BOX COMPANY

Incident Response Playbook

Zehra Nur Ozer

May 2024

Table of Contents

Introduction

This playbook provides an incident response workflow for Box Company, in collaboration with the SOC Team and Managed Security Service Provider (MSSP), to manage potential ransomware incidents. The steps this playbook follows are designed based on a standard set of procedures to identify, coordinate, remediate, recover from, and document incidents with a minimum impact on Box Company's operations.

Ransomware is a popular attack vector that involves holding an organization's data hostage and threatening destruction unless a ransom is paid. (Top_Security_Playbooks)

The playbook is structured into several key steps: preparation, detection and analysis, containment, eradication and recovery, post-incident activity, and coordination. Each step will be explained in detail, providing a comprehensive guide for managing potential ransomware incidents.

Preparation

The preparation step starts before the incident occurs. The goal is to be ready for any potential malicious activities. This phase can be broken down into six steps of preparation activities to understand the expectations.

The first activity is establishing the baseline in the network. This allows the team to determine a "normal." This activity allows us to limit the recovery time after containment. Decisions on the access levels and 3Ps (policies, procedures and personnel) significantly impact this phase.

Policies: Creating a team hierarchy will later help the team escalate issues, and preparing a contingency plan will help the team contact the legal authority and law enforcement at the right time.

Instruction: This step is crucial for maintaining the basics. According to Executive Order 14028, Develop and maintain an accurate picture of infrastructure (systems, networks, cloud platforms, and contractor-hosted networks) by widely implementing telemetry to support system and sensor-based detection and monitoring capabilities such as antivirus (AV) software; endpoint detection and response (EDR) solutions. (federalregistergov)

Cyber Threat Intelligence: This step shows the importance of communication with the other agencies. Integrating the system into SIEM and actively monitoring the threats or vulnerabilities are other steps that can be taken in this step.

Training: Ensuring the team is trained according to current threats is also crucial in preparation.

Detection & Analysis

This is the most challenging phase of the incident response process. Until now, the team prepared for the scenario, and at this point, all the phases occur after, and an alert is considered an incident.

This phase again can be divided into detection, declaring an incident, collection and preservation, and tool adjustment. At this point, the topic will be considered a ransomware attack.

Detection: A suspicious activity has occurred, and the SOC created a ransomware alert. The team also advised coordinating with a third-party agency before declaring the attack.

Declaration of the incident & determine investigation scope: Regardless of severity, every incident should be informed to CISA. In this step filling out the form and submission plays an important role. As the preparation phase creates the baseline, determining the scope helps the team to discover the malicious activity by following network data, firewall, proxy logs, etc. (cisagov)

Collect & Preserve Data: The team collects data from the perimeter, the internal network, and the endpoint. When necessary and possible, such information should be preserved and safeguarded as the best evidence for use in any potential law enforcement investigation. (cisagov)

Technical Analysis: In this step, the team needs to correlate the data to identify IoCs and TTPs. To find the answer to “What systems are detected?” as well as “What is the ransomware variant?”

Until the end of the detection and analysis phase, the team is unable to determine how to encapsulate the malicious attack. At that point, it is wise to modify the tool to slow down and minimize the data filtration, so the attack has less chance of spreading within the network.

Containment

Even though Containment is close to Detection and analysis, this phase is the most important in the playbook. This phase is the confirmation of the ransomware attack. By isolating the impacted system, the team now stops the spread. Consideration and containment activities can be the steps for this phase.

Considerations: If the incident blocking your access to data or ability of process, it is time to reevaluate. This step helps the team to determine the attacker's capability. It is also vital that the team should communicate with other agencies to inform them about the ransomware variant.

Containment activities: At this step, the team starts to take action to return to normal. First, the team should follow the activities of changing passwords, blocking unauthorized access, and updating firewall filtering to be sure they will not give any stealthy way to tip off the attackers.

Eradication & Recovery

The phase of returning to normal. In order to take control, the team continues scanning against any malicious activity. If any detected, the loop goes back again, scanning until no longer incidents are seen.

