efforts may require exceptions to certain policies or configurations to implement changes aimed at minimizing the organization's exposure to cyber threats.

Secure coding best practices are essential for developing robust and resilient software that can withstand various cyber threats. Here are some key practices:

Input validation: Always validate and sanitize user input to prevent injection attacks such as SQL injection, cross-site scripting (XSS), and command injection.

Output encoding: Encode output data to prevent XSS attacks. Use appropriate encoding techniques such as HTML encoding, URL encoding, and JavaScript encoding based on the context of output.

Session management: Implement secure session management techniques to prevent session hijacking and fixation. Use secure cookies, enforce HTTPS, and regenerate session identifiers after authentication.

Authentication: Implement strong authentication mechanisms, such as multi-factor authentication (MFA), password hashing, and account lockout mechanisms, to protect against unauthorized access.

Data protection: Encrypt sensitive data at rest and in transit using strong cryptographic algorithms. Follow encryption best practices and key management guidelines to safeguard data confidentiality.

Parameterized queries: Use parameterized queries or prepared statements to prevent SQL injection attacks. Avoid dynamic SQL queries constructed by concatenating user input.

Additionally, integrating secure coding practices into the Software Development Life Cycle (SDLC) is crucial. Here's how it can be done:

Secure software development life cycle (SDLC): Integrate security activities into each phase of the SDLC, including requirements gathering, design, development, testing, deployment, and maintenance. Incorporate security reviews, code analysis, and security testing into the development process.

Threat modeling: Conduct threat modeling exercises to identify potential security threats and vulnerabilities early in the development process. Analyze the system architecture, data flows, and trust boundaries to anticipate and mitigate security risks effectively.

Domain 3 Incident Response and Management

Cyber Kill Chain: The Cyber Kill Chain is a concept developed by Lockheed Martin to describe the stages of a cyber attack. It consists of seven stages: reconnaissance, weaponization, delivery, exploitation, installation, command and control (C2), and actions on objectives. Understanding each stage helps organizations identify and disrupt cyber attacks more effectively.

Diamond Model of Intrusion Analysis: The Diamond Model of Intrusion Analysis is a framework used for analyzing and visualizing cyber threats and intrusions. It consists of four elements: adversary, capability, infrastructure, and victim. By examining relationships between these elements, analysts can gain insights into the tactics, techniques, and procedures (TTPs) employed by threat actors.

MITRE ATT&CK: The MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework is a knowledge base of adversary tactics and techniques based on real-world observations. It categorizes techniques used by threat actors across different stages of the attack lifecycle. The framework helps organizations improve their threat detection, prevention, and response capabilities by providing a common language for discussing and analyzing cyber threats.

Open Source Security Testing Methodology Manual (OSSTMM): The OSSTMM is a methodology for assessing and improving the security of information systems. It provides a structured approach to security testing, covering various areas such as operational security, data networks, wireless networks, physical security, and human security. The OSSTMM helps organizations identify vulnerabilities and weaknesses in their security posture.

OWASP Testing Guide: The OWASP (Open Web Application Security Project) Testing Guide is a comprehensive guide for testing the security of web applications. It covers various aspects of web application security testing, including authentication, authorization, input validation, session management, and cryptography. The guide provides practical techniques and methodologies for identifying and mitigating common web application vulnerabilities.

Indicators of Compromise (IoC): Indicators of Compromise are artifacts or patterns observed in an organization's systems or network that indicate potential malicious activity. These can include unusual network traffic, file changes, unauthorized logins, or unexpected system behavior. IoCs are essential for detecting and responding to security incidents.

Evidence Acquisition:

Chain of Custody: The chain of custody is a documented trail that tracks the movement and handling of evidence from the time it's collected until it's presented in court. It

ensures the integrity and admissibility of evidence by documenting who accessed it and when.

Validating Data Integrity: Validating data integrity involves ensuring that the evidence collected remains unchanged and tamper-proof throughout the investigation process. Techniques such as cryptographic hashing and digital signatures can be used to verify data integrity.

Preservation: Preservation involves securely storing and protecting evidence to prevent any unauthorized alterations or deletions. It ensures that the integrity of the evidence is maintained for future analysis and legal proceedings.

