VISION

Incident Response Plan

Seran Sathyaseelan
April 10,2024

Table of Contents

1.1
Purpose

The Incident Response Plan (IRP) serves as the cornerstone of VISION's cybersecurity posture, underscoring its commitment to proactive threat mitigation and incident management. It articulates the organization's overarching strategy for identifying, assessing, and responding to security incidents, emphasizing the imperative of swift and coordinated action to safeguard critical assets, preserve business continuity, and uphold stakeholder trust. The IRP reflects VISION's proactive stance towards cybersecurity, positioning the organization to effectively address the evolving threat landscape and mitigate the impact of security incidents on its operations and reputation.

2.1
Scope

The Incident Response Plan (IRP) at VISION applies to all employees, contractors, vendors, and stakeholders involved in the operation, maintenance, and support of VISION's IT infrastructure, systems, and services. It covers various cybersecurity incidents, including unauthorized access, malware infections, data breaches, and physical security breaches. The plan encompasses assets such as IT infrastructure, cloud services, software applications, and physical facilities. It defines the roles and responsibilities of the Incident Response Team (IRT) and outlines communication channels for reporting incidents internally and externally. Procedures are established for incident detection, analysis, containment, recovery, and post-incident activities, ensuring compliance with legal and regulatory requirements. Training and awareness programs are implemented to prepare employees and stakeholders to respond effectively to security incidents.

3.1
Incident Response Team

VISION recognizes that an effective incident response capability hinges on the expertise, collaboration, and swift action of a dedicated incident response team. Comprising cross-functional members from IT, cybersecurity, legal, communications, and relevant departments, the incident response team brings diverse skill sets and perspectives to bear in addressing security incidents comprehensively. Each team member is assigned specific roles and responsibilities, ensuring clear lines of accountability and coordination during incident response activities. Rigorous training, skill development initiatives, and simulated exercises bolster the team's readiness to tackle security incidents promptly and effectively.

Fig. 1.1 - Response team roles

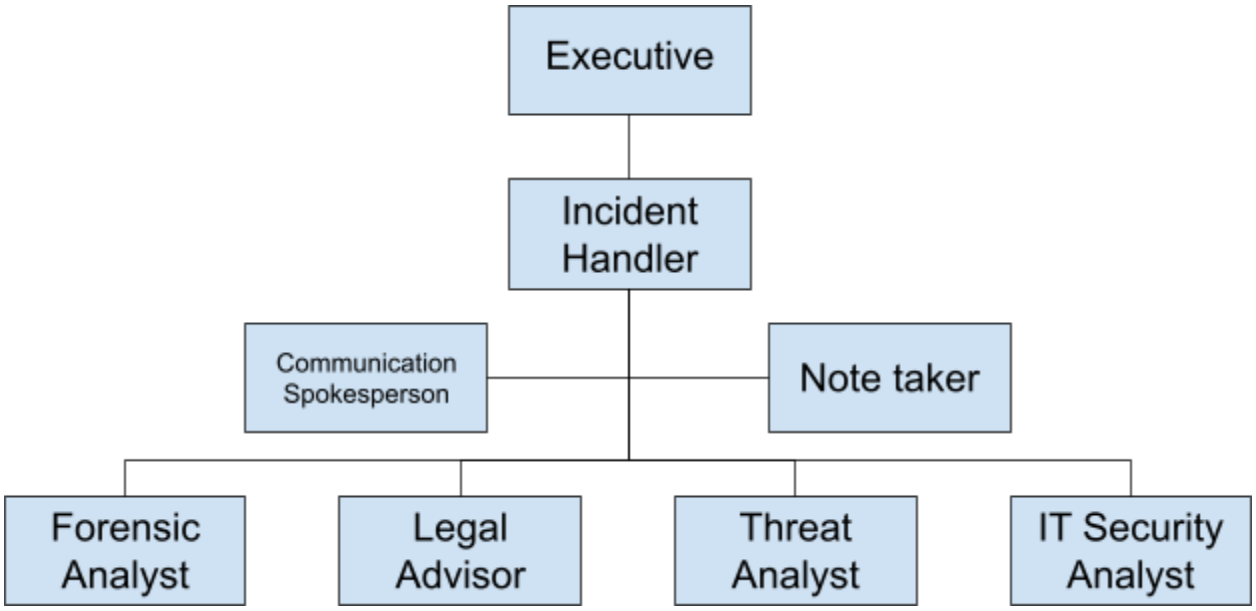

Table 1.1 - RACI chart

Responsibility	**R (Responsible)**	**A (Accountable)**	**C (Consulted)**	**I (Informed)**
Incident Detection	Incident Handler	IT Team	Forensic Analyst, IT Manager	Executive, Legal Advisor
Initial Triage	Incident Handler	IT Team	Legal Advisor	Executive, IT Manager, Forensic Analyst
Root Cause Analysis	Forensic Analyst	IT Manager	Incident Handler, IT Team	Executive, Legal Advisor
Containment	IT Team	IT Manager	Incident Handler	Executive, Forensic Analyst

Eradication	IT Team	IT Manager	Incident Handler	Executive, Forensic Analyst
Recovery and Restoration	IT Team	IT Manager	Incident Handler	Executive, Forensic Analyst
Post-Incident Review	Incident Handler	IT Manager	Forensic Analyst	Executive, Legal Advisor
Stakeholder Communication	Incident Handler	Executive	IT team, Legal Advisor	Forensic Analyst, Note Taker

4.1
Incident Classification

Incident classification is pivotal for VISION to accurately gauge the severity and ramifications of any security breach or operational disruption. By categorizing incidents into low, medium, and high levels based on their likelihood and impact, VISION can tailor its response strategies accordingly.

