HORIZONSHIELD

Securing Your Digital Future, Today.

BLUE TEAM SERIES · BOOK 03 OF 16

Incident Response Playbook 2026

Detect, Contain, Recover — NIST 800-61 Framework

A complete incident response framework covering preparation through post-incident review. Includes playbooks for ransomware, BEC, data breach, and insider threats, with checklists, timelines, and communication templates.

PHASES	PLAYBOOKS	CHECKLISTS	STANDARD
6	8	40+	NIST 800-61

Contents

INCIDENT RESPONSE PLAYBOOK 2026

CHAPTER 01

IR Framework & Team Structure

A well-defined IR structure enables fast, coordinated response when incidents occur. Build this before you need it.

NIST 800-61 | CSIRT | ROLES

NIST 800-61 Four-Phase Framework

1

Preparation

BEFORE THE INCIDENT

Establish IR capability: document playbooks, provision tools (SIEM, EDR, IR toolkit), train the team, establish out-of-band communication, identify legal/PR contacts, obtain cyber insurance, conduct tabletop exercises annually.

2

Detection & Analysis

EVENT → INCIDENT CLASSIFICATION

Monitor for indicators of compromise, triage alerts, confirm incident reality, scope the impact, classify severity (P1–P4), open incident record, activate relevant playbook, notify stakeholders per severity.

3

Containment, Eradication & Recovery

HOURS TO DAYS

Stop the spread, remove attacker access and persistence, restore systems and services in priority order, verify environment is clean before reconnecting, monitor for recurrence.

4

Post-Incident Activity

DAYS TO WEEKS POST-INCIDENT

Root cause analysis, timeline reconstruction, lessons learned session, control improvements, update playbooks, communicate with stakeholders, regulatory filings, forensic report if required.

CSIRT Team Roles

Role	Responsibility	On-Call
Incident Commander	Coordinate response, make containment decisions, stakeholder communications, timeline authority	YES
SOC Analyst (Tier 2/3)	Alert triage, log analysis, IOC identification, initial containment	YES
Forensic Analyst	Evidence preservation, disk/memory forensics, timeline reconstruction	On-call
Threat Intel Analyst	IOC correlation, actor attribution, TTP analysis, hunting	Business hours
Legal / Compliance	Regulatory notification, evidence chain of custody, privilege assertion	On-call
Communications Lead	Internal/external comms, press statements if required	On-call
IT Operations	System isolation, backup restoration, technical remediation tasks	YES

OUT-OF-BAND COMMUNICATION IS CRITICAL

During a ransomware attack, email, Slack, and Teams may be compromised or unavailable. Establish an out-of-band communication channel BEFORE an incident: Signal group, WhatsApp, or phone tree. Print emergency contact cards and post them physically in the office. Test the channel quarterly.

CHAPTER 07

Ransomware Response Playbook

Ransomware requires the fastest possible containment. Every minute of delay expands attacker access and increases recovery cost.

CONTAINMENT | T+0 ACTIONS | RECOVERY | RANSOM DECISION

Ransomware Response — Hour by Hour

T+0: FIRST 15 MINUTES — CRITICAL

ISOLATE affected systems IMMEDIATELY. Do NOT power off (preserve memory for forensics). Do NOT pay without legal and executive approval. Alert IR lead, legal, and executive team simultaneously. Open out-of-band communication channel.

1

T+0–15min: Isolate

CONTAINMENT — STOP THE SPREAD

Pull ethernet cable from affected systems (faster than software). Disable WiFi. Contact network team to segment at switch level. DO NOT shut down — memory forensics are invaluable. Identify scope: how many systems are affected?

2

T+15–30min: Credential Reset

PREVENT FURTHER PROPAGATION

Revoke Active Directory credentials for any accounts used on compromised systems. Reset all admin accounts. Disable compromised service accounts. Block attacker-controlled accounts identified in logs.

3

T+30–60min: Backup Verification

CRITICAL — DETERMINES RECOVERY PATH

CHECK BACKUP INTEGRITY IMMEDIATELY. Are backups online and accessible? Are they encrypted by the ransomware? Is your last clean backup point identifiable? This determines whether you can recover without paying.

4

T+1–2h: Scope & Identify

INTELLIGENCE GATHERING

Identify patient zero (first encrypted system). Determine initial access vector. Check logs: VPN, email gateway, firewall for the hours before encryption. Identify the ransomware family via ID Ransomware.

