Level 2 Certificate in Cybersecurity

Incident Response and Recovery

Incident Response and Recovery Key Terms and Vocabulary:

1. Incident Response: Incident response refers to the process of responding to and managing security incidents within an organization. It involves detecting, analyzing, containing, eradicating, and recovering from security incidents to minimize damage and prevent future incidents.

2. Incident Response Plan (IRP): An incident response plan is a documented set of procedures and guidelines that outline how an organization will respond to security incidents. It includes steps for identifying, containing, and recovering from incidents, as well as roles and responsibilities of team members.

3. Cybersecurity Incident: A cybersecurity incident is any event that poses a threat to the confidentiality, integrity, or availability of an organization's information systems and data. Examples of cybersecurity incidents include data breaches, malware infections, and denial of service attacks.

4. Threat Actor: A threat actor is an individual or group that carries out malicious activities against an organization. Threat actors can include hackers, cyber criminals, insiders, or nation-state actors.

5. Malware: Malware is malicious software designed to disrupt, damage, or gain unauthorized access to computer systems. Examples of malware include viruses, worms, Trojans, ransomware, and spyware.

6. Network Intrusion: A network intrusion occurs when an unauthorized individual gains access to a computer network without permission. Intruders may attempt to steal data, disrupt operations, or carry out other malicious activities.

7. Data Breach: A data breach is a security incident in which sensitive or confidential data is accessed, stolen, or disclosed without authorization. Data breaches can result in financial losses, reputation damage, and legal consequences for organizations.

8. Incident Detection: Incident detection involves identifying and recognizing potential security incidents within an organization's networks and systems. Detection mechanisms can include intrusion detection systems (IDS), security information and event management (SIEM) tools, and threat intelligence feeds.

9. Incident Analysis: Incident analysis is the process of investigating and understanding the nature and scope of a security incident. It involves identifying the root cause, impact, and extent of the incident to inform response and recovery efforts.

10. Incident Containment: Incident containment involves taking immediate actions to prevent a security incident from spreading further within an organization's networks and systems. This may include isolating affected systems, blocking malicious traffic, or disabling compromised accounts.

11. Incident Eradication: Incident eradication involves removing the cause of a security incident from an organization's networks and systems. This may involve removing malware, closing vulnerabilities, or implementing security patches to prevent future incidents.

12. Incident Recovery: Incident recovery is the process of restoring affected systems and data to normal operation after a security incident. Recovery efforts aim to minimize downtime, restore data integrity, and ensure business continuity.

13. Forensic Analysis: Forensic analysis involves collecting, preserving, analyzing, and presenting digital evidence to investigate security incidents and support legal proceedings. Forensic techniques can help identify the source of an incident and attribute it to a specific threat actor.

14. Chain of Custody: Chain of custody is the documented record of the chronological sequence of custody, control, and transfer of physical or digital evidence during a forensic investigation. Maintaining a chain of custody is essential to ensure the integrity and admissibility of evidence in court.

15. Threat Intelligence: Threat intelligence is information about potential and current cyber threats that can help organizations proactively defend against attacks. Threat intelligence sources include security vendors, government agencies, open-source feeds, and industry collaborations.

16. Security Incident Response Team (SIRT): A security incident response team is a dedicated group of individuals responsible for coordinating and executing incident response activities within an organization. SIRT members have specialized skills in incident detection, analysis, containment, and recovery.

17. Playbooks: Playbooks are predefined sets of procedures, workflows, and response actions that guide incident response teams through different types of security incidents. Playbooks can help standardize and streamline response efforts, ensuring consistency and efficiency.

18. Tabletop Exercise: A tabletop exercise is a simulated scenario-based training activity in which incident response team members practice their roles and responsibilities in responding to a security incident. Tabletop exercises help teams improve coordination, communication, and decision-making skills.

19. Business Impact Analysis (BIA): Business impact analysis is a process of assessing the potential impacts of a security incident on an organization's operations, assets, and reputation. BIA helps prioritize response efforts, allocate resources effectively, and mitigate risks to the business.

20. Recovery Time Objective (RTO): Recovery time objective is the maximum acceptable time within which an organization must recover its systems and operations after a security incident. RTO helps set recovery priorities, allocate resources, and minimize downtime during incident recovery.

21. Recovery Point Objective (RPO): Recovery point objective is the maximum acceptable data loss that an organization can tolerate after a security incident. RPO helps determine backup and recovery strategies, data retention policies, and recovery priorities based on data criticality.

22. Incident Response Maturity: Incident response maturity refers to an organization's capability to effectively detect, respond to, and recover from security incidents. Maturity levels can range from ad-hoc

reactive responses to proactive, well-defined incident response processes.

23. Continuous Improvement: Continuous improvement is the ongoing process of refining and enhancing incident response practices based on lessons learned, feedback, and emerging threats. By continuously improving incident response capabilities, organizations can better adapt to evolving security challenges.

24. Incident Response Metrics: Incident response metrics are key performance indicators (KPIs) used to measure the effectiveness, efficiency, and impact of incident response activities. Metrics can include mean time to detect (MTTD), mean time to respond (MTTR), and incident closure rates.

25. Legal and Regulatory Compliance: Legal and regulatory compliance refers to the requirements and obligations that organizations must follow when responding to security incidents. Compliance standards may include data protection laws, industry regulations, and contractual obligations.

26. Data Privacy: Data privacy is the protection of personal or sensitive information from unauthorized access, use, or disclosure. Maintaining data privacy is essential during incident response to prevent further exposure of confidential data and comply with privacy regulations.