To help detect related attacks, review cyber threat intelligence (including network situational awareness), and closely monitor the environment for evidence of threat actor activity. (cisagov)

Also, the team should remove the ransomware and malicious attack, discover how the malicious actors got access to the system by now, and clean the system for normal operations.

Post-Incident Activities

Successful recovery and restoration of the system. It can be considered a lesson-learned phase. The goal of the phase is to document the incident and inform the other agencies about precautions. The team should continue monitoring and testing the network. The primary objectives for the analysis include: Ensuring the root cause has been eliminated or mitigated, Identifying infrastructure problems to address, and Identifying organizational policy and procedural problems to address. Reviewing and updating roles, responsibilities, interfaces, and authority to ensure clarity, identifying technical or operational training needs, and improving tools required to perform protection, detection, analysis, or response actions. (cisagov)

Coordination

According to CISA, any incident must be reported to them. After the first submission, the situation is expected to be updated within an hour, and the Ticket assigned by CISA earlier must be closed.

This phase aims to benefit the company and protect others by learning about it. At this point, CISA will also share the incident with cyber intelligence; from that point, they will decide whether to escalate the situation.

References

(n.d.). Retrieved from https://learningimages.lighthouselabs.ca/Cyber+BC/Cyber+BC+C4/Top_Security_Playbooks_2022.pdf

(n.d.). Retrieved from https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

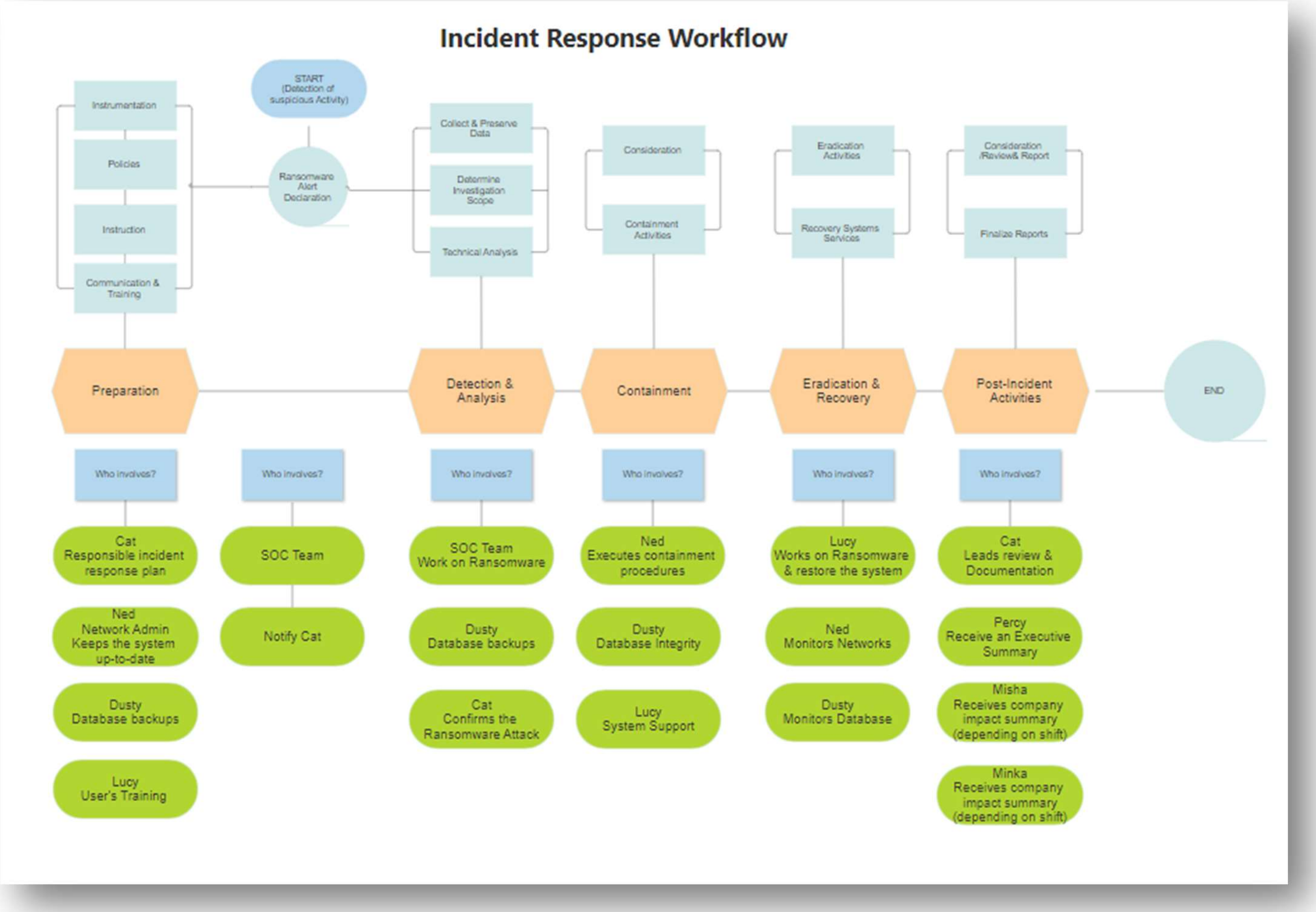
(n.d.). Retrieved from https://www.cisa.gov/sites/default/files/2024-03/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf

(n.d.). Retrieved from https://www.cisa.gov/forms/report

(n.d.). Retrieved from https://www.youtube.com/watch?v=gWXgChC9ANg

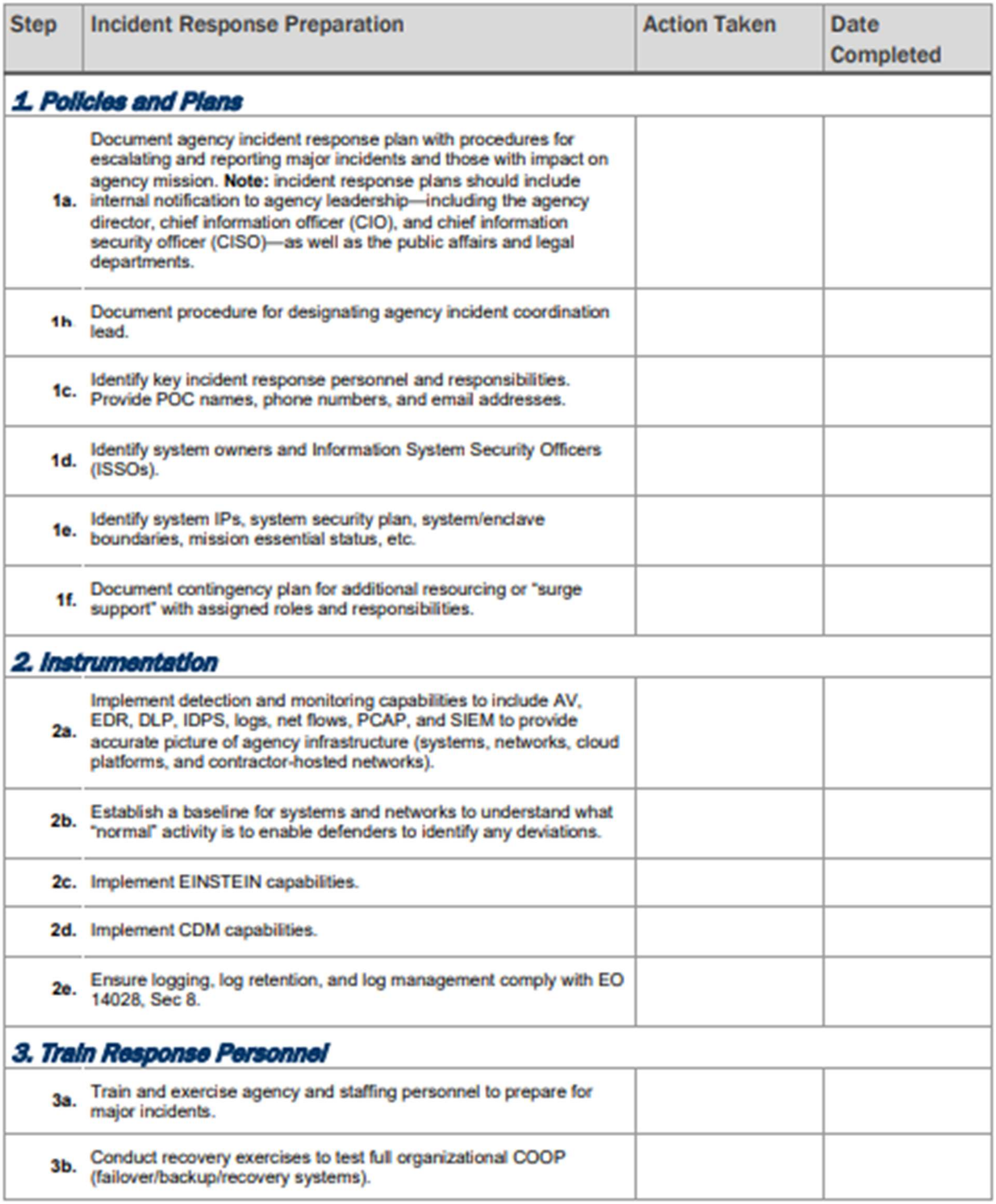
Appendix:

1. Incident Response Workflow

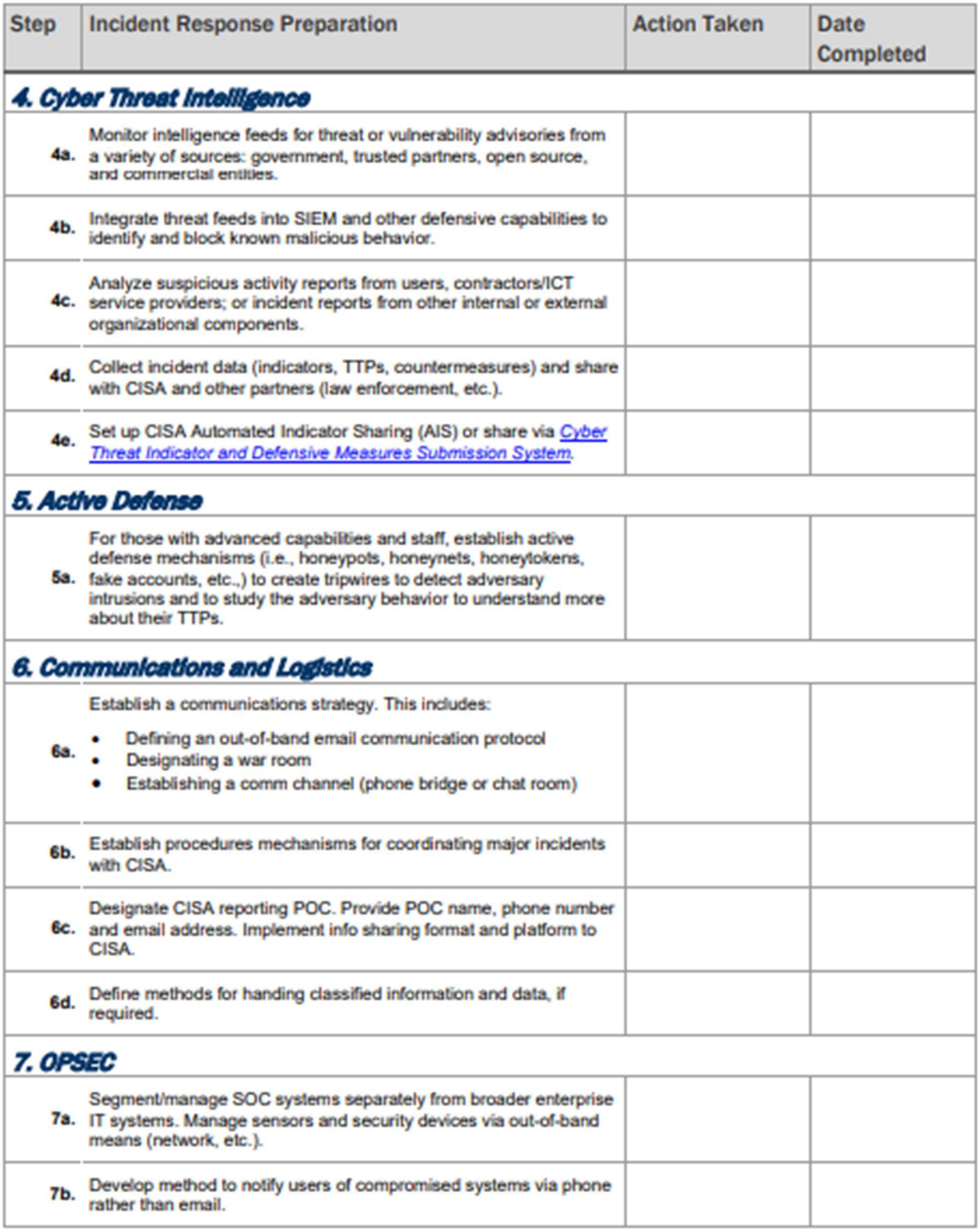

Incident Response Workflow
START (Detection of suspicious Activity)
Ransomware Alert Declaration
Instrumentation
Policies
Instruction
Communication & Training
Collect & Preserve Data
Determine Investigation Scope
Technical Analysis
Consideration
Containment Activities
Eradication Activities
Recovery Systems Services
Consideration /Review& Report
Finalize Reports
Preparation
Detection & Analysis
Containment
Eradication & Recovery
Post-Incident Activities
END
Who involves?
Cat Responsible incident response plan
Ned Network Admin Keeps the system up-to-date
Dusty Database backups
Lucy User's Training
Who involves?
SOC Team
Notify Cat
Who involves?
SOC Team Work on Ransomware
Dusty Database backups
Cat Confirms the Ransomware Attack
Who involves?
Ned Executes containment procedures
Dusty Database Integrity
Lucy System Support
Who involves?
Lucy Works on Ransomware & restore the system
Ned Monitors Networks
Dusty Monitors Database
Who involves?
Cat Leads review & Documentation
Percy Receive an Executive Summary
Misha Receives company impact summary (depending on shift)
Minka Receives company impact summary (depending on shift)

(Prepared using smartdraw.com)

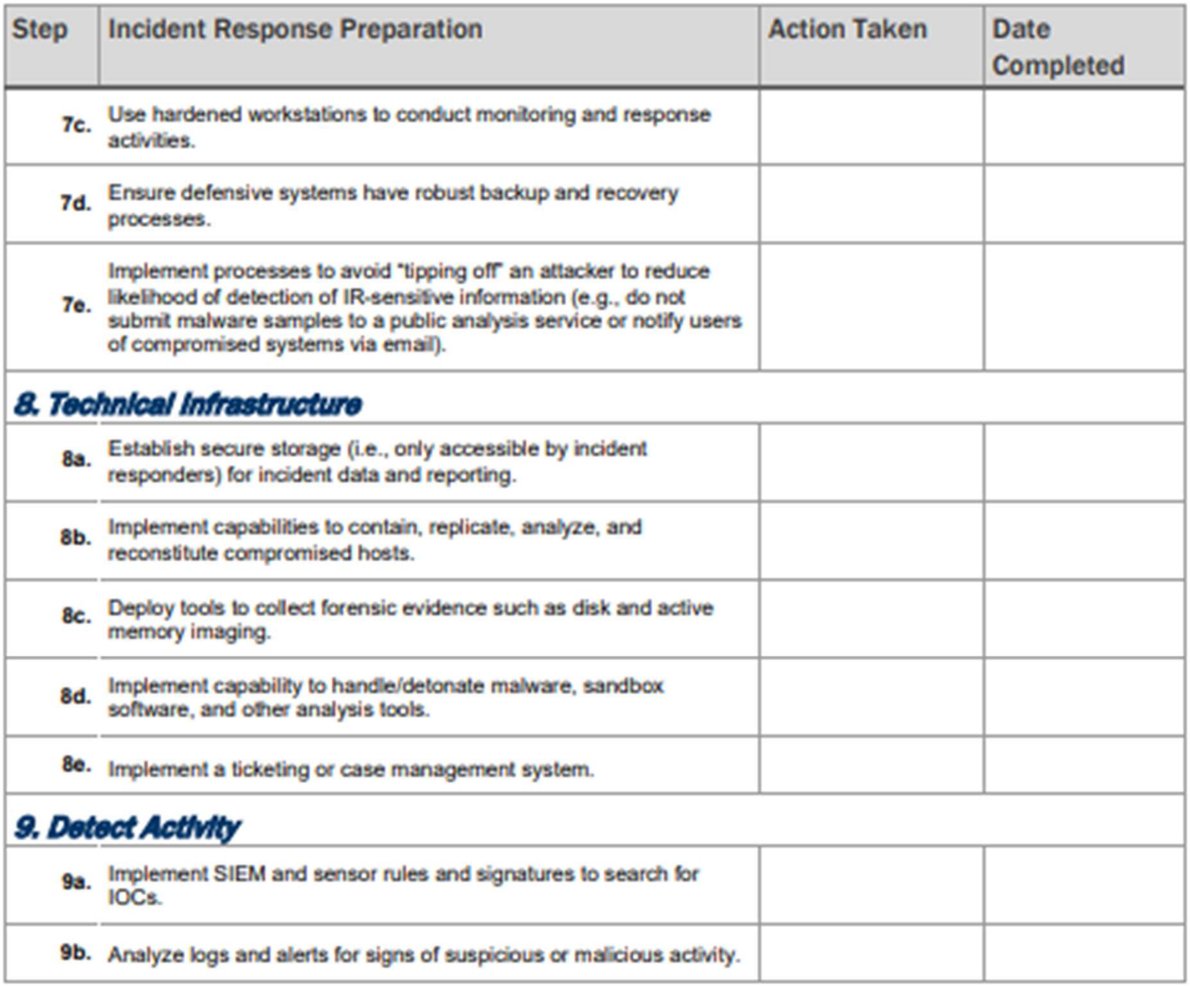
2. Incident Response Preparation Checklist



Step	Incident Response Preparation	Action Taken	Date Completed
1. Policies and Plans			
1a.	Document agency incident response plan with procedures for escalating and reporting major incidents and those with impact on agency mission. **Note:** incident response plans should include internal notification to agency leadership—including the agency director, chief information officer (CIO), and chief information security officer (CISO)—as well as the public affairs and legal departments.		
1h	Document procedure for designating agency incident coordination lead.		
1c.	Identify key incident response personnel and responsibilities. Provide POC names, phone numbers, and email addresses.		
1d.	Identify system owners and Information System Security Officers (ISSOs).		
1e.	Identify system IPs, system security plan, system/enclave boundaries, mission essential status, etc.		
1f.	Document contingency plan for additional resourcing or "surge support" with assigned roles and responsibilities.		
2. Instrumentation			
2a.	Implement detection and monitoring capabilities to include AV, EDR, DLP, IDPS, logs, net flows, PCAP, and SIEM to provide accurate picture of agency infrastructure (systems, networks, cloud platforms, and contractor-hosted networks).		
2b.	Establish a baseline for systems and networks to understand what "normal" activity is to enable defenders to identify any deviations.		
2c.	Implement EINSTEIN capabilities.		
2d.	Implement CDM capabilities.		
2e.	Ensure logging, log retention, and log management comply with EO 14028, Sec 8.		
3. Train Response Personnel			
3a.	Train and exercise agency and staffing personnel to prepare for major incidents.		
3b.	Conduct recovery exercises to test full organizational COOP (failover/backup/recovery systems).		



