SOC INCIDENT RESPONSE PLAYBOOK SUITE (PART 1)

Prepared by: Grace Awuma

Date: October 4, 2025

Version: 1.0

Classification: Internal Use

QUICK REFERENCE GUIDE

INCIDENT SEVERITY MATRIX

Incident Type	Severity	Response Time	Auto-Escalate?
Ransomware	Critical	0-15 min	YES - Always
Phishing	High	30-60 min	If creds used
Unauthorized Access	High	15-30 min	If admin account
Data Exfiltration	Critical	15-30 min	If >1GB or PII
Malware/C2	High	15-30 min	If persistence

EMERGENCY CONTACTS

├─ SOC Manager: [Contact Information]

├─ CISO: [Contact Information]

├─ IT Operations On-Call: [Contact Information]

└─ Legal/Compliance: [Contact Information]

SEVERITY DEFINITIONS

- Critical: Immediate business impact, data at risk, spreading threat
- High: Potential business impact, contained but active threat
- Medium: Limited scope, no immediate spread risk
- Low: Suspicious activity requiring monitoring

GENERAL RESPONSE WORKFLOW

1. DETECT → Alert received from monitoring tools

2. TRIAGE → Verify true positive, assess scope

3. INVESTIGATE → Collect evidence, determine root cause

4. CONTAIN → Stop spread, isolate affected systems

5. ERADICATE → Remove threat, close vulnerabilities

6. RECOVER → Restore systems, verify clean state

7. DOCUMENT → Record actions, update tickets

TOOLS REFERENCE

- EDR: CrowdStrike Falcon

- SIEM: [Splunk/ELK/Other]

- Threat Intel: MITRE ATT&CK, VirusTotal

- Ticketing: [ServiceNow/Jira/Other]

PLAYBOOK 1: RANSOMWARE DETECTION & RESPONSE

PLAYBOOK METADATA

├─ Severity Level: CRITICAL

├─ Estimated Response Time: Immediate (0-15 minutes)

├─ Escalation Required: YES - Always escalate to CISO/Management

└─ Last Updated: October 2025

INCIDENT OVERVIEW

Ransomware is malicious software that encrypts files and systems, demanding payment for decryption keys. Modern ransomware variants often exfiltrate data before encryption (double extortion) and can spread laterally across networks. Immediate containment is critical to prevent organizational-wide impact.

DETECTION INDICATORS

Alert Sources:

- CrowdStrike Falcon EDR - Behavioral IOA: Mass file encryption detected
- CrowdStrike Falcon - Process blocking: Suspicious executable activity
- SIEM Alert - Abnormal file modification rate (>500 files/minute)
- SIEM Alert - Shadow copy deletion detected
- User Report - Files inaccessible with unusual extensions
- Backup System Alert - Backup deletion attempts detected

Key Indicators of Compromise (IOCs):

- Ransom note files appearing on systems (README.txt, HOW_TO_DECRYPT.html, RESTORE_FILES.txt)

- Files with unusual extensions (.locked, .encrypted, .crypted, .REvil, .BlackCat)

- Network connections to Tor nodes or known C2 infrastructure

- Suspicious scheduled tasks or registry Run keys for persistence

- Commands for shadow copy deletion:

  - vssadmin delete shadows /all /quiet

  - wmic shadowcopy delete

  - bcdedit /set {default} recoveryenabled no

- PowerShell commands: Get-WmiObject Win32_ShadowCopy | Remove-WmiObject

- High CPU usage from encryption processes

- Unusual process names or executables in temp directories

- Disabled Windows Defender or security tools

INITIAL TRIAGE (Do this FIRST - 5-10 minutes)

□ Step 1: Verify alert is TRUE POSITIVE

  - Check multiple indicators (not just one alert)

  - Confirm files are encrypted (check file headers)

□ Step 2: Identify "Patient Zero" - the first infected system

  - Review CrowdStrike timeline for earliest detection

  - Check which system has oldest ransom note timestamp

□ Step 3: Determine if encryption is ACTIVE or COMPLETE

  - Active: Files currently being encrypted (CPU spike, processes running)

