**Brute Force Attack Workflow & Playbook**



Author: Sukhvir Kaur Sahota

Organization: Box Manufacturing

# **Table of Contents**

[**Executive Summary 2**](#_gbqfezrojoho)

[**Introduction 2**](#_3904eluvh9mj)

[**Incident Response Plan 3**](#_9i7j4h5lqnex)

[**Brute Force attack Incident response Playbook Plan 4**](#_dz87iq397516)

[**Explanation and Involved People 11**](#_5o24a89t4ewo)

[**Flow Diagram of Playbook Scenario 14**](#_epv095s7jzuj)

[**Conclusion 16**](#_92rewsfolo1r)

[**Appendix: Technical Letter to 3rd Party 16**](#_8bryxvl20b7u)

[**Appendix: Non-Technical Letter 18**](#_1ur0ee5gnimn)

[**Appendix: Contact Information 19**](#_bhmjrmervyqr)

[**References 19**](#_qj5llso4g4ju)

# 

# **Executive Summary**

Playbooks provide security teams with a single source of truth to turn to in high-pressure situations, helping to ensure response processes are executed systematically and repeatedly. (9)

This Report presents the Brute Force Attack Playbook, which is an Incident response type playbook. The playbook provides the Box manufacturing Company with a standard set of Procedures that help them to Identify, Contaminate, remediate, and recover from a Brute force attack if it happens.

In this report, we used the NIST incident response lifecycle to describe all phases of *pre-* and *Post* data breach. You will find a workflow describing the incidence response workflow and a customized use case diagram for Box manufacturing. The reason to use the playbook is to make sure the SOC team has a step-by-step play and is not relying on any gut feeling of someone in the team while responding to incidents.

The detailed description of incidence response, roles, and responsibilities of team members are described. The end goal of this report is to make sure the Box manufacturing is saved and recovered from the attack and further suggestions for improvement by fixing any vulnerabilities by doing system hardening and patching.

The workflow and playbook would be beneficial, however, the initial planning and continuous training from lessons learned play a vital role for every organization. The SOC team of Box Manufacturing should conduct internal training and should always look for any new vulnerabilities to update their playbook accordingly.

# **Introduction**

Cyber attacks are increasing at a fast pace which makes the job of cybersecurity professionals a little challenging when it comes to response time. Whenever an attack happens the cyber security blue team comes in front as a first line of defense. These teams consist of multiple members with different levels of expertise for better analysis and providing solutions for the issues.

When the team comes in front they need some form of communication flow to work and follow along. This is where the Workflow comes into the picture which consists of steps of communication and also has processes to follow the steps. Organisation’s IT and cyber experts create a playbook that has a plan that outlines the steps that need to be taken care of in the event of an attack or security incident (1)

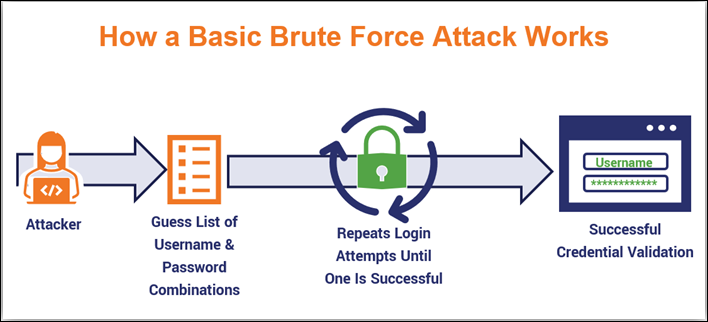
In this report, as a SOC team, we will be working to create a client-specific playbook for Box Manufacturing which is a small manufacturing company specializing in making cardboard boxes for all sizes of Cats. We will focus on SOP (Standard Operating Procedure) which will indicate the instructions of routine operations. The playbook will be a guideline for clients to detect, prevent, and respond to cybersecurity threats.

### **Scenario**

In this project scenario we have Box organization's management, managed security service provider (MSSP), a 3rd party SOC contractor, and we are a SOC specialist.