Legal Hold: Legal hold refers to the process of preserving all relevant data and information that may be subject to litigation or investigation. It ensures that potentially relevant evidence is retained and not altered or destroyed.

Data and Log Analysis: Data and log analysis involve examining various data sources, such as system logs, network traffic, and endpoint telemetry, to identify signs of suspicious or malicious activity. Analysis techniques may include correlation, anomaly detection, pattern recognition, and signature-based detection.

Containment, Eradication, and Recovery:

Scope: Scope refers to the extent of the incident and the affected systems, networks, or data. Understanding the scope helps determine the appropriate response actions.

Impact: Impact assessment involves evaluating the severity and consequences of the incident on the organization's operations, data integrity, and reputation.

Isolation: Isolation involves separating compromised systems or networks from the rest of the infrastructure to prevent further spread of the attack.

Remediation: Remediation involves implementing measures to remove or mitigate the effects of the incident, such as applying security patches, updating configurations, or deploying security controls.

Re-imaging: Re-imaging refers to the process of restoring compromised systems to a known, clean state by reinstalling the operating system and applications from trusted sources.

Compensating Controls: Compensating controls are security measures implemented to mitigate the risk of a security control deficiency. They help maintain or enhance security posture in situations where primary controls are inadequate or unavailable.

Preparation:

Incident Response Plan: An incident response plan outlines the procedures and actions to be taken in the event of a security incident. It typically includes roles and responsibilities, communication protocols, escalation procedures, and steps for containing, mitigating, and recovering from incidents.

Tools: Incident response teams utilize various tools to aid in the detection, analysis, containment, and eradication of security incidents. These tools may include SIEM (Security Information and Event Management) systems, forensic analysis tools, network monitoring tools, endpoint detection and response (EDR) solutions, and incident response platforms.

Playbooks: Incident response playbooks are predefined sets of procedures and response actions tailored to specific types of security incidents. They provide step-by-step guidance for responding to incidents effectively and efficiently.

Tabletop Exercises: Tabletop exercises are simulated scenarios that allow incident response teams to practice their response procedures and assess their readiness to handle security incidents. These exercises involve stakeholders from different departments and focus on testing communication, decision-making, and coordination.

Training: Training programs help prepare incident response teams and other stakeholders for their roles and responsibilities during security incidents. Training may include cybersecurity awareness training, technical skill development, and scenario-based exercises.

Business Continuity (BC) / Disaster Recovery (DR): Business continuity and disaster recovery plans outline the strategies and procedures for maintaining essential business operations and recovering IT systems and data following a disruptive event. These plans ensure that organizations can continue to operate and minimize the impact of incidents on business operations.

Post-Incident Activity:

Forensic Analysis: Forensic analysis involves collecting, preserving, analyzing, and presenting digital evidence related to a security incident. It helps uncover the root cause of the incident, identify the extent of the compromise, and support legal and regulatory requirements.

Root Cause Analysis: Root cause analysis aims to identify the underlying factors that contributed to a security incident. It helps organizations address systemic issues and implement corrective actions to prevent similar incidents from occurring in the future.

Lessons Learned: Lessons learned sessions involve reviewing the organization's response to a security incident, identifying strengths and weaknesses, and capturing insights and best practices for improvement. These sessions help enhance incident response capabilities and resilience against future incidents.

Domain 4 Reporting and Communication

Vulnerability Management Reporting:

Vulnerabilities: Vulnerability management reporting provides information on identified vulnerabilities within an organization's systems, applications, and network infrastructure. It includes details such as vulnerability names, descriptions, severity levels, and associated CVE (Common Vulnerabilities and Exposures) identifiers.

Affected Hosts: This section of the report lists the hosts or assets that are affected by the identified vulnerabilities. It helps prioritize remediation efforts by identifying the systems that are at the greatest risk of exploitation.

Risk Score: Vulnerability risk scores quantify the severity and potential impact of vulnerabilities on the organization's security posture. Risk scores are often based on factors such as exploitability, potential impact, and affected assets.

Mitigation: Mitigation measures describe the actions and controls recommended to remediate or mitigate identified vulnerabilities. This may include applying patches, implementing configuration changes, deploying security updates, or implementing compensating controls.

Recurrence: Recurrence information tracks whether vulnerabilities have reoccurred after initial remediation attempts. It helps assess the effectiveness of mitigation measures and identify systemic issues that may contribute to recurring vulnerabilities.