  - Complete: Encryption finished, ransom note displayed

□ Step 4: Notify Incident Commander/SOC Manager IMMEDIATELY

- This is a CRITICAL incident requiring immediate escalation

- Document notification time in incident ticket

INVESTIGATION STEPS

Phase 1: Scope Assessment (10-15 minutes)

1. Review CrowdStrike Falcon timeline for initial infection vector

→ Check for: Phishing email attachments, malicious downloads, RDP brute force

→ Document: Initial access timestamp and infection method

→ Look for: Suspicious parent processes (e.g., outlook.exe spawning PowerShell)

2. Identify ALL affected systems using CrowdStrike host search

→ Query: Search for hosts with same IOCs in last 24-48 hours

→ Create inventory: Hostname, IP address, Username, Encryption status (active/complete)

→ Priority check: Domain controllers, file servers, database servers

3. Check for lateral movement indicators

→ Review: SMB connections, PS Exec usage, WMI activity in CrowdStrike

→ Identify: Compromised credentials being used across systems

→ Check: Active Directory logs for unusual authentication patterns

Phase 2: Evidence Collection (15-20 minutes)

1. Collect CrowdStrike forensic data from Patient Zero

→ Generate: Real-Time Response (RTR) triage package

→ Include: Process tree, network connections, file modification timeline

→ Preserve: Memory dump if possible (before isolation)

2. Preserve ransom notes and encrypted file samples

→ Screenshot: Ransom note exactly as displayed

→ Save: 3-5 encrypted file samples (small files <1MB)

→ Document: Original file names and new encrypted extensions

→ DO NOT: Pay ransom or contact attackers yet

3. Extract network indicators from CrowdStrike detections

→ Collect: C2 domains/IPs, file download URLs

→ Check: Virus Total for additional context on domains/IPs

→ Action: Add indicators to threaten intelligence platform

4. Review authentication logs for compromised accounts

→ Windows Event Logs: Event ID 4624 (successful logon), 4625 (failed logon)

→ Look for: Off-hours logins, unusual source IPs, privilege escalation

→ Identify: All accounts used during attack chain

Phase 3: Impact Analysis (10 minutes)

1. Determine business-critical systems affected

→ Priority systems: ERP, financial systems, customer databases, email servers

→ Status classification: Encrypted / At-risk / Clean

→ Estimate: Downtime impact on business operations

2. Assess data exfiltration risk (double extortion check)

→ Review: Unusual egress traffic BEFORE encryption started

→ Check: Large file transfers to external IPs/cloud storage

→ Tools: NetFlow data, firewall logs, CrowdStrike network timeline

→ Risk: Threat of data leak if ransom not paid

3. Evaluate backup integrity

→ Verify: Recent backups exist and are accessible

→ Test: Backup files are NOT encrypted

→ Check: Backup retention (how far back can we restore?)

→ Confirm: Backups stored offline or air-gapped

ESCALATION CRITERIA

Escalate to Senior SOC/Manager/CISO IMMEDIATELY if:

- ANY ransomware activity detected (this is automatic escalation)
- More than 5 systems affected
- Domain Admin or privileged service accounts compromised
- Critical business systems encrypted (ERP, financial systems, production environments)
- Data exfiltration detected before encryption
- Backup systems compromised or encrypted
- Ransom demand exceeds $X threshold [set by organization]
- Media/regulatory notification may be required

CONTAINMENT & REMEDIATION

Immediate Actions (0-30 minutes):

1. ISOLATE affected systems using CrowdStrike network containment

→ Use: Falcon console "Network Containment" feature

→ DO NOT power off systems (preserves volatile memory for forensics)

→ Block: All inbound/outbound network traffic except CrowdStrike management

2. Disable compromised user accounts in Active Directory

→ Identify accounts from authentication log analysis

→ Force password reset for ALL accounts used during incident

→ Revoke active sessions and tokens

3. Block malicious indicators at security perimeter

→ Firewall: Block C2 domains/IPs

→ DNS: Sinkhole malicious domains

→ Proxy: Add URLs to block list

→ Email Gateway: Block sender domains if phishing was initial vector

4. Prevent lateral spread via network segmentation

→ Disable: SMB, RDP, WMI protocols to/from affected segments

→ Isolate: Critical systems not yet affected

→ Monitor: Network traffic for additional propagation attempts

Short-term Actions (1-24 hours):