A Security Operations Center (SOC) is a central unit that deals with security issues at the organizational and technical levels. The SOC analyzes the events made available by the IT security assets and identifies incidents that need to be processed. In a multi-stage escalation procedure, these are processed by the SOC with the help of best practices. (2)

We will create an Incidence Report Playbook for the Brute Force attack. What is a Brute Force Attack? A brute force attack is one of the most popular hacking methods that uses trial and error to crack passwords, login credentials, and encryption keys. The hacker tries multiple usernames and passwords, often using a computer to test a wide range of combinations until they find the correct login information. (3)



**Types of Brute Force Attacks & How They Work(4)**

Brute force attacks refer to both a category of different attack methods as well as a specific attack. Often, they’ll rely on botnets to carry out their attacks at scale. But just what are the different types of brute force methods?

MITRE divides brute force into four main categories:(5)

* Password guessing
* Password cracking
* Password spraying
* Credential stuffing

# **Incident Response Plan**

In Cyber security as per the NIST incident response lifecycle, Incidence plans can be defined in 4 or 6 phases.

We will be discussing Incident response plans with distinct phases that will help SOC and IT professionals deal with cyber attacks. An incident response plan should be set up to address a suspected data breach in a series of phases. Within each phase, there are specific areas of need that should be considered. (6)

The incident response phases are:

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons Learned

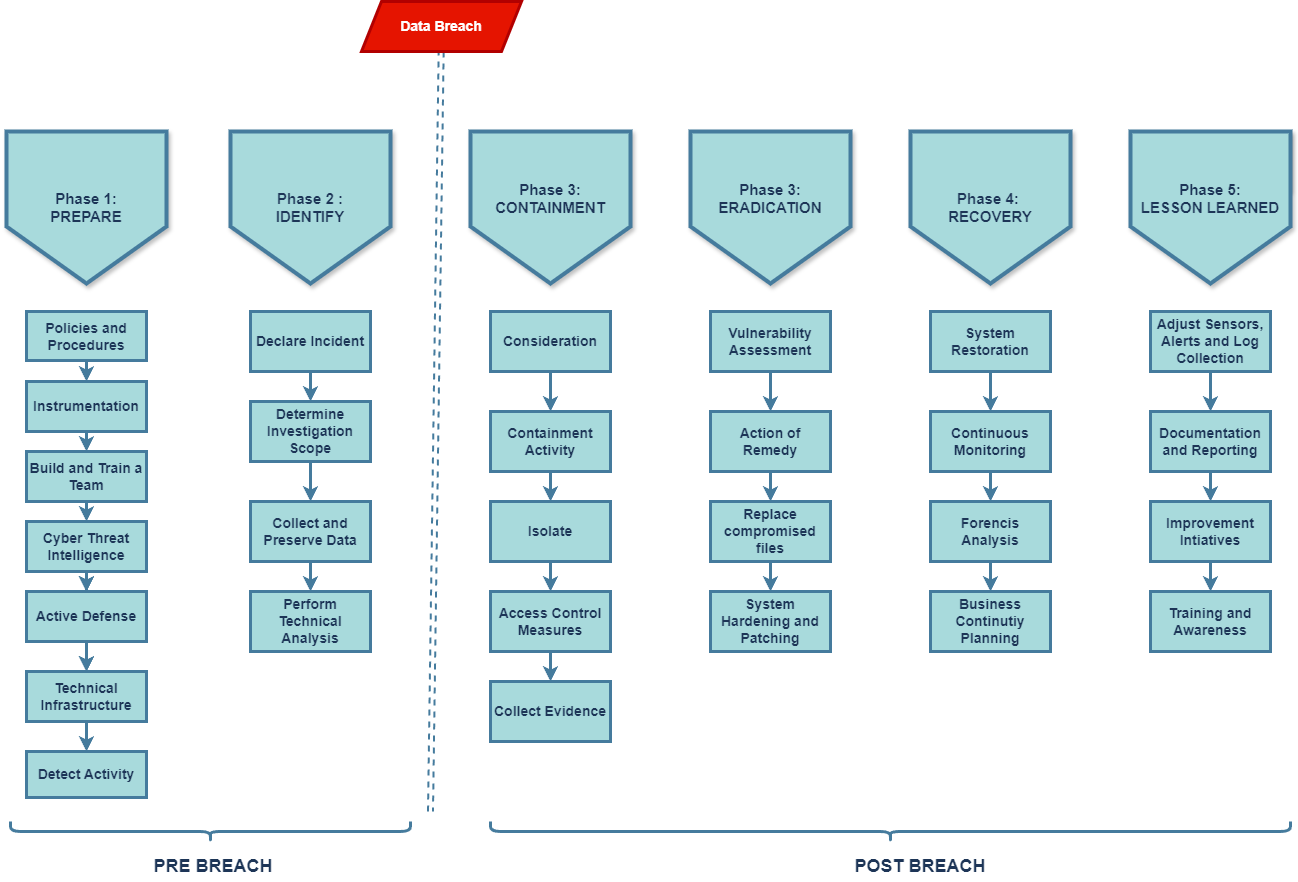
# **Brute Force attack Incident response Playbook Plan**

