Playbook for Cat & Box Scenario

Prepared by: Anastasiya Gruneva

Date: January 10th, 2025

Table of Contents

Executive Summary

This Incident Response Playbook outlines the strategy for managing ransomware incidents at Box Manufacturing. The playbook integrates NIST and MITRE frameworks to provide a structured approach to minimizing disruption, ensuring effective resolution, and protecting systems and data integrity. Key elements include:

Incident Type: Ransomware attacks targeting critical systems and data.

Main Roles:

- **SOC**: Monitors, identifies, and provides forensic analysis.
- **Cat (External MSSP)**: Oversees the overall security response and coordinates remediation efforts.
- **Internal Team**: Includes Misha/Minka (Operational Managers), Dusty (Database Specialist), Lucky (IT Support Specialist), and Ned (Network Administrator).

Essential Communication Strategies:

- Immediate notification to relevant stakeholders, including internal and external teams.
- Clear escalation paths for unresolved or critical incidents.
- Tailored communication templates for technical teams and non-technical stakeholders to ensure clarity and transparency.

This document ensures preparedness, swift containment, and effective communication to protect Box Manufacturing's systems and data integrity.

Incident Response Playbook: Ransomware

Objective

To outline a detailed workflow and assign roles and responsibilities for responding to a ransomware incident impacting Box Manufacturing, ensuring minimal disruption to operations and swift remediation.
The playbook aligns with the five core functions of the NIST CSF: Identify, Protect, Detect, Respond, and Recover. These functions will structure the incident workflow for clarity and industry alignment. (NIST CSF, retrieved 2025-01-10)

Workflow Steps
The steps come from NIST Computer Security Incident Handling Guide (NIST, retrieved 2025-01-10).

Step 1: Preparation

Establish readiness to prevent and respond to ransomware incidents.

Actions:

- Conduct risk assessments based on NIST Cybersecurity Framework (CSF).
- Ensure all systems are up-to-date with the latest patches.
- Conduct regular employee training on recognizing phishing and ransomware tactics.
- Maintain and test backups for all critical systems.
- Implement endpoint detection and response (EDR) tools.
- Develop and update incident response playbook annually.

Responsibilities:

SOC: Monitor and report on preparedness levels.
Cat: Oversee training sessions and ensure all playbooks are current.

Step 2: Identification

Detect and confirm ransomware incidents using industry best practices.

Trigger Items:

- Unusual file encryption activities or unauthorized file modifications (MITRE: T1486, retrieved 2025-01-10).
- Detection of known ransomware signatures or indicators of compromise (MITRE: T1078, retrieved 2025-01-10).
- Unexpected network traffic patterns suggesting data exfiltration (MITRE: T1020, retrieved 2025-01-10).
- User reports of inaccessible files or the presence of ransom notes.
- Security tool alerts (e.g., antivirus, EDR) indicating ransomware-related activities.
- SOC notifications of detected anomalies.

Actions:

- Gather forensic evidence such as memory dumps and system logs.
- Analyze anomalies using security tools and MITRE ATT&CK mappings.

Responsibilities:

SOC: Monitor and identify potential ransomware indicators.
Cat: Review detailed reports and confirm the incident.

Step 3: Containment

Prevent the spread of ransomware across systems.

Immediate Actions:

- Disconnect affected systems from the network.
- Isolate infected endpoints to prevent spread.

Responsibilities:

Ned (Network Admin): Perform network isolation.
Lucky (IT Support): Disable user access on affected systems.

Notification

Ensure clear and effective communication during the incident.

Internal Notifications:

- Inform Misha or Minka based on the time of the day.
- Escalate to Percy if unresolved after 48 hours or deemed critical.

External Notifications:

- **SOC:** Provide a summary to Cat for detailed analysis.
- Inform Dusty if databases are affected.

Responsibilities:

Cat: Ensure accurate and timely updates to stakeholders.

Step 4: Eradication

Remove ransomware and associated artifacts.

Actions:

- Analyze the ransomware strain using forensic tools.
- Remove malicious files and scripts (MITRE: T1053, retrieved 2025-01-10).
- Patch vulnerabilities exploited during the attack.

