PROACTIVE RISK

Adversaries Plan. We Preempt.

ManageIT™ — Managed Security Operations Center

Critical Security Alert Response Runbook

Incident Commander–led response to confirmed CRITICAL alerts — technology-provider agnostic

Document ID	PR-SOP-SOC-001
Version	1.0
Status	Approved — In Force
Classification	Confidential — Proactive Risk & Authorized Client Recipients
Document Owner	Director, Security Operations
Effective Date	June 1st 2026
Next Review	12 months from Effective Date (or upon material change)
Applies To	All ManageIT™ SOC monitored environments

CONFIDENTIALITY NOTICE
This runbook contains the proprietary operating procedures of Proactive Risk, Inc., a Service-Disabled Veteran-Owned Small Business (SDVOSB). It is provided to clients for transparency into Proactive Risk's managed SOC operations and may not be redistributed outside the recipient organization without written consent.

Document Control

Revision History

Version	Date	Summary of Change	Author
1.0	June 1st 2026	Initial release of vendor-agnostic critical alert response runbook.	Tom Brennan

Review & Approval

Role	Name	Signature	Date
Prepared By — SecOps Lead			
Reviewed By — vCISO / MeasureRISK™			
Approved By — Managing Director			

Distribution

Proactive Risk Security Operations Center personnel; Proactive Risk leadership; and designated security and executive points of contact at each monitored client. This document supersedes any prior critical-alert handling procedure of the same document ID.

Table of Contents

Document Control....2
Table of Contents....3
1. Purpose....4
2. Scope & Applicability....4
3. Intended Audience....4
4. Guiding Principles....5
5. Severity Classification....5
6. Roles & Responsibilities....6
7. Pre-Authorized Containment Authority....8
8. Critical Alert Response Lifecycle....10
  Phase 0 — Preparation (Standing Posture)....10
  Phase 1 — Detection & Triage....10
  Phase 2 — Declaration & Mobilization....10
  Phase 3 — Containment (Pre-Authorized Active Response)....10
  Phase 4 — Eradication....10
  Phase 5 — Recovery....11
  Phase 6 — Notification & Communications....11
  Phase 7 — Post-Incident Activity....11
9. Communication & Escalation Plan....12
10. Timeline & Service-Level Summary....12
11. Evidence Handling & Chain of Custody....13
12. Regulatory & Breach-Notification Awareness....13
13. Continuous Improvement & Metrics....13
Appendix A — Framework Cross-Reference....15
Appendix B — Critical Alert Decision Flow....15
Appendix C — Contact & Escalation Roster (Template)....15
Appendix D — Definitions & Acronyms....16

1. Purpose

This runbook defines the standard business operation Proactive Risk follows when its Security Operations Center (SOC) identifies and confirms a CRITICAL security alert within a client environment. It describes, in plain and repeatable terms, who does what, in what order, and how quickly — from the moment a critical alert surfaces through containment, recovery, client notification, and formal closure.

The runbook serves two audiences at once. Internally, it is the authoritative operating procedure for SOC analysts, the Incident Commander, and supporting roles. Externally, it gives every monitored client clear, written visibility into exactly how Proactive Risk will act on their behalf when a serious threat is detected — before that threat ever materializes.

> **DESIGN PRINCIPLE — TECHNOLOGY-PROVIDER AGNOSTIC**
> The detection technology is an input, not the process. Whether the originating signal comes from Blackpoint Cyber, CrowdStrike, Microsoft Defender / Sentinel, SecurityScorecard, a firewall, an identity provider, or any other tool, the response described here is identical. The platform changes; Proactive Risk's discipline does not.

2. Scope & Applicability

This runbook applies to any alert that Proactive Risk classifies as CRITICAL severity (see Section 5) across all environments enrolled in the ManageIT™ managed SOC service. It governs the operational response and client-facing communication for those events.

In Scope

- Confirmed or high-confidence CRITICAL alerts from any monitoring or detection source.
- The full response lifecycle: triage, declaration, containment, eradication, recovery, communication, and closure.
- Pre-authorized active-response containment actions executed by the SOC on the client's behalf.
- Coordination with client points of contact and, where applicable, third parties (insurers, counsel, law enforcement, upstream providers).

Out of Scope

- Routine, Low, and Medium-severity alerts handled under standard SOC monitoring procedures.
- Legal determinations of whether a regulatory "breach" has occurred — Proactive Risk advises; the client and its counsel decide (see Section 12).