1. **Preparation**

Preparation is the major and most important step. Preparing for major incidents before they occur can mitigate any impact on the organization and protect business. There could be multiple preparation activities that organizations could consider based on their requirement and budget. (7)

In our playbook, we are focusing on the following Preparation steps:

* 1. **Policies and Procedures:**
* Develop comprehensive policies and procedures outlining the organization's approach to detecting and responding to brute force attacks.
* Establish guidelines for incident categorization, severity assessment, and prioritization based on predefined criteria.
  1. **Instrumentation:**
* Deploy and configure instrumentation tools such as intrusion detection systems (IDS), intrusion prevention systems (IPS), and security information and event management (SIEM) solutions.
* Implement logging and monitoring mechanisms to capture relevant security events, including authentication attempts, failed login attempts, and suspicious activity.
* Ensure that instrumentation tools are properly integrated and aligned with the organization's security objectives and incident response requirements.

****

*The Workflow above is based on the Pre and Post Branch of Brute force. I have used draw.io, online workflow creation tool to create the diagram. (10)*

* 1. **Build and Train team:**
* Build a dedicated incident response team comprising individuals with diverse skills and expertise, including cybersecurity analysts, network engineers, and system administrators. From the case Scenario, one set of team could be
  + Percy F. (CEO)
  + Misha F. (Shift and Production Manager)
  + Cat (MSSP Consultant)
  + Dusty (Database Specialist)
  + Lucky (IT Support Specialist)
  + Ned (Network Administrator)
* Provide comprehensive training and ongoing skill development opportunities to enhance the team's proficiency in detecting, analyzing, and mitigating brute force attacks.
  1. **Cyber Threat Intelligence:**
* Actively monitor intelligence feeds for threat or vulnerability advisories from government, trusted partners, open sources, and commercial entities.
* Establish processes for collecting, analyzing, and disseminating cyber threat intelligence related to brute force attacks and emerging threat actors.
  1. **Active Defense:**

Develop proactive measures and countermeasures to disrupt, deter, and mitigate brute force attacks before they escalate into security incidents.

Implement techniques such as rate limiting, account lockout policies, and CAPTCHA challenges to thwart automated brute force attempts.

* 1. **Technical Infrastructure**:
* Evaluate the organization's technical infrastructure to ensure it is resilient and capable of withstanding brute force attacks.
* Implement network segmentation, firewalls, and intrusion prevention systems to enforce access controls and monitor network traffic for suspicious activity.
  1. **Detect Activity:**
* Leverage threat intelligence to create rules and signatures to identify the activity associated with the incident and to scope its reach.
* Configure tools and analyze logs and alerts.