Responsibilities:

SOC: Provide forensic details and remediation steps.
Cat: Approve actions and coordinate remediation efforts.

Step 5: Recovery

Restore normal operations and verify system integrity.

Actions:

- Restore data from clean backups.
- Test restored systems in a sandbox before reintegration.

Responsibilities:

Dusty: Restore databases.
Lucky: Validate endpoint recovery.
Ned: Monitor network for recurring signs of infection.

Step 6: Post-Incident Review

Learn from the incident to improve future response capabilities.

Actions:

- Conduct a full analysis of the incident.
- Update workflows and playbooks based on lessons learned.
- Review the incident for business impact insights.

Responsibilities:

Cat: Lead review and document findings.
SOC: Provide comprehensive incident report.
Percy: Review final report for business impact insights.

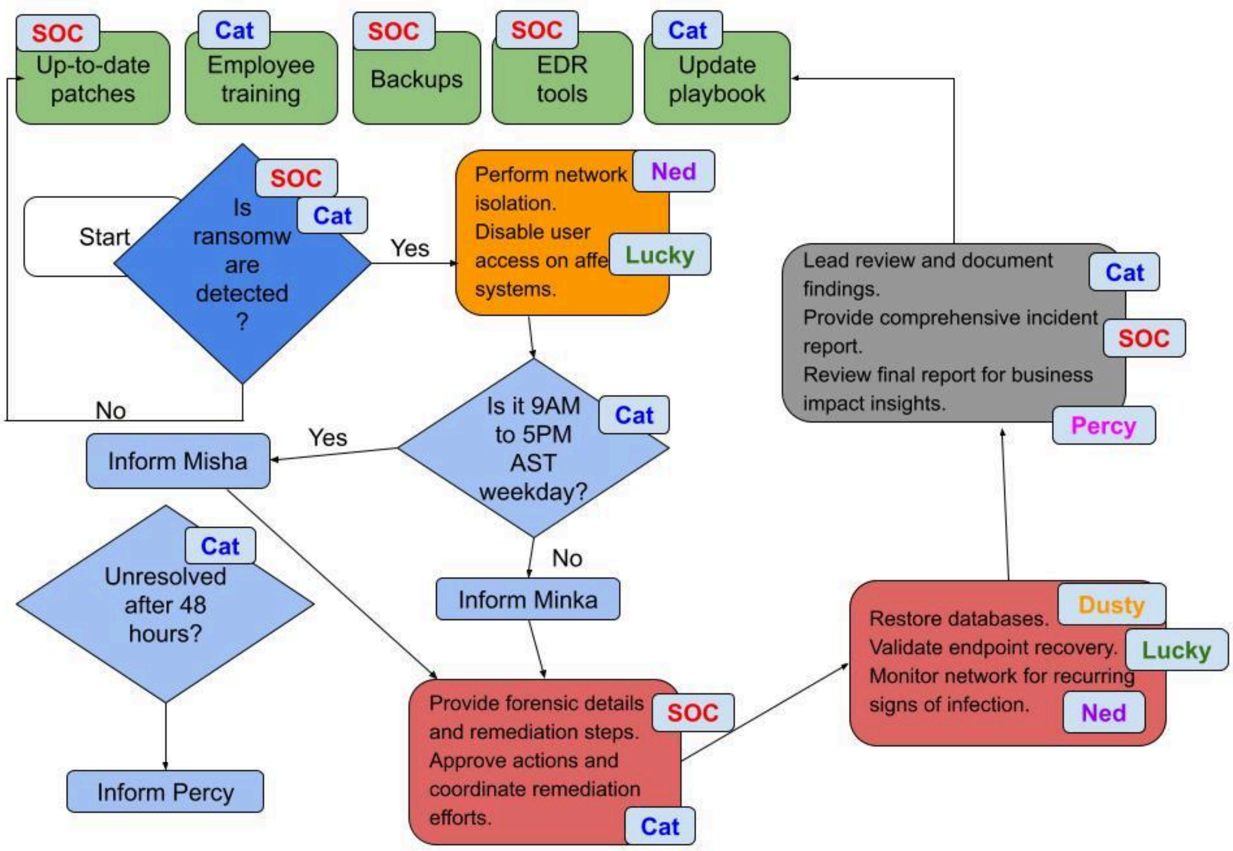
SOC
Up-to-date patches
Cat
Employee training
SOC
Backups
SOC
EDR tools
Cat
Update playbook
Start
SOC
Cat
Is ransomw are detected ?
Yes
No
Perform network isolation. Disable user access on affe systems.
Ned
Lucky
Lead review and document findings. Provide comprehensive incident report. Review final report for business impact insights.
Cat
SOC
Percy
Is it 9AM to 5PM AST weekday?
Cat
Yes
Inform Misha
No
Inform Minka
Cat
Unresolved after 48 hours?
Inform Percy
Provide forensic details and remediation steps. Approve actions and coordinate remediation efforts.
SOC
Cat
Restore databases. Validate endpoint recovery. Monitor network for recurring signs of infection.
Dusty
Lucky
Ned

