IR Plan & Phishing Playbook

By: Danielle Daza

TABLE OF CONTENTS

EXECUTIVE SUMMARY

In order to cover all bases when developing a succinct playbook template for Box Manufacturing, a Standard Operation Procedure for incident response was also created. To briefly touch on the steps of the SOP created, it would cover detection and reporting, the initial triage, incident analysis, containment, eradication and recovery, and the post-incident analysis and reporting. These steps have been thoroughly outlined in the following section with examples of actions that may need to be taken within those steps.

Several workflow charts have been designed for general incident response from a wide-perspective as well as specific to the tiers of the SOC Analysts as there would inevitably be nuances to their incidents and the workflow charts aim to address the most common questions that may come up. Included in the workflow charts are criteria for notifying specific individuals in the Box Manufacturing company as, varying case-by-case, there may be incidents that require the attention of one of their specialists or management if the incident may heavily impact their daily operations. Generally, the need for notifications to be made would be decided along the ticket escalation stage (i.e. if a ticket would be escalated from Tier 1 to Tier 2 or Tier 2 to Tier 3 only after confirming the need for a specific individual's attention.

With the steps in the SOP for incident response, a playbook template for phishing attacks has been designed. In practice, the SOP would be used as a guideline of steps to follow when approaching an incident but depending on the case and how sophisticated the attack may be, all steps may not be required for every incident.

EXECUTIVE SUMMARY FOR CLIENT

In order to cover all bases when developing a succinct playbook template for Box Manufacturing, a Standard Operation Procedure (SOP) for incident response was also created to formally establish logical procedures to follow during an incident response. To briefly summarize the steps of the SOP created, it would over detection and reporting (i.e. monitoring the network for indications of compromise), the initial triage (i.e. confirming if an incident is a genuine positive or false positive), incident analysis (i.e. investigating what the threat involves such as malware or threat actors, and what systems and business operations are affected), containment, eradication and recovery (i.e. eliminating the treat, resolving the incident, and recovering affected systems and data), and the post-incident analysis and reporting (i.e. providing detailed reports on the incident from detecting the threat to resolving it as well as providing recommendations for future prevention).

Several workflow charts have been designed for general incident response from a wide-perspective as well as specific to the tiers of the External SOC Analysts as there would inevitably be nuances to their incidents and the workflow charts aim to address the most common questions that may come up. Included in the workflow charts are criteria for notifying specific individuals in the Box Manufacturing company as, varying case-by-case, there may be incidents that require the attention of one of their specialists or management if the incident may heavily impact their daily operations. Recognizing that Box Manufacturing has numerous responsibilities apart from general security, the need for notifications to be made would be decided along the ticket escalation stage (i.e. if a ticket would be escalated from Tier 1 SOC Analysts to Tier 2 or Tier 2 to Tier 3 only after confirming the need for a specific individual's attention in special and/or severe cases.

With the steps in the SOP for incident response, a playbook template for phishing attacks has been designed. In practice, the SOP would be used as a guideline of steps to follow when approaching an incident but depending on the case and how sophisticated the attack may be, all steps may not be required for every incident. The playbook does not include the criteria for notifying the Box Manufacturing members as the playbook is meant to focus on the specific incident itself and to be referred to in combination with the relevant workflow chart as the SOC Analysts complete their tickets.

STANDARD OPERATING PROCEDURE (SOP)

Below is a general overview for Standard Operating Procedures (SOP) so as to establish a baseline for actions to take during and after an IoC occurs.

SOP step	Objectives and Outcomes
Detection and Reporting	• Monitor the network for indications of unusual behaviour on computer systems, unusual amounts or types of internal traffic, or changes in behaviours • Ascertain if system is being used remotely to send spam or contribute to a DDoS attack
Initial Triage	• To confirm if the incident is genuine or if it is a false positive ○ False positives are also documented and resolved and how to avoid it next time • Categorize what aspect the incident most affects and assign the incident to the analyst level tier it aligns best with

Incident Analysis	• Analysis to understand the nature of the incident and potential malware or threat actors involved
	• Identify
	  ○ Systems affected (i.e. Servers, Desktop, Laptop) and/or at risk
	  ○ User credentials compromised or at risk
	  ○ Any malicious code and on what systems
	  ○ Any IT services impacted
	  ○ Business implications due to the attack
	  ○ Tools used to detect the attack

Containment, eradication, recovery	• Determine the necessary containment strategy to prevent further damage. E.g.
	  ○ Isolate the devices involved, removing it from the shared network system
	  ○ Relegate any responsibilities/processing from affected systems onto a backup system
	• Eliminate the threat involved. E.g.
	  ○ Adjust Firewall rules
	  ○ Eradicate malware
	  ○ Patching software
	  ○ Changing compromised credentials
	• Recover affected systems and data. E.g.
	  ○ Restoring backups
	  ○ Reinstalling software
	  ○ Resetting credentials, implementing Multi-Factor Authentication (MFA)