Low-level incidents are those with a low likelihood of occurrence, occurring infrequently, and with minimal impact on operations, data integrity, or system functionality. These incidents typically pose little to no risk to VISION's operations and may include minor software glitches, individual user errors, or routine system alerts.

Medium-level incidents, on the other hand, have a moderate probability of occurrence and a noticeable impact on operations, data, or systems. They occur more frequently than low-level incidents but less so than high-level ones. Examples of medium-level incidents may involve malware infections affecting multiple systems, unauthorized access to sensitive data, or network outages impacting a department's functionality.

High-level incidents represent the most severe threats to VISION's operations, with a high likelihood of occurrence and significant impact. These incidents can cause severe disruptions, data breaches, or system downtime, resulting in substantial financial or reputational damage. Widespread ransomware attacks, major data breaches, or critical system failures are examples of high-level incidents that demand immediate and intensive response measures to mitigate their impact and prevent further harm to the organization.

5.1
Incident Response Procedure

Preparation and Prevention

VISION understands the critical importance of proactive measures in fortifying its defenses against potential cyber threats. To this end, the company conducts regular and comprehensive risk assessments that encompass all aspects of its infrastructure, applications, and data assets. These assessments are conducted using industry-standard methodologies and tools to identify vulnerabilities and weaknesses that could be exploited by malicious actors. Moreover, VISION employs vulnerability scanning tools that continuously monitor its systems for known security issues and misconfigurations. These scans are conducted on a regular basis to ensure that any newly discovered vulnerabilities are promptly identified and addressed.

Detection and Analysis

VISION's approach to incident detection and analysis is characterized by a multi-layered and proactive strategy. The company employs a range of advanced security technologies, including Security Information and Event Management (SIEM) systems, intrusion detection systems (IDS), and endpoint detection and response (EDR) solutions, to monitor its networks and systems for signs of suspicious activity. These tools generate alerts and notifications whenever they detect potential security incidents, which are then investigated by VISION's dedicated incident response team. This team consists of highly skilled security analysts who possess deep expertise in threat detection and analysis. They leverage their knowledge and experience to conduct thorough investigations into the nature and scope of detected incidents, employing techniques such as log analysis, packet capture, and malware analysis to uncover the tactics, techniques, and procedures (TTPs) employed by attackers.

Containment

In the event of a security incident, VISION's primary objective is to swiftly contain the threat and prevent it from spreading further within its environment. To achieve this, the company maintains a robust set of containment measures that are designed to isolate affected systems, networks, or applications from the rest of the infrastructure. This may involve segmenting networks, disabling compromised user accounts, or implementing access controls to restrict unauthorized access. Additionally, VISION's incident response team collaborates closely with other internal teams, such as network operations and system administrators, to coordinate containment efforts effectively. The goal is to minimize the impact of the incident on VISION's operations and protect its critical assets from further harm.

Eradication

Once the threat has been contained, VISION initiates a comprehensive eradication process to eliminate the root cause of the incident and restore affected systems to a secure state. This process begins with a thorough forensic analysis of the compromised systems and networks to identify the specific entry points used by attackers and the extent of their activities. VISION's incident response team leverages advanced forensic tools and techniques to gather evidence, analyze malware samples, and trace the attacker's movements within the environment. Based on the findings of this analysis, the team develops and implements a targeted remediation plan that addresses all identified security gaps and vulnerabilities. This may involve patching software vulnerabilities, removing malicious code, or reconfiguring security controls to mitigate similar attacks in the future. Throughout the eradication process, VISION places a strong emphasis on maintaining the integrity of its systems and data, ensuring that all remediation efforts are carefully documented and validated to prevent any inadvertent disruptions or further compromises.

Recovery

Following the successful eradication of the threat, VISION shifts its focus towards recovery efforts aimed at restoring affected systems and services to full operational capability. This involves leveraging comprehensive backup and recovery procedures to recover any data or configurations that may have been lost or corrupted during the incident. VISION maintains regular backups of its critical systems and data, which are stored in secure and isolated locations to prevent tampering or unauthorized access. These backups are regularly tested to ensure their integrity and reliability, allowing VISION to quickly recover from incidents with minimal disruption to its operations. In addition to data recovery, VISION also conducts thorough post-incident testing and validation to ensure that all affected systems are functioning properly and that any remaining security issues have been addressed. Finally, VISION conducts a detailed post-incident review and analysis to identify lessons learned, areas for improvement, and opportunities to enhance its incident response capabilities. This information is used to refine VISION's incident response procedures, update its security controls, and strengthen its overall cybersecurity posture.

