SOC Interview Scenarios – Real-World Model Answers

Scenario 1: Password Spray Attack (Authentication Logs)

This scenario tests whether the candidate can correctly identify a password spraying attack and distinguish between an alert and an incident. Interviewers want to see contextual reasoning, not just attack names.

Expected Analyst Explanation

The pattern of multiple failed login attempts from a single IP address against multiple user accounts within a short time window strongly indicates a password spraying attack. Unlike brute force attacks that target one account with many passwords, password spraying attempts to avoid account lockouts by using a common password across many users.

Incident Classification

At this stage, this remains a security alert rather than a confirmed incident because no successful authentication has occurred. SOC analysts should avoid premature escalation unless there is evidence of compromise or high-risk targeting.

Logs to Investigate

An interviewer expects the analyst to immediately mention authentication logs such as Entra ID sign-in logs, Azure AD audit logs, and conditional access logs. These logs help validate user targeting, authentication methods, and MFA enforcement.

Escalation Conditions

Escalation to high severity would occur if a successful login is observed, a privileged account is targeted, legacy authentication is used, or the source IP is associated with known malicious infrastructure.

Scenario 2: Successful Login After Failures (Account Compromise)

This scenario evaluates whether the candidate understands the transition from suspicious activity to a confirmed security incident.

Incident Determination

Multiple failed login attempts followed by a successful login from the same external IP address, especially with MFA disabled, constitutes a confirmed account compromise. This is no longer an alert and requires immediate response.

Immediate Verification

The first action is to validate whether the login was legitimate by checking user context, geolocation, historical login patterns, and device fingerprints.

Log Correlation

SOC analysts should correlate authentication logs with mailbox activity, file access logs, privilege changes, and CloudTrail or SaaS audit logs to assess post-compromise actions.

Containment Actions

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

Scenario 3: AWS Privilege Escalation via CloudTrail

This scenario checks cloud security awareness and understanding of attacker behavior in AWS environments.

Why This Is Dangerous

Assuming an administrative role followed by policy attachment and access key creation strongly indicates privilege escalation and persistence techniques. Attackers use this to maintain long-term access even if the original credentials are revoked.

Red-Flag Events

Interviewers expect candidates to identify AssumeRole, AttachRolePolicy, and CreateAccessKey as critical CloudTrail events indicating escalation.

Validation Steps

The analyst should review role trust policies, recent IAM changes, source IP reputation, and whether the role usage aligns with expected service behavior.

Severity Assessment

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

Scenario 4: AWS Data Exfiltration via S3

This scenario tests whether candidates understand the difference between management and data plane logging and can detect silent data theft.

Why Management Logs Miss This

S3 object-level access such as GetObject is recorded under CloudTrail Data Events, not Management Events. Since Data Events are disabled by default, many organizations lack visibility into data exfiltration.

Indicators of Suspicious Activity

Enumeration of buckets combined with bulk object downloads from a new ASN deviates from normal application behavior and strongly suggests data exfiltration.

Correlation Sources

SOC analysts should correlate Data Events with IAM role assumptions, VPC Flow Logs, GuardDuty findings, and historical S3 access baselines.

Immediate Controls

Recommended actions include revoking credentials, restricting IAM role permissions, applying temporary bucket-level restrictions, and rotating access keys.

Common SOC Mistake

A frequent failure is assuming no alerts or no management events means no breach, allowing attackers to quietly steal data without detection.