1. **Identify**

In this step the SOC team determines whether the organization has been breached or not. A breach, or incident, could originate from many different areas.(6)

* 1. **Declare Incident :**
* If any Suspicious activity related to brute force attack is detected, immediately declare an incident to initiate the response process.
* Informa the immediate point of contact (POC) or incident coordinator responsible for overseeing the incident response efforts and coordinating with relevant stakeholders.
* In our case it will be:
  + Misha F. (Shift and Production Manager)
  + Cat (MSSP Consultant)
  1. **Determine the Investigation scope :**
* Use the available data to identify the nature and scope of the brute force attack to determine the extent of potential compromise and impact on the organization's systems and data.
* Define the boundaries of the investigation, this could include the affected systems, users, and network segments. The purpose of this is to focus response efforts effectively.
  1. **Collect and Preserve Data :**
* Collect and preserve relevant data and evidence related to the brute force attack. This include :
  + log files
  + system snapshots
  + network traffic captures
  + user authentication records.
* When necessary and possible, such information should be preserved and safeguarded as best evidence or use in any potential law enforcement investigation.(7)
  1. **Perform Technical Analysis :**
* Conduct technical analysis of the collected data to identify patterns, signatures, and indicators of the brute force attack.
* Analyze the collected logs to determine the source, frequency, and methods used in the attack.

1. **Containment**

Before taking any further measure it is important to implement containment measures. The objective is to prevent further damage and reduce the immediate impact of the incident by removing the adversary’s access.(7)

* 1. **Consideration** :
* Find the scope and severity of the brute force attack. Determine which systems or accounts have been compromised or are at risk.
* Evaluate the effectiveness of existing security measures to find if any vulnerabilities were exploited.
* Consider potential collateral damage and prioritize containment efforts accordingly.
* Identify the source of the attack and any patterns or indicators of compromise (IOCs).
  1. **Containment Activity**
* Start the procedure to contain the attack and minimize its spread.
* Disable compromised accounts or services to prevent further unauthorized access.
* Capturing forensic images to preserve evidence for legal use (if applicable) and further investigation of the incident.(7)
  1. **Isolate**
* Isolate compromised systems or accounts from the network to prevent further unauthorized access.
* Use firewalls, access control lists (ACLs), or network segmentation techniques to contain the attack within a limited area.
* Quarantine affected devices or users until they can be thoroughly investigated and cleaned of any malicious activity.
* Coordinate with other teams, such as network operations or system administrators, to ensure that isolation measures are implemented effectively without disrupting critical business operations.
  1. **Access Control measures**
* Blocking (and logging) of unauthorized accesses; blocking malware sources.
* Closing specific ports and mail servers or other relevant servers and services.
* Changing system admin passwords, rotating private keys, and service/application account secrets where compromise is suspected and revocation of privileged access.
* Monitor user activity and implement anomaly detection mechanisms to identify suspicious behavior indicative of further intrusion attempts.
* Consider deploying deception technologies or honeypots to lure attackers away from critical assets and gather intelligence on their tactics, techniques, and procedures (TTPs).(7)(8)
  1. **Collecting Evidence**

In the Previous step we have collected logs and other data. In this step document any changes or anomalies observed during the attack, including timestamps, IP addresses, and user activities.

1. **Eradication**

After successful containment of the issue, you need to find and eliminate the root cause of the breach. The main objective of this Phase is to make sure to eliminate the artifacts of the incidence.

* 1. **Vulnerability Assessment**
* Conduct a vulnerability assessment to identify any weaknesses or gaps in your defense system..
* Take help of automated scanning tools and manual techniques to detect vulnerabilities in software, configurations, and infrastructure.
* Prioritize vulnerabilities based on severity and potential impact on the organization's operations.
* Additional step : Collaborate with system administrators and IT teams to address identified vulnerabilities promptly.
  1. **Action of Remedy**
* Develop a plan of action to address the vulnerabilities identified during the Vulnerability assessment phase.
* Assign responsibilities to relevant individuals of your SOC team for remediation tasks.
* Implement remediation measures according to the severity and criticality of each vulnerability. Make sure to consider the CIA triad while doing that.
* Monitor the progress of remediation efforts and track completion to ensure that all identified vulnerabilities are addressed effectively.
  1. **Replace compromised files :**
* Replace compromised files with clean, unaltered versions from secure backups or trusted sources.
* Test the integrity of replaced files to ensure that they have not been further modified or corrupted.
  1. **System hardening and patching**
* Do a system Hardening by removing or disabling unnecessary services, implementing firewall rules, and configuring access controls.
* Do a patching wherever required by updating the firewall, Do network Segmentation, configure access control.
* Use a Script to automated patch management tools to streamline the patching process and ensure timely updates across all systems.