Prioritization: Prioritization criteria help organizations prioritize remediation efforts based on factors such as vulnerability severity, potential impact, exploitability, and the criticality of affected assets. It ensures that limited resources are allocated effectively to address the most significant risks first.

Compliance Reports: Compliance reports provide an overview of the organization's adherence to regulatory requirements, industry standards, and internal policies related to cybersecurity and data protection. These reports typically include information on compliance status, audit findings, gaps in compliance, and remediation efforts.

Action Plans:

Configuration Management: Action plans for configuration management outline steps to ensure that IT systems and devices are configured securely and in accordance with organizational policies and best practices. This may involve implementing standardized configurations, conducting regular audits, and addressing configuration drift.

Patching: Patch management action plans detail processes and procedures for identifying, testing, deploying, and monitoring software patches and updates to address security vulnerabilities and software vulnerabilities.

Compensating Controls: Action plans for compensating controls describe alternative security measures implemented to mitigate risks when primary controls are inadequate or unavailable. These controls help address vulnerabilities and maintain security posture in situations where full mitigation may not be feasible.

Awareness, Education, and Training: Action plans for awareness, education, and training initiatives focus on educating employees, contractors, and other stakeholders about cybersecurity best practices, policies, and procedures. These programs aim to enhance cybersecurity awareness, reduce human error, and promote a security-conscious culture within the organization.

Changing Business Requirements: Action plans for adapting to changing business requirements involve evaluating and adjusting cybersecurity measures and controls to align with evolving business needs, technological advancements, regulatory changes, and emerging threats. It ensures that cybersecurity strategies remain relevant and effective in addressing current and future challenges.

Inhibitors to Remediation:

Memorandum of Understanding (MOU): MOUs between different entities can sometimes create complexities in remediation processes, especially if they outline specific procedures or limitations that may hinder the timely resolution of security issues.

Service-Level Agreement (SLA): SLAs, especially those related to third-party vendors or service providers, may impose constraints on response times or resolution procedures, impacting the organization's ability to remediate vulnerabilities promptly.

Organizational Governance: In some cases, organizational governance structures, such as bureaucratic decision-making processes or conflicting priorities among different departments, can slow down the remediation process.

Business Process Interruption: Remediation actions may be delayed if they risk interrupting critical business processes or operations. Organizations often need to balance security needs with operational continuity.

Degrading Functionality: Concerns about disrupting system functionality or user experience can lead to hesitancy in applying remediation measures, especially if there is uncertainty about the impact of the changes on system performance.

Legacy Systems: Legacy systems may pose challenges in terms of compatibility with modern security solutions or vendor support for patches and updates, making it difficult to address vulnerabilities effectively.

Proprietary Systems: Proprietary systems may have limited visibility or accessibility for security analysis and remediation, requiring specialized expertise or coordination with vendors to address security issues effectively.

Metrics and Key Performance Indicators (KPIs):

Trends: Monitoring trends in vulnerability discovery, remediation efforts, and security incidents can provide insights into the effectiveness of security controls and the organization's overall security posture over time.

Top 10: Identifying and tracking the top 10 most critical vulnerabilities or security issues within the organization can help prioritize remediation efforts and focus resources on addressing the most significant risks.

Critical Vulnerabilities and Zero-days: Monitoring critical vulnerabilities and zero-day exploits is essential for prioritizing remediation efforts and implementing timely security patches or mitigations to protect against emerging threats.

Service Level Objectives (SLOs): Establishing SLOs for vulnerability remediation can help set clear expectations for response times, resolution targets, and overall performance in addressing security issues.

Stakeholder Identification and Communication:

Identifying Stakeholders: It's crucial to identify all stakeholders involved in the remediation process, including IT teams, security teams, business unit leaders, executives, third-party vendors, and regulatory bodies.

Communication: Effective communication channels and protocols should be established to ensure timely dissemination of information regarding vulnerabilities, remediation efforts, progress updates, and any potential impacts on business operations. Clear and transparent communication helps maintain stakeholder trust and alignment throughout the remediation process.