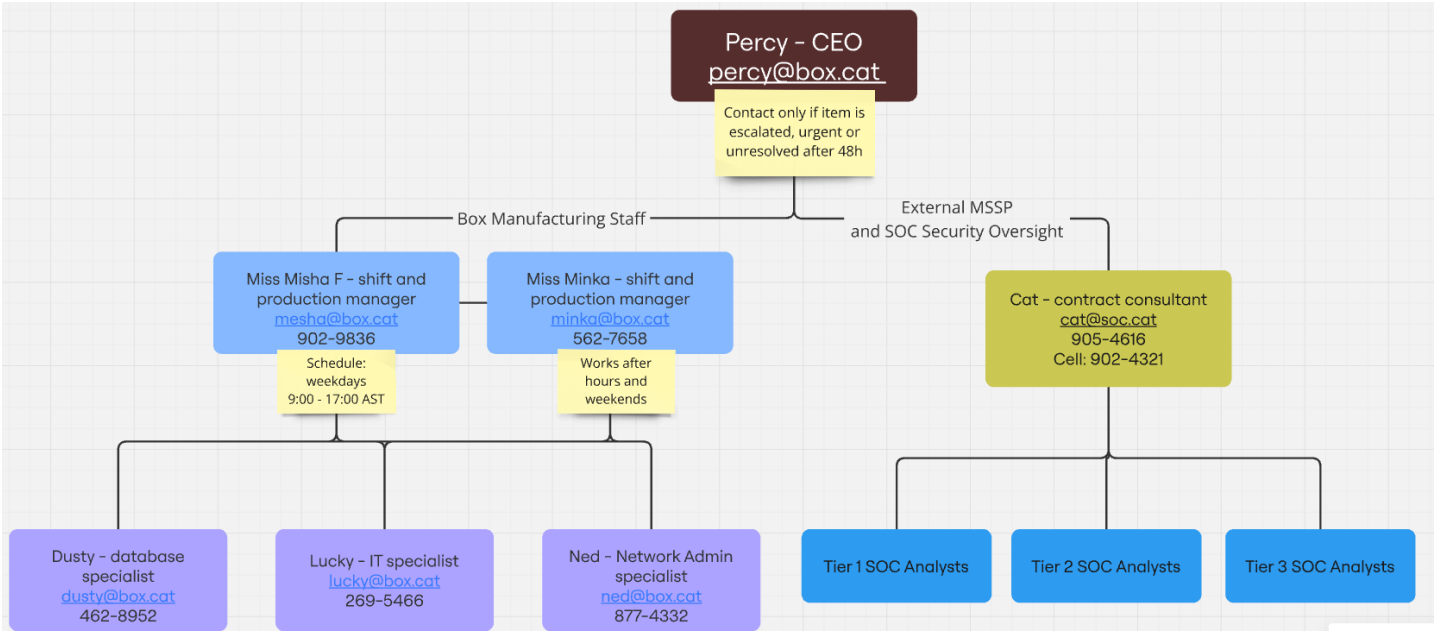
Post-Incident Analysis and Reporting	• Identify what was learned from the incident and what can be done to prevent similar incidents in the future

	• Provide a detailed overview of the incident, its impact on operations, the response actions taken, and recommendations for future prevention • Update policies and procedures if needed

(Standard operating procedures (SOPs) - definition & overview, 2022)

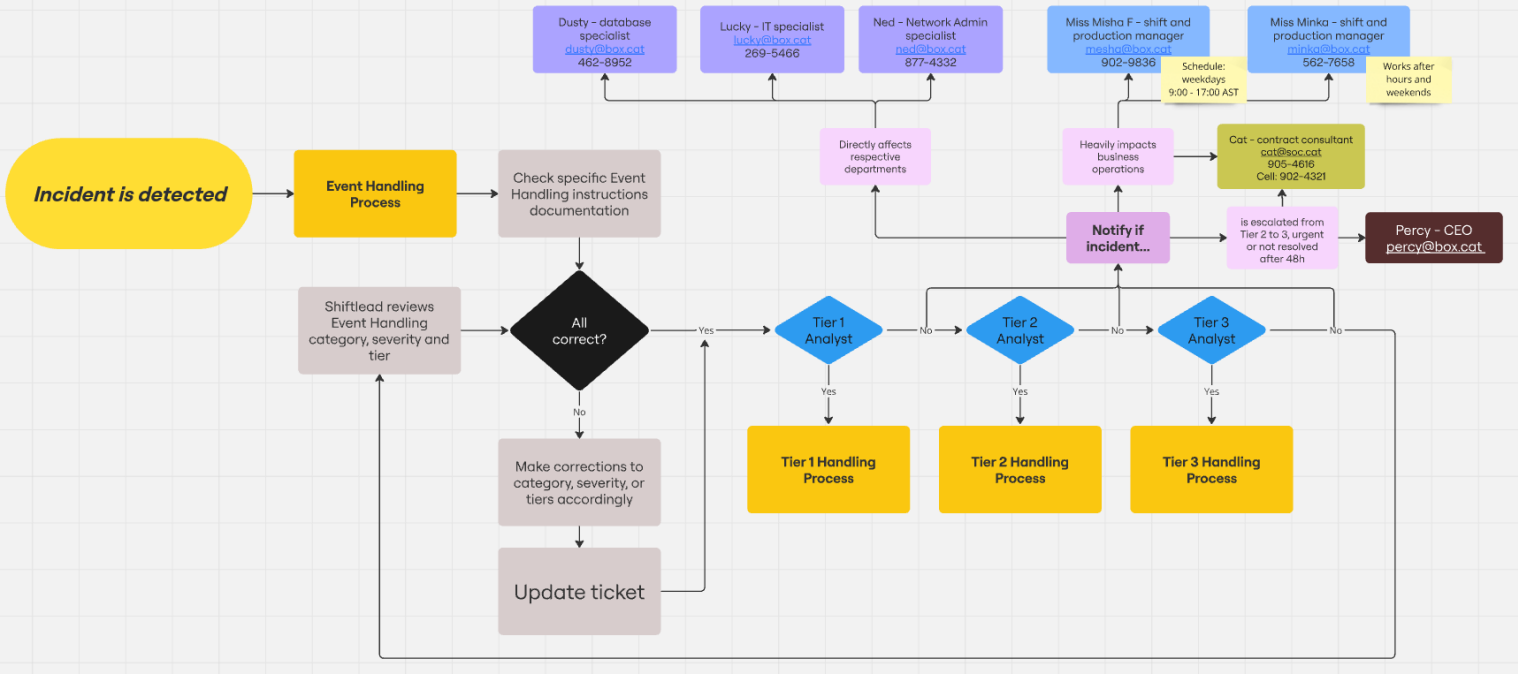
INCIDENT RESPONSE WORKFLOW

The following hierarchy flowchart was created for ease of understanding lines of communication and used as reference when developing the proceeding workflow charts for Box Manufacturing:



The following flowcharts are designed as a general guideline for the MSSP and SOC Security Oversight to follow in response to incidents as they occur. The flowcharts themselves aim to be self-explanatory, however, key notes regarding the rationale when designing them will be provided below.

