Logsign

Developing an Incident Response Strategy

Contents

Guide for Security Operations Metrics

Developing an Incident Response Strategy

1. Introduction

From large-scale enterprises to government bodies, manufacturing units, and hospitals, any organization can be a target of sophisticated cyberattacks. With growing networks and ever-evolving threat landscape, the number of opportunities for attackers to break into your system is only increasing. Without sufficient security controls in place, organizations impliedly give an open invitation to the attackers to disrupt their business operations. So often, it is reiterated that it is no longer a question of if, but when, the attackers will break into your network.

Attackers have plenty of attack vectors to choose from zero-day vulnerabilities, unauthorized access, malware, social engineering, a vulnerable vendor, and whatnot. Organizations need to implement sufficient security controls to defend their IT infrastructure against such attacks. A security program does not become successful merely because it was able to prevent threats. Your security program can only succeed when it can provide swift response and mitigation for an incident, i.e., when an attacker successfully bypasses your defenses.

Modern-day organizations require streamlined incident response strategy to manage and coordinate their response activities for security incidents. An incident response strategy must be measurable, repeatable, and consistent. Ad hoc strategic often results in increased costs, process and communication roadblocks, and undesirable results for an organization. Ideally, well-thought incident response strategies help the incident response team in doing their job quickly, effectively, and accurately.

Incident response programs encompass people, process, and technology. When an organization starts preparing its incident response plan, it faces specific challenges that do not have a straight forward solution. Three such challenges that have maximum impact is:

i. The number of cybersecurity incidents is increasing continuously.

ii. There exists a skill-shortage in the cybersecurity industry.

iii. Existing processes are complicated and not flexible enough to cover incident response.

To overcome first and second challenges, an organization can adopt tools such as SIEM and SOAR by utilizing automation to its benefits. For the third challenge, adequate planning and preparedness are required to respond to cyberattacks. In a crisis, the response team cannot keep on addressing one bottleneck after another and let the situation get worsen. For effectively managing challenging like these, organizations need to align their people, process, and technology. Incident response is a process; it requires trained personnel, tried and tested processes, and integrated technologies. These building blocks lay down the foundation for successful incident response strategies.

2. Understanding Threats and Liabilities

Every organization faces its own set of threats, internal as well as external. When it comes to identifying threats, the one-size-fits-all approach does not work. You are setting up an incident response plan to deal against the threats that may impact your business operations. Hence, the first step is to develop a detailed understanding of organization-specific threat landscape. If your organization has recorded information about previous security incidents, their documentation can provide valuable inputs here.

Another starting point is to understand the threats that your industry regularly faces. For example, malware attacks on healthcare providers and DDoS attacks on cloud service providers are expected. To develop a robust understanding of potential threats, an organization must consider all possible incidents and threat actors. The spectrum of threats faced by modern-day organizations is relatively broad, and the prospective incident response plan must be capable of responding to all such threats.

Checking news articles and white papers about attacks on your competitors, industry-leading organizations, and business vendors can further contribute at this stage. Once external threats are, the next step is to identify internal threats and challenges. Apart from skills shortage, insider's threat is a daunting challenge that organizations need to address. If there have been prior incidents of data leakage or data theft, they must be accounted for.

3. Documenting Your Incident Response Plan

The most significant barriers to effective incident response are lack of planning and preparedness. Without a proper incident response in place, ad hoc decisions lead to a slow, ineffective, and inefficient response to security incidents. This, in turn, raises the chances of a costly security incident, employee and customer dissatisfaction, and prolonged operational disruptions.

With the help of a documented and tested incident response plan, your team would know what it is supposed to do and how they are going to execute their responsibilities.

Adequate documentation and regular reviews help your organization in pushing for continual improvements so that your security posture stays ahead of cyber threats.

Successful cyberattacks do not only disrupt your business operations, but they also bring reputational and financial damages alongside. With regulations like GDPR, your organization may be bound by various laws to pay regulatory fines for poor security practices. To sum up, these are the questions that you need an answer for:

i. What are the types of attacks that your organization has faced in the past?

ii. Have your employees received phishing or spear-phishing emails in the last six months?

iii. Has your organization previously experienced malware or DDoS attacks?