Stakeholder Identification and Communication:

Stakeholder identification involves identifying all parties who have a vested interest or are affected by the incident response process. This includes internal teams such as IT, security, legal, and executive leadership, as well as external entities like regulatory bodies, law enforcement agencies, customers, and third-party vendors. Effective communication with stakeholders is essential throughout the incident response process to ensure alignment, coordination, and timely decision-making. Clear channels of communication should be established, and regular updates should be provided to keep stakeholders informed about the incident's status, impact, and remediation efforts.

Incident Declaration and Escalation:

Incident declaration involves formally acknowledging the occurrence of a security incident and initiating the incident response process. This may involve activating predefined incident response plans, assembling response teams, and escalating the incident to appropriate personnel or authorities for further action. Escalation procedures should be clearly defined, outlining the criteria for escalating incidents to higher levels of management or involving external parties such as law enforcement or regulatory agencies. Timely and accurate incident declaration and escalation are critical for mobilizing resources and initiating an effective response to mitigate the impact of security incidents.

Incident Response Reporting:

Incident response reporting involves documenting key details and actions taken during the incident response process to provide stakeholders with a comprehensive understanding of the incident, its impact, and the organization's response efforts. Incident response reports typically include:

Executive Summary: A high-level overview of the incident, including its nature, severity, and potential impact on the organization.

Who, What, When, Where, and Why: Detailed information about the incident, including the affected systems, the timeline of events, the methods used by attackers, and the motivations behind the attack.

Recommendations: Actionable recommendations for improving security controls, closing gaps, and preventing similar incidents in the future.

Timeline: A chronological timeline of events related to the incident, including initial detection, containment, eradication, and recovery efforts.

Impact: Assessment of the incident's impact on the organization, including financial losses, operational disruptions, reputational damage, and regulatory implications.

Scope: Description of the incident's scope, including the number of systems or users affected and the extent of data exposure or compromise.

Evidence: Documentation of evidence collected during the incident response process, including logs, forensic analysis reports, and any other relevant artifacts.

Communications:

Legal: Legal communications involve interactions with the organization's legal team or external legal counsel to address legal implications of security incidents, such as compliance with data protection laws, contractual obligations, and potential liabilities. Legal guidance may be sought to navigate regulatory requirements, engage with law enforcement agencies, and manage any litigation or disputes arising from security incidents.

Public Relations: Public relations communications focus on managing the organization's reputation and public image in the aftermath of a security incident. This includes crafting and disseminating messages to various stakeholders, including customers, partners, investors, and the media. Effective public relations efforts aim to minimize reputational damage, restore stakeholder trust, and demonstrate transparency and accountability in the organization's response to the incident.

Customer Communication: Direct communication with customers affected by the incident, providing them with timely updates, guidance, and support to address any concerns or impacts on their end.

Media: Interaction with journalists, reporters, and media outlets to provide accurate information about the incident, mitigate misinformation, and manage media inquiries in a controlled manner.

Regulatory Reporting: Reporting to regulatory authorities or industry regulators as required by applicable laws, regulations, or contractual obligations. This may involve notifying regulatory agencies of data breaches, security incidents, or violations of compliance standards, and providing detailed reports on the incident, its impact, and the organization's response efforts.

Law Enforcement: Collaboration with law enforcement agencies, such as local police departments, federal agencies, or cybercrime units, to report security incidents, share relevant information, and coordinate investigative efforts. Law enforcement involvement may be necessary for criminal investigations, evidence collection, and pursuit of legal action against threat actors.

Root Cause Analysis:

Root cause analysis involves identifying the underlying factors or systemic weaknesses that contributed to the occurrence of a security incident. It aims to uncover the fundamental reasons behind the incident, rather than just addressing its symptoms. Root cause analysis helps organizations understand how and why security incidents occur, enabling them to implement effective corrective actions and preventive measures to reduce the likelihood of similar incidents in the future.

Lessons Learned:

Lessons learned refer to insights and key takeaways gained from the analysis of security incidents and response efforts. It involves documenting successes, failures, challenges, and opportunities encountered during incident response, as well as identifying areas for improvement. Lessons learned help organizations enhance their incident response capabilities, refine security policies and procedures, and better prepare for future incidents.

Metrics and Key Performance Indicators (KPIs):

Metrics and KPIs are quantitative measures used to assess the effectiveness and efficiency of the incident response process. Common metrics and KPIs in incident response include:

Mean Time to Detect (MTTD): The average time taken to detect security incidents from the moment they occur until they are identified or reported.

