SOC Interview Scenarios – Questions & Model Answers (SOC-Grade)

Scenario 1: Password Spraying Attack

Alert Details: 120 failed login attempts from a single external IP targeting 15 different users within 8 minutes on O365 / Entra ID. No successful login observed.

Interview Questions

1. What type of attack is this and why?
2. Is this an alert or an incident?
3. Which logs would you review first?
4. When would you escalate this?
5. What immediate actions would you take?

Model Answer (How Interviewers Expect)

This activity strongly indicates a password spraying attack because a single password is attempted across multiple user accounts in a short timeframe, which is a common technique to avoid account lockouts. At this stage, it remains an alert rather than a confirmed incident since there is no successful authentication. I would review Entra ID sign-in logs, conditional access logs, and identity protection alerts to validate targeting and authentication methods. Escalation would be required if a login succeeds, a privileged account is targeted, or MFA is bypassed. Immediate action would be monitoring, tightening conditional access, and blocking the source IP if repeated.

Scenario 2: Successful Login After Multiple Failures

Alert Details: User finance.admin shows 10 failed logins followed by a success from the same external IP at 03:12 AM with MFA disabled.

Interview Questions

1. Is this still an alert or now an incident?
2. What is your first validation step?
3. Which logs do you correlate next?
4. What containment actions are required?
5. What must be documented?

Model Answer

This is a confirmed security incident because failed attempts followed by a successful login without MFA strongly suggest account compromise. The first step is to validate legitimacy by checking user location, device history, and prior login behavior. I would correlate authentication logs with mailbox activity, file access, role changes, and audit logs. Containment includes revoking sessions, forcing password reset, enabling MFA, and temporarily disabling the account. Documentation must capture timeline, evidence, actions taken, and impact assessment.

Scenario 3: AWS Privilege Escalation via CloudTrail

CloudTrail logs show dev-user assuming AdminRole from an external IP, followed by AttachRolePolicy and CreateAccessKey.

Interview Questions

1. Why is this dangerous?
2. What attacker technique does this represent?
3. Which CloudTrail events are red flags?
4. How do you confirm compromise?
5. What severity is this?

Model Answer

This indicates privilege escalation and persistence, as attackers gain administrative access and create long-term credentials. This behavior aligns with MITRE ATT&CK; cloud privilege escalation and persistence techniques. AssumeRole, AttachRolePolicy, and CreateAccessKey are critical red flags. Confirmation involves reviewing trust policies, IAM change history, IP reputation, and usage anomalies. This should be classified as a high to critical severity incident due to full account risk.

Scenario 4: AWS S3 Data Exfiltration

IAM role performs ListBuckets and large-volume GetObject calls from a new ASN. Data Events are enabled.

Interview Questions

1. Why might this not appear in Management Events?
2. What makes this suspicious?
3. What logs would you correlate?
4. What immediate controls would you recommend?
5. What mistake do many SOC teams make?

Model Answer

S3 object access is logged under CloudTrail Data Events, not Management Events, which is why this activity is often missed. Bulk object downloads combined with enumeration from a new ASN deviate from normal application behavior. Correlation should include IAM role assumptions, VPC Flow Logs, GuardDuty findings, and access baselines. Controls include revoking credentials, restricting role permissions, rotating keys, and applying temporary bucket restrictions. Many SOC teams mistakenly assume no alerts or management logs mean no breach, allowing silent data theft.

Scenario 5: False Positive VPN Login Failures

40 failed VPN logins from an internal IP during business hours. User reports VPN instability.

Interview Questions

1. Is this malicious or benign?
2. What evidence supports your decision?
3. Close or monitor?
4. How do you document this?
5. What would make this suspicious next time?

Model Answer

This is likely a benign alert due to internal source, business hours, and user confirmation. Evidence includes internal IP, lack of automation patterns, and supporting user ticket. I would close this as low severity with justification while monitoring for recurrence. Documentation should include alert details, evidence, user confirmation, and closure rationale. If activity shifts to external IPs, off-hours, higher volume, or successful login, it would require escalation.