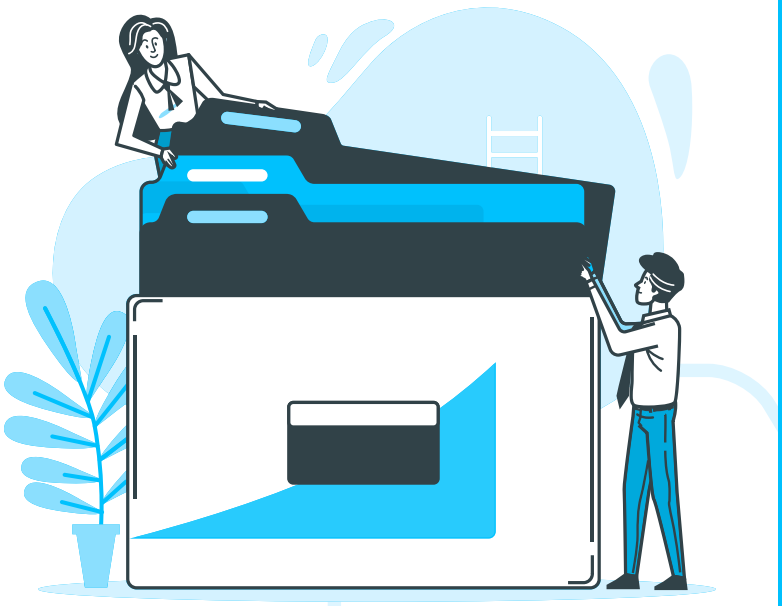
iv. Were you able to successfully recover from such attacks on your own, or you availed external help?

v. What is the total time taken by your organization to respond to a security incident?

vi. What are your information security responsibilities? (Regulations and laws, industry standards, contractual obligations)

vii. Are you required to notify a data breach or security incident?

viii. Do you have a defined procedure for notification? Is there a mandatory time limit?



There is no denying that creating an effective incident response plan requires organization-wide time and efforts. For the same, support from the top management is crucial, and it should be the top priority of your organization's Chief Information Security Officer (CISO). To avail organization-wide resources, it is recommended to organize an incident response planning session with all the stakeholders. The security team can engage with the top management to ensure that everybody understands the risks your organization faces and how they can contribute. Incident response also requires support from other organizational functions such as marketing, legal, human resources, etc.

At this stage, you should be able to define various steps needed to resolve an incident, from its detection to mitigation. Roles and responsibilities must be clearly defined for the designated incident response team. An incident response team generally consists of:

i. **Team leader:** The primary objective of the team leader is to ensure that the incident response team functions as expected, and all the required resources are available. Mostly, this role will be assigned to your organization's CISO.

ii. **Incident Manager:** This role will be responsible for the day-to-day functioning of the incident response team. They look after team affairs and act as a single point of contact for the team leader. Based on the size of your organization, the number of incident managers can vary.

iii. **Investigators:** This group of individuals are security analysts that will investigate various security incidents as they are detected. Based on the size of your organization, the number of investigators will vary. Out of all such investigators, one of them can be appointed as the lead investigator.

iv. **Communications/PR:** This role is generally assigned to either the marketing or public relationships team for answering to external queries, deliver public statements, and draft notifications for customers, partners, and stakeholders.

v. **Legal:** This role is assigned to an individual who is familiar with various applicable laws and regulations in the context of information security. A specialized legal professional can help your organization in preparing data breach notifications, disclosing information about security incidents, and representing the organization in regulatory proceedings due to a successful cyber attack.

vi. **Human Resources:** This role looks after sorting out personnel-related issues that might occur during a crisis. They can also share important insights for communicating a data breach to your employees.

After deciding the composition of your incident response team, it is reasonable to develop plans and processes. Instead of staring in the dark, you can refer to guidance documents published by organizations such as SANS, NIST, and CERTs across the globe to start with. At this stage, when you are preparing your documentation; your processes and procedures would have loopholes that you will discover later. Therefore, continual improvement is necessary. After the completion of this stage, your organization should have a well-defined incident response plan. It should be consistent, repeatable, and understood by every team member.

4. Communication During Incident Response

Communication of incident is a vital activity when you are responding to an incident. The parties that must be communicated with are either internal or external. However, the incident response team has to ensure that all such communications maintain an adequate balance between protection and disclosure. During a crisis, every organization must follow some basic principles such as:

i. Instead of denying, acknowledge that there exists a problem and control your subsequent communications.

ii. Without using complicated jargons, put together facts and convey them to the intended recipients.

iii. Designate a trusted executive to act as the spokesperson until the crisis is over.

iv. Avoid reacting defensively and address the loopholes to prevent the same incident from happening again.

After defining your incident response processes in the last stage, you must check if you have included an incident response team activation process. This process will specify when your security team requests the incident response team to take over. As far as external communications are concerned, there shall be a single point of contact to avoid any chances of fake news or misinterpretation from your side. As you prepare for real-life incidents using simulations in the next phase, keep communication templates handy to minimize the time involved in preparing the entire statements.

5. Assessing the Readiness of Your Incident Response Plan

As threats evolve and attacks get sophisticated, your security team must not be left behind. The ideal way to asset the readiness of your incident response plan is to conduct simulated crisis exercises. Simulations help your team in being ready for real-life situations and uncover the areas for improvement in the upcoming exercises.

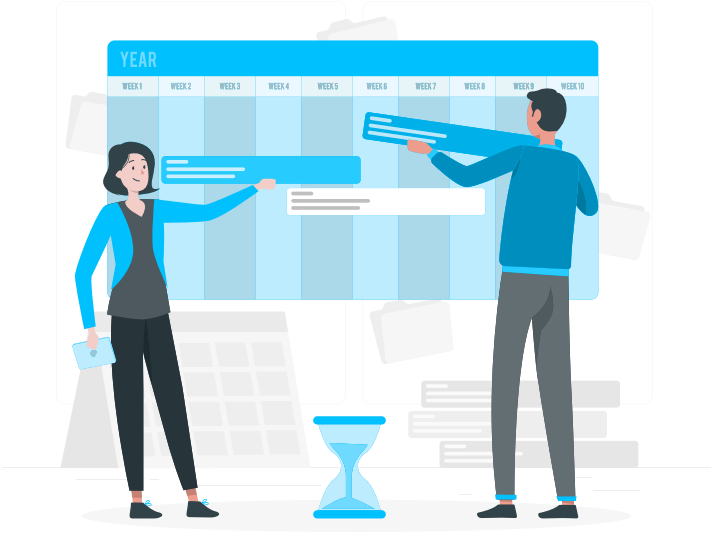
i. Finding loopholes in the existing incident response strategy

ii. Offers a cost-effective solution without disrupting business operations

iii. Helps in removing communication barriers during a crisis

iv. Enables the incident response team members to understand their roles and responsibilities better

v Minimizes the scope for disputes



While designing simulation exercises, the audience must be taken into consideration. Simulations must be well-thought, and it should have an initial outline, middle story, and a possible conclusion. Instead of incorporating superficial or impossible situations in a simulation exercise, realistic factors and relevancy to an organization's security operations increase the chances of success. All the activities of a simulation exercise must be documented and presented in the form of a report once the exercise is over. For long-term benefits, organizations can explore measuring various parts of their simulation exercise. It is a recommended practice to share the reports of simulations exercise with all the individuals involved. After the initial wheels are set in motion, you can consider adopting maturity models like the Security Incident Management Maturity Model (SIM3) to improvise your incident response capabilities.

i. Is there any overlapping in roles and responsibilities of the incident response team?

ii. Are there any communication barriers that impact the escalation route?

iii. Is there a skills gap that may affect the operations of your incident response team?

iv. Is the incident response team familiar with their processes and procedures?

v Who can report an incident to the incident response team?

vi. Does the organization need to report an incident to a regulatory authority?

vii. Is the incident response team capable of collecting and handling digital evidence?

viii. Can the incident response team derive actionable insights from threat intelligence (TI) feeds?

