Professional Certificate in Digital Forensics Fundamentals

Incident Response

Alert: An alert is a notification that an incident has occurred or is in progress. Alerts can be generated by various systems and tools, such as intrusion detection systems (IDS), security information and event management (SIEM) systems, and endpoint detection and response (EDR) tools.

Anti-Forensics: Anti-forensics refers to techniques used to evade or frustrate digital forensic investigations. These techniques can include data hiding, data destruction, and tampering with logs and other evidence.

Asset: An asset is any resource that has value to an organization. Assets can include data, systems, networks, applications, and physical infrastructure.

Breach: A breach is an unauthorized access or disclosure of sensitive or confidential information. Breaches can be caused by various factors, such as hacking, insider threats, and physical theft.

Chain of Custody: The chain of custody is a record of the movement and handling of evidence from the time it is collected to the time it is presented in court. Maintaining a clear and accurate chain of custody is essential for the integrity and admissibility of evidence in legal proceedings.

Computer Forensics: Computer forensics is the process of collecting, analyzing, and preserving digital evidence in a way that is admissible in court. It involves using specialized tools and techniques to recover and examine data from digital devices, such as computers, servers, and mobile devices.

Containment: Containment is the process of limiting the scope and impact of an incident. This can include isolating affected systems, disconnecting them from the network, and blocking known attack vectors.

Data Breach: A data breach is an unauthorized access or disclosure of sensitive or confidential information. Data breaches can be caused by various factors, such as hacking, insider threats, and physical theft.

Digital Forensics: Digital forensics is the process of collecting, analyzing, and preserving digital evidence in a way that is admissible in court. It involves using specialized tools and techniques to recover and examine data from digital devices, such as computers, servers, and mobile devices.

Endpoint Detection and Response (EDR): EDR is a category of security tools that continuously monitor and respond to threats on endpoints, such as laptops, desktops, and servers. EDR tools can detect and respond to threats in real-time, providing visibility into endpoint activity and enabling rapid incident response.

Evidence: Evidence is any information or object that can be used to prove or disprove a fact in a legal

proceeding. In digital forensics, evidence can include data from digital devices, logs, and other sources.

Forensic Image: A forensic image is an exact copy of a digital device's contents, including any hidden or deleted data. Forensic images are used in digital forensics investigations to preserve and analyze evidence.

Hashes: Hashes are mathematical functions that generate a fixed-size output, known as a hash value, based on an input. Hashes are used in digital forensics to verify the integrity of data and to detect changes or tampering.

Incident: An incident is an event or series of events that compromise the confidentiality, integrity, or availability of an asset. Incidents can include security breaches, cyber attacks, and other types of security incidents.

Incident Handler: An incident handler is a person responsible for responding to and managing security incidents. Incident handlers are responsible for containing, investigating, and remediating incidents to minimize their impact on the organization.

Incident Response: Incident response is the process of identifying, investigating, and responding to security incidents. It involves a series of steps, including preparation, detection and analysis, containment, eradication, and recovery.

Incident Response Plan (IRP): An IRP is a document that outlines the steps an organization should take in response to a security incident. The IRP should include procedures for detecting, analyzing, containing, eradicating, and recovering from incidents, as well as roles and responsibilities, communication plans, and other relevant information.

Incident Response Policy: An incident response policy is a high-level document that outlines an organization's approach to incident response. It should include the organization's definition of a security incident, the scope of the policy, and the roles and responsibilities of key stakeholders.

Incident Response Playbook: An incident response playbook is a detailed document that outlines the steps an organization should take in response to specific types of incidents. Playbooks should be tailored to the organization's unique needs and should include detailed procedures for each step of the incident response process.

Incident Response Team (IRT): An IRT is a group of individuals responsible for responding to and managing security incidents. The IRT should include representatives from various departments, such as IT, security, legal, and public relations.

Indicators of Compromise (IOCs): IOCs are pieces of information that indicate a compromise or intrusion, such as unusual network traffic, suspicious registry entries, or unusual system activity. IOCs can be used to detect and respond to security incidents.

Intrusion Detection System (IDS): An IDS is a security tool that monitors network traffic and alerts security personnel to suspicious activity. IDS can be used to detect and respond to security incidents.

Logs: Logs are records of system or application activity. Logs can be used to detect and respond to security incidents, as well as to investigate and analyze incidents after they have occurred.

Malware: Malware is malicious software that is designed to disrupt, damage, or gain unauthorized access to a system or network. Malware can take many forms, such as viruses, worms, and Trojan horses.

Memory Analysis: Memory analysis is the process of examining the contents of a system's memory to recover data and evidence. Memory analysis can be used to detect malware, identify user activity, and investigate security incidents.

Mobile Device Forensics: Mobile device forensics is the process of collecting, analyzing, and preserving data from mobile devices, such as smartphones and tablets. It involves using specialized tools and techniques to recover and examine data from mobile devices, such as text messages, call logs, and location data.

Network Forensics: Network forensics is the process of collecting, analyzing, and preserving data from network traffic. It involves using specialized tools and techniques to recover and examine data from network devices, such as routers, switches, and firewalls.

Patch Management: Patch management is the process of identifying, acquiring, testing, and installing software updates and patches. Patch management is an important aspect of incident response, as it can help prevent incidents by addressing known vulnerabilities.

Preparation: Preparation is the first step in the incident response process. It involves developing and maintaining an incident response plan, training personnel, and ensuring that the necessary tools and resources are in place.

Remediation: Remediation is the process of restoring systems and data to a secure and stable state after an incident. This can include removing malware, repairing damaged systems, and restoring data from backups.

Response: Response is the process of identifying, investigating, and containing an incident. It involves using the incident response plan to guide the response, collecting and analyzing evidence, and taking action to limit the impact of the incident.

Risk Assessment: A risk assessment is the process of identifying and evaluating potential risks to an organization's assets. It involves analyzing the likelihood and impact of different types of risks, and developing strategies to mitigate or eliminate them.

Security Information and Event Management (SIEM): SIEM is a category of security tools that aggregate and analyze security-related data from multiple sources, such as logs and network traffic. SIEM tools can be used to detect and respond to security incidents.

Threat Intelligence: Threat intelligence is information about potential or current threats to an organization's assets. Threat intelligence can be used to detect and respond to security incidents, as well as

to proactively identify and mitigate risks.

Triage: Triage is the process of prioritizing and assigning incidents based on their severity and impact. It involves assessing the information available about each incident and determining the appropriate response.

Volatile Data: Volatile data is data that is stored in a system's memory and is lost when the system is shut down. Volatile data can be used to detect and respond to security incidents, as it can provide insight into system activity and user behavior.