1. **Recovery**

This is the process of restoring and returning affected systems and devices back into your business environment. The main challenge of this phase is to make sure of the steps taken for remediation has been successful or not.(6)(7)

* 1. **System Restoration**
* Restore affected devices, systems and services to their pre-incident state using backups from time when there was no attack.
* Test the restored system for its integrity to ensure that they are free from any malicious activity and to make sure they are functioning as expected and are resilient to further attacks.
  1. **Continuous Monitoring**
* Configure alerts and thresholds to notify SOC analysts of suspicious activities or anomalies in real-time.
* Implement continuous monitoring tools and processes to detect any signs of recurring brute force attacks or other security incidents.
  1. **Forensic Analysis**
* In previously collected data conduct a detailed forensic analysis or involve the Forensic team.
* understand its origins, tactics, and impact on the organization.
* Identify any weaknesses or gaps in existing security controls and procedures that may have contributed to the success of the attack.
* Document findings and lessons learned from the forensic analysis to improve incident response processes and enhance security defenses.
  1. **Business Continuity Planning**
* Identify critical systems, applications, and data assets that require prioritized protection and recovery measures.
* Communicate with stakeholders, including executive leadership and business unit managers, to reinforce the importance of business continuity planning and resilience.

1. **Lesson Learned / Review**

Our job is not done even after the successful recovery. After completing the investigation, it is important to have an after action meeting with your team, management and IT team to discuss your learnings for this data breach.

* 1. **Adjust Sensor, Alerts and log collection**
* Review existing sensors, alerting mechanisms, and log collection strategies to identify any gaps that may have impacted the detection or response to the brute force attack.
* Adjust monitoring sensor configurations in your network monitoring tools to enhance visibility into relevant network and system activity, ensuring that critical events are adequately monitored..
* Expand log collection capabilities to capture additional data sources or enrich existing logs with contextual information for more effective analysis.
  1. **Documentation and Reporting**
* Document key findings, observations, and actions taken during the incident response process, including timelines, response activities, and outcomes.
* Generate incident reports summarizing the details of the brute force attack, its impact on the organization, and the effectiveness of response efforts.
* Communicate incident findings and recommendations to relevant stakeholders, including executive leadership, IT teams, and other business units.
  1. **Improvement Initiatives**
* Identify improvement opportunities based on lessons learned from the brute force attack and other security incidents.
* Prioritize improvement initiatives according to their potential impact on security posture and operational efficiency.
* Develop action plans to address identified weaknesses or deficiencies in security controls, processes, or technologies.
  1. **Training and Awareness:**
* Conduct security awareness training sessions for employees to educate them on the risks associated with brute force attacks and other common security threats.
* Provide guidance on best practices for password management, authentication, and incident reporting to empower employees to play an active role in maintaining security.

By incorporating these steps into your SOC playbook, you can effectively recover from the brute force attack, minimize its impact on the organization, and strengthen your defenses against future security incidents.

# **Flow Diagram of Playbook Scenario**

# 

# **Explanation and Involved People**

1. **Build Team in Initial Phase**

* Cat : Consultant at MSSO
* Misha: Production Manager
* Minka: Alternative Production Manager
* Dusty: Database Specialist
* Lucky: IT Support Specialist
* Ned: Network Administrator

1. **Initial Phase of Identification**

* ***Initial Detection***: The SOC, through continuous monitoring, identifies suspicious login attempts which Indicate the Brute Force Attack.
* **Notification** : SOC contacts Cat, the designated MSSP liaison. Cat evaluates the severity and urgency of the Attack.

Trigger: Confirmation of a confirmed or suspected breach

1. **Client Confirmation**

* ***Person Involved*** :
  + Cat from MSSP
  + Miss Misha F ( if the attack happened on Weekdays from (9 AM to 5PM)
  + Minka F ( if its weekend or after hours on Weekdays
* ***Steps Taken***
  + Cat, as the primary contact at the MSSP, receives alerts regarding the detected incident and initiates the incident response process.
  + Cat Contacted with Box Manager ( whoever is available) to confirm the Impact of Breach.

