Incident Response Playbooks: A Comprehensive Guide

Written by: Harshitaa Ashish

Introduction

Incident response playbooks is a document that consists of steps and procedures to help us as a guide to follow while handling a security incident. It is necessary and essential to follow a process to get a clear and pre-defined set of actions to be taken to avoid problems. It also helps us understand how a security situation is handled in an organization and how resources are allocated and optimized. The main goal of an incident response playbook is to ensure working on managing the security incidents effectively. The scope is the roles, procedures and actions for different types of incidents, incident detection, eradication, recovery and post incident analysis.

An overview of the incident response playbooks:

- Structure and format: The playbook follows a structure and standard format for consistent and clear process working.
- Incident classification: The incidents are categorized in the playbook based on the security severity, impact and
- Predefined actions: Actions that are needed to be taken at each stage of the process including gathering evidence, forensic analysis and coordinating with law enforcement.
- Decision trees and flowcharts: To help visually represent the steps and decision points that are involved while responding to the incident.
- Automation: due to the complexity and volume of security incidents that are being tackled, organizations mostly use the automation features to handle the processes.
- Customization: The playbooks are customizable for the requirements of different organizations.
- Integration: The playbooks are connected to the organization's SOC or incident response team, which allows them to coordinate and collaborate during security situations.

Incident response team roles and responsibilities

Working in a team is very essential when it comes to handling a security incident. Hence, the incident response team consists of various roles each with different responsibilities to analyze information, observe and share important reports and communicate across the organization. The incident response team includes the following positions for the functioning:

(1) Incident commander - leads the response team and makes critical decisions.
(2) Technical Lead - Looks after the technical aspects like analyzing the incident and implementing measures.
(3) Communication coordinator - manages the internal and external communication.
(4) Forensics specialist - conducts digital forensics analysis to determine the cause and extent of the incident. And works on collecting evidence.
(5) System administrator - implements technical actions required such as restoring backups and applying security patches of the system.

(6) Network administrator - to monitor the network traffic and analyze logs for threat identification.

Communication channels and procedures play a very significant role in the incident response management process to have a good workflow. The most used methods and tools for the communication and escalation process are: emails and SMS, chat and collaboration section on the incident management platform, and other modes are monitoring and alerting systems.

Incident classification and prioritization

Classifying threats and prioritizing them helps the teams to allocate resources and respond to the security threats. The severity is classified based on the severity, type, regulatory requirements, and incident lifecycle. The severity ranges from low to critical, which is determined by the impact on the organization's assets and operations. The type of incident is based on nature, and every type of incident has its own method specific method to respond. Detection, containment, eradication, and recovery are the lifecycle stages that are required to respond and allocate resources effectively.

The various prioritization methodologies to address the critical incidents depend on the impact on the operations and urgency of resolution. Factors like data sensitivity and business continuity prioritize the incidents based on potential risks.

To allocate resources involves studying the needs, priorities, choices and factors like urgency and resources available. The decisions are also made based on considering the cost, circumstances, funding, feasibility, and review performance.

Preparation phase

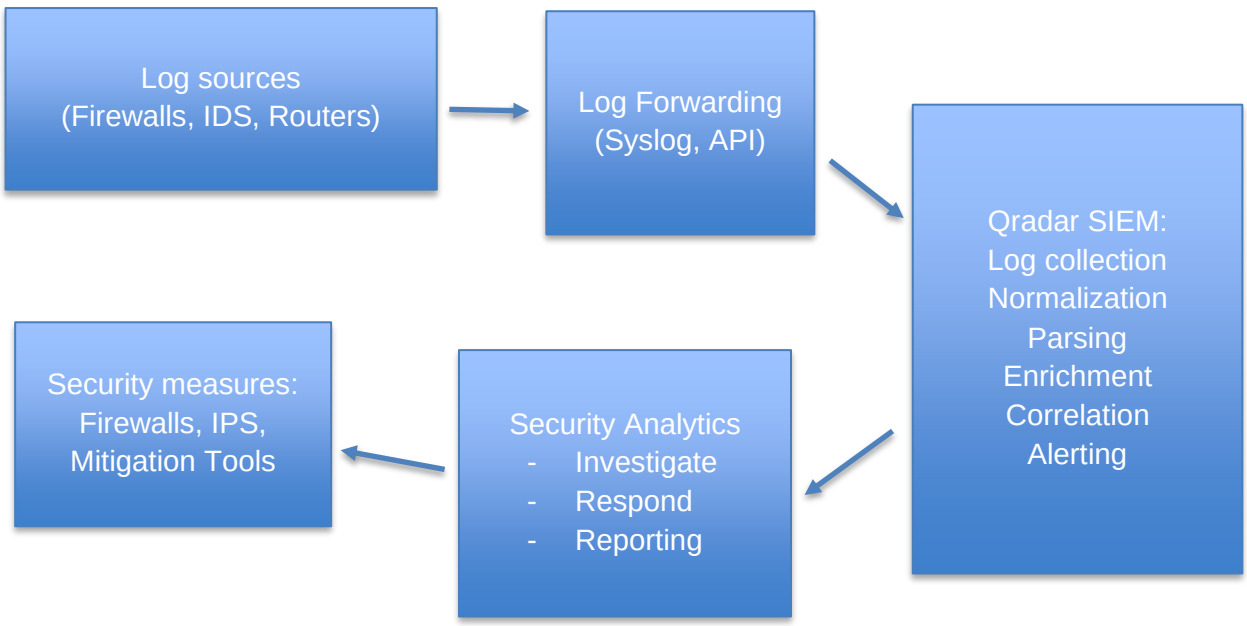
The incident response preparation phase includes a checklist to cover various technical aspects to be ready to respond to any security situation successfully. It is necessary to develop and maintain incident response procedures and documentation. Implementing and maintaining incident detection and monitoring tools such as SIEM and IDS/IPS tools. To capture relevant event data, we need to set up logs and auditing mechanisms. Automated alerting mechanisms are established to notify the incident response team when a security incident is detected. For internal and external communications, various kinds of communication channels are established. Disk imaging and forensic analysis tools are used to preserve evidence in case of security incidents. Regular backups and documenting reports of the incidents are other preparation phases required.