Lessons Learned

The incident response process offers invaluable insights that can shape future strategies and enhance cyber resilience. Through thorough analysis, organizations can identify successes, challenges, and areas for improvement. Documenting these lessons learned is crucial, capturing best practices, procedural gaps, and recommendations for future incidents. Updating the Cyber Security Incident Response Plan (CSIRP) and training materials based on these findings ensures that the organization remains agile and responsive to evolving threats. Furthermore, sharing insights and recommendations with relevant stakeholders fosters a culture of collaboration and continuous improvement, strengthening the organization's overall cyber resilience posture. By embracing these lessons learned, organizations can effectively navigate future incidents and safeguard against emerging cyber threats.

6.1
Security Tooling

The incident response plan (IRP) relies on a suite of tools and technologies to facilitate effective detection, analysis, containment, eradication, and recovery of security incidents. These tools play a critical role in enhancing the organization's ability to respond swiftly and decisively to cyber threats. Here's an overview of some key tools and technologies that support the incident response plan:

- **Security Information and Event Management (SIEM) Systems**: These systems aggregate and analyze security event data from various sources across the network, including logs, alerts, and telemetry data. They enable organizations to detect suspicious activities, identify security incidents, and prioritize response efforts.

- **Intrusion Detection and Prevention Systems (IDPS):** IDPS solutions monitor network traffic and systems for signs of unauthorized access, malicious activities, or security policy violations. They can detect and block known threats in real-time, mitigating the impact of security incidents.

- **Endpoint Detection and Response (EDR) Solutions:** EDR solutions provide advanced threat detection and response capabilities at the endpoint level. They continuously monitor endpoints for anomalous behavior, file changes, and suspicious activities, facilitating rapid detection and containment of endpoint-based security incidents.

- **Threat Intelligence Platforms:** These platforms aggregate, analyze, and disseminate threat intelligence data from various sources. By leveraging this intelligence, organizations can proactively identify emerging threats, assess their relevance and impact, and adjust their security controls and response strategies accordingly.

- **Forensic Analysis Tools:** Forensic analysis tools enable organizations to conduct thorough investigations into security incidents, collect digital evidence, and reconstruct the timeline of events. They support the identification of root causes, attribution of attacks, and legal and regulatory compliance requirements.

- **Incident Response Automation and Orchestration (IRAO) Platforms:** IRAO platforms streamline and automate various aspects of the incident response process, including alert triage, investigation, and remediation. They enhance the efficiency and effectiveness of incident response operations by orchestrating workflows and automating repetitive tasks.

- **Data Backup and Recovery Solutions:** These solutions are essential for restoring critical systems and data following a security incident. By maintaining regular backups of

essential assets and implementing robust recovery procedures, organizations can minimize downtime, mitigate data loss, and expedite the restoration of services.

- **Collaboration and Communication Tools:** Collaboration and communication tools facilitate real-time communication and coordination among incident response team members, stakeholders, and external partners. They enable rapid information sharing, decision-making, and crisis management during security incidents.

Closing remarks

Incident response planning is integral to safeguarding business functions in today's cyber-threat landscape. It serves as a proactive approach to mitigate risks and minimize the impact of security incidents, ensuring business continuity and protecting critical assets, data, and reputation.

The key takeaways from VISION's incident response plan underscore its significance:

Proactive Risk Management: The plan emphasizes proactive risk management through continuous monitoring, threat intelligence, and vulnerability assessments. This enables VISION to detect and address potential security threats before they escalate into full-blown incidents.

Rapid Detection and Response: By leveraging advanced monitoring tools, intrusion detection systems, and security analytics platforms, VISION can swiftly detect and respond to security incidents. This minimizes dwell time and mitigates the impact on business operations.

Comprehensive Incident Handling: The plan outlines a comprehensive incident handling process encompassing preparation, detection, analysis, containment, eradication, and recovery. This structured approach ensures a coordinated and effective response to security incidents, reducing downtime and financial losses.

Post-Incident Analysis and Improvement: VISION conducts thorough post-incident reviews to analyze the root causes of security incidents, identify lessons learned, and implement corrective actions. This continuous improvement cycle enhances the organization's incident response capabilities and resilience against future threats.

Collaboration and Communication: Effective communication and collaboration are critical during incident response. VISION's plan establishes clear communication channels and protocols to keep stakeholders informed throughout the incident lifecycle, fostering transparency and trust.

Overall, incident response planning plays a vital role in protecting business functions by enabling organizations to detect, respond to, and recover from security incidents effectively. By implementing a robust incident response plan like VISION's, organizations can minimize the impact of cyber threats and maintain operational resilience in the face of evolving cyber risks.