- Full digital forensics and incident response (DFIR) engagements, which may be scoped as a separate statement of work when an incident's scale exceeds standard managed response.

3. Intended Audience

Audience	How They Use This Runbook
SOC Analysts (Tier 1–3)	Execute triage, validation, and pre-authorized containment under Incident Commander direction.
Incident Commander (IC)	Owns the incident end-to-end: declares severity, directs response, controls communication, and authorizes closure.
Proactive Risk Leadership	Provides executive oversight, client-relationship continuity, and escalation authority for high-impact events.
Client Security & Executive POCs	Understand what Proactive Risk will do on their behalf, what is pre-authorized, and what decisions remain with the client.

4. Guiding Principles

Every critical-alert response is governed by five principles that hold regardless of the threat or the tooling involved:

- **Preempt the adversary.** Speed of containment is prioritized over completeness of analysis. A contained threat can be studied; an uncontained one spreads.
- **Single point of command.** One Incident Commander owns each incident. Authority and accountability are never diffuse.
- **Act first, within mandate.** On confirmed CRITICAL events, the SOC executes pre-authorized containment immediately and notifies the client promptly thereafter (see Sections 7 and 9).
- **Communicate with discipline.** Clients receive timely, factual, jargon-controlled updates through agreed channels — no speculation, no silence.
- **Protect the evidence.** Containment is performed in a manner that preserves forensic and legal integrity wherever operationally feasible (see Section 11).

5. Severity Classification

Proactive Risk classifies all alerts on a four-tier severity scale. This runbook is triggered only by the CRITICAL tier. The table below defines the tiers; the criteria that follow define what qualifies an alert as CRITICAL.

Severity	Definition	Standard SOC Action
CRITICAL	Confirmed or high-confidence active threat with material impact potential to confidentiality, integrity, or availability.	This runbook — immediate IC-led response and pre-authorized containment.
High	Credible threat or significant exposure not yet confirmed as active impact.	Expedited investigation; escalation to CRITICAL if confirmed.
Medium	Suspicious activity or policy violation warranting analyst review.	Standard investigation and remediation guidance.
Low / Informational	Routine noise, benign anomalies, or tuning candidates.	Logged, correlated, and tuned; no client action required.

What Qualifies as CRITICAL

An alert is classified CRITICAL when, upon validation, it meets one or more of the following conditions:

- Active ransomware behavior or unauthorized mass encryption of data.
- Confirmed or strongly indicated exfiltration of sensitive or regulated data.
- Evidence of a hands-on-keyboard adversary (interactive intrusion / lateral movement).
- Compromise of privileged or administrative credentials (e.g., domain admin, global admin, or equivalent).
- Compromise of a designated business-critical system or service.
- Active command-and-control (C2) communication paired with internal spread.
- Destructive activity — deletion, tampering, or sabotage of systems, backups, or logs.

CALIBRATED, NOT MECHANICAL

Severity is a judgment made by the analyst and confirmed by the Incident Commander, informed — but never dictated — by a single tool's severity label. A vendor "critical" that proves benign is downgraded; a vendor "medium" that proves to be an active intrusion is escalated. The IC owns the final classification.

6. Roles & Responsibilities

A critical incident mobilizes a defined response team. On smaller events one person may hold more than one role; the Incident Commander role is never combined away and is always explicitly held by a named individual.

Role	Core Responsibilities
Incident Commander (IC)	Single owner of the incident. Confirms CRITICAL classification, directs all response actions, authorizes containment beyond the pre-approved baseline, controls the communication cadence, and declares closure.
Tier 1 SOC Analyst	First responder. Performs initial triage and validation, captures the timeline, and executes pre-authorized containment under IC direction.
Tier 2 / Tier 3 Analyst	Deep investigation, scoping, root-cause analysis, threat hunting, and eradication planning.
Communications Lead	Drafts and delivers client notifications and status updates on the IC's instruction; maintains the single source of truth for what the client has been told.
Scribe / Documentarian	Maintains the contemporaneous incident log — every observation, decision, and action with timestamps. May be the same person as Tier 1 on small events.
Client Incident Liaison	The named Proactive Risk relationship contact who coordinates with the client's designated POC and bridges operational and business concerns.
Executive Sponsor (PR)	Proactive Risk leadership engaged for high-impact events; owns escalation, resourcing, and client-executive relationship.

