security-event-investigation-policy.md

Security Event Investigation Policy

Purpose

Define steps for triaging and investigating security-relevant events detected in application and admin audit logs.

Scope

Applies to all security events that could affect confidentiality, integrity, or availability of Platform Data.

Investigation steps

1. Triage
   - Confirm the event source and severity.
   - Determine whether it is a false positive (e.g., scheduled maintenance, expected automation) or a candidate for investigation.
2. Containment
   - If the event indicates an active compromise or unauthorized access, isolate affected accounts or services as necessary.
3. Evidence collection
   - Preserve logs and timestamps (redact PII for sharing), capture system snapshots where relevant.
4. Root cause analysis
   - Reconstruct actions leading to the event using correlated logs and timestamps.
5. Remediation
   - Apply fixes (configuration changes, patching, rotating credentials). Document the actions taken.
6. Post-incident
   - Create a report, update detection rules, and update policies/processes to prevent recurrence.

False positives

- Document common false positive patterns and the steps to dismiss them.

Escalation rules

- Any confirmed unauthorized access or data exfiltration must be escalated to the security lead within 1 hour.

Evidence to provide to Facebook reviewers

- A written policy describing the steps above (highlight triage, evidence collection and escalation sections).
- A sample ticket/alert (redacted) showing an automated alert was created and assigned.