1. **Investigation and Analysis**

The Team decides to work together to do technical Analysis, find Root Cause and to Collect Data for Forcensic as follows

* ***Technical Analysis***: Cat asks Dusty ( the database specialist) to conduct a detailed analysis of the attack vectors and compromised systems.
* ***Root Cause Analysis***: Lucky (IT support specialist) assists in identifying any vulnerabilities or misconfigurations that facilitated the attack.
* ***Data Collection***: Ned (the network administrator) gathers relevant logs and forensic evidence for further analysis.

1. **Containment, Eradication, and Recovery**

* ***Containment:*** Based on the findings, Cat and Dusty collaborate to implement immediate containment measures to halt the attack's progression. Such as Ip and Source.
* ***Eradication:*** Cat and Lucky work together to eradicate the attacker's footprint from the system, patching any identified vulnerabilities.
* ***Recovery:*** Ned oversees the restoration of affected systems and data from backups to minimize downtime.
* ***Resolution:*** Team, Verify successful containment and restoration of affected systems and Confirmation of breach resolution and system stability.

1. **Escalation**

* ***Internal Escalation(Only if needed)*:** Cat escalates the incident to Percy only if deemed urgent or unresolved after 48 hours, adhering to the client's preference.
* ***External Notification*:** Cat promptly notifies Misha during business hours and Minka after hours, ensuring timely communication with Box's management.

1. **Post-Incident Review and Documentation**

* ***Debriefing***: Cat conducts a post-incident debriefing session with the internal team to review lessons learned and identify areas for improvement.
* ***Documentation***: Cat prepares an incident report detailing the incident timeline, response actions taken, and recommendations for future mitigation.

# **Conclusion**

To be concluded, this Incident Response Workflow and Client Playbook provide a comprehensive framework for Box Manufacturing to effectively respond to cybersecurity incidents. We have provided the detailed Explanation along with steps taken and roles and response. By following the steps and Procedures as described, Box manufacturing can mitigate risks, minimize impact, and ensure business continuity.

# **Appendix A: Technical Letter to 3rd Party**

Dear Cat,

I hope this message finds you well. I am reaching out to inform you of a recent incident that has been detected within our client, Box Manufacturing's network. As you are a designated MSSP consultant overseeing the Security Needs of Box Organisation’s security needs, it is crucial for you to be aware of the incident and to provide your expertise in managing and mitigating the situation. The Incidence Details are as follows:

| **Type** | Brute Force Attack |
| --- | --- |
| **Affected Entity** | Box Manufacturing |
| **Detection Date and Time** | 26th April, 2022 (18:00) |
| **Initial Detection Source** | SOC monitoring systems |

| **Summary of Incident** |
| --- |
| * The incident involves multiple unauthorized login attempts targeting various systems and accounts within Box Manufacturing's network. * Initial analysis indicates characteristics consistent with a Brute Force Attack, with the warning attempting to gain unauthorized access by systematically trying different username and password combinations. |

| **List of Trigger Items Affecting Incident Response Workflow** |
| --- |
| * **High Volume of Failed Login Attempts**: A significant increase in failed login attempts has been observed across multiple systems and accounts, indicating a potential security threat. * **Unusual Authentication Patterns**: Patterns of authentication attempts deviating from normal user behavior have been detected, raising suspicion of malicious activity. * **Multiple Accounts Locked Out**: Several user accounts have been automatically locked out due to repeated failed login attempts, signaling a potential brute force attack. * **Anomalies in Network Traffic**: Unusual spikes in network traffic associated with authentication processes have been identified, suggesting automated login attempts. |