RACI Summary

R = Responsible · A = Accountable · C = Consulted · I = Informed

Activity	IC	SOC	Comms	Liaison	Client POC
Confirm CRITICAL classification	A/R	C	I	I	I
Execute pre-authorized containment	A	R	I	I	I
Authorize non-baseline action	A/R	C	I	C	C
Notify the client (≤1 hour)	A	I	R	C	I
Eradication & recovery	A	R	I	I	C
Declare incident closed	A/R	C	I	C	I

7. Pre-Authorized Containment Authority

This section is the operational and contractual heart of the runbook. By enrolling in the ManageIT™ managed SOC service, the client grants Proactive Risk standing authorization to take defensive containment action on confirmed CRITICAL events without waiting for per-incident approval. Minutes matter; this mandate lets Proactive Risk preempt damage rather than request permission while it spreads.

THE MANDATE

Upon confirmation of a CRITICAL alert, the SOC is pre-authorized to execute the baseline containment actions below immediately, and to notify the client within one (1) hour of confirmation. *Action precedes notification by design.*

Pre-Authorized Baseline Actions

The following actions may be taken immediately, choosing the least-disruptive option that effectively contains the threat:

- Isolate or network-quarantine a compromised endpoint or server.
- Disable, suspend, or force re-authentication of a compromised user or service account.
- Revoke active sessions, tokens, or API keys associated with the compromise.
- Terminate malicious processes and quarantine malicious files.
- Block malicious IP addresses, domains, URLs, and file hashes at available control points.
- Sever identified command-and-control (C2) communication channels.

Guardrails on Pre-Authorized Action

- Choose the least-disruptive effective action; prefer reversible measures over destructive ones.
- Scope containment to the threat — contain the affected hosts, accounts, and paths, not the whole environment by default.
- Preserve evidence while containing (see Section 11); isolate rather than wipe wherever feasible.
- Log every action in real time, with timestamp, actor, and rationale.

Actions That Require Client Approval (Even on CRITICAL)

The following are excluded from the standing mandate and require explicit client approval before execution, because their business impact may exceed the threat impact:

- Taking offline any system on the client’s designated business-critical / exclusion list.

- Isolation of an entire site, network segment, or production service affecting normal operations.
- Mass disablement of accounts beyond those directly implicated.
- Any action against operational technology (OT) / industrial control systems (ICS).
- Destructive or irreversible actions — reimaging, wiping, or rebuilding — outside an agreed recovery plan.

CLIENT EXCEPTION REGISTER

Each client may maintain an Exception Register defining business-critical assets, blackout windows, and any narrowing of the standing mandate. Where a client elects an approval-required posture for specific systems, the SOC will contain to the boundary of its authority and immediately escalate for the decision on the remainder. The Register is reviewed at onboarding and at each service review.

8. Critical Alert Response Lifecycle

The response follows the NIST SP 800-61 incident-handling lifecycle, adapted for managed-SOC delivery. Phases are sequential in intent but overlap in practice; the Incident Commander manages the flow.

Phase 0 — Preparation (Standing Posture)

Readiness is maintained continuously so that response is execution, not improvisation:

1. Current client profiles, asset inventories, exception registers, and contact rosters on file.
2. Detection sources integrated and health-monitored; baseline tuning maintained.
3. Pre-authorized containment tested against each environment's tooling.
4. On-call rotation, IC roster, and escalation tree published and current.

Phase 1 — Detection & Triage

A candidate alert arrives from any monitoring source and enters triage:

1. Receive the alert and record time of receipt as the official start of the clock.
2. Validate the signal — confirm it is a true positive and not benign or duplicate activity.
3. Enrich and scope — identify affected hosts, accounts, data, and the apparent blast radius.
4. Assess against the CRITICAL criteria in Section 5 and recommend a severity to the IC.

Phase 2 — Declaration & Mobilization

1. The Incident Commander confirms CRITICAL classification and formally declares the incident.
2. A response channel ("war room") is opened and the Scribe begins the contemporaneous log.
3. Roles are assigned by name; the one-hour client-notification timer is acknowledged.
4. Containment authority (Section 7) is confirmed against the client's Exception Register.

Phase 3 — Containment (Pre-Authorized Active Response)

1. Execute the pre-authorized baseline actions to halt spread — immediately, least-disruptive first.

2. Where the threat extends into excluded systems, contain to the boundary of authority and escalate for the decision on the remainder.
3. Verify containment held — confirm isolation, revoked access, and severed C2.
4. Record every action with timestamp and rationale as it is taken.

