INCIDENT RESPONSE PLAYBOOK

Publication: December 2024

Authors:

Loveth Odozor

Precious Ufomba

Chandani Navadiya

Lynda Omini

Yuval Nitzan

Table of Contents

INTRODUCTION **3**

PREPARATION 3
DETECTION 4
ANALYSIS 4
CONTAINMENT AND ERADICATION: 5
RECOVERY: 6
REFERENCES 8

Introduction

Organizations use incident response strategies to tackle cyberattacks and cybersecurity incidents, reducing recovery time and costs and minimizing damage caused by breaches. Several incident response services are available to manage cyber incidents, including cyber incident response, data breach response, business email compromise response, ransomware response, and digital forensics response.

The following Phases are involved to successfully create an incident response playbook:

Preparation

A typical incident response methodology emphasizes preparation, not only establishing an incident response capability so that the organization is prepared to respond to incidents, but also ensuring that systems, networks, and applications are sufficiently secure to prevent incidents. This phase ensures readiness to handle cybersecurity incidents effectively, fostering resilience and reducing response time.

Preparing to handle Incidents:

- Identifying key assets during preparation phase involves determining the systems, data, and resources that are critical to an organization's operations. This includes pinpointing assets like servers, databases, intellectual property, and sensitive customer information that, if compromised, could significantly impact the business. By prioritizing these assets, the organization can allocate appropriate protections and ensure they are included in the incident response plan.
- Ensuring adequate configurations means setting up systems and devices securely with proper settings to reduce vulnerabilities. Ensuring system backups and recovery involves creating regular backups and testing restoration processes to guarantee data can be recovered quickly in case of an incident. Network segmentation involves dividing the network into smaller parts to limit the spread of threats and protect sensitive information. Patches, updates, and risk assessments involve keeping software up to date, fixing known vulnerabilities, and regularly evaluating potential risks to strengthen defenses against attacks using the appropriate tools.
- Incident Response Team are responsible for selecting a specific playbook, preparing tabletop exercise, maintaining sufficient staffing by assigning roles and responsibilities, so that team members can have uninterrupted time off work (e.g., vacations). Accordingly, incident response teams often manage the organization’s incident information sharing efforts, incident record keeping such as aggregating information related to incidents and effectively communicating with other relevant stakeholders, as well as ensuring that pertinent information is shared within the enterprise.
- Continuous monitoring in the preparation phase involves consistently tracking network traffic, system activities, and security logs to detect potential threats before they escalate.

It ensures real-time visibility into the environment, allowing early identification of vulnerabilities or suspicious behavior that may indicate future incidents.

Detection

The detection phase of an incident response playbook is critical for identifying potential security incidents as early as possible to minimize damage. This phase involves recognizing, analyzing, and confirming anomalous activity that may indicate a cybersecurity incident. The most challenging aspect of the incident response process is often accurately detecting and assessing cybersecurity incidents: determining whether an incident has occurred and, if so, the type, extent, and magnitude of the compromise within cloud, operational technology (OT), hybrid, host, and network systems.

Activities involved in the Detection Phase

Threat monitoring involves deploying and configuring tools such as SIEM systems, IDS/IPS, firewalls, and endpoint detection tools to ensure continuous monitoring and anomaly detection. Security logs from servers, applications, firewalls, user activity, and third-party threat intelligence feeds are analyzed to identify suspicious activities. Automated alerts are generated by security tools when rule violations or unusual patterns, like failed logins or malware signatures, are detected. Additionally, employees or users can manually report suspicious behaviours, such as phishing attempts or abnormal system activity.

Alerts are initially triaged by classifying them based on severity, potential impact, and the systems affected. High-priority alerts concerning sensitive data or critical assets are addressed promptly, while low-priority ones, often involving minimal risk, are deprioritized.

Analysis

This phase aims to systematically understand the scope, impact, and potential risks of the incident, enabling an informed and effective response. This also involves gathering and examining all relevant data and evidence related to a detected activity to understand its nature, scope and potential impact.

Activities in the Analysis Phase:

- Verify previously collected data by cross-checking its accuracy and relevance to the incident while identifying any information gaps. Ensure that all affected systems and endpoints are accounted for in the preliminary findings.
- Scope validation involves assessing verified data to ensure all endpoints and affected systems have been identified. If the scope is incomplete, it is updated with additional data before proceeding; otherwise, the process moves to the next step.

- Identify and collect Indicators of Compromise (IOCs) such as malicious files, IP addresses, and URLs across affected systems using tools like endpoint detection and response (EDR) and system logs. Consolidate these IOCs to facilitate correlation and further analysis.
- Perform Technical Analysis by Conducting in-depth forensic analysis of affected systems, networks, and data by examining file systems, memory dumps, and network traffic for malicious activity. Identify the attacker's tactics, techniques, and procedures (TTPs) to understand the nature of the threat.
- Threat intelligence involves matching discovered indicators of compromise (IOCs) with threat intelligence feeds to determine if an incident aligns with known attack patterns or threat actors.
- Damage assessment evaluates the impact on data, systems, and operations, quantifying losses and identifying potential exfiltration or modification of sensitive information. During risk identification, gaps in security controls and potential vulnerabilities are pinpointed, along with mitigation strategies to address them. Incident analysis is completed by verifying all systems and data involved, ensuring findings are actionable, and deciding whether additional data collection is needed before proceeding. Finally, a summary report is prepared and shared with the incident response team, leadership, and stakeholders, transitioning to the next response phase with clear action steps.

