WEEK 4 Day 5 PROJECT

Cybersecurity Playbook for BOX

Submitted By: NAVNEET KAUR

Contents:

EXECUTIVE SUMMARY

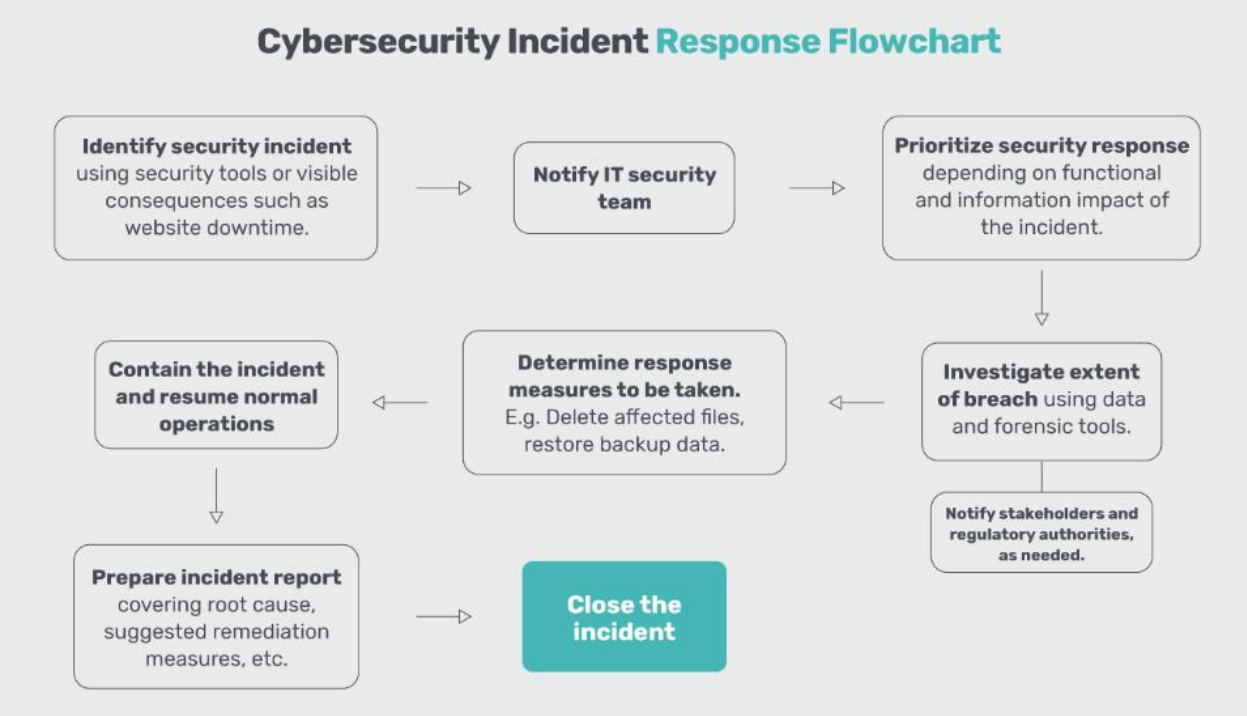
This scenario BOX is a small company that manufactures cardboard boxes for all sizes of cats. And CAT is a consultant that works for Managed Security Service Provider (MSSP) and hired by BOX to look after their security needs. Mr. Percy the CEO of BOX has contracted the SOC to monitor their network, system and data of the company. Mr. Percy wants a manual with all instructions to stop or remediate the RANSOMWARE attack from CAT since CAT is overseeing all of their security needs.

As a small manufacturing company, RANSOMWARE is most common cyber threat because it leads to stolen credential, phishing emails that cause a financial and reputational harm to small companies.

I'm working as Incident Response Designer in this scenario to create playbook and workflow for BOX and CAT.

This playbook would apply to BOX and third part providers

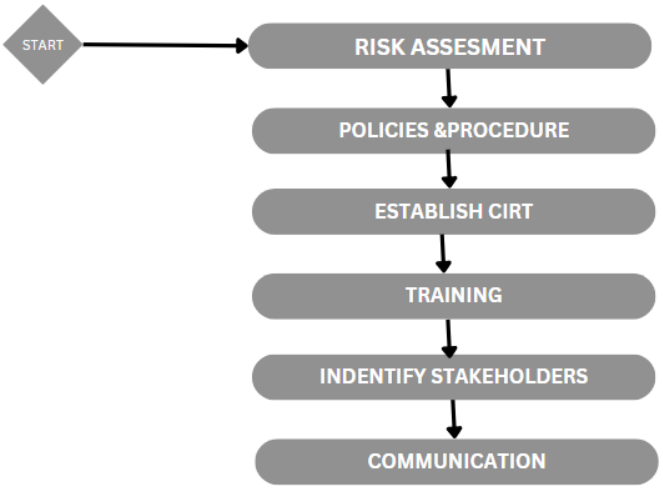
INCIDENT RESPONSE PLAYBOOK FLOW CHART



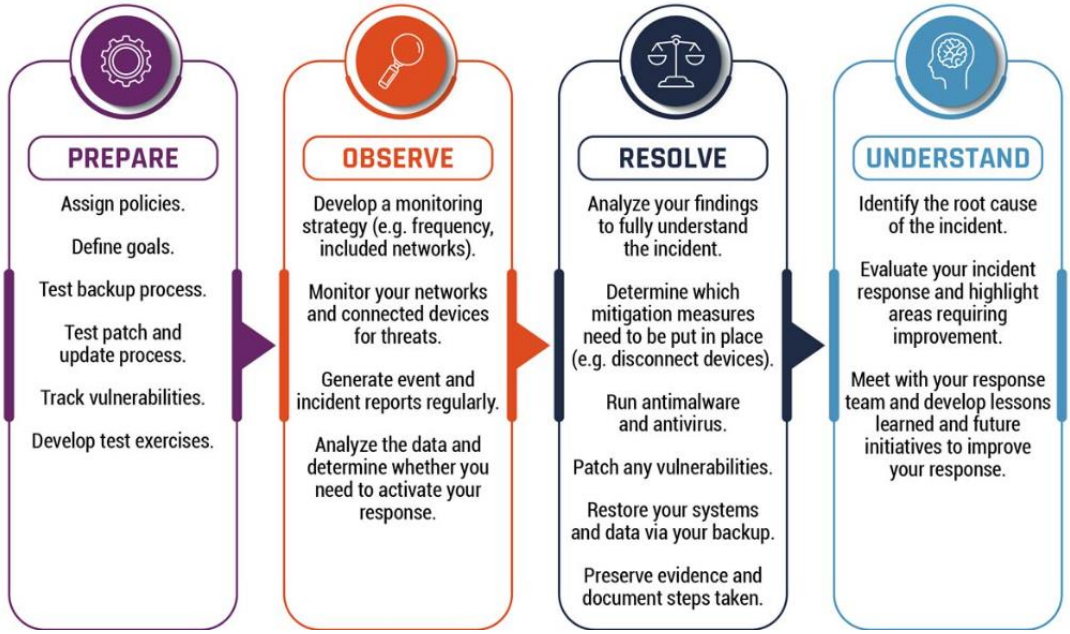
This playbook provides a description of the incident response process if an attack occurs and provides the set of instructions to mitigate that attack in efficient and in timely manner.

It includes Preparation, Detection and Analysis, Containment, Recovery and Post-incident activities in case of ransomware, phishing attack.

INCIDENT RESPONSE CHECKLIST



SOC WORK FLOW for INCIDENT RESPONSE PLAN



PREPARTION PHASE:

In this initial phase, the threat actors used phishing to infect the system, hence its responsibility of Incident Response team to investigate and create a phishing policy for the company. Using phishing policy, the routine tests for the phishing may significantly decrease the chance of compromised by ransomware. The playbook guides the employees and third part providers to detect the phishing emails before they click the malicious links. The preparation phase must include the following steps:

1. Identify all users, operators and all roles and responsibilities
2. Implement cyber security solutions for defense in depth using SIEM, MFA etc.
3. Anti-social engineering attack preparation
4. Backup of critical assets
5. Implement patch management

DETECTION & ANALYSIS PHASE:

It is highly recommended practice to use threat intelligence source to detect the attack and then analyse it to prevent the impact of the attack. In this phase IPS, IDS prevention system can be used to detection and preventions after that performing full scan on the whole network infrastructure of the BOX with SIEM to monitor the logs and File activity control to check the files modifications. The following steps in must in action in this phase:

1. Performing IDS/IPS signatures and IOS's implementation
2. Perform full scans and implement cyber solutions such as SIEM, FIM and EDR(endpoint, malware detection, scanning and protection)
3. Check the hash of the email attachments or any suspicious file
4. Manual intervention and detection

CONTAINMENT:

The objective is to prevent further damage and reduce the immediate impact of the incident by removing adversary's access. In the case of ransomware attack, the process of the system corruption and encryption will not take much time, hence we have limited time to take actions. Endpoints must be isolated from the network to stop the spread of attack. The steps must be taken in this phase are:

1. Identify affected assets
2. Physical Isolate and contain potential threat sources such as blocking external IP address, external domain, external URL, block sender on emails
3. Identify the vulnerability that cause the exploitation and contain fir remediation such as reconfigure the firewall and continue to monitor the malicious activities and block the backdoor entrance for threat actors

RECOVERY:

Recovery plan should be aligned with the incident response and backup plans. In this scenario, we will identify the third part stakeholders, vendors and managers and their roles and responsibilities. We will take the inventory of hardware, secure the logins and passwords with MFA, passwords should be changed after specific time limit, invest in cyber security insurance and prepare the emergency documents, such employee, vendor list so that quickly react and inform in case of ransomware attack. Following are the steps in recovery phase:

1. Identify affected assets
2. Prepare backups
3. Perform scans and preventive measures
4. Restore the system
5. Continuous monitoring

LIST OF TRIGGER ITEMS

In this scenario, the workflow of detecting the security breach:

- The detection of security incident through SOC monitoring or other means
- Receipt of a report from an employee or system indicating a potential security breach
- Confirmation of an attack during the SOC investigation
- Impact of assessment of the cyber attack
- Completion of the incident report for approval by CAT

These are the basic list of triggers in case of ransomware attacks.

1. Unusual network activities
2. Abnormal file access
3. Suspicious emails
4. Antivirus alerts
5. File encryption
6. User reports
7. Unwanted processes
8. Failed backup
9. Data corruption
10. System outages

A sample or letter template to the client

Mr. Percy, CEO

Box Manufacturing

percy@box.ca

Calgary, Alberta.

Subject: Cyber security playbook for the company

Dear Mr. Percy,

I hope this letter finds you well. I have created a manual and set of instructions known as playbook in case of cyber-attacks on the company. It includes detail instructions of how to detect, prepare and mitigate the cyber threats. There are some flow charts also to with simple layman's term so everyone can easily understand the terms.
Please feel free to reach out, if you have any questions, concerns or additional information. We are here to support you during any security breach and will work diligently to resolve the issue.

Sincerely,
Navneet kaur

A sample or letter template to the third party provider CAT

External MSSP & SOC security Oversight

CAT

cat@soc.cat

Subject: Suspected Data Breach Incident - Request for Incident Response Support
Dear CAT,
I hope this letter finds you well. We are writing to inform you about a suspected data breach incident involving our esteemed client, BOX manufacturing. As a third-party provider with expertise in incident response and cybersecurity, we kindly request your support and assistance in handling this critical matter. I have created a playbook for ransomware attack on company which has detailed steps of instructions how to detect, investigate and prevent the attack. I understand the importance of maintaining the highest level of security and confidentiality throughout this process.
If you have any question, please feel to contact.
Regards,
Navneet

CITATION:

https://www.dts-solution.com/ransomware-incident-response-plan
https://www.cyber.gc.ca/en/guidance/top-measures-enhance-cyber-security-small-and-medium-organizations-itsap10035
https://www.cyber.gc.ca/en/guidance/developing-your-it-recovery-plan-itsap40004
https://www.rapid7.com/globalassets/_pdfs/whitepaperguide/rapid7-insightidr-ransomware-playbook.pdf