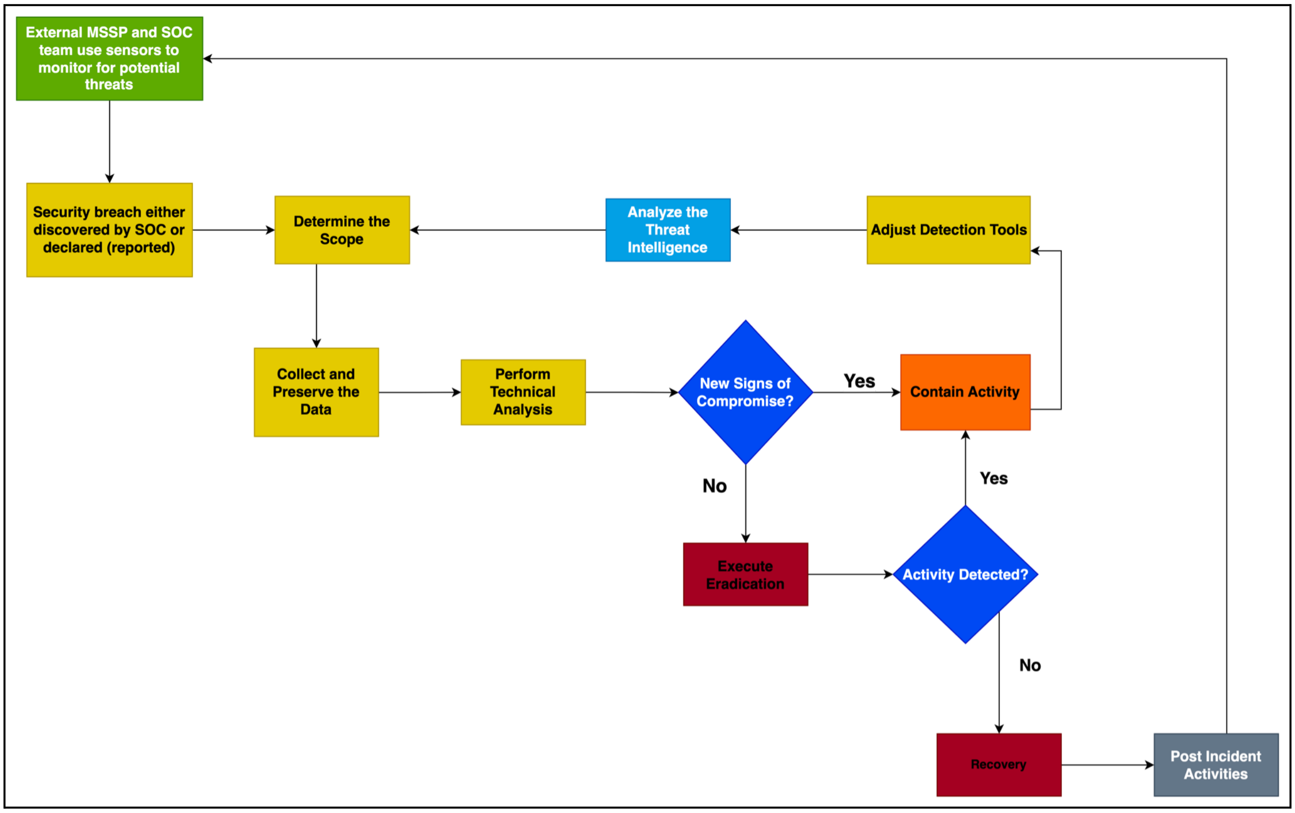
In the case of a data breach within the Box manufacturing company, it is essential that the guidelines within this playbook are followed to minimize the effects of the attack and resolve them as soon as possible.

Company Contact Information:

- Mr. Percy F. is the CEO of Box and he has stated that he would only like to be informed personally if a situation is escalated, urgent or unresolved after 48 hours
  - His email is percy@box.cat
- Misha is Percy's shift and production manager who works from 9AM to 5PM.
  She should be informed of any potential threats against the system
  - Her email is mesha@box.cat
  - She can be reached during her working hours at 902 66-9999
- Minka is the alternate shift/production manager that covers for Misha after hours and during weekends
  - Her email is minka@box.cat
  - She can be reached at 902 66-9999
- Cat is a consultant for a managed security service provider and she is contracted by Box
  - Her email is cat@soc.cat
  - She can be reached during the day at 902 88-1234
  - She can be reached after-hours and weekends at 902 77-4321

Playbook Flowchart showing the steps to take in case of a Data Breach:



External MSSP and SOC team use sensors to monitor for potential threats
Security breach either discovered by SOC or declared (reported)
Determine the Scope
Analyze the Threat Intelligence
Adjust Detection Tools
Collect and Preserve the Data
Perform Technical Analysis
New Signs of Compromise?
Yes
Contain Activity
No
Yes
Execute Eradication
Activity Detected?
No
Recovery
Post Incident Activities

List of trigger items that may affect the flow of the playbook:

- The severity of the incident may affect the playbook:
  - If the threat is escalated/urgent or unresolved after 48 hours, Mr. Percy F. should be informed personally
  - If it is not as severe or resolved within 48 hours, you may just notify the shift/production manager as the company representative
- The timing of the incident can also affect the playbook procedure:
  - If the item is discovered during regular working hours (9AM to 5PM weekdays), Misha is the representative for Box that should be informed
  - If the item is discovered outside regular hours or on the weekend, Minka is the person from Box who should be informed

Scenario for letters is a regular data breach that is not too severe. The threat was discovered by the SOC at 1:45PM.

Sample Letter to the client:

Hello Miss Misha,

This is Robert Ajegbo from the SOC team contracted by Box Company. I hope that you are doing well at work today. We regret to inform you that we have been monitoring some suspicious traffic on the company network and can now confirm that your organization has suffered a data breach. At this time, we can say that it is not as severe as what it could be. We recommend you to make sure that all employee logins are secured thoroughly. We will be emailing Cat with further information for her investigation but she may still need some information from you to assist her in resolving the issue in a timely manner.

Regards,
Robert Ajegbo.

Sample Letter to Third-party provider:

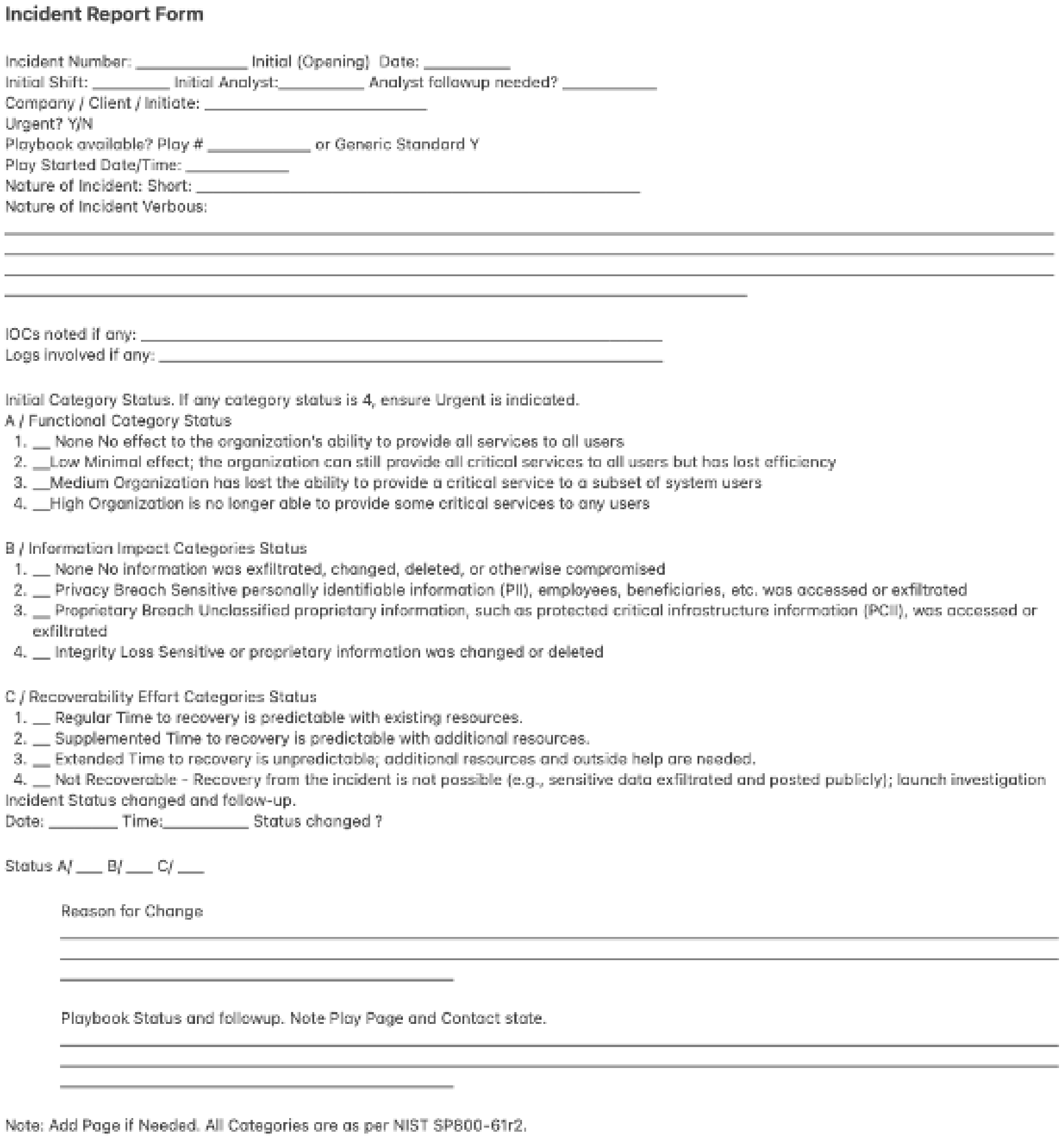
Hello Cat,

This is Robert Ajegbo. Unfortunately, I have to inform you that we have discovered a data breach for Box Company. The attack was discovered at 1:45PM and we believe that it was conducted from a Windows system with an IP of **172.16.14.50.** We can also state with confidence that the attacker breached the security using a type of Phishing attack. It appears that the attacker can not access the company's highly confidential data as they do not have the appropriate privileges. It would be best for you to ensure that there are no traces of malware or other malicious software left on the company's systems. Also, make sure that the employees are aware that they must not enter their company information into any kind of suspicious data field. As the attack is not too severe, we do not have to inform Mr. Percy but we have already gone ahead to let Misha know about the current situation. She is aware that you may need her assistance in getting some further information for your investigation. Make sure you fill out an incident report form following the recovery of the system for future reference.

Regards,
Robert Ajegbo.

Following the completion of the Incident Response steps, Cat will fill out an incident report form to discuss with the rest of the MSSP and SOC team. This will help to record the details of the event and can be used as a reference when approaching future attacks.

Example of Incident Report Form



Incident Report Form

Incident Number: _____________ Initial (Opening) Date: __________
Initial Shift: _________ Initial Analyst:__________ Analyst followup needed? ___________
Company / Client / Initiate: __________________________
Urgent? Y/N
Playbook available? Play # ____________ or Generic Standard Y
Play Started Date/Time: ____________
Nature of Incident: Short: ____
Nature of Incident Verbous:

IOCs noted if any: ____
Logs involved if any: ____

Initial Category Status. If any category status is 4, ensure Urgent is indicated.
A / Functional Category Status

1. __ None No effect to the organization's ability to provide all services to all users
2. __Low Minimal effect; the organization can still provide all critical services to all users but has lost efficiency
3. __Medium Organization has lost the ability to provide a critical service to a subset of system users
4. __High Organization is no longer able to provide some critical services to any users

B / Information Impact Categories Status

1. __ None No information was exfiltrated, changed, deleted, or otherwise compromised
2. __ Privacy Breach Sensitive personally identifiable information (PII), employees, beneficiaries, etc. was accessed or exfiltrated
3. __ Proprietary Breach Unclassified proprietary information, such as protected critical infrastructure information (PCII), was accessed or exfiltrated
4. __ Integrity Loss Sensitive or proprietary information was changed or deleted

C / Recoverability Effort Categories Status

1. __ Regular Time to recovery is predictable with existing resources.
2. __ Supplemented Time to recovery is predictable with additional resources.
3. __ Extended Time to recovery is unpredictable; additional resources and outside help are needed.
4. __ Not Recoverable - Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly); launch investigation

Incident Status changed and follow-up.
Date: ________ Time:__________ Status changed ?

Status A/ ___ B/ ___ C/ ___

Reason for Change

Playbook Status and followup. Note Play Page and Contact state.

Note: Add Page if Needed. All Categories are as per NIST SP800-61r2.

References

Benjamin, A. (2023, January 16). *Playbook for Cat & Box Scenario*. Lighthouse Labs Compass. Retrieved July 27, 2023, from https://cyber.compass.lighthouselabs.ca/projects/cat-playbook

Benjamin, A. (2023, January 16). *Playbooks for Incident Handling*. Lighthouse Labs Compass. Retrieved July 27, 2023, from https://cyber.compass.lighthouselabs.ca/p/2/days/w04d4/activities/2901

Federal Government Cybersecurity Incident and Vulnerability Response Playbooks. (n.d.). CISA. Retrieved July 26, 2023, from https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf

Top Security Playbooks. (n.d.). Google Cloud. Retrieved July 26, 2023, from https://inthecloud.withgoogle.com/top-security-playbooks/on-demand.html