INITIAL INCIDENT DETECTION WORKFLOW



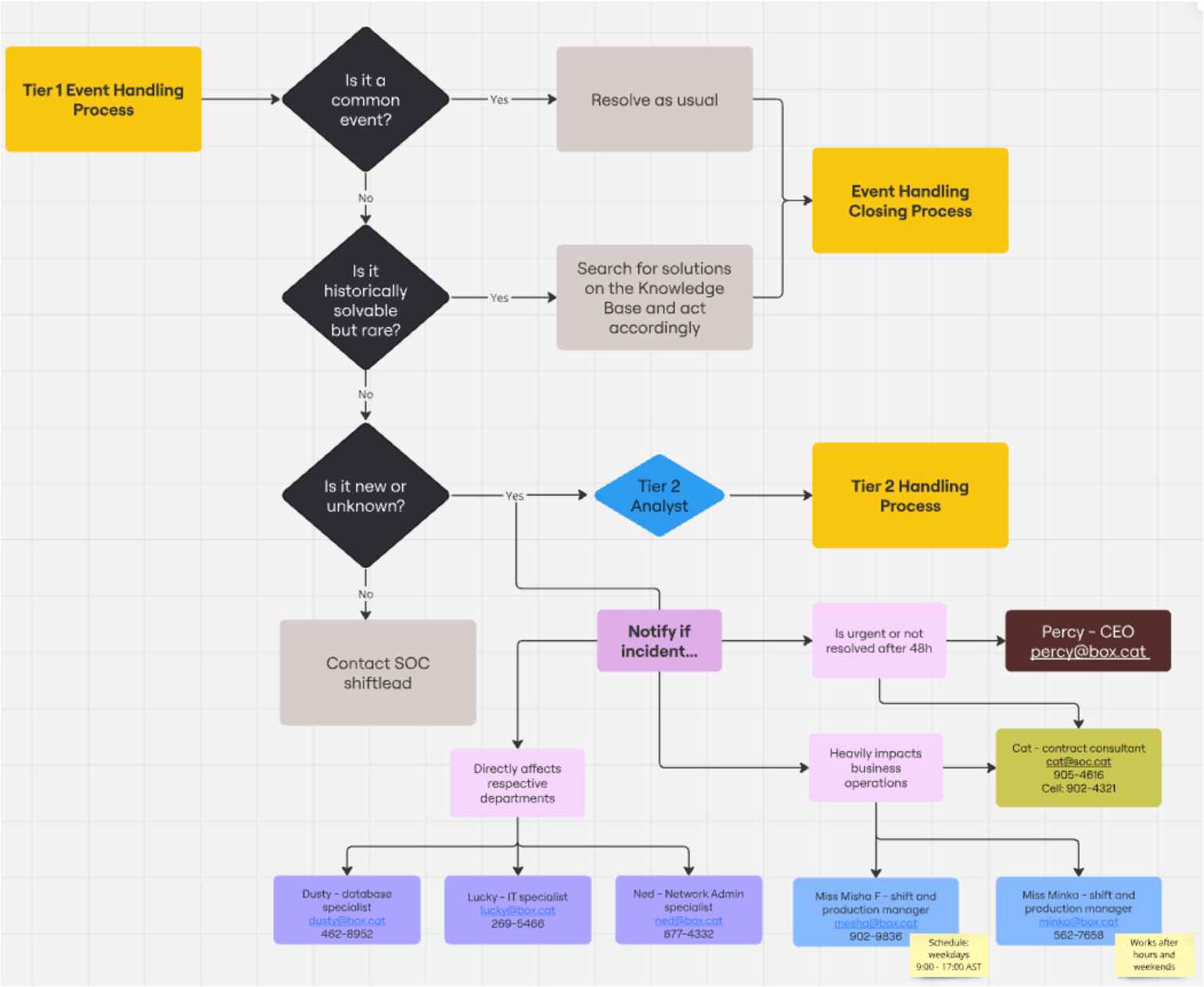
KEY NOTES

- In order to ensure timely and effective incident responses, all tickets will first reach Tier 1 SOC Analysts and triaged from that point if necessary so as to best utilize the more experienced SOC analysts' time.
- Incidents and events of will warrant the notification being delivered to other members of Box Manufacturing if:
    - The incident occurring directly affects respective departments and operations.
        - i.e. Dusty the Database Specialist, Lucky the IT Specialist, Ned the Network Admin Specialist.
    - The incident heavily impacts business operations.
        - Miss Misha F and Miss Minka the Shift and Product Managers.
    - The incident is escalated from Tier 2 to 3, is urgent, or unresolved after 48 hours
        - i.e. Percy the CEO.
- References: (WagnerAndreas, 2018) (iCybersecurity, 2021)

- Rationale for notification criteria:

Box Manufacturing Member	Role	Notification Criteria	Rationale
Dusty	Database Specialist	The incident directly affects respective departments and operations.	Security is not a major concern in their daily operations but if an incident may have an impact on their ability to complete their work, then they should be notified and aware of the situation.
Lucky	IT Specialist		
Ned	Network Admin Specialist		
Miss Misha F	Shift and Product Manager	The incident heavily impacts business operations.	These individuals ensure the success of business operations directly under the CEO. As such, they should be the first line of communication when an incident will affect business operations so as to best plan for recovery steps on their end.
Miss Minka	Shift and Product Manager		
Cat	Contract Consultant	The incident heavily impacts business operations *OR* The incident is escalated from Tier 2 to 3, is urgent, or unresolved after 48 hours	Cat works directly under the CEO to manage all security operations. So if any incident becomes severe enough that it would heavily impact the company operations, escalated to the expertise of Tier 3 SOC Analysts or has become unresolved after 48 hours, she should be notified immediately in order to begin the necessary defensive steps in order to mitigate any further damage.
Percy	CEO	The incident is escalated from Tier 2 to 3, is urgent, or unresolved after 48 hours	As the CEO has numerous other responsibilities under him, he should only be notified when an incident has become severe enough that it requires urgent attention and potential recovery planning.