| **Rationale for Incident Escalation** |
| --- |
| * **Severity of Threat**: A Brute Force Attack poses a significant risk to Box Manufacturing's security posture, potentially compromising sensitive data and disrupting business operations. * **Client Impact**: Given Box Manufacturing's reliance on our services for security oversight, it is imperative to promptly address and mitigate any security incidents to maintain client trust and satisfaction. * **Need for Specialized Expertise**: Brute Force Attacks require specialized knowledge and expertise in cybersecurity incident response, making your involvement as our MSSP consultant crucial in effectively managing the incident. |

| **Requested Action** |
| --- |
| We kindly request your immediate attention and assistance in coordinating the incident response efforts, including:   * Conducting detailed technical analysis to identify attack vectors and mitigate the threat. * Providing recommendations for containment, eradication, and recovery strategies tailored to the specific incident. * Collaborating with our internal team and client stakeholders to ensure a coordinated and effective response. * Your prompt response and collaboration in addressing this incident are greatly appreciated. |

Best regards,

Sukhvir Sahota

SOC Specialist

# **Appendix B: Non- Technical Letter**

Dear Box Manufacturing team,

I hope this message finds you well.

I am writing to inform you of an ongoing situation that requires your attention. At this time, our team has detected an incident within your network that may potentially impact your operations. While I understand the technical aspects of the incident may not be of immediate concern to you, it is important for us to keep you informed of any developments that may affect your business.

Please be assured, we are taking proactive measures to address the situation and mitigate any potential impact. Our team is working diligently to investigate and resolve the issue, and we will keep you updated on our progress.

If you have any questions or concerns, please do not hesitate to reach out to me directly. Your understanding and cooperation are greatly appreciated as we work to ensure the security and stability of your systems.

Best regards,

Sukhvir Sahota

SOC Specialist

# **Appendix C: Contact Information**

**Box Manufacturing Management:**

* Percy F.: percy@box.cat
* Miss Misha F.: misha@box.cat | Phone: 902-9836 (Weekdays)
* Minka F.: minka@box.cat | Phone: 562-7658 (After hours and Weekends)

**Internal Specialists:**

* Dusty: dusty@box.cat | Phone: 462-8952
* Lucky: lucky@box.cat | Phone: 269-5466
* Ned: ned@box.cat | Phone: 877-4332

**External MSSP & SOC:**

* Cat: cat@soc.cat | Work Phone: 905-4616 (Daytime) | Cell: 902-4321 (After-hours)

# 

# **References**

1. Cofense. (2023, August 22). *What is Cybersecurity Playbook? | Learn how Cofense helps*. Cofense. <https://cofense.com/knowledge-center/what-is-a-cyber-response-playbook/#:~:text=What%20is%20a%20security%20playbook,incidents%20with%20cyber%20response%20playbooks>.
2. Wagner, A. (2018, June 19). The CSIRT methodology - SecureGlobal. SecureGlobal. <https://secureglobal.de/the-csirt-methodology>
3. What is a Brute Force Attack? | Definition, Types & How It Works. (n.d.). Fortinet. <https://www.fortinet.com/resources/cyberglossary/brute-force-attack>
4. Crane, C. (2023b, March 31). A brute force attack definition & look at how brute force works. Hashed Out by the SSL StoreTM. <https://www.thesslstore.com/blog/brute-force-attack-definition-how-brute-force-works/>
5. MITRE ATT&CK®. (n.d.). <https://attack.mitre.org/>
6. 6 phases in the Incident Response plan. (n.d.). Securitymetrics. <https://www.securitymetrics.com/blog/6-phases-incident-response-plan>
7. Cybersecurity and Infrastructure Security Agency. (2021). Federal Government Cybersecurity Incident & Vulnerability Response Playbooks. In Cybersecurity and Infrastructure Security Agency. <https://www.cisa.gov/sites/default/files/2024-03/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf>
8. What is Deception Technology? | Rapid7. (n.d.). Rapid7. <https://www.rapid7.com/fundamentals/deception-technology/>
9. Chronicle. (2022). Top Security Playbooks (Third Edition) [Whitepaper]. <https://learningimages.lighthouselabs.ca/Cyber+BC/Cyber+BC+C4/Top_Security_Playbooks_2022.pdf>
10. draw.io - free flowchart maker and diagrams online. (n.d.). <https://app.diagrams.net/>