NEXAGEN FINANCIAL SERVICES

Security Operations Center

Daily Operations • Alert Triage • Escalation • Incident Response
Evidence Logging • Vulnerability Support • Shift Handoff

Document No.	NFS-SOC-ORM-2026-01
Classification	INTERNAL USE ONLY
Version	3.2
Effective Date	January 6, 2026
Review Cycle	Quarterly
Document Owner	SOC Operations Management
Prepared By	Bradley Documentation & Learning

Table of Contents

1. Document Control and Scope

1.1 Purpose

This Operations Reference Manual establishes standardized procedures for analysts and team leads assigned to the NexaGen Financial Services Security Operations Center (SOC). It provides the operating framework for daily shift activities, alert triage, incident escalation, evidence documentation, vulnerability management support, and shift continuity. Consistent application of these procedures ensures operational quality, audit readiness, and effective threat response across all coverage periods.

1.2 Scope and Audience

This manual applies to all personnel performing SOC analyst, SOC lead, and incident coordination functions. It does not supersede approved incident response plans, security policy frameworks, or enterprise risk management directives. Where conflicts exist, those governing documents take precedence.

Role	Primary Use	Update Authority
SOC Analyst	Daily operations, triage, case notes, escalation	No — submit change request
SOC Lead	Queue oversight, severity confirmation, handoff review	Minor corrections with manager approval
Documentation Owner	Version control, distribution, review coordination	Full authority within review cycle
Security Management	Policy alignment, audit review, exception approval	Full authority — immediate effect

1.3 Document History

Version	Date	Author	Summary of Changes
1.0	2024-01-15	SOC Management	Initial release
2.0	2024-07-01	Documentation Team	Added vulnerability support section; revised severity matrix
3.0	2025-01-06	Bradley Documentation & Learning	Full restructure; MTTR metrics added; shift handoff updated
3.2	2026-01-06	Bradley Documentation & Learning	Incident response integration section added; evidence quality standards revised

2. SOC Operations Environment Overview

2.1 Mission Statement

The NexaGen SOC monitors security events, validates suspected incidents, coordinates threat response, and supports vulnerability management across enterprise systems. The SOC serves as the central triage and detection function within the organization's defense-in-depth security model.

SOC analysts are not expected to independently resolve every security issue. Their core responsibility is to evaluate available evidence consistently, classify activity against defined criteria, maintain accurate case records, and escalate to the appropriate response function when defined thresholds are met.

2.2 Organizational Structure and Responsibilities

Team	Primary Responsibility	Escalation Contact
SOC Tier 1 Analyst	Alert monitoring, triage, initial case creation, routine escalation	SOC Lead
SOC Tier 2 Analyst	Complex event review, deeper investigation, tool validation	SOC Lead / Cyber Defense
SOC Lead	Queue oversight, severity confirmation, inter-team coordination	Security Operations Manager
Cyber Defense Response	Active investigation, containment, threat neutralization	Security Operations Manager
Vulnerability Mgmt.	Exposure validation, remediation tracking, patch coordination	CISO / Risk Lead
Security Intelligence	Threat context, intelligence enrichment, indicator sharing	Cyber Defense Lead
Security Operations Mgr.	Operational governance, escalation authority, SLA oversight	CISO

2.3 Core Tools and Systems

The SOC utilizes a layered toolset for monitoring, detection, investigation, and case management. Analysts should be familiar with the following tool categories and their operational roles. Specific product names and configurations are maintained in the approved System Inventory document (NFS-SOC-INV-2026).

- SIEM Platform — Primary event correlation, alert generation, and query workspace.
- Endpoint Detection & Response (EDR) — Endpoint telemetry, behavioral alerting, and containment support.
- Network Monitoring — Traffic analysis, anomaly detection, and connection logging.
- Vulnerability Scanner — Scheduled and on-demand scan results; asset exposure inventory.
- Case Management System — Incident lifecycle tracking, case notes, evidence logging, and SLA timers.
- Threat Intelligence Feed — Indicator enrichment, adversary context, and pattern correlation.

3. Daily Shift Workflow

3.1 Shift Rhythm Overview

Every SOC shift follows a defined operating rhythm. This rhythm maintains queue awareness, ensures continuity between analysts, keeps escalation paths active, and preserves a complete record of each coverage period. Deviations from this workflow should be documented in the shift log with a brief explanation.

Phase	Time Frame	Analyst Action	Expected Output
Shift Start Briefing	First 15 min	Review previous handoff notes, open critical/high cases, active escalations, and maintenance windows.	Shift awareness and initial priority list.
Queue Review	15–45 min	Sort queue by severity, timestamp, asset criticality, and repeated patterns. Identify top response targets.	Ranked queue and confirmed first response targets.
Active Monitoring	Throughout shift	Review incoming alerts, validate events, update case records, and confirm escalation status.	Ongoing case notes and queue cleared to SLA.
Mid-Shift Check	Halfway point	Confirm escalation status, review pending evidence items, update unresolved cases, recheck priority items.	Updated case notes; escalation status confirmed.
End-of-Shift Handoff	Final 20 min	Document all unresolved cases, owner assignments, monitoring targets, and required follow-up times.	Complete handoff record for incoming analyst.

3.2 Alert Volume Pattern

Understanding typical alert volume distribution helps analysts prioritize queue management and identify anomalies. The chart below reflects a representative 24-hour pattern. Peak hours (14:00–18:00) typically require the highest triage throughput.

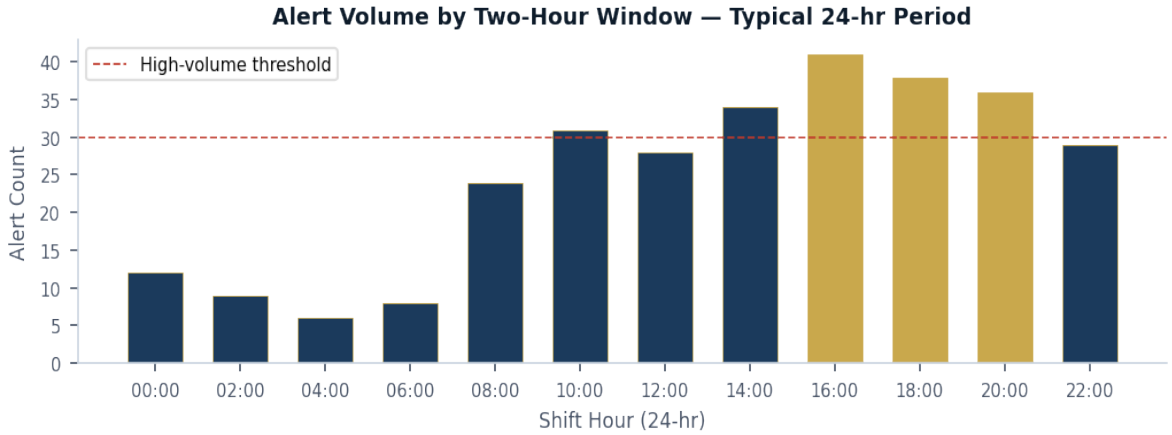


Figure 1 — Typical alert volume by two-hour window. Gold bars indicate above-threshold volume periods.

■ **RULE**	Do not close an event unless the final status and reviewed evidence are recorded. Escalate based on defined criteria, not personal judgment. Use consistent terminology for severity, asset impact, and action taken.

4. Alert Triage Workflow

4.1 Triage Process

Alert triage is the structured process of reviewing a security event, confirming its source, assessing available context, assigning an initial classification, and documenting the finding. Each step must produce a documented output before the analyst proceeds to the next step.

Step	Action	Documentation Requirement
1 — Receive	Open the event from the monitoring queue. Record the alert identifier and timestamp.	Case ID, timestamp, alert source, tool origin.
2 — Validate Source	Confirm the system, user, endpoint, or network source involved. Cross-reference asset inventory if needed.	Asset name/category, known ownership, asset criticality.
3 — Review Context	Check related events, recent activity on the same asset, known maintenance windows, and threat intelligence context.	Evidence reviewed, related signals noted, maintenance or known exceptions.
4 — Classify	Assign initial category: Informational, Suspicious, Actionable, or False Positive. Reference the Severity Matrix (Section 5).	Classification, rationale, confidence level.
5 — Decide Action	Based on classification and severity: Close, Monitor, Request SME Review, or Escalate.	Final action, assigned owner, next review time or SLA commitment.

4.2 Classification Definitions

- **Informational** — Activity aligns with known, expected behavior. No security concern identified. Document and close.
- **Suspicious** — Activity is unusual but not confirmed as malicious. Additional review, context, or monitoring is required before escalation.
- **Actionable** — Activity meets escalation criteria. Case must be escalated per Section 6 with evidence documentation.
- **False Positive** — Activity confirmed as benign. Document the reason for false positive determination to support tuning recommendations.

SECURITY	Do not include passwords, credentials, encryption keys, or restricted system configurations in case notes. When sensitive evidence must be preserved, follow approved secure evidence handling procedures.

5. Severity Matrix and Prioritization Rules

5.1 Severity Definitions

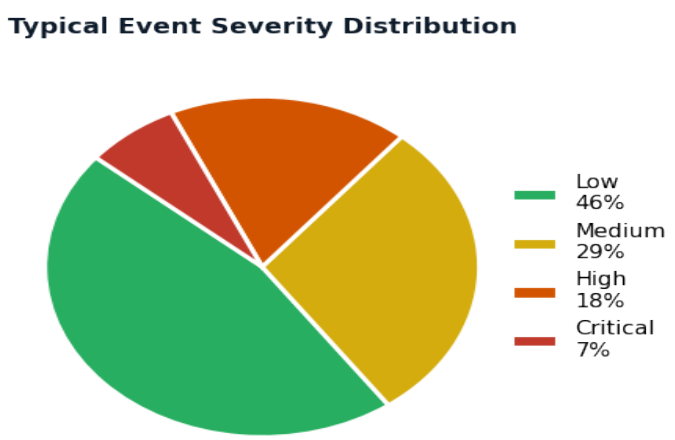
Consistent severity assignment across analysts and shifts is essential for predictable escalation timing and accurate reporting. All severity decisions must reference this matrix. Analysts who are uncertain about severity assignment should request SOC Lead review before escalating.

Severity	Indicators	Response Target	Escalation Path
CRITICAL	Confirmed compromise, active malware execution, privileged account misuse, sensitive data exposure, active data exfiltration, external attacker confirmed.	Immediate — notify SOC Lead within 5 minutes.	Cyber Defense / Incident Response engaged immediately.
HIGH	Suspicious behavior on critical assets, repeated failed controls, high-risk vulnerability exposure, credible threat pattern, privileged account anomaly.	Review and escalate within current shift.	SOC Lead review; possible Cyber Defense engagement.
MEDIUM	Unusual but contained activity, single host concern, policy exception, incomplete evidence, moderate-risk vulnerability without active exploitation.	Review and document during shift.	Monitor or request SME/lead validation. Escalate only if pattern develops.
LOW	Informational alert, expected maintenance activity, known benign pattern, no immediate business impact, single low-risk event.	Document and close or schedule for next review.	No escalation unless pattern or context changes.

5.2 Confidence / Impact Decision Matrix

When the severity is not immediately clear, analysts should use the confidence/impact matrix below. Confidence refers to certainty that the observed activity is malicious or anomalous. Impact refers to potential business or operational harm.

Confidence / Impact	Low Impact	Moderate Impact	High Impact
High Confidence	**Medium**	**High**	**Critical**
Medium Confidence	**Low**	**Medium**	**High**
Low Confidence	**Low**	**Low**	**Medium**



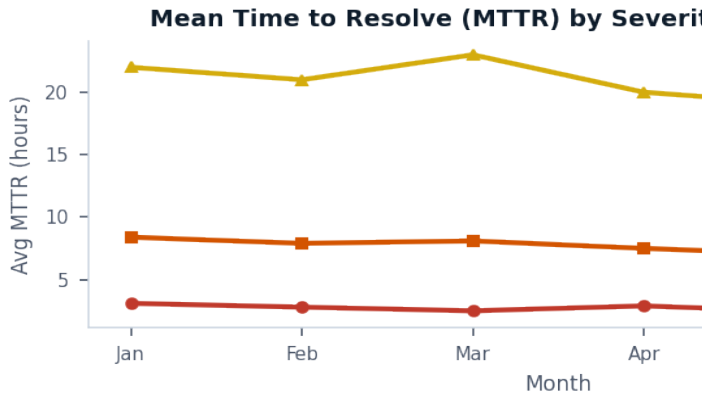


Figure 2 (left) — Typical event severity distribution. Figure 3 (right) — Mean Time to Resolve by severity, 6-month trend.

6. Escalation and Communication Protocol

Escalation is used when an event requires review, ownership, or action beyond the scope of the initial analyst. Escalation documentation must be complete enough for another team to understand the issue without repeating triage from the beginning.