The Goal is to enable an informed and structured approach to mitigating the incident, ensuring a comprehensive understanding of its impact and residual risks.

Containment and Eradication:

Containment is a critical focus during incident response, particularly in major incidents, to prevent further harm and minimize immediate impact by cutting off the adversary's access. The type of containment strategy depends on the specific nature of the threat, such as the approach to handling fileless malware differing from that for ransomware. The goal for Eradication is to restore normal operations by removing any traces of the attack, such as malicious code, and addressing the vulnerabilities exploited by the attacker. Before proceeding to eradication, it's essential to ensure that all potential access points have been secured, adversary activities are fully contained, and all relevant evidence has been gathered, often requiring several iterations.

Actions to be taken as soon as there's a new sign of compromise.

- Identify the affected systems impacted by the incident by determining which endpoints, servers, or network segments are compromised. Review logs from IDS, IPS, and EDR tools to analyse and understand the nature of the attack.
- Isolate affected systems by disconnecting them from the network, such by removing network cables or disabling wireless connections.
- Temporarily enforce least privilege on all critical systems to ensure only authorized users have access. Implement network segmentation to prevent the spread of threats, such as by

isolating affected subnets, VLANs, or servers. Additionally, update firewall filters and perform network scans to enhance security and detect potential threats.

- If new signs of compromise are detected, revisit the technical analysis step to reassess the incident. Once containment is successful and no new signs are found, preserve evidence for potential legal investigation, update detection tools, and proceed to the eradication phase.
- During the incident response, capturing forensic analysis involves reviewing logs, malware, and affected systems to determine the root cause, such as the exploited vulnerability or attack vector, while updating detection tools. For high-risk systems, re-imaging may be necessary to fully remove anomalies, using standard OS templates to rebuild the affected systems.
- Restore impacted systems and files from backups that are confirmed to be clean and secure. Ensure the backups haven't been compromised by the ransomware, using offline or cloud-based backups whenever possible.

Recovery:

A key requirement for a successful recovery is enhanced vigilance and controls to ensure the recovery plan has been successfully executed and that threat actors are not actively operating. As soon as data has been restored from backup sources, verify data integrity, test to ensure all backups are incident-free, and then develop methods to detect lingering threats and re-infection signs.

Activities involved:

Reconnect systems to the network and ensure the restored data are from a clean source using tightened perimeter security while testing systems thoroughly to ensure there are no traces of threats. To confirm that normal operations have resumed, perform an independent test or review of compromise/response-related activities.

The goal is to detect related attacks, review cyber threat intelligence, and closely monitor the environment for signs of threats.

Post-Incident review:

This phase focuses on evaluating the incident response, identifying areas for improvement, and integrating lessons learned into organizational practices to prevent future occurance.

Activities Involved:

- Conducting incident review consists of a team with representatives from IT, security, legal, and management to review the incident, analysing the timeline and effectiveness of response actions. Identify any delays, gaps, or communication issues, and gather feedback from all team members involved in the response.
- Identifying and documenting lessons learned involves organizing a workshop with stakeholders to discuss challenges, solutions, and opportunities for improvement.

- Reviewing and updating the Incident Response Plan (IRP) involves comparing the IRP against findings from the incident review and updating protocols, checklists, and procedures to address identified gaps.
- Sharing insights with relevant teams involves conducting a debriefing meeting to present key findings, summarize the incident, and discuss its impact on operations, reputation, and financials.
- Implementing prevention measures involves introducing new protocols to prevent future incidents, while testing these measures ensures their effectiveness. Integrating new measures includes incorporating them into existing systems and processes to enhance overall security and preparedness.
- Conducting employee training involves developing materials based on lessons learned and organizing regular sessions to cover updated policies and preventive measures. It also includes using real-world scenarios for engagement, ensuring role-specific training, and tracking participation and knowledge retention through assessments and simulations.
- In the post-incident phase of an incident response, officially closing the incident involves finalizing all documentation, signing off on the closure report, and notifying stakeholders that the incident has been resolved. It also includes securely storing incident documentation for future reference and compliance audits.

References

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident handling guide. *Computer Security Incident Handling Guide*, *2*(2). https://doi.org/10.6028/nist.sp.800-61r2

CISA. (2021). *Cybersecurity Incident & Vulnerability Response Playbooks Operational Procedures for Planning and Conducting Cybersecurity Incident and Vulnerability Response Activities in FCEB Information Systems*. https://www.cisa.gov/sites/default/files/2024-08/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf