Cat and Box Playbook Project Report

Created by: Harsh Patel

Date: January 10th, 2025

Table of Contents

Executive Summary

Incident Type

Incident Response Workflow

Technical Letter

Non-Technical Letter

Trigger List

Rationale

Flowchart

References

**Executive Summary**

This incident response playbook provides a structured approach for handling a cybersecurity breach at Box Manufacturing, with a focus on ransomware attacks. Developed according to the NIST Incident Response Lifecycle and CISA guidelines, this document outlines the workflow, communication protocols, and key responsibilities to ensure a swift and coordinated response to incidents. Given the limited in-house IT capabilities at Box, Cat (an MSSP consultant) oversees all cybersecurity activities, while a third-party SOC handles real-time monitoring and detection. This playbook ensures clear communication and prompt escalation, aligning with the client’s specific needs.

**Incident Type: Ransomware Attack**

Ransomware attacks pose a critical risk to Box’s operations by potentially halting production and compromising sensitive business data. This playbook focuses on early detection, containment, and recovery to minimize downtime and impact.

**Incident Response Workflow**

1. ***Preparation***  
   **SOC Monitoring**: Continuous network monitoring for unusual activity.

**Access Control**: Periodic review and restriction of access to sensitive systems.

1. ***Identification*Trigger Event**: Anomalies detected by the SOC, such as suspicious file encryption or unauthorized access.

**Initial Analysis**: The SOC verifies the alert by contacting the IT, Database and Network team (Lucky, Dusty and Ned).

**Escalation**: If confirmed as ransomware, the SOC escalates to Manager (Misha/Minka) and Consultant (Cat).

1. ***Containment***

**Immediate Action**: SOC isolates affected systems to prevent lateral movement.

**Communication**: Notify Security Provider (Cat) for further instructions and update Shift Manager regarding operational impact.

1. ***Eradication***

**Approval**: Security Consultant (Cat) reviews the containment efforts and approves eradication steps.

**Execution**: IT Support Specialist (Lucky) assists with malware removal and verification of system integrity.

1. ***Recovery***

**Restoration**: Systems are restored from clean backups.

**Testing**: IT Support, Database Specialist and Network Administrator (Lucky, Dusty and Ned) conduct thorough testing to ensure the absence of residual malware.

**Business Resumption**: Consultant (Cat) confirms the recovery process completion and authorizes the resumption of normal operations.

1. ***Post Incident Review***

**Review**: After everything is fixed, hold a meeting to discuss what happened and how to improve for the future.

**Report**: The SOC writes a detailed report, while Consultant (Cat) provides a simple summary to CEO (Percy).

**Technical Letter to MSSP Consultant** (**CAT**)

**Subject:** Urgent: Ransomware Attack at Box Manufacturing

Dear Cat,

We have detected a ransomware incident affecting several critical systems at Box Manufacturing. Immediate containment measures have been implemented to prevent further spread.

Details:

* **Incident Type:** Ransomware
* **Time of Detection:** 5:20 p.m. January 10, 2025
* **Actions Taken:** Isolation of affected systems, initial notifications sent.

Your expertise is required for eradication and recovery efforts. Please provide guidance on the next steps.

Thank you,  
Harsh Patel  
SOC Specialist

**Non-Technical Letter to Client** (**Mr.Percy**)

**Subject**: Security Incident Notification: Ransomware Detected

Dear Percy,

We want to inform you about a cybersecurity incident involving ransomware. Our SOC team detected unauthorized encryption of files and has taken steps to isolate the affected systems.

Currently, we are working with Cat, our cybersecurity consultant, to resolve the issue. We will continue to provide updates as more information becomes available.

Thank you for your understanding.

Best regards,

Harsh Patel

SOC Specialist

**Trigger List**

* **Unauthorized Access Attempts**: Multiple failed login attempts or use of compromised credentials.
* **Abnormal File Activity**: Detection of mass encryption or deletion of files.
* **Unusual Network Traffic**: High volumes of outbound traffic to unfamiliar IP addresses.
* **Endpoint Detection Alerts**: Alerts from EDR tools indicating potential malware.

**Rationale**

***Incident Selection***

Ransomware incidents were selected as a high-priority focus for this playbook because they pose a significant risk to Box Manufacturing’s operations. Ransomware can cause:

**Operational Downtime**: Since Box specializes in manufacturing custom boxes, downtime directly impacts revenue and production timelines.

**Data Integrity Risks**: Encrypted or lost data can lead to delays in fulfilling customer orders.

**Reputational Damage**: A prolonged incident could harm client trust and the company’s reputation in the industry.

***For Individual Involvement***

The involvement of specific individuals at various stages is triggered by the nature and severity of the incident:

**Ned (Network Administrator)**, **Lucky (IT Support Specialist)** and **Dusty (Database Specialist)** are involved during the detection and recovery phase to confirm if the abnormal behavior is malicious.

**Misha (Shift Manager)** and **Minka (Alternate Shift Manager)** are notified based on their availability.

**Cat (MSSP Consultant)** is engaged immediately after detection to guide containment, eradication, and recovery efforts due to her expertise in handling such incidents.

**Percy (CEO)** is informed only when incidents are escalated to critical status, unresolved beyond 48 hours, or have a potential significant business impact.

**Flowchart**

1. **Detection:** SOC identifies unusual activity.
2. **Verification:** Confirm the incident.
3. **Containment:** Disconnect affected systems.
4. **Eradication:** Remove the ransomware with Security Consultant’s approval and support.
5. **Recovery:** Restore data from backups and verify system integrity.
6. **Post-Incident Review:** Conduct a lesson learned session and prepare documentation for future.

**References**

StopRansomware: RansomHub Ransomware | CISA. (2024, August 29). Cybersecurity and Infrastructure Security Agency CISA. <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-242a>

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology. <https://doi.org/10.6028/nist.sp.800-61r2>

Kim, A. (2024, July 31). 2023 Survey Event | Incident Response | SANS Institute. <https://www.sans.org/white-papers/2023-survey-event-incident-response/>

Bevin, L. (2020, May 10). *Risk Assessment Checklist NIST 800-171*. ZenGRC. <https://www.zengrc.com/blog/risk-assessment-checklist/>

What is Ransomware? | UpGuard. (n.d.). <https://www.upguard.com/blog/ransomware>

Cisternelli, E. (2024, February 27). The top 7 cybersecurity frameworks. Bitsight. <https://www.bitsight.com/blog/7-cybersecurity-frameworks-to-reduce-cyber-risk>