Phase 4 — Eradication

1. Determine root cause and full scope — initial access vector, persistence, and footholds.
2. Remove malicious artifacts, accounts, persistence mechanisms, and unauthorized changes.
3. Hunt for related activity to confirm the adversary has no remaining presence.

Phase 5 — Recovery

1. Restore affected systems and accounts to known-good state, in coordination with the client.
2. Apply hardening to close the exploited path; reset credentials as warranted.
3. Return systems to production with heightened monitoring for a defined watch period.
4. Confirm business operations restored before standing down enhanced posture.

Phase 6 — Notification & Communications

> **ONE-HOUR COMMITMENT**
> **The designated client contacts are notified within one (1) hour of CRITICAL confirmation** — via the primary channel, with a backup channel if unacknowledged. Notification follows containment; the client is informed of what was detected, what was contained, and what comes next.

1. Issue the initial notification within the one-hour window (detection, impact, actions taken, next steps).
2. Provide status updates at an agreed cadence until the incident stabilizes.
3. Coordinate any client-directed engagement of insurer, counsel, or law enforcement.
4. Deliver a written incident summary at closure (see Phase 7).

Phase 7 — Post-Incident Activity

1. Incident Commander declares the incident closed once eradication and recovery are verified.
2. Produce the final incident report: timeline, root cause, impact, actions, and recommendations.

3. Hold a lessons-learned review; feed improvements into detections, tuning, and this runbook.
4. Update metrics (Section 13) and the client's risk picture under MeasureRISK™ advisory.

9. Communication & Escalation Plan

Communication is deliberate and role-driven. The Communications Lead delivers messages on the IC's authority; the IC owns what is said and when.

Notification Channels

- Primary: the channel agreed with the client at onboarding (e.g., phone call to the designated POC followed by written confirmation).
- Backup: a secondary contact and channel used if the primary is unacknowledged within the agreed interval.
- Out-of-band: a pre-agreed alternative used if the client's normal systems are themselves affected (critical for ransomware and email-compromise scenarios).

Internal Escalation Matrix

Trigger	Escalate To	Purpose
CRITICAL confirmed	Incident Commander	Declaration and command of the response.
Action beyond standing mandate needed	Client POC + PR Liaison	Obtain decision on excluded / high-impact action.
High client / business impact	PR Executive Sponsor	Executive oversight and relationship management.
Suspected regulated-data exposure	vCISO / MeasureRISK™	Advisory on notification obligations (Section 12).
Scale exceeds managed response	DFIR engagement (separate SOW)	Surge forensic and response capacity.

10. Timeline & Service-Level Summary

Targets below define the standard operating cadence for a CRITICAL event. Specific contractual SLAs, where they differ, are governed by the client's service agreement and prevail over these defaults.

Milestone	Target	Owner
Triage begins	Immediately on alert receipt	SOC Analyst
CRITICAL confirmation	Promptly upon validation	Incident Commander
Pre-authorized containment initiated	Immediately on confirmation	SOC Analyst / IC
Client notification	Within 1 hour of confirmation	Communications Lead

Milestone	Target	Owner
Status updates	At agreed cadence until stable	Communications Lead
Final incident report	Following verified closure	Incident Commander

11. Evidence Handling & Chain of Custody

Containment and investigation are performed to preserve forensic and legal value wherever operationally feasible, recognizing that some incidents may later involve insurers, regulators, or litigation.

- Prefer isolation over destruction — quarantine endpoints rather than wipe them when containment allows.
- Capture volatile and relevant data before it is lost; document what was collected, by whom, and when.
- Maintain a clear chain of custody for any artifacts retained as evidence.
- Restrict access to incident evidence to authorized responders on a need-to-know basis.
- Retain incident records per the client agreement and applicable obligations.

12. Regulatory & Breach-Notification Awareness

> **PROACTIVE RISK ADVISES — THE CLIENT DECIDES**
> Proactive Risk is not the client's legal counsel and does not make the legal determination of whether a reportable "breach" has occurred. Proactive Risk surfaces the facts, flags potential obligations, and supports the client's decision-making. Notification decisions rest with the client and its counsel.