5

T+2–4h: Decision Point

RECOVER VS. NEGOTIATE

With legal and executive: If clean backups exist — begin restore, do NOT pay. If no viable backups — engage cyber insurance IR firm and legal for negotiation guidance. Never pay without legal and insurance approval.

6

T+4h+: Recovery

RESTORE OPERATIONS

Restore critical systems from verified clean backups. Build from scratch where needed. Patch all vulnerabilities before reconnecting. Monitor rebuilt systems intensively. The attacker likely still has access via a backdoor — find it before reconnecting.

MODERN RANSOMWARE DESTROYS BACKUPS FIRST

Sophisticated ransomware operators spend weeks inside networks before encrypting. They specifically identify and delete or encrypt backup systems before detonating. In 2025, 73% of ransomware incidents affected backup systems. Test your backup offline isolation assumption BEFORE an incident.

Investigation Question	Data Source	Why It Matters
What ransomware family?	File extension, ransom note text, ID Ransomware (id-ransomware.malwarehunterteam.com)	May have free decryptor available — check No More Ransom project
How did attacker get in?	Firewall logs, email gateway, VPN auth logs, RDP logs	Patch initial access vector before reconnecting or reinfection is guaranteed
How long were they in?	SIEM event timeline, AV logs, EDR telemetry, Windows event logs	Determines safe backup restore point — all backups since attacker entry are suspect

Investigation Question	Data Source	Why It Matters
What was exfiltrated?	DLP logs, DNS logs, proxy logs, firewall egress logs	Double-extortion assessment — attacker may publish data if ransom not paid
Are any backdoors remaining?	EDR scheduled task audit, new user accounts, startup items, netstat	Reconnecting with active backdoor restarts the attack immediately

CHAPTER 08

Business Email Compromise Playbook

BEC generates more financial losses than ransomware — and leaves virtually no technical indicators.

DETECTION | WIRE RECALL | INVESTIGATION | PREVENTION

Business Email Compromise Response

1

Detect & Confirm

T+0

Confirm the BEC — is this a fraudulent email, fraudulent wire transfer, or account compromise? Identify affected accounts. Determine scope: how many employees received or responded to the BEC attempt?

2

CALL YOUR BANK IMMEDIATELY

T+0 — IF WIRE TRANSFER INVOLVED

Wire recalls succeed in ~70% of cases if called within 24 hours. They drop to under 10% after 24 hours and are virtually impossible after 72 hours. Call the fraud hotline on the BACK OF YOUR BUSINESS CARD — not a number from an email.

3

Account Investigation

T+0-2H

If email account compromised: Check inbox rules for unauthorized forwarding rules (attackers set these to redirect replies). Check email forwarding settings. Review recent sent items for fraudulent emails sent to your clients. Review login history for unusual locations or times.

4

Contain & Remediate

T+2-8H

Reset compromised account credentials. Remove unauthorized inbox rules and forwarding settings. Block the attacker's IP addresses. Notify clients who may have received fraudulent

emails from your account. Review all financial transactions in the past 90 days for other fraud.

5

Report to Authorities

T+0–72H (PARALLEL)

File FBI Internet Crime Complaint Center (IC3) report at ic3.gov for all wire fraud. Contact local FBI field office for losses over $50,000. Law enforcement international wire recovery (Operation Wire Cutter) has recovered millions — but requires rapid reporting.

6

Post-BEC Hardening

POST-INCIDENT

Implement MFA on all email immediately. Add external sender banners. Configure DMARC p=reject to prevent your domain being spoofed. Establish verbal verification policy for all wire transfers. Brief ALL finance staff — not just the victim.

WIRE TRANSFER RECALL PROCESS

(1) Call your bank fraud hotline immediately — time is everything, (2) Provide: sending account number, destination account/routing, amount, date/time, transaction ID, (3) Request SWIFT gpi recall if international, (4) Get a STAR/CHIPS recall case number, (5) File FBI IC3 report with the case number, (6) Keep calling daily — persistence increases recovery probability.

HS

HORIZONSHIELD

Securing Your Digital Future, Today.

Incident Response Playbook 2026

Part of the HorizonShield Security Series — 16 comprehensive professional cybersecurity manuals covering every domain of modern enterprise security.