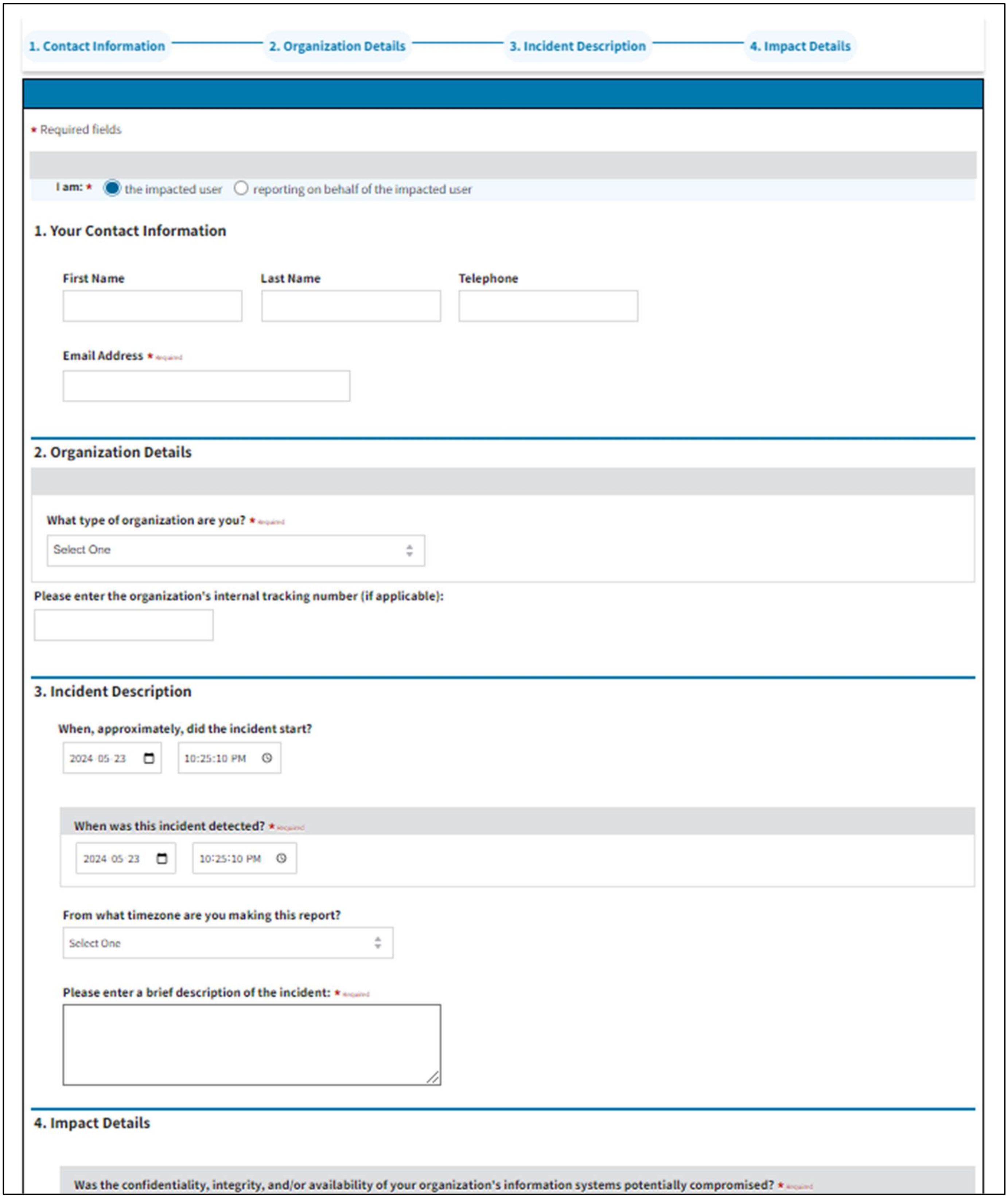
Step	Incident Response Preparation	Action Taken	Date Completed
4. Cyber Threat Intelligence			
4a.	Monitor intelligence feeds for threat or vulnerability advisories from a variety of sources: government, trusted partners, open source, and commercial entities.		
4b.	Integrate threat feeds into SIEM and other defensive capabilities to identify and block known malicious behavior.		
4c.	Analyze suspicious activity reports from users, contractors/ICT service providers; or incident reports from other internal or external organizational components.		
4d.	Collect incident data (indicators, TTPs, countermeasures) and share with CISA and other partners (law enforcement, etc.).		
4e.	Set up CISA Automated Indicator Sharing (AIS) or share via *Cyber Threat Indicator and Defensive Measures Submission System*.		
5. Active Defense			
5a.	For those with advanced capabilities and staff, establish active defense mechanisms (i.e., honeypots, honeynets, honeytokens, fake accounts, etc.,) to create tripwires to detect adversary intrusions and to study the adversary behavior to understand more about their TTPs.		
6. Communications and Logistics			
6a.	Establish a communications strategy. This includes: • Defining an out-of-band email communication protocol • Designating a war room • Establishing a comm channel (phone bridge or chat room)		
6b.	Establish procedures mechanisms for coordinating major incidents with CISA.		
6c.	Designate CISA reporting POC. Provide POC name, phone number and email address. Implement info sharing format and platform to CISA.		
6d.	Define methods for handing classified information and data, if required.		
7. OPSEC			
7a.	Segment/manage SOC systems separately from broader enterprise IT systems. Manage sensors and security devices via out-of-band means (network, etc.).		
7b.	Develop method to notify users of compromised systems via phone rather than email.		



Step	Incident Response Preparation	Action Taken	Date Completed
7c.	Use hardened workstations to conduct monitoring and response activities.		
7d.	Ensure defensive systems have robust backup and recovery processes.		
7e.	Implement processes to avoid "tipping off" an attacker to reduce likelihood of detection of IR-sensitive information (e.g., do not submit malware samples to a public analysis service or notify users of compromised systems via email).		
8. Technical Infrastructure			
8a.	Establish secure storage (i.e., only accessible by incident responders) for incident data and reporting.		
8b.	Implement capabilities to contain, replicate, analyze, and reconstitute compromised hosts.		
8c.	Deploy tools to collect forensic evidence such as disk and active memory imaging.		
8d.	Implement capability to handle/detonate malware, sandbox software, and other analysis tools.		
8e.	Implement a ticketing or case management system.		
9. Detect Activity			
9a.	Implement SIEM and sensor rules and signatures to search for IOCs.		
9b.	Analyze logs and alerts for signs of suspicious or malicious activity.		

(cisagov)

3. CISA Webpage Incident Report Sample



1. Contact Information — 2. Organization Details — 3. Incident Description — 4. Impact Details

* Required fields

I am: * ● the impacted user ○ reporting on behalf of the impacted user

1. Your Contact Information

First Name

Last Name

Telephone

Email Address * required

2. Organization Details

What type of organization are you? * required

Select One

Please enter the organization's internal tracking number (if applicable):

3. Incident Description

When, approximately, did the incident start?

2024-05-23 10:25:10 PM

When was this incident detected? * required

2024-05-23 10:25:10 PM

From what timezone are you making this report?

Select One

Please enter a brief description of the incident: * required

4. Impact Details

Was the confidentiality, integrity, and/or availability of your organization's information systems potentially compromised? * required

Incident Response Emails

The following two pages contain the emails sent to explain the situation after the incident.

The first email is for Mr. Percy (CEO), and the second is for Ms. Cat.

Dear Mr. Percy F.,

I am writing to inform you that a recent ransomware incident occurred within our network 48 hours earlier.

Our security team promptly detected and contained the incident. All affected systems have been restored, and we are currently monitoring for further issues. Mrs. Cat from MSSP and the SOC team also provided a detailed report.

Date of Incident: 05/21/2024 14:30:11

Effected System: Operation systems (a malicious file is downloaded; it executes the ransomware payload)

Nature of attack: Ransomware

Please reach out if you need any further clarifications.

Best regards,

Zehra Nur Ozer

Cyber Security Analyst

Dear Cat,

I hope you had an excellent long weekend. I am sending this email to inform you of a ransomware attack on Box Company's Network.

Please find the attack report below:

Detection: The SOC Team detected suspicious activity in the operating system on May 21, 2024, at 14:30:11. The team also confirmed the ransomware within fifteen minutes. (From an email sent by a client with a Word document labelled as 'invoice.')

Analysis: The ransomware detected in the operation system executes the ransomware payload. (The team suspect it was 'SimpleLocker')

Containment: Immediate action was taken to disconnect the affected system and isolate the impacted data.

Eradication and Recovery: The ransomware was successfully removed, and all the systems were restored from clean backups.

Post-incident: To implement the security measure, a team is assigned to review the process and identify the weaknesses that must be addressed. The team performed a full system scan to ensure all traces of the ransomware were eliminated.

Please review the report and feel free to contact me with any suggestions our company suggests as an action plan for the Dog Company.

Best regards,

Zehra Nur Ozer

Cyber Security Analyst