

SOC Interview Scenarios – Complete Question-by-Question Answers

This document contains real SOC interview scenarios. Each scenario includes context, interviewer questions, and detailed answers written the way SOC interviewers expect candidates to explain their thinking.

Scenario 1: Password Spraying Attack

Scenario Context: SIEM alert shows 120 failed login attempts from a single external IP targeting 15 different user accounts within 8 minutes on O365 / Entra ID. No successful login observed.

Question 1: What type of attack is this and why?

This activity indicates a password spraying attack. Unlike brute-force attacks that target a single user with many passwords, password spraying uses one or a few common passwords across many accounts to avoid account lockouts. The pattern of one IP targeting many users within a short time window strongly supports this conclusion.

Question 2: Is this an alert or an incident?

At this stage, this should be treated as a security alert rather than a confirmed incident. While the activity is suspicious, there is no evidence of successful authentication or account compromise. SOC analysts should avoid escalating prematurely unless risk increases.

Question 3: Which logs would you review first?

I would review Entra ID sign-in logs to confirm failure reasons, conditional access logs to check policy enforcement, and identity protection logs to identify risky sign-ins or user risk flags.

Question 4: When would you escalate this?

Escalation is required if a login succeeds, if privileged or service accounts are targeted, if MFA is bypassed or disabled, or if the IP is associated with known malicious infrastructure.

Question 5: What immediate actions would you take?

Immediate actions include monitoring closely, applying conditional access controls, rate limiting, and blocking the source IP if attempts continue or expand.

Scenario 2: Successful Login After Multiple Failures

Scenario Context: User finance.admin shows 10 failed logins followed by a successful login from the same external IP at 03:12 AM local time. MFA is disabled.

Question 1: Is this an alert or an incident?

This is a confirmed security incident. Failed login attempts followed by a successful login from the same external source without MFA strongly indicate account compromise.

Question 2: What is your first validation step?

The first step is to validate whether the login is legitimate by checking user location, device history, prior login patterns, and whether the user confirms the activity.

Question 3: Which logs would you correlate next?

I would correlate authentication logs with mailbox access logs, file activity logs, audit logs, and any role or privilege change events to assess post-compromise behavior.

Question 4: What containment actions are required?

Containment includes revoking active sessions, forcing a password reset, enabling MFA, rotating credentials, and temporarily disabling the account if necessary.

Question 5: What must be documented?

Documentation should include timeline of events, indicators of compromise, actions taken, impacted resources, and next steps for remediation.

Scenario 3: AWS Privilege Escalation via CloudTrail

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

Question 1: Why is this dangerous?

This is dangerous because administrative access allows full control over AWS resources. Creating access keys establishes persistence even if initial access is revoked.

Question 2: What attacker technique does this represent?

This represents cloud privilege escalation and persistence, where attackers elevate permissions and create long-term access mechanisms.

Question 3: Which CloudTrail events are red flags?

AssumeRole, AttachRolePolicy, and CreateAccessKey are critical red flags indicating escalation and persistence.

Question 4: How do you confirm compromise?

I would review IAM trust policies, recent IAM changes, source IP reputation, and compare activity against expected usage patterns.

Question 5: What severity is this?

This should be classified as a high to critical severity incident due to the risk of full AWS account compromise.

Scenario 4: AWS S3 Data Exfiltration

Scenario Context: An IAM role performs ListBuckets and large-volume GetObject calls from a new ASN. CloudTrail Data Events are enabled.

Question 1: Why might this not appear in Management Events?

Management Events log control-plane activity, not data-plane actions. S3 object-level access is logged under CloudTrail Data Events, which are often disabled, causing visibility gaps.

Question 2: What makes this suspicious versus normal usage?

Bucket enumeration combined with bulk downloads from a new ASN deviates from baseline behavior and suggests unauthorized access or data theft.

Question 3: What logs would you correlate?

I would correlate IAM role assumption logs, VPC Flow Logs, GuardDuty findings, and historical S3 access patterns.

Question 4: What immediate controls would you recommend?

Immediate controls include revoking credentials, restricting IAM permissions, rotating keys, and applying temporary bucket restrictions.

Question 5: What mistake do many SOC teams make?

Many teams assume no alerts or management logs mean no breach, allowing silent data exfiltration to go unnoticed.

Scenario 5: False Positive VPN Login Failures

Scenario Context: 40 failed VPN logins from an internal IP during business hours. The user reports VPN instability.

Question 1: Is this malicious or benign?

This is likely a benign alert due to internal source, business hours, and user confirmation.

Question 2: What evidence supports your decision?

Internal IP, lack of automation patterns, business-hour timing, and supporting user report indicate non-malicious activity.

Question 3: Close or monitor?

I would close this as low severity with justification while monitoring for recurrence or pattern changes.

Question 4: How do you document this?

Documentation should include alert details, evidence reviewed, user confirmation, and reason for closure.

Question 5: What would make this suspicious next time?

External IPs, off-hours attempts, increased volume, or successful login after failures would require escalation.