TIER 1 EVENT HANDLING PROCESS



KEY NOTES

- The Tier 1 Analysts' Event Handling Process is intended to be as uncomplicated as possible as this tier is expected to receive and handle the most tickets sent their way while the more complex and severe tickets are passed onto the following tiers.
- Notifications regarding escalation will be sent to the relevant members of Box Manufacturing if the incidents' fall under one of the three criteria explained in the Initial Incident Response workflow chart.
- References: (WagnerAndreas, 2018) (iCybersecurity, 2021)

TIER 2 EVENT HANDLING PROCESS

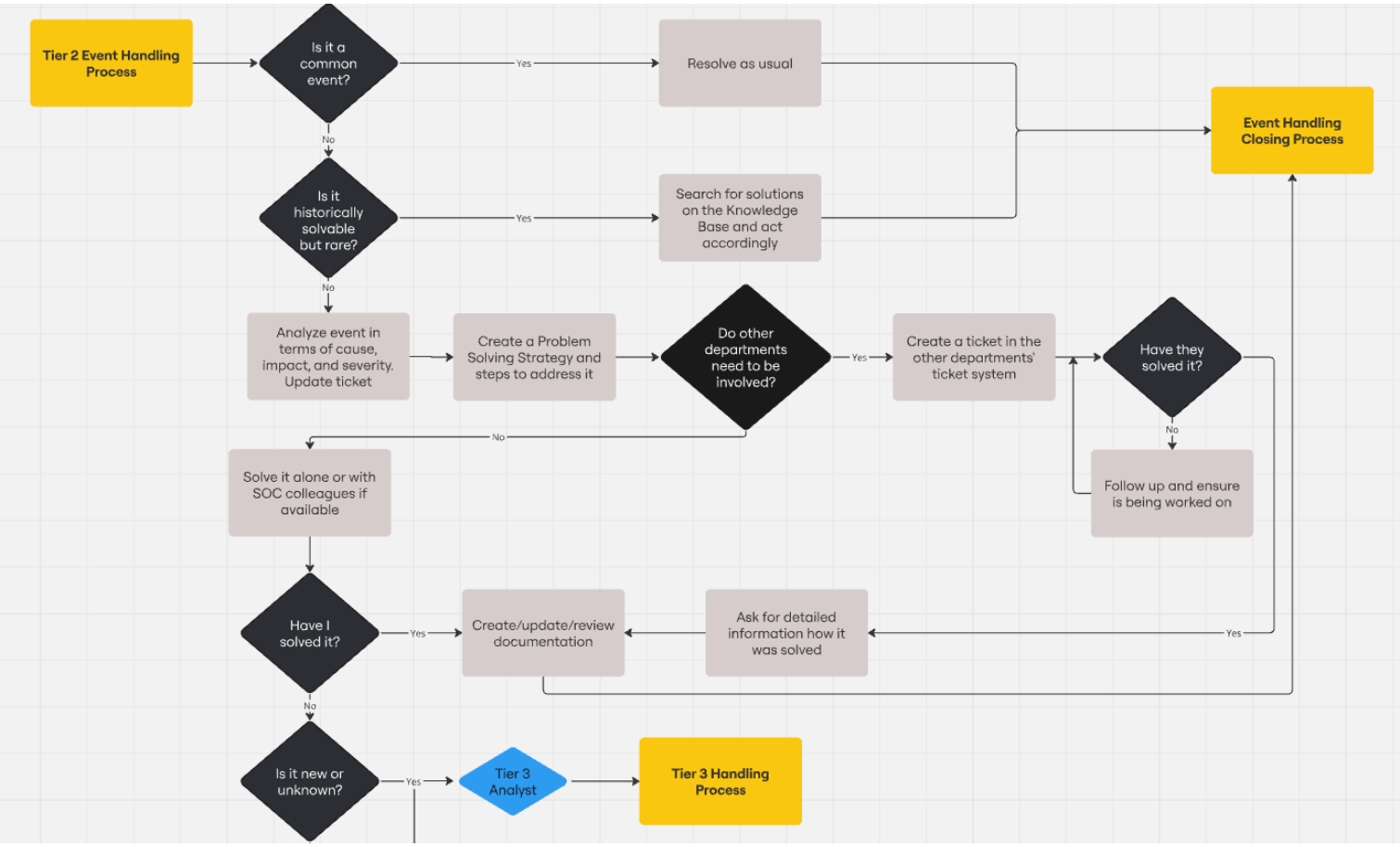


Figure 1.1 – Tier 2 Workflow 1/2

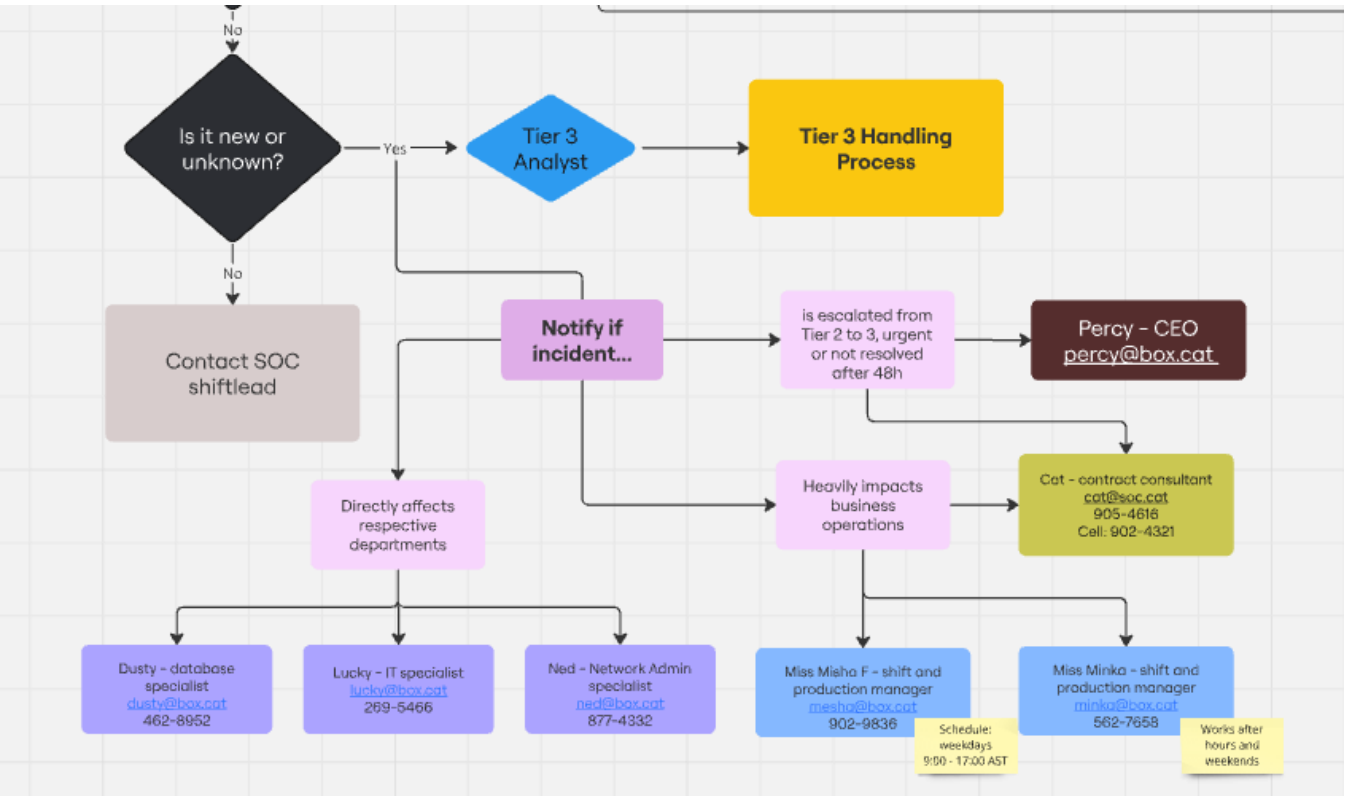


Figure 1.2 – Tier 2 Workflow 2/2

KEY NOTES

- Tier 2 SOC Analysts' workflow chart is designed with slightly more variables in mind when approaching an incident. This is to ensure that however an incident response may play out, there are steps outlined in a standard format to refer back to. This is also to minimize the potential downtime of waiting for responses from superiors on next steps for any particular case.
- This workflow includes the addition of involving other departments if needed as it is common for tickets to be referred another department more suited to resolving the incident
- Notifications regarding escalation will be sent to the relevant members of Box Manufacturing if the incidents' fall under one of the three criteria explained in the Initial Incident Response workflow chart.
- References: (WagnerAndreas, 2018) (iCybersecurity, 2021)