Figure 1. Incident Response Workflow: Ransomware

Step 1: Preparation
Step 2: Identification
Step 3: Containment
Notification
Step 4: Eradication
Step 5: Recovery
Step 6: Post-Incident Review

Communication Templates

1. Technical Letter (Third-Party Provider)

Subject: Ransomware Incident: Immediate Technical Assistance Required

Dear [SOC Team],

We have identified a ransomware incident impacting Box Manufacturing's network. The following technical specifics outline the situation:

- Date/Time of Detection: [Insert Details]
- Affected Systems: [Insert Affected Systems]
- Indicators of Compromise (IoCs): [List Detected IoCs]

Immediate Actions Taken:

- Isolated infected systems.
- Disabled user accounts on compromised endpoints.

We require your expertise to:

1. Analyze the ransomware strain and provide eradication strategies.
2. Confirm the integrity of our backup data.
3. Assist with patching vulnerabilities and system recovery.

Please prioritize this matter and coordinate directly with Cat (cat@soc.cat, 905-4616 or 902-4321).

Best Regards,
[Your Name]
[Your Position]
Box Manufacturing

2. Non-Technical Letter (Client)

Subject: Important Update: Ransomware Incident Under Control

Dear Team,

We want to inform you about a security incident involving ransomware that has affected certain parts of our network. Our security teams and third-party specialists are actively working to contain and resolve the issue.

Here’s what you need to know:

Impact: Some systems were temporarily inaccessible. There is no evidence of data theft at this time.

Actions Taken:

- Infected systems were isolated to prevent further spread.
- Backups are being restored where necessary.
- Enhanced security measures are being implemented to prevent recurrence.

Next Steps: Operations are expected to return to normal within [Insert Timeframe].

If you have any questions or concerns, please don’t hesitate to reach out to Misha F. at mesha@box.cat or 902-9836 during business hours, or Minka F. at minka@box.cat or 562-7658 after hours.

Thank you for your understanding as we ensure the security of our systems and data.

Best Regards,
[Your Name]
[Your Position]
Box Manufacturing

References

Cybersecurity Incident & Vulnerability Response Playbooks. Cybersecurity and Infrastructure Security Agency. (2021-11) https://www.cisa.gov/sites/default/files/2024-08/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf

Bykowski, K. (2022-08-01) How to Build an Incident Response Playbook. https://swimlane.com/blog/incident-response-playbook/

Top 15 Cyber Incident Response Use Cases (2023-03-28) https://www.logsign.com/blog/top-15-incident-response-use-cases/

Cyber Security Playbooks (retrieved 2025-01-10) https://soc.cyber.wa.gov.au/guidelines/playbooks/

MITRE ATT&CK (retrieved 2025-01-10) https://attack.mitre.org/

NIST CyberSecurity Framework (retrieved 2025-01-10) https://www.nist.gov/cyberframework

NIST Computer Security Incident Handling Guide (retrieved 2025-01-10) https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf