Advanced Certificate in Healthcare Fraud Investigation Best Practices

Unit 7: Managing and Analyzing Electronic Evidence

Advanced Persistent Threat (APT): A type of cyber threat in which a unauthorized user gains access to a network and remains undetected for a period of time while stealing sensitive data. APTs are often associated with nation-state or criminal organizations and require sophisticated defensive measures to detect and mitigate.

Computer Forensics: The process of collecting, analyzing, and preserving digital evidence in a way that is admissible in court. This can include searching for and recovering deleted files, analyzing network traffic, and identifying suspicious patterns of behavior.

Data Breach: An incident in which sensitive, protected, or confidential data is accessed or disclosed without authorization. Data breaches can be caused by a variety of factors, including hacking, insider threats, and physical theft.

Digital Evidence: Any data that is stored or transmitted in digital form and can be used as evidence in a legal investigation. This can include email, text messages, social media posts, and files stored on computers or mobile devices.

Electronic Discovery (eDiscovery): The process of identifying, collecting, and producing electronically stored information (ESI) in response to a legal request or litigation. eDiscovery can be a time-consuming and costly process, and requires specialized tools and expertise to manage.

Forensic Image: A bit-for-bit copy of a digital storage device, such as a hard drive or USB flash drive, that can be used for analysis and investigation. Forensic images are created using specialized software and hardware, and are admissible as evidence in court.

Hash Value: A unique numerical value that is calculated based on the contents of a file or data block. Hash values are used to verify the integrity of digital evidence, as any change to the contents of the file or data block will result in a different hash value.

Incident Response: The process of identifying, containing, and mitigating a security incident, such as a data breach or cyber attack. Incident response plans should be in place to ensure a swift and effective response to minimize the impact of the incident.

Insider Threat: A security risk posed by an individual within an organization who has authorized access to sensitive information or systems. Insider threats can be malicious, such as an employee stealing data for personal gain, or non-malicious, such as an employee accidentally disclosing sensitive information.

Log Files: Records of events that occur on a computer or network, such as login/logoff events, file access, and network traffic. Log files can be used to investigate security incidents and are an important source of digital evidence.

Malware: Software that is designed to harm or exploit a computer system, such as viruses, worms, and Trojan horses. Malware can be used to steal sensitive data, disrupt operations, or launch cyber attacks.

Network Forensics: The process of analyzing network traffic to detect and respond to security incidents. Network forensics can include analyzing logs, packet capture, and network device configurations.

Ransomware: A type of malware that encrypts a victim's files and demands a ransom payment in exchange for the decryption key. Ransomware attacks are increasingly common and can result in significant financial and reputational damage.

SQL Injection: A type of cyber attack in which an attacker injects malicious SQL code into a web application's input fields in order to gain unauthorized access to a database. SQL injection attacks can be used to steal sensitive data or disrupt operations.

Threat Intelligence: Information about potential or current threats to an organization's security, such as malware, hacking attempts, or insider threats. Threat intelligence can be used to inform security decisions and improve incident response.

Two-Factor Authentication (2FA): A security measure that requires users to provide two forms of authentication, such as a password and a fingerprint, in order to access a system or service. 2FA increases the security of accounts by making it more difficult for attackers to gain unauthorized access.

Vulnerability Assessment: The process of identifying and evaluating weaknesses in an organization's security posture. Vulnerability assessments can be used to identify areas where security measures can be improved and to prioritize remediation efforts.

Wireless Forensics: The process of analyzing wireless network traffic to detect and respond to security incidents. Wireless forensics can include analyzing logs, packet capture, and wireless device configurations.

Zero-Day Exploit: A type of cyber attack that takes advantage of a previously unknown vulnerability in a system or software. Zero-day exploits are particularly dangerous because they can be used before the vulnerability is discovered and patches are released.

Data Leakage: The unauthorized transfer of sensitive or confidential information from an organization to an external entity. Data leakage can be caused by a variety of factors, including hacking, insider threats, and physical theft.

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

Digital Preservation: The process of maintaining the integrity and accessibility of digital evidence over time. Digital preservation can include measures such as creating forensic images, storing evidence in secure environments, and regularly verifying the integrity of the evidence.

Email Forensics: The process of analyzing email messages and headers to detect and respond to security

incidents. Email forensics can include analyzing logs, message metadata, and attachment contents.

Encryption: The process of converting plaintext into ciphertext, which can only be deciphered with the correct key. Encryption is used to protect the confidentiality and integrity of sensitive data.

Firewall: A security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules. Firewalls are used to protect networks from unauthorized access and attacks.

Honey pot: A security resource whose value lies in being probed or attacked. Honeypots are used to detect, deflect, or study attempts to access a computer or network system for malicious purposes.

Incident Response Plan: A set of instructions and procedures that an organization follows in response to a security incident, such as a data breach or cyber attack. An incident response plan should include steps for identifying, containing, and mitigating the incident, as well as for reporting the incident to relevant authorities.

Intrusion Detection System (IDS): A security system that monitors network traffic for signs of malicious activity and sends alerts when such activity is detected. IDS can be used to detect and respond to cyber attacks, such as hacking attempts and malware infections.

Log Management: The process of collecting, analyzing, and storing log files from various systems and devices in order to detect and respond to security incidents. Log management can include measures such as centralizing log data, filtering and correlating events, and creating alerts for suspicious activity.

Mobile Device Forensics: The process of analyzing data stored on mobile devices, such as smartphones and tablets, to detect and respond to security incidents. Mobile device forensics can include analyzing call logs, text messages, and application data.

Penetration Testing: The process of simulating a cyber attack on an organization's systems and networks in order to identify vulnerabilities and test security measures. Penetration testing can be used to evaluate the effectiveness of security controls and to inform remediation efforts.

Security Information and Event Management (SIEM): A security system that aggregates and correlates log data from various systems and devices in order to detect and respond to security incidents. SIEM systems can be used to identify patterns and trends in security-related events, and to generate alerts for suspicious activity.

Vulnerability Management: The process of identifying, evaluating, and addressing vulnerabilities in an organization's systems and networks. Vulnerability management can include measures such as regular vulnerability scanning, patch management, and configuration management.

Web Application Firewall (WAF): A security system that monitors and filters incoming HTTP traffic to a web application in order to protect against common web attacks such as SQL injection and cross-site scripting (XSS). WAFs can be used to protect web applications from