Where an incident may implicate regulated or contractual obligations, the IC engages the vCISO / MeasureRISK™ advisory function to help the client understand potential exposure, including:

- Health information obligations (e.g., HIPAA) for healthcare-adjacent clients.
- State data-breach notification statutes applicable to affected individuals' residency.
- Sector and contractual requirements (e.g., CMMC / DFARS for defense-supply-chain clients, cyber-insurance reporting clauses).
- Timelines that may begin at the point of discovery — reinforcing the value of prompt, documented response.

13. Continuous Improvement & Metrics

Each critical incident is measured to drive improvement of detections, procedures, and this runbook. Standard measures include:

Metric	What It Measures
MTTD — Mean Time to Detect	From threat activity to alert generation.
MTTA — Mean Time to Acknowledge	From alert generation to analyst triage.
MTTC — Mean Time to Contain	From CRITICAL confirmation to verified containment.
MTTR — Mean Time to Recover	From containment to verified restoration of operations.
Notification Adherence	Percentage of CRITICAL events with client notified within one hour.

Appendix A — Framework Cross-Reference

This runbook is built on the NIST SP 800-61 incident-handling lifecycle and aligns to the control families clients most often must demonstrate. Mappings are indicative, supporting audit and assessment readiness.

Runbook Element	NIST SP 800-61	CMMC 2.0 (IR)	CIS v8.1 / CISA CPG
Standing posture (Phase 0)	Preparation	IR.L2-3.6.1 (IR capability)	CIS 17.1–17.3 / CPG 2.S
Triage & classification (Ph. 1–2)	Detection & Analysis	IR.L2-3.6.1	CIS 17.4 / CPG 1.B
Containment (Phase 3)	Containment	IR.L2-3.6.2 (handling)	CIS 17.6–17.7 / CPG 2.M
Eradication & recovery (Ph. 4–5)	Eradication & Recovery	IR.L2-3.6.2	CIS 17.8 / CPG 5.A
Notification (Phase 6)	Coordination	IR.L2-3.6.2	CPG 4.B (reporting)
Lessons learned (Phase 7)	Post-Incident Activity	IR.L2-3.6.3 (test/review)	CIS 17.9 / CPG 2.T

Note: Control identifiers are provided for orientation. Formal compliance scoping is delivered through CyberAdvisor™ and MeasureRISK™ engagements.

Appendix B — Critical Alert Decision Flow

A condensed decision path for the responding analyst and Incident Commander:

1. Alert received from any source → record start time.
2. Valid true positive? If no → close / tune. If yes → continue.
3. Meets CRITICAL criteria (Section 5)? If no → route to standard severity handling. If yes → continue.
4. IC confirms CRITICAL and declares the incident.
5. Threat confined to systems within the standing mandate? If yes → execute pre-authorized containment now. If it reaches excluded systems → contain to the boundary and escalate for the decision.
6. Notify client within one hour of confirmation.
7. Eradicate → recover → verify → close → report.

Appendix C — Contact & Escalation Roster (Template)

Completed per client at onboarding and kept current. Stored with the client profile and referenced by the IC during an incident.

Role / Function	Name	Contact (Primary / Backup)
Client — Primary Security POC	_____	_____
Client — Executive POC	_____	_____
Client — After-Hours / Out-of-Band	_____	_____
Proactive Risk — Incident Commander (on-call)	_____	_____
Proactive Risk — Client Liaison	_____	_____
Proactive Risk — Executive Sponsor	_____	_____
Third Party — Cyber Insurer	_____	_____
Third Party — Legal Counsel	_____	_____

Appendix D — Definitions & Acronyms

Term	Meaning
C2	Command and Control — adversary infrastructure used to direct compromised systems.
Containment	Action that stops a threat from spreading or causing further impact.
DFIR	Digital Forensics and Incident Response — a deeper engagement scoped separately when needed.
Eradication	Removal of the adversary’s presence, artifacts, and persistence from the environment.
Exception Register	Per-client record of business-critical assets and any narrowing of the standing mandate.
Incident Commander (IC)	The single accountable owner of an incident’s response.
OT / ICS	Operational Technology / Industrial Control Systems.
Pre-Authorized	Containment the SOC may perform immediately on a CRITICAL

Term	Meaning
Action	event under the standing mandate.
SOC	Security Operations Center — Proactive Risk's ManageIT™ monitoring and response function.

Adversaries Plan. We Preempt.

Semper Fi.

Proactive Risk, Inc. · Service-Disabled Veteran-Owned Small Business (SDVOSB)