Postgraduate Certificate in Aviation Security Management

Aviation Cybersecurity

Advanced Persistent Threat (APT): A type of cyber threat in which an unauthorized user gains access to a system and remains undetected for a prolonged period, with the intention of stealing sensitive data or causing damage. APTs typically target organizations in critical infrastructure sectors, such as aviation.

Aircraft Communications Addressing and Reporting System (ACARS): A digital datalink system used for the transmission of short messages between aircraft and ground stations. ACARS messages can include information about flight status, weather conditions, and maintenance data.

Air Traffic Control (ATC) system: A system responsible for providing safe and efficient management of aircraft movements in controlled airspace. ATC systems rely on a combination of human controllers and automation to ensure the safe separation of aircraft.

Anti-virus (AV) software: Software designed to detect, prevent, and remove malicious software (malware) from a system. AV software uses signature-based detection, heuristics, and behavioral analysis to identify and block known and unknown threats.

Authentication: The process of verifying the identity of a user, device, or system. Authentication typically involves a combination of something the user knows (e.g., a password), something the user has (e.g., a security token), and something the user is (e.g., biometric data).

Availability: A key component of information security, referring to the ability of authorized users to access information and systems when needed. Availability is often targeted by cyber threats such as Distributed Denial of Service (DDoS) attacks.

Cyber Threat Intelligence (CTI): The collection, analysis, and dissemination of information about potential or current cyber threats. CTI is used to inform cybersecurity decisions and improve an organization's ability to detect, prevent, and respond to cyber threats.

Cybersecurity Framework (CSF): A voluntary framework developed by the National Institute of Standards and Technology (NIST) to help organizations manage cybersecurity risks. The CSF includes a set of core functions, categories, and subcategories that provide a common language for discussing cybersecurity.

Data Diode: A one-way network device that allows data to flow in only one direction, preventing unauthorized access or data exfiltration. Data diodes are often used in high-security environments, such as critical infrastructure sectors, to prevent cyber threats from moving laterally within a network.

Denial of Service (DoS) attack: A type of cyber attack in which an attacker attempts to make a system or network unavailable to authorized users by overwhelming it with traffic or other types of requests.

Distributed Denial of Service (DDoS) attack: A type of DoS attack in which an attacker uses a network of

compromised systems (botnet) to flood a target system or network with traffic.

Encryption: The process of converting plaintext into ciphertext, making it unreadable to unauthorized users. Encryption is a key component of information security and is used to protect data in transit and at rest.

Firewall: A network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules. Firewalls can be hardware-based or software-based and are often used to protect networks from unauthorized access.

Incident Response (IR): The process of identifying, investigating, and mitigating cybersecurity incidents. IR plans typically include procedures for containing the incident, eradicating the threat, and restoring normal operations.

Insider threat: A cyber threat posed by an individual within an organization who has authorized access to systems and data. Insider threats can be malicious (e.g., a disgruntled employee stealing sensitive data) or accidental (e.g., an employee clicking on a phishing link).

Intrusion Detection System (IDS): A network security device that monitors network traffic for signs of malicious activity and alerts security personnel when a potential threat is detected.

Intrusion Prevention System (IPS): A network security device that monitors network traffic for signs of malicious activity and takes automated action to prevent the threat from causing harm.

Malware: Software designed to cause harm to a system or network, including viruses, worms, Trojans, and ransomware.

Multi-Factor Authentication (MFA): A security process in which users are required to provide two or more forms of authentication to access a system or network. MFA can include something the user knows (e.g., a password), something the user has (e.g., a security token), and something the user is (e.g., biometric data).

Network Segmentation: The process of dividing a network into smaller, isolated segments to improve security and reduce the risk of lateral movement by cyber threats.

Penetration Testing: The process of simulating a cyber attack on a system or network to identify vulnerabilities and weaknesses. Penetration testing is used to evaluate the effectiveness of an organization's cybersecurity controls and identify areas for improvement.

Phishing: A type of social engineering attack in which an attacker sends a fraudulent email or message that appears to be from a trusted source, with the goal of tricking the recipient into providing sensitive information or clicking on a malicious link.

Ransomware: A type of malware that encrypts a victim's files and demands payment in exchange for the decryption key.

Security Information and Event Management (SIEM) system: A security tool that collects and analyzes security-related data from various sources, such as firewalls, IDS/IPS, and servers, to provide real-time

visibility into security threats and incidents.

Security Operations Center (SOC): A dedicated team responsible for monitoring and managing an organization's cybersecurity posture. SOCs typically use a combination of tools, such as SIEM systems, to detect and respond to cyber threats.

Social Engineering: The use of psychological manipulation to trick individuals into divulging sensitive information or performing actions that compromise security.

Supply Chain Security: The protection of the supply chain from cyber threats, including the theft or manipulation of data, sabotage of equipment, and disruption of operations.

Threat Hunting: The proactive search for cyber threats that may have bypassed traditional cybersecurity controls. Threat hunting involves analyzing security data and using advanced analytics to identify indicators of compromise (IOCs) and other signs of malicious activity.

Vulnerability Management: The process of identifying, classifying, remediating, and mitigating vulnerabilities in systems and applications. Vulnerability management is a critical component of cybersecurity and is used to reduce the attack surface and minimize the risk of compromise.

Zero Day Exploit: A previously unknown vulnerability in a system or application that has not been patched or mitigated. Zero day exploits are highly valued by attackers because they can be used to compromise systems without detection.

Note: The above glossary terms and definitions are provided for educational purposes only and are not intended to be exhaustive or comprehensive. The use of any of the above terms in a specific context may have different or additional meanings.