Trigger Condition	Required Action	Required Message Content
Critical event indicators present	Notify SOC Lead immediately; open response coordination channel.	Case ID, severity, asset category, evidence summary, action requested.
High severity — confirmed event	Notify SOC Lead within same shift; document evidence.	Known facts, asset risk, related events, suggested next step.
High severity — unconfirmed / unclear	Request SOC Lead review; gather additional context first.	Observed activity, confidence level, uncertainty stated, suggested validation step.
Possible vulnerability exposure	Notify vulnerability management queue or owner.	Finding description, asset category, current risk level, remediation status.
Tool output unclear or contradictory	Request SME validation before making escalation decision.	Tool output summary, interpretation question, decision needed.
Repeated low/medium pattern emerging	Reassess severity; escalate if pattern indicates coordinated activity.	Pattern description, timeframe, assets involved, current case IDs.

6.2 Escalation Message Template

Escalation messages should follow this structure to ensure the receiving team has all information needed for immediate action:

ESCALATION NOTICE — NexaGen SOC

Case ID: [Case Identifier]
Severity: [Critical / High / Medium]
Time Opened: [Timestamp]
Analyst: [Your Name / Badge ID]

Summary: [Two to four sentences describing the observed activity, affected asset category, evidence reviewed, and why this meets escalation criteria. Be specific about what was observed, not just that "something looked suspicious."]

Evidence on File: [Brief list — e.g., endpoint alert logs, blocked outbound attempts, policy failure records, prior related case IDs]

Action Requested: [Confirm severity and advise — or — Initiate containment review — or — Assign to Cyber Defense for investigation]

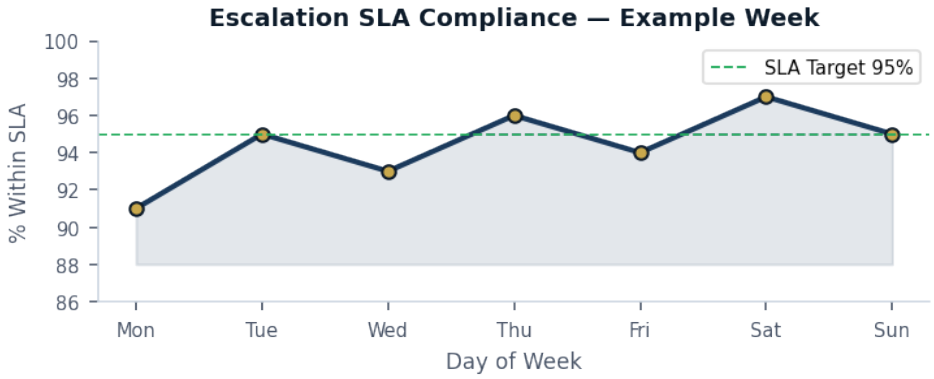


Figure 4 — Escalation SLA compliance, example week. Green dashed line = 95% target.

7. Evidence Collection and Case Documentation

A complete case record allows a lead analyst, response team, or auditor to understand what occurred, what was reviewed, and why a decision was made — without needing to ask the original analyst to reconstruct the sequence from memory. Case documentation quality is an operational standard, not optional.

Case Field	Description	Example Entry
Case ID	Unique identifier assigned by the case management system.	E-2026-1042
Alert Source	Monitoring tool, endpoint agent, email gateway, vulnerability scan, or analyst observation.	EDR platform — endpoint behavioral alert
Affected Asset	System, endpoint group, server, application tier, or user category. Do not record individual user names without authorization.	Finance workstation group — Tier 2 criticality
Evidence Reviewed	Events, timestamps, tool outputs, related logs, prior case references, and analyst notes.	Repeated blocked outbound attempts; endpoint policy status active; no approved maintenance window found.
Initial Assessment	Analyst interpretation of evidence. Must be based on observable indicators, not assumption.	Suspicious endpoint behavior consistent with potential data staging. Escalation criteria met.
Action Taken	Specific action: Closed, Monitoring, Escalated, Assigned for SME Review, Transferred.	Escalated to SOC Lead and Cyber Defense Response Team.
Final Status	Open, Closed — No Action, Closed — False Positive, Escalated — Pending, Transferred.	Escalated — Cyber Defense investigation in progress.

7.2 Documentation Quality Standard

The table below shows examples of insufficient versus acceptable case documentation. Analysts should review these examples during onboarding and whenever documentation quality reviews are conducted.