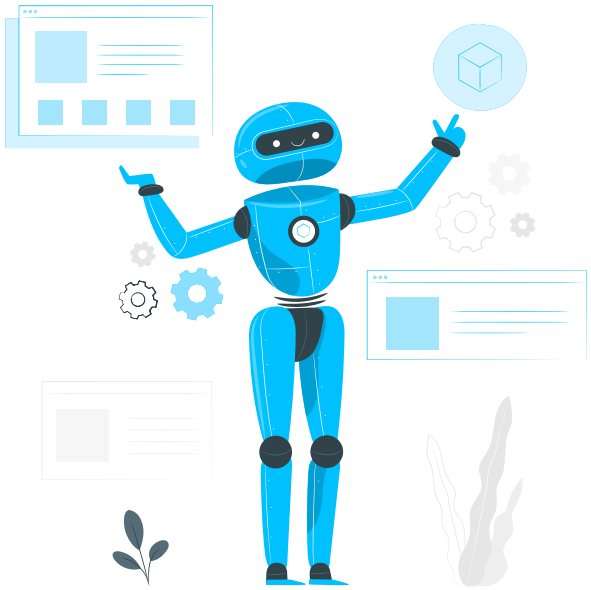
ix. Is the incident response team familiar with the business requirements of the organization?

6. Using Machine Learning, Automation, and Threat Intelligence

Manual response to individual alerts can result in significant alert fatigue. Instead of keeping your team continuously overburdened with alerts, tools like Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) can help in decreasing their workload. Subsequently, they can focus on high-risk alerts that may have a severe impact on your business operations. In the last few years, organizations are increasingly relying on TI feeds for comprehensive insights and knowledge about the latest threat activities. If your organization has uses a SIEM tool, there are chances that this tool is already receiving data from multiple TI feeds to equip your security team with real-time detection capabilities.

Logsign SIEM and SOAR platforms provide our clients with a single-window solution to manage incident detection, mitigation and response from a single point. A majority of investigation and response processes can be automated with the help of playbooks. For alerts requiring manual intervention, security teams get access to detailed contextual information about those alerts to make informed decisions. Other added benefits include automated documentation of activities so that your compliance requirements are duly met.

In our experience of working with our clients in setting up SIEM and SOAR solutions, we have come to an understanding that automation shall always start from low-level tasks. As security teams start getting familiar with SIEM and SOAR platforms, they can find more opportunities to automate incident response process and procedures. As repetitive tasks get seemingly automated, a substantial burden is reduced on your incident response team. Over time, your team is empowered to deal with security incidents like strategic decision-makers. If you have recently adopted a SIEM or SOAR platform, it is recommended that your automated processes must involve human approval. Once these automated processes are refined, you can move towards full automation



About Us

Logsign was established in 2010 to enable cyber security practitioners to work more efficiently with smart, clutter-free and next-generation softwares. Securing the IT systems and managing cyber security operations should not be so complex, time consuming and over-priced. This is why we developed our smart and simple-to-use SIEM and SOAR softwares considering the market's current and future needs. Automation starts the new era in cybersecurity. We believe with this era, automation handles the manual workload of humans upto 98%. Thus, efficiency in cybersecurity operations is not a dream anymore. SOAR software is in the heart of operations enhancing security teams work in a smart, collaborative and effective environment. You can't protect before you see and detect. Collecting any data, visualizing and turning into actionable intelligence are possible via our infinitely scalable and cluster SIEM. With 10 years of experience, Logsign is a sincere team player for all internal & external parties, trusted by more than 500 enterprises, ministries and state agencies.

www.logsign.com | support.logsign.net | 0 850 660 0 850

Info Security Products Guide 2020 GLOBAL EXCELLENCE BRONZE ★★★★★

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2020

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2019

Info Security Products Guide 2019 GLOBAL EXCELLENCE SILVER ★★★★★

Info Security Products Guide 2019 GLOBAL EXCELLENCE GOLD ★★★★★

CYBER DEFENSE GLOBAL AWARDS CYBER DEFENSE MAGAZINE 2018 WINNER