1. Identify ransomware variant

→ Use: ID Ransomware tool (https://id-ransomware.malwarehunterteam.com)

→ Upload: Ransom note + encrypted file sample

→ Check: If free decrypt or available (No More Ransom Project)

→ Document: Ransomware family name (e.g., LockBit, BlackCat, REvil)

2. Coordinate with backup/IT teams for restoration strategy

→ Prioritize: Business-critical systems first

→ Verify: Clean restore points exist (pre-infection)

→ Test: Small-scale restore before full recovery

→ Plan: Phased restoration approach

3. Conduct organization-wide EDR hunt

→ Use: CrowdStrike Falcon Insight for threat hunting

→ Hunt for: Additional infections, persistence mechanisms

→ Deploy: Real-Time Response to clean additional compromised systems

→ Scan: All endpoints with updated detection signatures

4. Engage external stakeholders

→ Law Enforcement: FBI IC3 (https://www.ic3.gov)

→ Legal: Assess regulatory notification requirements

→ Insurance: Notify cyber insurance carrier

→ Forensics: Consider third-party IR firm if needed

Long-term Actions (1-7 days):

1. Rebuild affected systems from known-good images

→ DO NOT restore from potentially compromised system backups

→ Use: Clean gold images or manufacturer restore

2. Implement additional security controls

→ Deploy: MFA on ALL remote access (VPN, RDP, email, cloud apps)

→ Enable: Application whitelisting on critical servers

→ Configure: CrowdStrike prevention policies to maximum

3. Conduct organization-wide credential reset

→ Reset: All privileged account passwords

→ Rotate: Service account credentials

→ Review: And remove unnecessary admin rights

4. Review and harden backup procedures

→ Implement: 3-2-1 backup rule (3 copies, 2 media types, 1 offsite)

→ Test: Backup restoration procedures weekly

→ Airgap: Critical backup copies

5. User awareness and training

→ Conduct: Organization-wide security briefing

→ Update: Security awareness training with this incident as case study

→ Simulate: Phishing exercises to test preparedness

MITRE ATT&CK MAPPING

Tactics & Techniques Observed:

├─ Initial Access (TA0001)

│ └─ T1566.001 - Phishing: Spear phishing Attachment

│ └─ T1133 - External Remote Services (RDP compromise)

│

├─ Execution (TA0002)

│ └─ T1059.001 - PowerShell

│ └─ T1204.002 - User Execution: Malicious File

│

├─ Persistence (TA0003)

│ └─ T1053.005 - Scheduled Task/Job

│ └─ T1547.001 - Registry Run Keys

│

├─ Defense Evasion (TA0005)

│ └─ T1562.001 - Impair Defenses: Disable or Modify Tools

│ └─ T1070.001 - Clear Windows Event Logs

│

├─ Lateral Movement (TA0008)

│ └─ T1021.001 - Remote Desktop Protocol

│ └─ T1021.002 - SMB/Windows Admin Shares

│

└─ Impact (TA0040)

└─ T1486 - Data Encrypted for Impact

└─ T1490 - Inhibit System Recovery (Shadow copy deletion)

└─ T1489 - Service Stop (Disabling security services)

DOCUMENTATION REQUIREMENTS

Document the following in incident ticket:

- Timeline of Events: First detection timestamp → Full containment timestamp
- Affected Asset Inventory: All systems with encryption status
- User Impact: Number of users affected, business processes disrupted
- Actions Taken: Every containment/remediation step with timestamps
- Evidence Collected: Screenshots, log exports, forensic artifacts
- Business Impact Assessment: Estimated downtime, data loss, financial impact
- Communication Log: Who was notified, when, and via what method
- Root Cause: How ransomware initially entered the environment

POST-INCIDENT ACTIVITIES

□ Conduct hot wash meeting within 24 hours of containment

□ Update CrowdStrike detection rules based on observed TTPs

□ Improve backup verification and testing procedures

□ Deploy additional monitoring for early ransomware indicators

□ Executive briefing with lessons learned and recommendations

□ Update security awareness training with real-world example

□ Conduct ransomware tabletop exercise within 30 days

□ Review and update this playbook based on lessons learned