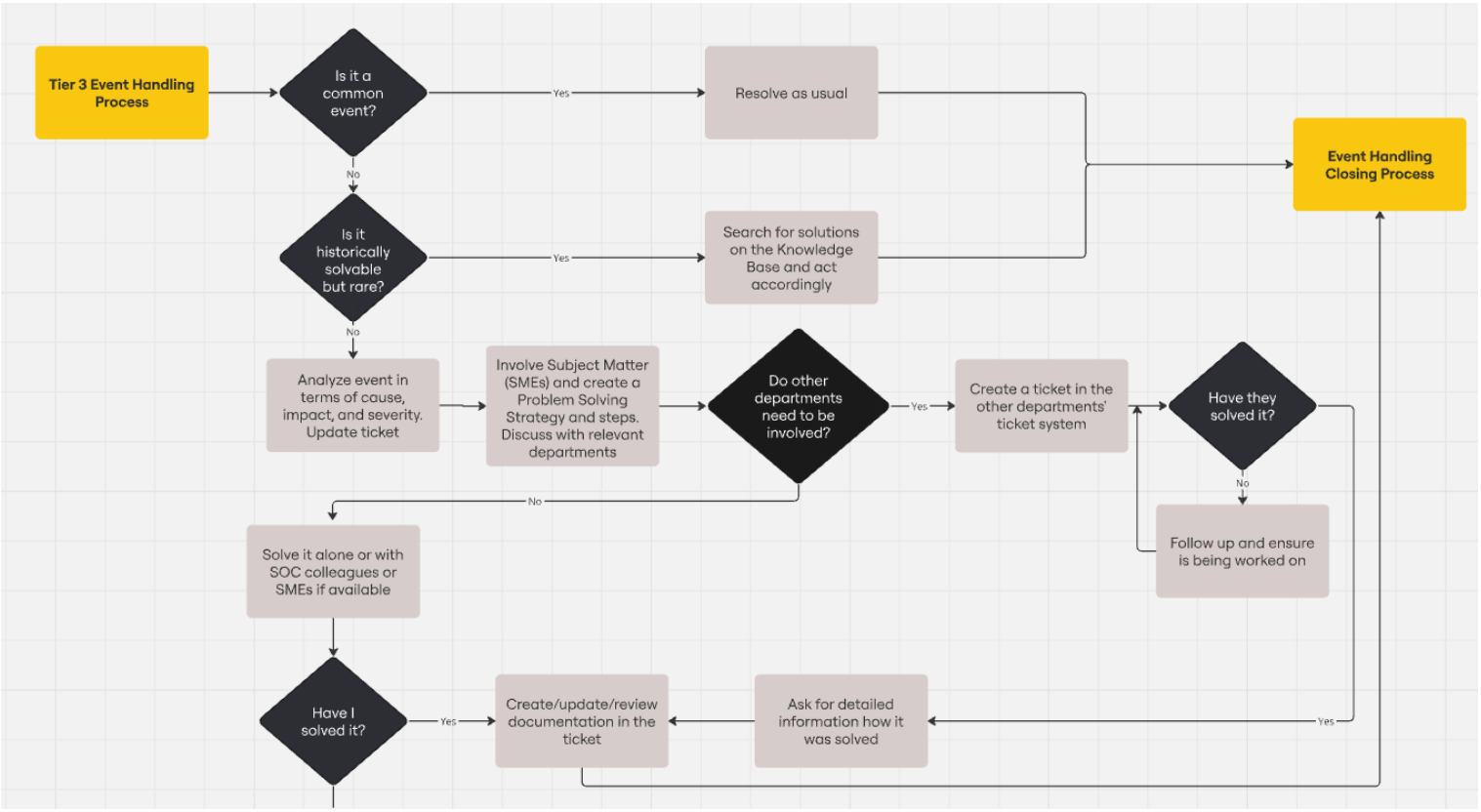


Figure 2.1 – Tier 3 Workflow 1/2

