Professional Certificate in Preventing Insider Threats

Insider Threat Investigation Procedures

Account takeover (ATO): A type of insider threat where an authorized user's credentials are stolen or compromised, allowing an unauthorized user to gain access to sensitive information or systems.

Advanced Persistent Threats (APTs): A stealthy threat actor, typically a nation-state or well-resourced group, that gains unauthorized access to a system or network and remains undetected for a period of time while stealing sensitive data or disrupting operations.

Asset: Any data, system, or network that has value to an organization and requires protection from insider threats.

Authentication: The process of verifying the identity of a user, device, or system before granting access to sensitive information or systems.

Behavioral analytics: The use of data analysis techniques to identify patterns of behavior that may indicate an insider threat, such as unusual access to sensitive data or systems.

Bring Your Own Device (BYOD): A policy that allows employees to use their personal devices, such as laptops or smartphones, for work purposes, increasing the risk of insider threats due to the lack of control over these devices.

Cloud computing: The use of remote servers and networks to store, manage, and process data, increasing the risk of insider threats due to the lack of physical control over these resources.

Data Loss Prevention (DLP): A set of technologies and practices designed to prevent the unauthorized access, use, or disclosure of sensitive information.

Denial of Service (DoS) attack: A type of cyber attack where the attacker floods a network or system with traffic, making it unavailable to authorized users, which can be carried out by an insider.

Endpoints: Devices such as laptops, smartphones, and tablets that connect to a network and can be a source of insider threats.

Exfiltration: The unauthorized transfer of sensitive data from a system or network, often carried out by insiders.

Firewall: A security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules, helping to prevent insider threats.

Honeypot: A decoy system or network used to lure and detect insider threats, often used in conjunction with other security measures.

Identity and Access Management (IAM): The processes and technologies used to ensure that only authorized users have access to sensitive information and systems, helping to prevent insider threats.

Incident response: The process of detecting, investigating, and responding to security incidents, including insider threats.

Insider threat: A security risk posed by authorized users, such as employees, contractors, or partners, who have access to sensitive information or systems and may use that access for malicious purposes.

Insider Threat Investigation Procedures: A set of best practices and guidelines for detecting, investigating, and responding to insider threats, as taught in the Professional Certificate in Preventing Insider Threats course.

Intrusion Detection System (IDS): A system that monitors network traffic for signs of suspicious activity, helping to detect insider threats.

Least privilege: A principle of security that grants users the minimum level of access necessary to perform their job functions, reducing the risk of insider threats.

Malware: Software designed to disrupt, damage, or gain unauthorized access to a system or network, which can be used by insiders for malicious purposes.

Mobile Device Management (MDM): A set of technologies and practices used to manage and secure mobile devices, helping to prevent insider threats.

Network segmentation: The practice of dividing a network into smaller, isolated segments to limit the spread of insider threats.

Phishing: A type of social engineering attack where the attacker sends a fraudulent email or message in an attempt to trick the recipient into revealing sensitive information, which can be carried out by insiders.

Privileged Access Management (PAM): The processes and technologies used to manage and monitor users with elevated privileges, helping to prevent insider threats.

Ransomware: A type of malware that encrypts a victim's data and demands a ransom in exchange for the decryption key, which can be used by insiders for malicious purposes.

Removable media: Devices such as USB drives and external hard drives that can be used to transfer data between systems, increasing the risk of insider threats.

Single Sign-On (SSO): A technology that allows users to access multiple systems or applications with a single set of credentials, reducing the risk of insider threats.

Social engineering: The use of psychological manipulation to trick users into revealing sensitive information or performing actions that compromise security, which can be carried out by insiders.

Spear phishing: A targeted form of phishing where the attacker tailors the message to the specific

recipient, increasing the likelihood of success, which can be carried out by insiders.

Two-factor authentication (2FA): A security process that requires users to provide two forms of authentication, such as a password and a fingerprint, helping to prevent insider threats.

User and Entity Behavior Analytics (UEBA): The use of machine learning and artificial intelligence to analyze user behavior and detect anomalies that may indicate an insider threat.

Vulnerability: A weakness in a system or network that can be exploited by an attacker, including insiders.

Whitelisting: A security practice where only approved applications or devices are allowed to access a system or network, helping to prevent insider threats.

Note: The above glossary terms are provided as a starting point for understanding Insider Threat Investigation Procedures and may not be comprehensive. The field of insider threat prevention and investigation is constantly evolving, and new terms and concepts may emerge over time. It is important for professionals in this field to stay up-to-date with the latest developments and best practices.