Insufficient Note	Acceptable Note — Why It Is Better
Alert looked suspicious. Escalated.	Reviewed endpoint alert E-2026-1042. Observed repeated blocked outbound connection attempts from Finance workstation group. Policy status active; no maintenance window applies. Activity consistent with potential data staging. Escalated to SOC Lead per high-severity criteria.
False positive. Closed.	Reviewed alert for asset group WS-MKTG-14. Confirmed asset was included in approved patch maintenance window (MW-2026-0203). Activity matches expected update behavior. Closed as false positive — no further action required.

Insufficient Note	Acceptable Note — Why It Is Better
Not sure. Assigned to lead.	Reviewed alert E-2026-1050. Evidence unclear — endpoint agent shows policy failure but asset is not in current inventory. Unable to confirm asset criticality. Assigned to SOC Lead for inventory verification before classification. Next review: within 2 hours.

8. Vulnerability Management Support

SOC analysts may support vulnerability management activities by providing alert context, validating asset exposure, confirming whether affected systems are monitored and controlled, and communicating urgency when active exploitation is suspected. The SOC does not own remediation decisions but frequently provides the earliest operational visibility into vulnerability-related risk.

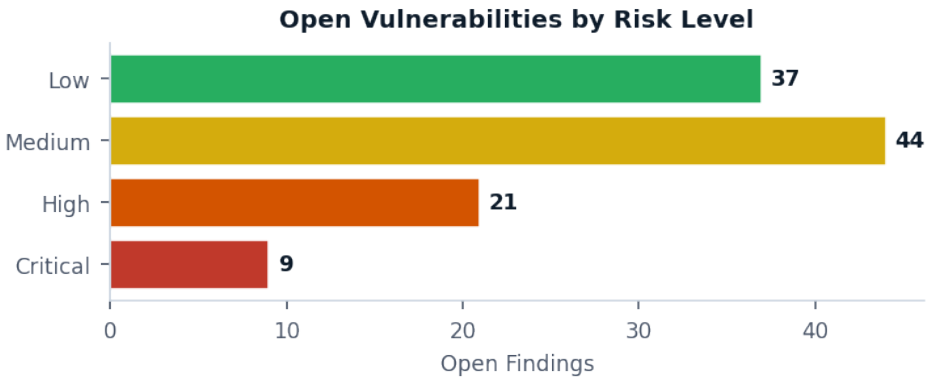


Figure 5 — Open vulnerabilities by risk level at time of last scan. Data is illustrative.

Risk Factor	SOC Analyst Question	Documentation Note
Asset Criticality	Is the affected system business critical, externally exposed, or privileged?	Record asset category and known business impact classification.
Exploitability	Is active exploitation known, in-the-wild, or indicated by intelligence context?	Reference threat context without including restricted intelligence details.
Control Status	Are endpoint and security controls active and reporting on this asset?	Note any control failures, policy gaps, or monitoring blind spots.
Remediation Status	Is there an identified owner, approved patch, workaround, or documented exception?	Document owner name or team, current status, and next review date.
Escalation Need	Does the risk profile require immediate security leadership notification?	Record escalation decision and notification path used.

GUIDANCE	Vulnerability support documentation exists to preserve a clear operational record of what was known, what was reviewed, who owns follow-up, and when the item should be re-checked. It is not intended to expose sensitive remediation configurations.

9. Incident Response Integration

9.1 SOC Role in Incident Response

The SOC serves as the initial detection and triage layer in the NexaGen incident response lifecycle. When an event meets incident-level criteria, the SOC lead initiates formal handoff to the Incident Response team and maintains a parallel monitoring record until the incident is contained and the SOC queue is confirmed clear of related activity.

IR Phase	SOC Responsibility	Handoff Point
Detection	Identify alert, validate source, and determine if incident-level criteria are met.	SOC Lead notifies Incident Coordinator when criteria met.
Initial Triage	Complete evidence review, classify severity, document case, and prepare escalation notice.	Formal escalation sent per Section 6 template.
Containment Support	Continue monitoring for related activity; confirm no additional impacted assets appear in queue.	Cyber Defense or IR team assumes containment ownership.
Eradication / Recovery	Monitor for recurrence; report any new related indicators to IR team.	IR team owns eradication. SOC provides ongoing detection support.
Post-Incident Review	Provide case timeline, evidence log, and triage notes to the IR post-mortem documentation process.	SOC Lead submits case package within 48 hours of incident closure.