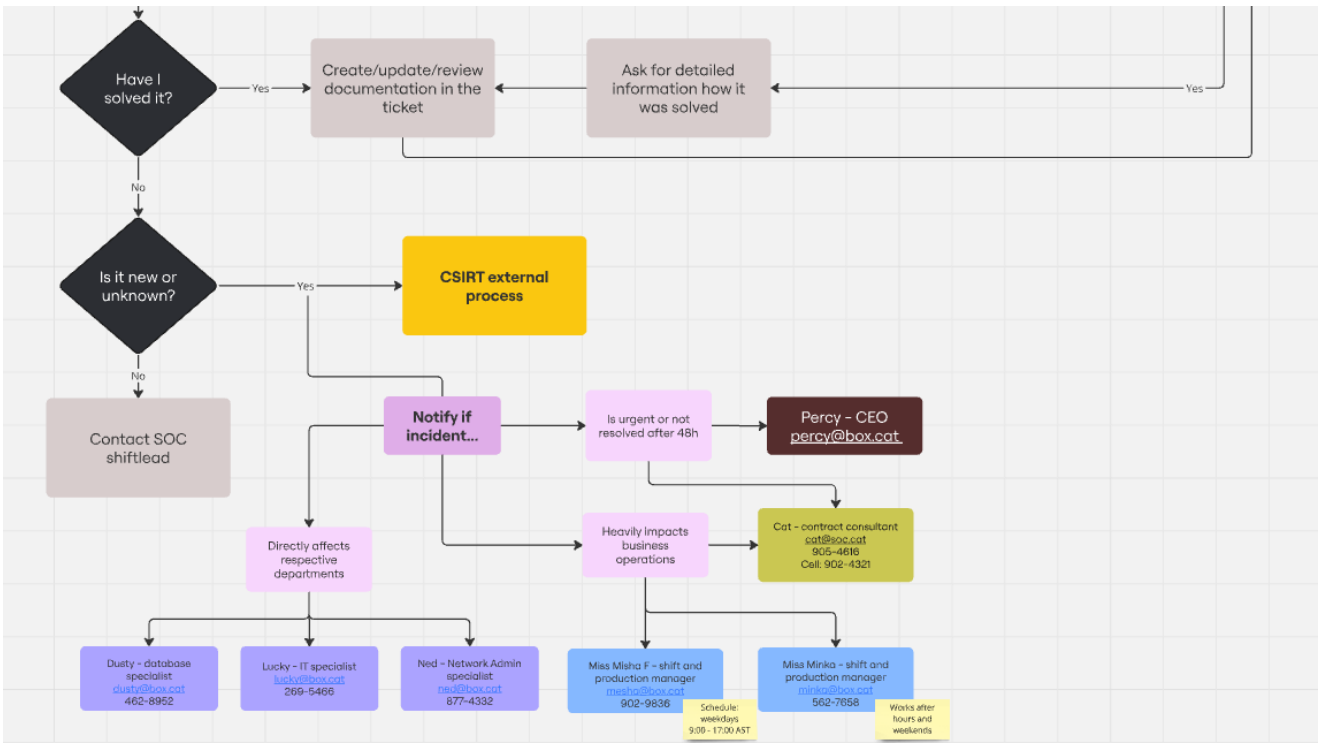
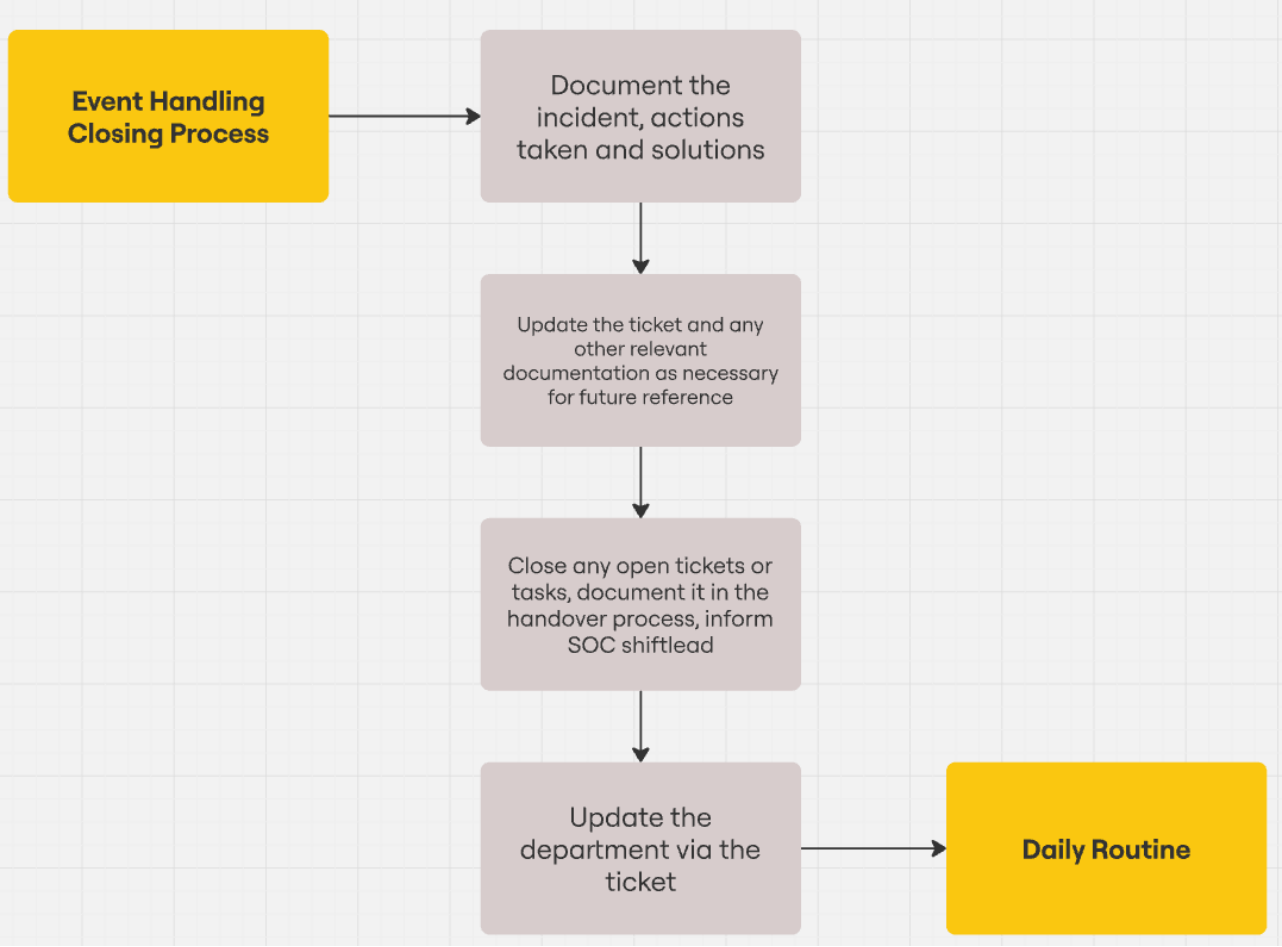


