SOC / Cyber Security Interview Questions (Additional – No Overlap)

1. Event vs Alert vs Incident
Event is any logged activity, alert is a suspicious event flagged by tools, incident is a confirmed security issue requiring response.

2. What is a False Positive and False Negative?
False positive is benign activity flagged as malicious. False negative is a real attack that goes undetected.

3. What is a SOC Playbook?
A documented step-by-step response guide used by analysts during specific security incidents.

4. What is Log Correlation?
The process of analyzing multiple log sources together to identify attack patterns.

5. Difference between HIDS and NIDS
HIDS monitors individual hosts, while NIDS monitors network traffic.

6. What is MITRE ATT&CK; framework?
A knowledge base mapping real-world attacker tactics and techniques.

7. What is Privilege Escalation?
When an attacker gains higher access rights than initially authorized.

8. What is Lateral Movement?
Attackers moving across systems within a network after initial compromise.

9. What is MTTD and why is it important?
Mean Time To Detect measures how quickly threats are identified; lower MTTD reduces damage.

10. What actions are taken after incident containment?
Eradication, recovery, root cause analysis, and lessons learned.