Module 5 – Final Quiz: Threat Detection and Incident Response

1 - What is the primary purpose of threat detection?

A) To guarantee no attacks occur
B) To identify potential attacks and compromises early
C) To automatically remove malware
D) To encrypt all system data

2 - Which of the following is an example of an Indicator of Compromise (IOC)?

A) A strong password policy
B) An unusual outbound connection to an unknown IP
C) Running a scheduled backup
D) Installing system updates

3 - Which tool is designed to collect and analyze large volumes of security logs?

A) Packet sniffer
B) SIEM
C) Disk defragmenter
D) Registry cleaner

4 - What is the role of an EDR (Endpoint Detection and Response) tool?

A) Encrypt endpoint drives
B) Detect, investigate, and respond to suspicious activity on endpoints
C) Optimize CPU usage
D) Replace operating system firewalls

5 - What is the main responsibility of a SOC analyst?

A) Write encryption algorithms
B) Monitor security events and respond to alerts
C) Develop new operating systems
D) Design secure hardware chips

6 - Which best describes the IOC lifecycle?

A) Creation → Detection → Sharing → Expiration
B) Backup → Recovery → Patch → Removal
C) Scan → Encrypt → Hash → Store
D) Identify → Block → Delete → Forget

7 - Where are IOCs commonly found?

A) Disk cleanup tools
B) System logs, memory, and network traffic
C) File compression utilities
D) Power management settings

8 - Which is NOT a typical data source for a SIEM?

A) Firewall logs
B) Intrusion detection alerts
C) Application audit logs
D) Computer wallpaper images

9 - Which step is first in the incident response lifecycle (NIST model)?

A) Containment
B) Preparation
C) Eradication
D) Recovery

10 - Which action is part of the containment phase of incident response?

A) Restoring affected systems to production
B) Isolating compromised machines from the network
C) Writing new security policies
D) Performing a lessons-learned review

11 - Why is preparation considered the most important step in incident response?

A) It ensures attacks never happen
B) It reduces impact by having clear plans and tools in place
C) It eliminates the need for detection
D) It prevents insider threats completely

12 - Which of the following should be included in an incident report?

A) A summary of system performance
B) Incident timeline, affected assets, actions taken, and resolution
C) Employee vacation schedules
D) Encryption key backups

13 - Why is post-incident documentation critical?

A) It reduces system performance
B) It enables compliance, accountability, and future learning
C) It allows attacks to repeat
D) It replaces patching requirements

14 - What is the chain of custody in digital forensics?

A) A record of who accessed and handled evidence to maintain legal integrity
B) A list of all encryption algorithms used
C) A backup of forensic tools
D) The order of attacks in a timeline

15 - Which of these is a forensic tool commonly used in investigations?

A) Wireshark
B) Photoshop
C) Disk Cleanup
D) Excel

Lab 5.1 – Analyzing a Simulated Security Incident

16 - During log review, which of the following could indicate a possible intrusion?

A) A successful login from an unusual geographic location at odd hours
B) A user opening a Word document
C) A scheduled backup completing
D) A normal DNS request

17 - After confirming an incident, what is the first response step?

A) Recovery
B) Containment
C) Eradication
D) Documentation

18 - Why is preserving logs and volatile data important?

A) It reduces system performance issues
B) It ensures evidence remains valid for investigation and legal purposes
C) It speeds up hardware
D) It replaces the need for backups

19 - What is the purpose of a post-incident review?

A) To assign blame to employees
B) To identify lessons learned and improve processes
C) To replace antivirus software
D) To reinstall the operating system

20 - Which of the following is considered a common mistake in incident response?

A) Failing to document every step taken during the response
B) Running a containment strategy
C) Preserving chain of custody
D) Conducting a lessons-learned session

Answer Key

1. **B** – Detection = spotting compromises early, not prevention alone.
2. **B** – Unusual outbound IPs are strong IOCs.
3. **B** – SIEMs aggregate and analyze log data.
4. **B** – EDR detects/responds at endpoints.
5. **B** – SOC analysts monitor and respond to alerts.
6. **A** – IOC lifecycle includes creation, detection, sharing, expiration.
7. **B** – Found in logs, memory, and traffic.
8. **D** – Wallpapers are not a SIEM data source.
9. **B** – Preparation comes first.
10. **B** – Containment = isolate affected systems.
11. **B** – Preparation ensures readiness and reduces impact.
12. **B** – Reports need timeline, assets, actions, resolution.
13. **B** – Documentation enables compliance and lessons learned.
14. **A** – Chain of custody = evidence integrity record.
15. **A** – Wireshark is a forensic/analysis tool.
16. **A** – Unusual logins are red flags.
17. **B** – Containment comes first after confirmation.
18. **B** – Evidence preservation keeps data reliable and admissible.
19. **B** – Post-incident reviews improve future response.
20. **A** – Not documenting properly is a major pitfall.