Figure 2.2 – Tier 3 Workflow 2/2

KEY NOTES

- Tier 3 SOC Analysts' workflow chart very similar to Tier 2's, however, if a truly new or unseen incident occurs, it is recommended that it be referred to a CSIRT (Cyber Security Incident Response Team) external process for additional aid.
- Notifications regarding escalation will be sent to the relevant members of Box Manufacturing if the incidents' fall under one of the three criteria explained in the Initial Incident Response workflow chart.
- References: (WagnerAndreas, 2018) (iCybersecurity, 2021)

ALL TIERS' EVENT HANDLING CLOSING PROCESS



KEY NOTES

- The Event Handling Closing Process is meant to include everything regarding documenting the incident both the factual record of the incident as well as recommendations for further prevention.
- Ensuring all of the incident's data is thoroughly documented allows for easy referrals if a similar issue arises and to reveal any vulnerabilities that are in need of addressing.
- References: (WagnerAndreas, 2018) (iCybersecurity, 2021)

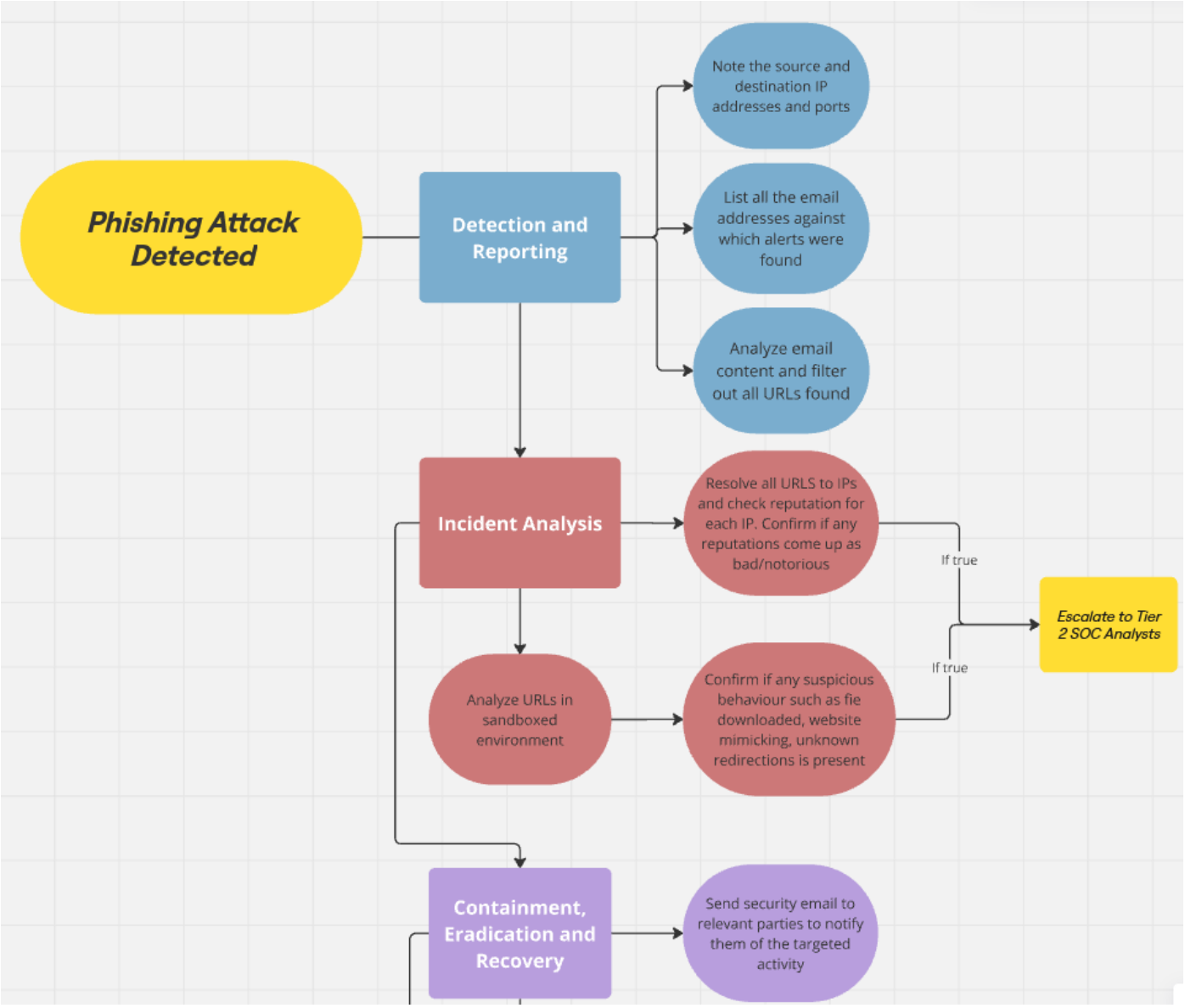


Figure 3.1 – Phishing Attack Playbook 1/2

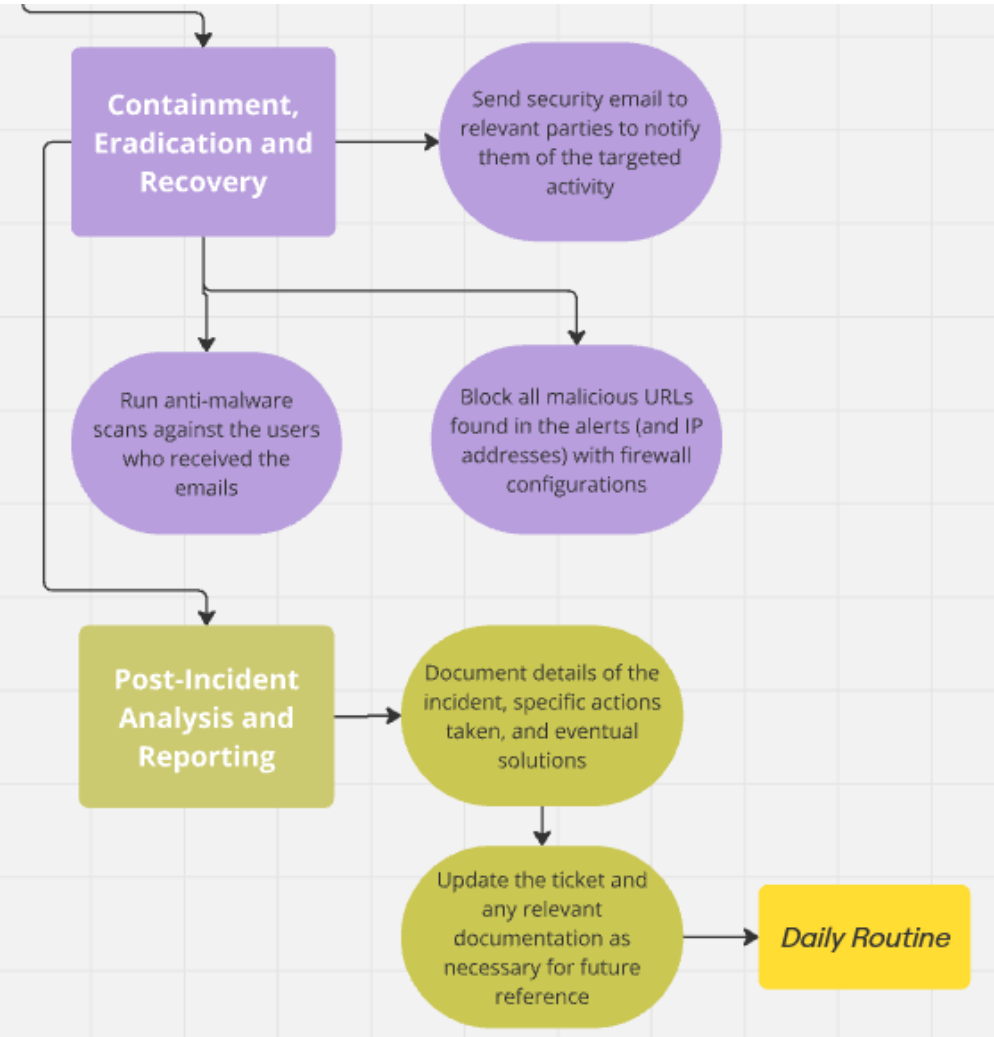


Figure 3.2 – Phishing Attack Playbook 2/2

KEY NOTES

- In this sample playbook, the steps toward resolution follows the SOP outlined earlier in this report.