27. Incident Reporting: Incident reporting involves documenting and communicating security incidents to relevant stakeholders, including internal teams, management, legal counsel, and regulatory authorities. Timely and accurate incident reporting is crucial for transparency, accountability, and compliance.

28. Crisis Communication: Crisis communication is the process of managing and coordinating communication efforts during a security incident to inform, reassure, and guide internal and external stakeholders. Effective crisis communication can help maintain trust, credibility, and reputation during and after an incident.

29. Root Cause Analysis: Root cause analysis is a methodical process of identifying the underlying cause or causes of a security incident to prevent recurrence. By addressing root causes, organizations can implement corrective actions and improve overall security posture.

30. Lessons Learned: Lessons learned are insights, experiences, and best practices gained from past security incidents that inform future incident response strategies. By documenting and sharing lessons learned, organizations can enhance their incident response capabilities and resilience.

31. Incident Simulation: Incident simulation is a controlled exercise that replicates real-world security incidents to test incident response capabilities, identify weaknesses, and train response teams. Simulations help organizations validate their incident response plans and improve readiness for actual incidents.

32. Incident Response Automation: Incident response automation involves using technology tools and scripts to streamline and accelerate response actions during security incidents. Automation can help reduce manual tasks, improve response time, and enhance overall efficiency in incident response.

33. Third-Party Incident Response Services: Third-party incident response services are external providers that offer specialized expertise, resources, and support for organizations during security incidents. These services can supplement internal incident response teams and provide additional capabilities for handling complex

incidents.

34. Incident Response Software: Incident response software is a set of tools and platforms designed to facilitate and automate various aspects of incident response, such as detection, analysis, containment, and recovery. Examples of incident response software include security orchestration, automation, and response (SOAR) platforms.

35. Security Posture: Security posture refers to an organization's overall security readiness and resilience against cyber threats. A strong security posture includes robust security policies, controls, technologies, and practices to protect against security incidents.

36. Threat Hunting: Threat hunting is a proactive security practice that involves actively searching for signs of malicious activity or potential threats within an organization's networks and systems. Threat hunters use advanced tools, techniques, and threat intelligence to identify and mitigate security risks.

37. Ransomware Recovery: Ransomware recovery is the process of restoring systems and data after a ransomware attack, in which malicious software encrypts files and demands a ransom for decryption. Ransomware recovery efforts may involve data backups, decryption tools, and negotiations with threat actors.

38. Cloud Incident Response: Cloud incident response involves responding to security incidents that affect cloud-based services, applications, or data. Cloud incident response strategies may include coordination with cloud service providers, incident detection in cloud environments, and data protection in cloud storage.

39. Insider Threat: An insider threat is a security risk posed by individuals within an organization who misuse their access privileges to compromise data, systems, or operations. Insider threats can be intentional or unintentional and require proactive monitoring and controls to detect and prevent incidents.

40. Supply Chain Security: Supply chain security refers to the protection of the end-to-end supply chain from cyber threats, including suppliers, vendors, partners, and third-party service providers. Strengthening supply chain security involves assessing risks, implementing controls, and monitoring third-party activities to prevent security incidents.

41. Incident Response Challenges: Incident response challenges are obstacles and complexities that organizations may face when responding to security incidents. Common challenges include limited resources, complex IT environments, evolving threats, regulatory requirements, and coordination with external parties.

42. Incident Response Best Practices: Incident response best practices are recommended strategies, techniques, and principles for effectively responding to security incidents. Best practices include developing incident response plans, conducting regular training and exercises, implementing security controls, and collaborating with stakeholders.

43. Incident Response Frameworks: Incident response frameworks are structured guidelines and

methodologies that organizations can use to plan, implement, and improve their incident response processes. Common frameworks include the NIST Cybersecurity Framework, SANS Incident Handling Steps, and ISO/IEC 27035.

44. Incident Response Training: Incident response training is educational programs and workshops that provide knowledge, skills, and hands-on experience for incident response teams. Training topics may include incident detection, analysis, containment, recovery, communication, and legal considerations.

45. Incident Response Certification: Incident response certification is a formal credential that validates an individual's knowledge and expertise in incident response practices, tools, and techniques. Common incident response certifications include Certified Incident Handler (ECIH), Certified Incident Response Professional (CIRP), and GIAC Certified Incident Handler (GCIH).

46. Incident Response Exercises: Incident response exercises are simulated scenarios or drills that test and evaluate an organization's incident response capabilities, processes, and team readiness. Exercises can include tabletop simulations, full-scale simulations, red team exercises, and incident response drills.

47. Incident Response Documentation: Incident response documentation includes records, reports, logs, and artifacts generated during the incident response process. Documentation is essential for tracking incident details, actions taken, evidence collected, and lessons learned for future reference and improvement.

48. Incident Response Communication: Incident response communication involves sharing timely and accurate information with internal and external stakeholders during a security incident. Effective communication channels, messages, and protocols help coordinate response efforts, maintain transparency, and manage stakeholder expectations.

49. Incident Response Coordination: Incident response coordination is the process of aligning and synchronizing activities among incident response team members, departments, and external partners during a security incident. Coordination ensures a cohesive and collaborative response effort to address the incident effectively.

50. Incident Response Readiness: Incident response readiness is the state of preparedness and capability of an organization to respond promptly and effectively to security incidents. Readiness includes having well-defined processes, trained personnel, up-to-date tools, and tested plans to handle incidents proactively.

These key terms and vocabulary are essential for understanding the concepts, processes, and challenges involved in incident response and recovery in cybersecurity. By familiarizing yourself with these terms and applying them in practice, you can enhance your incident response skills, improve organizational resilience, and effectively mitigate security risks.