# Box Manufacturing Playbook

Violet Figueroa

# Introduction

The following is the incident response procedures for Box Manufacturing, a specialized cardboard box manufacturer. It details the communication and escalation protocols between the SOC team, Cat (MSSP Security Consultant), and key stakeholders. It provides comprehensive guidelines for handling security incidents, including specific triggers, escalation criteria, and communication templates tailored to Box's operational requirements and security needs. The playbook ensures that all stakeholders receive appropriate information based on their roles: Percy F. (CEO) receives executive summaries for urgent matters, Cat receives detailed technical reports, and Misha/Minka are informed of operational impacts during their respective shifts.

# Roles and Responsibilities

Each individual or group has specific duties to ensure efficient detection, communication, escalation, and resolution of security incidents.

1. Box Manufacturing (Client)

Percy F. (CEO of Box)

- Role: Business decision-maker and ultimate authority on escalated incidents.
- Responsibilities:
    - Receives executive summaries only for: Urgent incidents.
    - Makes business-impact decisions based on escalated reports.
    - Delegates operational oversight to Misha F. and Minka F.

Misha F. (Shift and Production Manager)

- Role: First point of contact during regular business hours (9 AM–5 PM AST) for operational impacts.
- Responsibilities:
    - Receives updates on any major highlights or potential impacts to production.
    - Communicates operational concerns to Percy if necessary.
    - Coordinates with Cat or SOC when operational disruptions occur.

Minka F. (Alternate Shift Manager)

- Role: Backup contact for operational impact notifications during after-hours and weekends.
- Responsibilities:
    - Steps in for Misha F. outside of regular hours.
    - Handles communication regarding operational concerns during her shift.

2. SOC (soc.cat Monitoring Team)

Role: First line of defense for detecting and responding to security incidents.

- Responsibilities:
    - Monitors Box's network, systems, and data in real-time using soc.cat tools.
    - Identifies and triages potential security incidents based on predefined triggers.
    - Escalates incidents to Cat when:Severity level meets escalation criteria (e.g., SEV 1 or SEV 2).
    - Provides detailed technical logs, evidence, and reports to Cat for further analysis and remediation.

3. Cat (External MSSP Security Consultant)

Role: Oversees all aspects of Box's cybersecurity strategy and incident response.

- Responsibilities:
    - Acts as the primary point of contact for all escalated security incidents.
    - Reviews and approves all playbooks, workflows, and remediation plans developed for Box.
    - Coordinates with SOC to ensure timely containment, eradication, and recovery from incidents.

- Communicates with third-party providers or additional stakeholders as necessary.
- Provides Percy with high-level executive summaries when required.