Mean Time to Respond (MTTR): The average time taken to respond to and begin addressing security incidents after they have been detected.

Mean Time to Remediate (MTTR): The average time taken to fully remediate and resolve security incidents, including containment, eradication, and recovery efforts.

Alert Volume: The number of security alerts generated by detection systems or monitoring tools within a given time period. High alert volumes may indicate a need for tuning or optimization of detection capabilities.

These metrics and KPIs provide valuable insights into the performance of the incident response team, the efficiency of response processes, and the overall effectiveness of security controls and measures implemented by the organization. They help identify areas for improvement, measure progress over time, and demonstrate the organization's security posture to stakeholders.

CompTIA CySA+ CS0-003 Acronym List

ACL (Access Control List): A list of permissions attached to an object that specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects.

API (Application Programming Interface): A set of protocols, tools, and definitions that allows different software applications to communicate with each other.

APT (Advanced Persistent Threat): A prolonged, targeted cyberattack in which an unauthorized user gains access to a network and remains undetected for an extended period, typically with the intention of stealing data or causing damage.

ARP (Address Resolution Protocol): A protocol used to map an IP address to a physical machine address (MAC address) that is recognized in the local network.

AV (Antivirus): Software designed to detect, prevent, and remove malicious software (malware), such as viruses, worms, and trojans, from computer systems.

BC (Business Continuity): The process and procedures an organization puts in place to ensure that essential functions can continue during and after a disaster or other disruptive event.

BCP (Business Continuity Plan): A documented plan that outlines how an organization will maintain essential functions during and after a disaster or other disruptive event.

BGP (Border Gateway Protocol): A standardized exterior gateway protocol designed to exchange routing and reachability information among autonomous systems on the internet.

BIA (Business Impact Analysis): A process used to identify and evaluate the potential effects of disruptions to critical business operations.

C2 (Command and Control): Refers to the communication channel used by attackers to remotely control compromised systems or devices.

CA (Certificate Authority): A trusted entity that issues digital certificates used to verify the identity of individuals, organizations, or devices in a networked environment.

CASB (Cloud Access Security Broker): A security tool or service that helps organizations monitor and manage the security of data and applications hosted in cloud environments.

CDN (Content Delivery Network): A distributed network of servers designed to deliver web content and other internet-based services to users based on their geographic location.

CERT (Computer Emergency Response Team): A team of cybersecurity experts responsible for responding to and coordinating the response to cybersecurity incidents, vulnerabilities, and threats.

CHD (Cardholder Data): Refers to any personally identifiable information (PII) associated with a payment card, including account numbers, expiration dates, and cardholder names.

CI/CD (Continuous Integration and Continuous Delivery): A set of practices used in software development to automate the process of integrating code changes into a shared repository and delivering applications to production environments.

CIS (Center for Internet Security): An organization that provides cybersecurity resources, best practices, and benchmarks to help organizations improve their security posture.

COBIT (Control Objectives for Information and Related Technologies): A framework for the governance and management of enterprise IT environments, focusing on risk management, compliance, and value delivery.

CSIRT (Cybersecurity Incident Response Team): See CERT.

CSRF (Cross-site Request Forgery): A type of cyberattack in which an attacker tricks a user into executing unauthorized actions on a web application in which the user is authenticated.

CVE (Common Vulnerabilities and Exposures): A standardized list of publicly known cybersecurity vulnerabilities and exposures.

CVSS (Common Vulnerability Scoring System): A framework used to assess and prioritize the severity of software vulnerabilities based on various factors.

DDoS (Distributed Denial of Service): A type of cyberattack in which multiple compromised systems are used to flood a target system or network with an overwhelming amount of traffic, causing a denial of service to legitimate users.

DoS (Denial of Service): See DDoS.

DKIM (DomainKeys Identified Mail): An email authentication method designed to detect email spoofing and verify the authenticity of email messages.

DLP (Data Loss Prevention): A set of technologies and processes used to prevent the unauthorized transmission of sensitive data outside of an organization's network.

DMARC (Domain-based Message Authentication, Reporting, and Conformance): An email authentication protocol that builds on SPF and DKIM to help organizations prevent email spoofing and phishing attacks.

