RESTRICTED - INTERNAL USE ONLY

Cybersecurity Incident Response Playbook

Version 3.2 - November 2025

Table of Contents:

1. Introduction and Scope

This playbook provides standardized procedures for responding to cybersecurity incidents within our organization. It establishes clear roles, responsibilities, and escalation paths to ensure rapid and effective incident response.

1.1 Incident Definition

A cybersecurity incident is defined as any event that compromises or threatens to compromise the confidentiality, integrity, or availability of information systems or data.

1.2 Scope of Coverage

- Malware infections and advanced persistent threats
- Unauthorized access attempts and successful breaches
- Data theft or exfiltration incidents
- Denial of service attacks
- Insider threat activities
- Third-party vendor security incidents

2. Incident Classification Matrix

2.1 Severity Levels

CRITICAL (P1) - Immediate Response Required:

- Active data exfiltration in progress
- Complete system compromise of critical infrastructure
- Ransomware encryption of production systems
- Nation-state actor attribution with ongoing activity

HIGH (P2) - Response Within 2 Hours:

- Confirmed malware on production systems
- Successful lateral movement detected
- Privilege escalation attempts
- Suspicious administrative account activity

MEDIUM (P3) - Response Within 8 Hours:

- Failed authentication attempts from external sources
- Suspicious network traffic patterns
- Policy violations by authorized users
- Vulnerability exploitation attempts

3. Incident Response Team Structure

3.1 Core Team Members

- Incident Commander - Overall response coordination
- Security Analyst - Technical investigation and analysis
- Systems Administrator - Infrastructure containment and recovery
- Communications Lead - Internal and external notifications
- Legal Counsel - Regulatory compliance and legal implications
- Executive Sponsor - Senior leadership representation

3.2 Contact Information

- Emergency Hotline: +1-555-SECURITY (24/7)
- Incident Commander: incident-commander@company.com
- Security Operations Center: soc@company.com
- Executive Escalation: ciso@company.com

4. Phase 1: Detection and Analysis

4.1 Initial Triage Checklist

- Verify the incident report and gather initial details
- Classify the incident severity using the matrix above
- Activate appropriate response team members
- Establish incident tracking and documentation
- Begin preliminary technical analysis
- Preserve evidence and maintain chain of custody

4.2 Evidence Collection Procedures

All evidence collection must follow forensically sound practices:

- Create bit-for-bit disk images using validated tools
- Capture volatile memory contents before system shutdown
- Document all actions taken with timestamps
- Maintain proper chain of custody documentation
- Store evidence in secure, access-controlled environment

5. Phase 2: Containment and Eradication

5.1 Short-term Containment

- Isolate affected systems from the network
- Disable compromised user accounts
- Block malicious IP addresses and domains
- Update firewall rules and IPS signatures
- Implement temporary access controls

5.2 Long-term Containment and Eradication

- Remove malware and malicious artifacts
- Patch vulnerabilities that enabled the incident
- Rebuild compromised systems from known-good sources
- Update security controls and monitoring
- Implement additional protective measures

6. Phase 3: Recovery and Post-Incident

6.1 System Recovery Procedures

- Restore systems and data from clean backups
- Validate system integrity and functionality
- Implement enhanced monitoring for affected systems
- Gradually restore normal operations
- Document all recovery actions taken

6.2 Post-Incident Activities

- Conduct lessons learned session within 48 hours
- Update incident response procedures based on findings
- Complete regulatory notification requirements
- Provide final incident report to stakeholders
- Schedule follow-up security assessments

7. Communication Protocols

7.1 Internal Notifications

Critical incidents (P1) require immediate notification to:

- Chief Information Security Officer (CISO)
- Chief Technology Officer (CTO)
- Chief Executive Officer (CEO)
- Legal and Compliance teams
- Human Resources (if insider threat suspected)
- Public Relations (if media exposure likely)

7.2 External Notifications

- Law enforcement (if criminal activity suspected)
- Regulatory bodies (within required timeframes)
- Cyber threat intelligence sharing organizations
- Affected customers and business partners
- Cyber insurance providers
- External legal counsel (if required)

8. Appendices and References

Appendix A: Emergency Contact List

[Contact information would be listed here with current phone numbers, email addresses, and escalation procedures]

Appendix B: Technical Tools and Resources

- SIEM Platform: Splunk Enterprise Security
- Endpoint Detection: CrowdStrike Falcon
- Network Analysis: Wireshark, tcpdump
- Forensic Imaging: EnCase, FTK Imager
- Malware Analysis: IDA Pro, Ghidra
- Threat Intelligence: MISP, OpenCTI

Appendix C: Regulatory Requirements

This playbook addresses requirements from:

- NIST Cybersecurity Framework
- ISO 27035 Incident Management
- GDPR Article 33 Breach Notification
- SOX Section 404 Internal Controls
- PCI DSS Requirement 12.10
- State and federal breach notification laws

Document Classification: RESTRICTED
Last Updated: November 11, 2025
Next Review Date: February 11, 2026