SOC Interview Questions & Answers

Q: What is an alert vs an incident?

A: An alert is a notification from a security tool indicating potential suspicious activity. An incident is a confirmed security event with real or potential impact. Every incident starts as an alert, but not all alerts become incidents.

Q: What is a false positive and true positive?

A: A false positive is an alert that appears malicious but is legitimate after investigation. A true positive is an alert that correctly identifies real malicious activity.

Q: Explain SOC severity levels.

A: Low is informational with no impact. Medium is suspicious and requires investigation. High is a confirmed threat with limited impact. Critical is an active breach or major business risk.

Q: What does a Tier-1 SOC analyst do?

A: A Tier-1 SOC analyst monitors alerts, performs triage, identifies false positives, validates incidents, escalates confirmed threats, and documents findings.