DNS (Domain Name Service): A hierarchical decentralized naming system for computers, services, or other resources connected to the internet or a private network.

DR (Disaster Recovery): See BC and BCP.

EDR (Endpoint Detection and Response): A cybersecurity technology that monitors and responds to suspicious activities and threats on endpoint devices, such as desktops, laptops, and servers.

FIM (File Integrity Monitoring): A security measure that monitors and detects unauthorized changes to files and directories on a computer system.

FTP (File Transfer Protocol): A standard network protocol used to transfer files between a client and a server on a computer network.

GDB (GNU Debugger): A powerful debugger for troubleshooting and analyzing software programs written in various programming languages.

GPO (Group Policy Objects): A feature of the Microsoft Windows operating system that allows administrators to manage user and computer settings centrally in an Active Directory environment.

HIDS: Host-based Intrusion Detection System - Monitors and analyzes the internals of a computing system as well as network packets on its network interfaces.

HIPS: Host-based Intrusion Prevention System - Similar to HIDS but can also take action to block or prevent detected intrusions.

HTTP: Hypertext Transfer Protocol - The protocol used for transmitting data over the World Wide Web.

HTTPS: Hypertext Transfer Protocol Secure - An extension of HTTP used for secure communication over a computer network, especially the internet.

IaaS: Infrastructure as a Service - A cloud computing service model that provides virtualized computing resources over the internet.

ICMP: Internet Control Message Protocol - A network layer protocol used to send error messages and operational information indicating, for example, that a requested service is not available or that a host or router could not be reached.

ICS: Industrial Control Systems - Computer systems that monitor and control industrial processes.

IDS: Intrusion Detection System - A security tool that monitors network or system activities for malicious activities or policy violations.

IoC: Indicators of Compromise - Pieces of forensic data, such as file hashes or IP addresses, that indicate potential malicious activity on a system or network.

IP: Internet Protocol - The principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries.

IPS: Intrusion Prevention System - A security tool that monitors network or system activities for malicious activities or policy violations and takes action to block or prevent them.

IR: Incident Response - The process of managing and mitigating the aftermath of a security breach or cyberattack.

ISO: International Organization for Standardization - An international standard-setting body composed of representatives from various national standards organizations.

IT: Information Technology - The use of computers to store, retrieve, transmit, and manipulate data or information.

ITIL: Information Technology Infrastructure Library - A set of detailed practices for IT service management (ITSM) that focuses on aligning IT services with the needs of business.

JSON: JavaScript Object Notation - A lightweight data-interchange format that is easy for humans to read and write and easy for machines to parse and generate.

KPI: Key Performance Indicator - A measurable value that demonstrates how effectively an organization is achieving key business objectives.

LAN: Local Area Network - A computer network that interconnects computers within a limited area such as a residence, school, laboratory, university campus, or office building.

LDAPS: Lightweight Directory Access Protocol Secure - An extension of LDAP (Lightweight Directory Access Protocol) that uses SSL/TLS for secure communication.

LFI: Local File Inclusion - A type of vulnerability that allows an attacker to include files on a server through the web browser.

LOI: Letter of Intent - A document outlining one or more agreements between two or more parties before the agreements are finalized.

MAC: Media Access Control - A unique identifier assigned to a network interface controller for use as a network address in communications within a network segment.

MFA: Multifactor Authentication - A security process that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction.

MOU: Memorandum of Understanding - A document describing a bilateral or multilateral agreement between parties.

MSF: Metasploit Framework - An open-source penetration testing framework that helps find security vulnerabilities in systems.

MSP: Managed Service Provider - A company that remotely manages a customer's IT infrastructure and/or end-user systems, typically on a proactive basis.

MSSP: Managed Security Service Provider - A company that provides outsourced monitoring and management of security devices and systems.

MTTD: Mean Time to Detect - The average time it takes an organization to detect a security incident.

MTTR: Mean Time to Repair - The average time it takes an organization to recover from a security incident.

NAC: Network Access Control - A security approach that uses a set of protocols to define and implement a policy that describes how to secure access to a network.

NDA: Non-disclosure Agreement - A legal contract between at least two parties that outlines confidential material, knowledge, or information that the parties wish to share with one another for certain purposes but wish to restrict access to or by third parties.