    - Depending on the incident, the SOP steps may not all be present and used, but would be used as a universal template when creating playbooks.
- The triggers for notifying specific individuals was not explicitly shown in this playbook as they are all detailed in the workflows in previous sections.

    - The workflows act as a general conduct framework as SOC Analysts complete tickets. The playbook acts as a more specific guideline of prudent actions to take when faced with specific incidents.
    - So as to not complicate the playbook template, the criteria for pushing notifications to senior staff or specific members of Box Manufacturing were not included. SOC Analysts can refer to the workflow charts as well to confirm if further notifications need to be pushed depending on the severity of the incidents.
- References: (iCybersecurity, 2021) (CloudGoogle, 2023) (Security Orchestration and Automation Playbook, 2019)

REFERENCES

Cloud, G. (2023). *Top Security Playbooks.* Whitepaper.

i, C. a. (2021). *Cybersecurity Incident & Vulnerability Response Playbooks.*

(2019). *Security Orchestration and Automation Playbook.* Rapid7.

Standard operating procedures (SOPs) - definition & overview. (2022). Retrieved from Sumo Logic: https://www.sumologic.com/glossary/standard-operating-procedures-sops/

Wagner, A. (2018, July 01). *The SOC methodology*. Retrieved from Secure Global: https://secureglobal.de/the-soc-methodology