Professional Certificate in Preventing Insider Threats

Insider Threat Mitigation Strategies

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

Advanced Persistent Threat (APT): A type of cyber threat in which an unauthorized user gains access to a network and remains undetected for a prolonged period, allowing them to steal sensitive data or disrupt operations. APTs often involve insiders who have authorized access to the network.

Behavioral Analytics: The use of data and algorithms to identify patterns of behavior that may indicate malicious intent or insider threats. This can include monitoring user activity, network traffic, and other data points to detect anomalies that may indicate a potential threat.

Data Loss Prevention (DLP): A set of technologies and practices designed to prevent the unauthorized disclosure, modification, or destruction of sensitive information. DLP can include measures such as encryption, access controls, and monitoring for suspicious activity.

Employee Monitoring: The practice of tracking and analyzing employee behavior and activity, often using software tools, to detect potential insider threats. This can include monitoring email and internet usage, tracking access to sensitive data, and analyzing patterns of behavior.

Insider Threat: A type of security threat that originates from within an organization, often involving authorized users who have access to sensitive information or systems. Insider threats can take many forms, including malicious insiders, negligent insiders, and compromised insiders.

Insider Threat Mitigation: The process of identifying, assessing, and mitigating potential insider threats. This can involve a variety of measures, including access controls, monitoring and analytics, training and awareness, and incident response planning.

Insider Threat Program: A formal program within an organization designed to identify, assess, and mitigate potential insider threats. An insider threat program typically includes a cross-functional team of stakeholders, a defined process for identifying and assessing threats, and a plan for responding to incidents.

Malicious Insider: An authorized user who intentionally causes harm to an organization by misusing their access to sensitive information or systems. Malicious insiders may be motivated by a variety of factors, including financial gain, revenge, or ideology.

Negligent Insider: An authorized user who inadvertently causes harm to an organization by failing to follow security policies or procedures. Negligent insiders may not intend to cause harm, but their actions can still result in data breaches, system disruptions, or other security incidents.

Privileged Access Management (PAM): A set of technologies and practices designed to manage and monitor

access to sensitive systems and data by users with elevated privileges. PAM can include measures such as access controls, monitoring for suspicious activity, and requiring multi-factor authentication.

Security Information and Event Management (SIEM): A set of technologies and practices for collecting, analyzing, and correlating security-related data from multiple sources. SIEM can help organizations detect potential insider threats by identifying anomalies or suspicious patterns of behavior.

Social Engineering: The use of deception to manipulate individuals into divulging sensitive information or performing actions that compromise security. Social engineering attacks can be used to gain unauthorized access to sensitive systems or data, often involving insiders who are tricked into revealing their credentials or other sensitive information.

User and Entity Behavior Analytics (UEBA): A type of behavioral analytics that focuses on monitoring and analyzing user behavior to detect potential insider threats. UEBA can help organizations identify anomalous behavior patterns that may indicate a potential threat, such as unusual access to sensitive data or systems.

Zero Trust: A security model that assumes that all users and systems are untrusted by default, and requires verification and authentication before granting access to sensitive information or systems. Zero trust can help prevent insider threats by limiting the amount of access granted to users and systems, and by requiring multi-factor authentication for all access requests.