9.2 Incident Criteria Quick Reference

Any of the following conditions, when confirmed, meets the threshold for formal incident declaration and IR team notification:

- Confirmed unauthorized access to systems containing sensitive or regulated data.
- Active malware execution confirmed on one or more endpoints, regardless of containment status.
- Privileged account compromise — confirmed or highly probable.
- Evidence of data exfiltration or staging activity.
- Critical system unavailability with suspected security cause.
- Third-party vendor or partner system activity that creates risk to NexaGen environment.
- Coordinated attack pattern across three or more assets within a single shift.

IMPORTANT	When in doubt about incident-level criteria, escalate to the SOC Lead immediately. It is always better to initiate a review that turns out to be unnecessary than to delay incident declaration.

10. Shift Handoff Procedures

Shift handoff is a formal transfer of queue ownership and situational awareness between analysts. A complete handoff prevents unresolved events from falling through coverage gaps and ensures the incoming analyst has enough context to act without re-triaging work already completed.

10.1 Handoff Document Requirements

Handoff Item	Required Detail	Complete ?
Open Critical / High Cases	Case ID, severity, current owner, latest action taken, next required step, and due time.	■
Active Escalations	Team notified, notification time, expected response timeline, follow-up responsibility.	■
Monitoring Items	Asset or pattern being watched, observation start time, trigger condition for action.	■
Tool / Queue Issues	Any tool outage, alert delay, integration failure, or unusual queue volume affecting coverage.	■
Vulnerability Follow-Up	Risk item in queue, assigned owner, current status, next review date.	■
Outstanding SME Requests	Pending validation items, who was contacted, response expected, case ID.	■
Completed Shift Summary	Total alerts reviewed, cases opened/closed, escalations initiated, anomalies noted.	■

RULE	A shift handoff is not complete until the incoming analyst verbally confirms receipt of all open critical and high cases. Both analysts are accountable until this confirmation occurs.

11. Quick Reference and Checklists

11.1 Shift Start Checklist

- Review previous shift handoff document before taking any queue action.
- Confirm all open Critical and High cases from previous shift are acknowledged.
- Review active escalation status — confirm response teams are engaged where expected.
- Check for tool outages, alert backlog, or queue anomalies before beginning triage.
- Confirm your contact roster is current — SOC Lead, Cyber Defense, Vulnerability Management.
- Note any approved maintenance windows that may affect alert context for this shift.

11.2 Triage Decision Quick Reference

If this happens...	Do this...
Confirmed Critical indicators appear in queue	Notify SOC Lead immediately — do not wait to complete triage. Document Case ID, asset, evidence summary, and action requested.
Evidence is ambiguous or tool output is unclear	Document the uncertainty clearly. Request SME or SOC Lead validation. Do not close or escalate until validation is received.
Repeated Low/Medium alerts form a pattern	Reassess severity using the confidence/impact matrix. Note related case IDs and escalate if pattern meets High criteria.
Asset is not in inventory or criticality unknown	Do not assume low criticality. Treat as moderate until confirmed. Flag for asset inventory review.
Approved maintenance window covers the activity	Confirm window documentation, record the reference, and close as false positive with maintenance window noted.
Tool or security control appears inactive/reporting gap	Document the gap. Notify SOC Lead. Do not skip related alerts due to tool uncertainty — treat them conservatively.
Shift ends with unresolved Critical or High cases	Complete full handoff entry. Verbally confirm with incoming analyst. Do not mark shift complete until confirmed.

11.3 Contact Escalation Path

Situation	First Contact	Second Contact	Emergency Contact
Critical Event / Active Incident	SOC Lead (on-shift)	Security Operations Manager	CISO On-Call
High Severity — Confirmation Needed	SOC Lead	Senior Analyst / Tier 2	—
Cyber Defense Engagement Required	SOC Lead (initiates handoff)	Cyber Defense Response Lead	Security Operations Manager
Vulnerability — Active Exploitation Risk	Vulnerability Management Queue	Vulnerability Management Lead	Security Operations Manager

Situation	First Contact	Second Contact	Emergency Contact
Tool Outage / Alert Gap	SOC Lead	IT Operations On-Call	Security Operations Manager

Portfolio Demonstration Note

This document is a non-proprietary technical writing sample prepared by Bradley Documentation & Learning. It demonstrates the ability to organize complex security operations content into structured, usable reference material for real-world SOC teams. It does not represent a live operational procedure, does not contain client-specific configurations, and should not be used as a production security policy without SME validation and organizational review.

Prepared by: Mark R. Bradley | Bradley Documentation & Learning | bradleyconsultingoh.io