Identifying the critical assets within the organization like servers, databases, network devices and applications to conduct thorough assessment for asset detailed documentation and maintain updated records of the asset information. Document and map the organization's network infrastructure to identify connections and dependencies between critical assets to identify where to pay attention during the security incident. The data flows, storage locations, access controls and encryption mechanisms should be documented as the inventory sensitive data are stored in the critical assets. Efficient incident response starts with thorough software

and hardware inventories. Documenting versions, licenses and critical components streamlines mitigation efforts and enhances security resilience.
During the preparatory phase, it is also important to understand the scenario and identify the incident and classify it to develop the playbook. And for it, we have to follow the technical procedures, communication protocols and test the incident response process to validate it. An example for a scenario would involve a phishing attack where an employee receives a suspicious email prompting them to click on a malicious link. In this case, the incident response playbook would outline steps for identifying, containing, and remediating the attack, including isolating affected systems, notifying stakeholders, and implementing security awareness training.

Detection and alerting with SIEM

SIEM stands for Security Information and Event Management, is a very important cybersecurity infrastructure used for collecting, analyzing, and monitoring security events from various sources of an organization's network infrastructure. It helps to work on real time monitoring, threat detection and incident response.
An example of a SIEM solution is IBM QRadar, which is used for detecting and alerting incidents. It involves data collection across the network, pre-defined threat rules to identify suspicious activities and threats. It generates alerts and notifications to provide information about the nature of the incident according to the severity through email, SMS or the QRadar console. The QRadar also consists of additional tools and capabilities for investigating security incidents in detail including features like visualizing and analyzing the root cause of the incident.
Configuring SIEM rules involves defining criteria based on known threats, abnormal behaviors, or compliance requirements. Alerts are set to trigger when these criteria are met, indicating potential security incidents. Fine-tuning rules ensures accurate detection while minimizing false positives, enabling timely response to threats within the organization's network infrastructure.
Additionally, SIEM integrates with IDS/IPS, EDR, firewalls, and vulnerability scanners for a holistic approach to threat detection and response.



Initial response actions

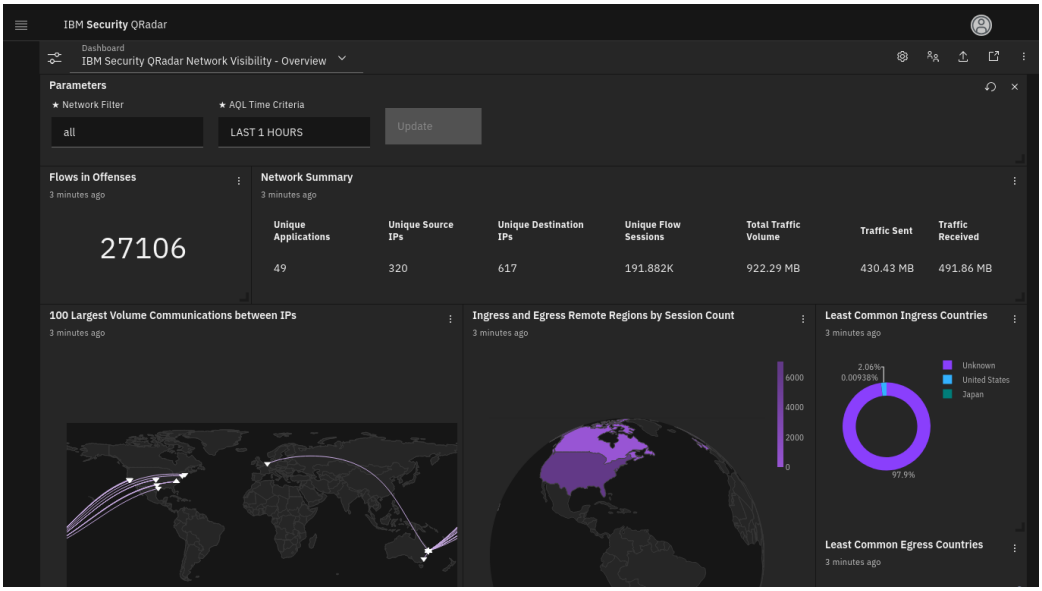
After the incident is identified and confirmed, immediate steps are taken to mitigate the situation. The response team is notified of the action and the affected systems are isolated to prevent the other unaffected systems from getting harmed. All the evidence is preserved and the incident response plan is implemented to guide the process. A person is designated or automated alerts can also be utilized to activate the incident response team after the detection of the incident. Pre-defined channels for communication are also established including reporting mechanisms. This also ensures the coordination and collaboration of the team members and facilitates cohesive response efforts. Another part of the process involves preserving the evidence with the help of screenshots, time stamps, logs, etc.

Investigation and analysis

The different techniques that are used for conducting investigation and analysis using SIEM are:

- Log collection: ensuring detailed collection of logs from various sources within the network, servers, endpoints, firewalls, and applications.
- Behavioral analytics: SIEM helps to detect anomalous activities and deviations from normal patterns of behaviors, which is used to detect potential threats.
- Threat intelligence integration: it helps prioritizing alerts and understanding the threat landscape.
- Automated response playbooks: Developed within the SIEM to streamline incident response processes, which accelerate investigation workflow and mitigate security incidents better.

In conducting investigations using SIEM data, correlation and analysis of security events are pivotal. By creating correlation rules, reconstructing timelines, and assessing impact, analysts can identify incident scope and severity. This ensures precise response actions and aids in preventing future threats, enhancing overall cybersecurity resilience.



IBM Qradar SIEM analysis platform (Reference: https://www.ibm.com/products/qradar-siem)

Mitigation and recovery

To handle an incident and deal with the recovery, the real cause of the incident must be determined. For determining the cause, certain strategies such as the systems or networks need to be isolated to prevent further spread of the incident and additional damage. Apply patches and updates to address the vulnerabilities exploited in the incident to avoid similar situations in the future. Backup also needs to be stored regularly to recover the lost or compromised data ensuring minimal disruption to business operations.

Communication and reporting

The Incident Response Playbook serves as a comprehensive guide for effectively managing security incidents, emphasizing clear communication and thorough reporting throughout the response process. Firstly, it outlines predefined communication channels and escalation paths, ensuring timely notification of key stakeholders upon incident detection. Secondly, it provides templates and guidelines for crafting concise and informative incident reports, detailing incident specifics, impact assessment, and mitigation strategies. Thirdly, the playbook emphasizes the importance of regular status updates to keep stakeholders informed of progress and maintain transparency. Lastly, it includes protocols for post-incident debriefing and reporting, facilitating lessons learned analysis and continuous improvement of incident response capabilities. Through adherence to these four key points, the playbook facilitates a coordinated and efficient response effort, minimizing disruption and maximizing resilience in the face of security incidents.

Conclusion

In conclusion, the Incident Response Playbook serves as a vital resource in ensuring organizations are well-prepared to effectively manage security incidents. It provides a structured framework for response activities, streamlining communication, and coordination efforts among stakeholders. By offering predefined procedures and templates, it enables swift and consistent responses, reducing response times and mitigating the impact of incidents. Through its emphasis on post-incident analysis and continuous improvement, the playbook fosters a culture of learning and resilience, enabling organizations to adapt and evolve their incident response capabilities over time. Overall, the Incident Response Playbook is an indispensable tool for strengthening cyber resilience and safeguarding against emerging threats in today's dynamic threat landscape.

References:

https://learn.microsoft.com/en-us/security/operations/incident-response-playbooks

https://www.atlassian.com/incident-management/incident-response/how-to-create-an-incident-response-playbook#incident-response-lifecycle

https://www.sciencedirect.com/science/article/abs/pii/S0167404812000624

https://www.researchgate.net/profile/Philip-Empl/publication/376581705_Do_You_Play_It_by_the_Books_A_Study_on_Incident_Response_Playbooks_and_Influencing_Factors/links/658290630bb2c7472bf9bda1/Do-You-Play-It-by-the-Books-A-Study-on-Incident-Response-Playbooks-and-Influencing-Factors.pdf

https://aisel.aisnet.org/acis2011/37/