4. Third-Party Providers (If Applicable)

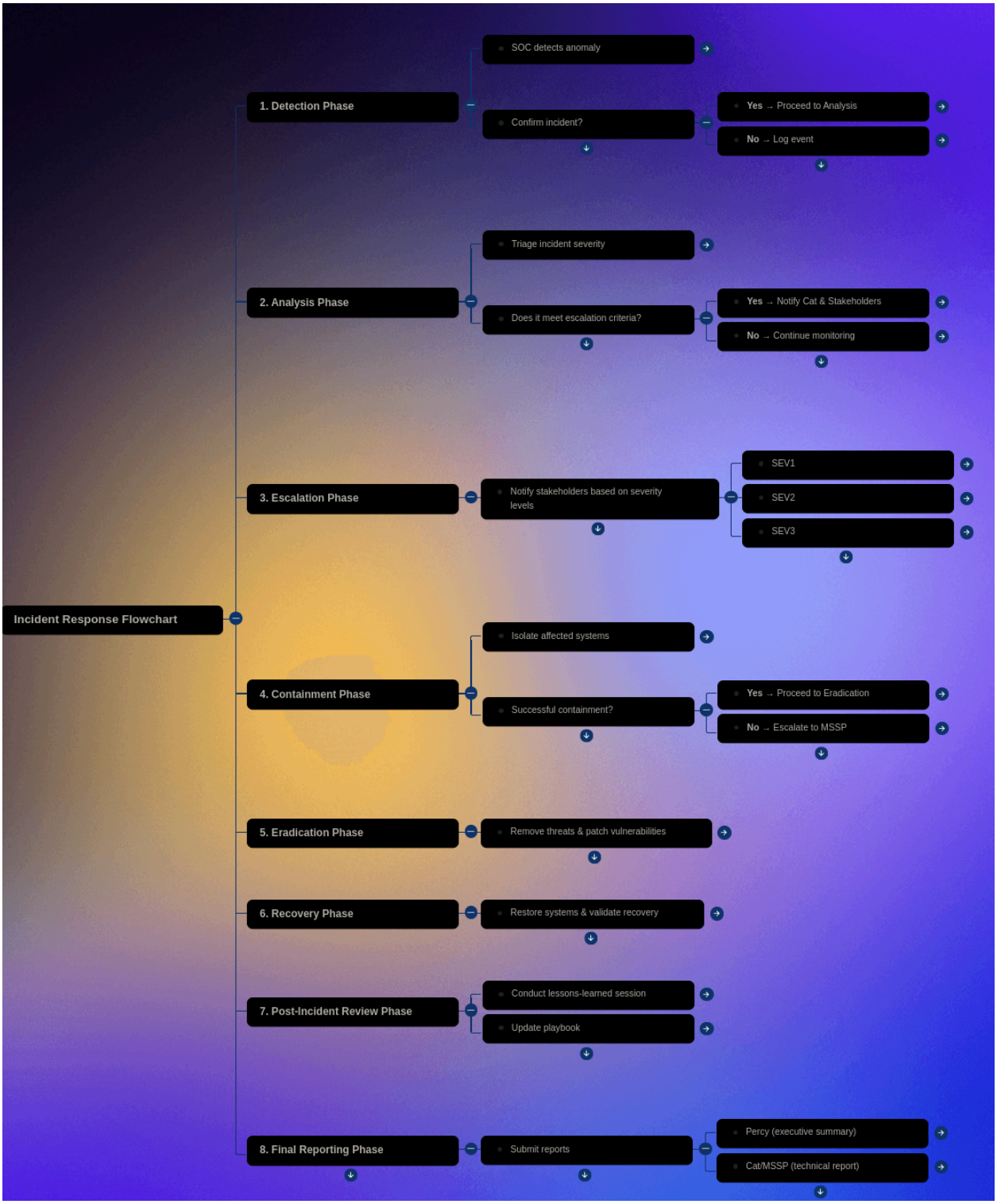
Role: External entities engaged by Cat or SOC for specialized incident response tasks.

- Responsibilities:
  - Assist in advanced remediation efforts if required (e.g., malware removal, forensic analysis).
  - Provide additional expertise or resources beyond SOC capabilities.

# Incident Response Steps

1. Detection Phase
   → SOC detects anomaly
   → Confirm incident?
   → Yes → Proceed to Analysis
   → No → Log event
2. Analysis Phase
   → Triage incident severity
   → Does it meet escalation criteria?
   → Yes → Notify Cat & Stakeholders
   → No → Continue monitoring
3. Escalation Phase
   → Notify stakeholders based on severity levels (SEV1/SEV2/SEV3)
4. Containment Phase
   → Isolate affected systems
   → Successful containment?
   → Yes → Proceed to Eradication
   → No → Escalate to MSSP
5. Eradication Phase
   → Remove threats & patch vulnerabilities
6. Recovery Phase
   → Restore systems & validate recovery
7. Post-Incident Review Phase
   → Conduct lessons-learned session
   → Update playbook
8. Final Reporting Phase
   → Submit reports to Percy (executive summary) & Cat/MSSP (technical report)

# Flowchart


Incident Response Flowchart
1. Detection Phase
SOC detects anomaly
Confirm incident?
Yes → Proceed to Analysis
No → Log event
2. Analysis Phase
Triage incident severity
Does it meet escalation criteria?
Yes → Notify Cat & Stakeholders
No → Continue monitoring
3. Escalation Phase
Notify stakeholders based on severity levels
SEV1
SEV2
SEV3
4. Containment Phase
Isolate affected systems
Successful containment?
Yes → Proceed to Eradication
No → Escalate to MSSP
5. Eradication Phase
Remove threats & patch vulnerabilities
6. Recovery Phase
Restore systems & validate recovery
7. Post-Incident Review Phase
Conduct lessons-learned session
Update playbook
8. Final Reporting Phase
Submit reports
Percy (executive summary)
Cat/MSSP (technical report)

# Trigger Items

Incident triggers are conditions or events that initiate an incident response process.
Trigger 1: Unusual Network Activity

- Detection of abnormal traffic patterns, unauthorized access attempts, or large data transfers.
- Initial Response: The SOC (soc.cat) investigates the anomaly by reviewing logs and system activity. (NIST, 2023)
- Escalation Criteria:
    - If confirmed as malicious or unresolved after 24 hours → Escalate to Cat for further analysis.
    - Notify Misha if there is potential for operational disruption.

Trigger 2: Indicators of Compromise (IoCs)

- Presence of malware signatures, unauthorized file changes, or alerts from threat intelligence feeds. (MITRE, 2023)
- Initial Response: SOC isolates affected systems and collects evidence for analysis. (NIST, 2023)
- Escalation Criteria:
    - If critical systems are impacted or IoCs suggest a widespread attack → Immediately escalate to Cat.
    - Notify Percy if unresolved after 48 hours or if business-critical systems are compromised.

Trigger 3: System Downtime or Failures

- Unexpected downtime of critical systems or failure to meet service-level agreements (SLAs).
- Initial Response: SOC investigates root cause using soc.cat monitoring tools. (NIST, 2023)
- Escalation Criteria:
    - If downtime exceeds 2 hours or affects production → Notify Misha (during business hours) or Minka (after-hours).
    - Escalate to Cat if technical expertise is required for resolution.

Trigger 4: Unauthorized Access Attempts

- Repeated failed login attempts, access from unrecognized devices, or privilege escalation attempts.
- Initial Response: SOC blocks suspicious accounts/IPs and reviews access logs. (NIST, 2023)

- Escalation Criteria:
    - If unauthorized access is confirmed or involves sensitive systems → Escalate to Cat immediately.
    - Notify Percy if unresolved after escalation or if sensitive data is at risk.

Trigger 5: Third-Party Alerts

- Notifications from vendors, partners, or threat intelligence feeds about vulnerabilities or attacks targeting Box's systems.
- Initial Response: SOC validates the alert and assesses potential impact on Box's environment. (NIST, 2023)
- Escalation Criteria:
    - If the alert indicates immediate risk → Escalate to Cat for further action.
    - Notify Misha/Minka if operational impact is expected.

# Severity Levels and Escalation

SEV 1 (Critical):

- Criteria: Business-critical systems are compromised; significant data breach; regulatory violations. (ISO, 2023)
- Action: Immediate escalation to executive leadership (e.g., Percy) and external MSSP (Cat).

SEV 2 (High):

- Criteria: Major operational disruptions; partial data exposure; unresolved after a set timeframe (e.g., >48 hours). (ISO, 2023)
- Action: Notify Misha/Minka during business hours and escalate to Cat after-hours if unresolved.

SEV 3 (Moderate):

- Criteria: Minor operational disruptions; no immediate business impact. (ISO, 2023)
- Action: SOC handles internally but informs Cat for awareness.

Time-Based Escalation:

- Criteria: Incidents unresolved within predefined timeframes (e.g., >24 hours for SEV 2).
- Action: Escalate to Cat and notify Percy if the issue persists beyond the SLA. (NIST, 2023)

Functional Escalation:

- Criteria: Incident requires expertise beyond the current responder's capability (e.g., malware removal).
- Action: Escalate to specialized teams or external MSSP. (NIST, 2023)

# Client Email Template

To: percy@box.cat
Cc: mesha@box.cat (if during business hours) / minka@box.cat (if after-hours or weekends)
Subject: SEV3 - [Incident Type] - [Status] Executive Summary of Security Incident
Date: [Weekday], [Month] [Day], [Year]
Time: [12 hour clock time] [AM or PM] AST
Dear Mr. Percy F.,
I hope this message finds you well. I am writing to provide you with an executive summary regarding a security incident that has been detected and escalated by our SOC team.
Incident Overview

- Date/Time Detected: [Weekday], [Month] [Day], [Year], at approximately [12 hour clock time] [AM or PM] AST
- Incident Type: [Brief description of the incident, e.g., Unauthorized Access Attempt or Unusual Network Activity]
- Affected Systems: [Specify affected systems or areas, e.g., Internal File Server or Manufacturing Network]
- Business Impact: [Briefly state the impact on operations, e.g., "No immediate operational disruptions detected" or "Production delays of approximately 1 hour observed."]

Current Status
The SOC team has taken immediate steps to contain the issue and has escalated it to Cat for further analysis and remediation. At this time:

- The threat has been isolated to [specific system/network segment].
- No evidence of data exfiltration has been found (if applicable).
- Operations are expected to resume without further delays (if applicable).

Next Steps
Cat is currently overseeing the remediation process and coordinating with third-party providers as necessary. We will continue to monitor the situation closely and keep you informed if there are any significant updates or unresolved issues after 48 hours. If you have any questions or require additional information, please do not hesitate to reach out to me directly.
Best regards,
[Name]
[Title/Role]
[Your Contact Information]

# Third-Party Email Template

To: cat@soc.cat
Cc: [Optional: SOC team or other relevant parties]
Subject: [SEV1/2/3] - [Incident Type] - [Status] Detailed Technical Findings and Action Plan
Date: [Weekday], [Month] [Day], [Year]
Time: [12 hour clock time] [AM or PM] AST
Dear Cat,
I hope this message reaches you well. I am writing to provide you with a detailed report regarding a security incident that has been detected and escalated by the SOC team at Box Manufacturing. Below are the key findings and actionable items for your review and further action.
Incident Overview

- Date/Time Detected: [Weekday], [Month] [Day], [Year], at approximately [12 hour clock time] [AM or PM] AST
- Incident Type: [e.g., Unauthorized Access Attempt, Unusual Network Activity]
- Affected Systems: [Specify affected systems or areas, e.g., Internal File Server or Manufacturing Network]
- Indicators of Compromise (IoCs):
    - [List specific IoCs detected, e.g., IP addresses, file hashes, malicious domains]

Technical Findings

1. Summary of Events
    - [Describe the sequence of events leading to detection, e.g., "At 3:30 PM AST, the SOC detected unusual login attempts from IP address X.X.X.X targeting the internal file server."]
    - [Include any relevant logs or timestamps.]
2. Analysis
    - [Provide a brief analysis of what was observed, e.g., "The IP address was flagged as suspicious based on threat intelligence feeds and matched known IoCs for brute-force attacks."]
3. Impact Assessment
    - [Assess the impact on systems and operations, e.g., "No immediate operational disruptions were observed; however, access to sensitive data may have been attempted."]

Actions Taken by SOC

- Isolated affected systems from the network to prevent further spread.
- Blocked suspicious IPs and accounts associated with unauthorized activity.
- Collected evidence (e.g., logs, screenshots) for further analysis.

Recommended Next Steps

1. Perform in-depth forensic analysis of affected systems to confirm root cause.
2. Validate that no data exfiltration has occurred using network traffic analysis tools.
3. Apply additional security measures (e.g., MFA enforcement or patching vulnerabilities) as needed.

Attachments

- Relevant logs and evidence collected by SOC:
    - [Attach files such as log files, screenshots, or reports.]
- Additional reference materials:
    - [Include links or attachments related to IoCs or threat intelligence.]

If you require any additional information or assistance from the SOC team during your investigation and remediation efforts, please do not hesitate to reach out. We will remain available to support you throughout this process.

Best regards,
[Your Name]
[Your Title/Role]
[Your Contact Information]

# References and Citation


1. National Institute of Standards and Technology. (2023). Computer security incident handling guide (Special Publication 800-61, Rev. 3). U.S. Department of Commerce.
2. MITRE. (2023). MITRE ATT&CK® framework. The MITRE Corporation.
3. Atlassian. (2023). Incident management best practices. Atlassian Documentation.
4. International Organization for Standardization. (2023). ISO/IEC 27035-1:2023 Information security incident management. ISO.
5. International Organization for Standardization. (2023). ISO/IEC 27035-1:2023 Information technology — Information security incident management — Part 1: Principles and process. ISO.
6. National Institute of Standards and Technology. (2024). Computer security incident handling guide (NIST Special Publication 800-61, Rev. 3). U.S. Department of Commerce.
7. IBM. (2023, May 18). What is the MITRE ATT&CK framework? IBM Think.
8. Atlassian. (2024). Incident management: Processes, best practices & tools. Atlassian Documentation.
9. PECB. (2024). ISO/IEC 27035 Information security incident management. Professional Evaluation and Certification Board.
10. Atlassian. (2023, October 6). Incident communication tips. Statuspage Documentation.