NGFW: Next-generation Firewall - A network security device that integrates intrusion detection and prevention, application awareness, and other features to provide advanced threat protection capabilities beyond traditional firewalls.

NIDS: Network-based Intrusion Detection System - An intrusion detection system that monitors and analyzes network traffic for signs of malicious activity.

NTP: Network Time Protocol - A networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.

OpenVAS: Open Vulnerability Assessment Scanner - An open-source vulnerability scanner used to detect security issues in computer systems and networks.

OS: Operating System - The software that manages computer hardware resources and provides services for computer programs.

OSSTMM: Open Source Security Testing Methodology Manual - A methodology for performing security tests and metrics.

OT: Operational Technology - The hardware and software that detects or causes changes through the direct monitoring and/or control of physical devices, processes, and events in the enterprise.

OWASP: Open Web Application Security Project - A nonprofit foundation that works to improve the security of software.

PAM: Privileged Access Management - A cybersecurity approach that focuses on managing and monitoring the use of privileged accounts and access within an organization.

PCI DSS: Payment Card Industry Data Security Standard - A set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment.

PHP: Hypertext Preprocessor - A server-side scripting language designed primarily for web development.

PID: Process Identifier - A unique identifier that is assigned to each process running on a computer operating system.

PII: Personally Identifiable Information - Any information that can be used to identify a particular person.

PKI: Public Key Infrastructure - A set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.

PLC: Programmable Logic Controller - A ruggedized computer used for automating processes, such as control of machinery on factory assembly lines, amusement rides, or lighting fixtures.

POC: Proof of Concept - A demonstration to verify that certain concepts or theories have the potential for real-world application.

RCE: Remote Code Execution - The ability for an attacker to execute arbitrary code on a target system without having physical access to it.

RDP: Remote Desktop Protocol - A proprietary protocol developed by Microsoft that enables users to remotely connect to a computer running Microsoft Windows.

REST: Representational State Transfer - An architectural style for distributed hypermedia systems, typically used in web services development.

RFI: Remote File Inclusion - A type of vulnerability that allows an attacker to include a remote file on a website.

RXSS: Reflected Cross-site Scripting - A type of cross-site scripting attack where the injected script is reflected off a web application, such as in an error message displayed to the user.

SaaS: Software as a Service - A software delivery model in which software is hosted on a cloud and accessed via the internet.

SAML: Security Assertion Markup Language - An XML-based open-standard data format for exchanging authentication and authorization data between parties.

SASE: Secure Access Secure Edge - A network architecture that combines security functions with wide-area network (WAN) capabilities to support the dynamic, secure access needs of organizations.

SCADA: Supervisory Control and Data Acquisition - A control system architecture that uses computers, networked data communications, and graphical user interfaces for high-level process supervisory management.

SDLC: Software Development Life Cycle - A series of phases that software goes through from conception to retirement.

SDN: Software-defined Networking - A networking architecture that aims to make networks more flexible and agile by separating the network's control plane from the data plane.

SFTP: Secure File Transfer Protocol - A network protocol used for securely transferring files over a computer network.

SIEM: Security Information and Event Management - A technology that provides real-time analysis of security alerts generated by applications and network hardware.

SLA: Service-level Agreement - A contract between a service provider and a customer that defines the level of service expected from the service provider.

SLO: Service-level Objective - A target value or range of values for a service level that is measured by an SLA.

SOAR: Security Orchestration, Automation, and Response - A set of technologies that enable organizations to collect security threat data and respond to low-level security events without human intervention.

SMB: Server Message Block - A network communication protocol used for providing shared access to files, printers, and other resources on a network.

SMTP: Simple Mail Transfer Protocol - A protocol used for sending email messages between servers.

SNMP: Simple Network Management Protocol - A protocol used for collecting and organizing information about managed devices on IP networks.

SOC: Security Operations Center - A centralized unit responsible for monitoring and analyzing an organization's security posture.

SPF: Sender Policy Framework - An email authentication method designed to detect forged sender addresses during the delivery of the email.

SQL: Structured Query Language - A programming language used for managing and manipulating relational databases.

SSL: Secure Sockets Layer - A cryptographic protocol designed to provide secure communication over a computer network.

SSO: Single Sign-On - An authentication process that allows a user to access multiple applications with one set of login credentials.

SSRF: Server-side Request Forgery - A vulnerability that allows an attacker to manipulate the server into making unauthorized requests to other internal or external resources.

STIX: Structured Threat Information Expression - A standardized language for describing cyber threat information in a structured manner.

SWG: Secure Web Gateway - A security solution that filters and monitors web traffic to protect users from internet-borne threats.

TCP: Transmission Control Protocol - A connection-oriented protocol used for transmitting data reliably across networks.

TFTP: Trivial File Transfer Protocol - A simple file transfer protocol used for transferring files between devices on a network.

TLS: Transport Layer Security - A cryptographic protocol used to secure communication over a computer network.

TRACE: Trade Reporting and Compliance Engine - An electronic system used by FINRA to facilitate the collection, consolidation, and dissemination of trade data for publicly traded securities.

TTP: Tactics, Techniques, and Procedures - The methods and strategies used by threat actors to carry out cyber attacks.

UEBA: User and Entity Behavior Analytics - A cybersecurity process that focuses on detecting insider threats, targeted attacks, and financial fraud by analyzing user and entity behavior.

URI: Uniform Resource Identifier - A string of characters used to identify a resource on the internet.

URL: Uniform Resource Locator - A specific type of URI that specifies the location of a resource on the internet.

USB: Universal Serial Bus - A standard interface used for connecting peripherals to computers.

VLAN: Virtual LAN - A logical grouping of devices within a network, regardless of their physical location, to facilitate network management and security.

VM: Virtual Machine - A software-based emulation of a physical computer that runs an operating system and applications.

VPN: Virtual Private Network - A secure network connection that allows users to access resources on a private network over a public network.

WAF: Web Application Firewall - A security solution designed to protect web applications from common web-based attacks.

WAN: Wide Area Network - A network that connects multiple local area networks (LANs) over a large geographic area.

XDR: Extended Detection Response - A cybersecurity approach that integrates data across multiple security layers to provide more comprehensive threat detection and response capabilities.

XML: Extensible Markup Language - A markup language used for encoding documents in a format that is both human-readable and machine-readable.

XSS: Cross-site Scripting - A type of security vulnerability typically found in web applications that allows attackers to inject malicious scripts into web pages viewed by other users.

XXE: XML External Entity - A type of attack that exploits XML parsers that process external entity references in XML documents.

ZAP: Zed Attack Proxy - An open-source web application security scanner used for finding vulnerabilities in web applications.

ZTNA: Zero Trust Network Access - A security model that requires strict identity verification for every person and device attempting to access resources on a private network, regardless of whether they are located inside or outside the network perimeter.

Equipment:

Workstations/Laptops: These are used for running virtual machines (VMs) to simulate different environments or to perform security testing.

Firewall: Provides network security by monitoring and controlling incoming and outgoing network traffic based on predetermined security rules.

IDS/IPS: Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) are used to detect and prevent malicious activities on the network.

Servers: These could host various services and applications used in the cybersecurity environment.

Software:

Windows Operating Systems: Commando VM is a Windows-based distribution for penetration testing and red teaming activities.

Linux Operating Systems: Kali Linux is a popular Linux distribution specifically designed for penetration testing, ethical hacking, and security auditing.

Open-source UTM Appliance: Unified Threat Management (UTM) appliances provide multiple security features such as firewall, intrusion detection/prevention, antivirus, VPN, and content filtering.

Metasploitable: A vulnerable Linux virtual machine designed for practicing penetration testing techniques.

SIEM (Security Information and Event Management): Tools like Greylog, ELK (Elasticsearch, Logstash, Kibana), and Splunk are used for centralized logging, analysis, and correlation of security events.

Packet Analysis Tools: TCPDump and Wireshark are used for capturing and analyzing network traffic.

Vulnerability Scanners: OpenVAS and Nessus are used to identify vulnerabilities in systems and networks.

Access to Cloud Instances: Utilizing cloud platforms like Azure, AWS, and GCP provides flexibility in deploying and testing applications and services in a cloud environment.

BLACK **TOWER**
ACADEMY

Thank you for putting your trust in Black Tower Academy

We believe in QUALITY education and aim to make it affordable on the internet to all who wish to learn.

ajay Menendez