Logsign®

Guide for Security Operations Metrics

Contents

Guide for Security Operations Metrics

3. Important Metrics

Guide for Security Operations Metrics

1. Overview

The threat landscape in our ever-evolving cyberspace has continued to expand at a rapid pace. The attackers are launching sophisticated attacks which often go undetected by single-point security devices. To defend against such attacks, organizations need to implement comprehensive security programs that cover their people, process, and technology. Mature security programs focus on continual improvements to successfully defend against incoming threats.

In the present scenario, no organization can claim that they are absolutely secure against cyberattacks. Every organization, irrespective of its size and industry, is a target for security incidents and data breaches. At times, attackers spend months in planning an attack, and they only need to be successful once to disrupt your business operations. However, on the other hand, your security team is expected to prevent such attempts 24x7. On the other hand, there is no plausible way for an organization to find out the number of potential attackers; however, the number of individuals in the security team are limited.

In this context, it becomes challenging for organizations to measure the success of their security initiatives. While the executive decisions are most certainly going to rely on data, security teams invest a substantial amount of time in tracking the right metrics. Measuring security operations, whether qualitatively or quantitatively, demonstrates how well a security program is functioning. These results can be further utilized to request additional budget approvals for new technologies and tools.

We often encounter situations where our clients have implemented the best of security measures, but they were not adequately tracking their security operations. There is no denying that reporting on metrics for their operations is a highly time-consuming process. With a lack of interoperability among various security tools and skill shortages, the problem further worsens. However, what security managers and CISOs need to understand is that recording metrics for security operations providers value for overall security strategy.

2. Initial Preparation

Before building a plan for your organization's security practices, the security team must have clarity in terms of data they are collecting and why. It is recommended to prepare long-term objectives from security metrics that align with your organization's business requirements. These objectives must fit into the organization's overall security strategy. Another consideration here is properly defining roles and responsibilities for individuals responsible for your organization's security metrics program. Once these pieces of information are documented and ready, it would become more comfortable for a security team to avail support from the top management.

Consider a situation when a security team approaches the top management without any documentation and clarity on what they seek to do. Most likely, they will receive an unfavorable response. If your organization is setting up a security operations center (SOC), it is crucial to record metrics right from the beginning for deriving benefits in the long run. With proper documentation, a security team can expect swift approvals from the top management with adequate support.

As the preparations for the proposed security metrics program start, it may encounter resistance for specific groups or individuals of the security team itself. Some managers may believe that another team recording their day-to-day tasks will add additional pressure to their teams. However, a security metrics program must be presented as a solution to improvise security operations; instead of an organizational program to keep tabs on various managers and their teams. Having a well-defined roles and responsibilities document that should be prepared before approaching the top management helps in mitigating concerns like this.

2.1 Identifying Relevant Security Metrics for Your Organization: Key Performance Indicators (KPIs)

A Key Performance Indicator (KPI) helps an organization in measuring whether their business process or objective has been a success or failure. It provides actionable information for the decision-makers and eventually, helps in the decision-making process. Generally, KPIs for security operations aim to identify positive and negative trends. For example, one KPI can be the number of false-positive security alerts over the last six months. Similarly, for administrative processes, a KPI can be the number of exceptions raised in the previous three months. Recording KPIs can have tremendous benefits for security operations, whether they are strategic or tactical.

Well-defined KPIs can serve as the drivers for a continuously improving security program. KPIs ensure that your security program remains effective and gaps are addressed before they can impact your security posture. To find out the relevant security metrics, a security team should start with identifying various operations or functions that they need to assess. If your organization has an information security management system (ISMS) in place, the existing document can help you with this. For the identified operations and functions, you should identify various security metrics (or KPIs) that would help in assessing the performance.

Recording KPIs comes with a cost, be in terms of time or money. Before finalizing the list of KPIs to track, a cost-benefit analysis may be useful. Every KPI must have the following SMART characteristics:

i. **Simple:** A KPI should be easy to measure. It should not be complicated, and the purpose behind recording it must be documented and communicated.

ii. **Measurable:** A KPI that cannot be measured will not help in the decision-making process. The selected KPIs must be measurable, whether qualitatively or quantitatively. The procedure for measuring the KPIs must be consistent and well-defined.

iii. **Actionable:** KPIs should contribute to the decision-making process of your organization. A KPI that does not make any such contributions servers no purpose.

iv. **Relevant:** KPIs must be related to operations or functions that a security team seeks to assess.

v. **Time-based:** KPIs should be flexible enough to demonstrate changes over time. In a practical sense, an ideal KPI can be grouped together by different time intervals.

3. Important Metrics

3.1 For Security Operations

One of the most apparent metrics that should be recorded is the number of total security alerts and incidents. This metric will answer questions such as:

i. Whether overall security incidents are increasing or decreasing?

ii. What are the types of security incidents being detected?

iii. How many high-risk security incidents were detected in the last month?

This metric will further help in determining the proportion of false-positive alerts, the average time taken to mitigate an incident, and average number of alerts per security analyst. If there is a large number of security alerts being handled by individual team members, it gives an actionable insight that the organization lacks in human resources. On top of this, captured information from security alerts and incidents will assist in pinpointing weaknesses in your technical infrastructure. Moreover, for security alerts and incidents caused due to user errors, you can observe the team members that require additional security training.

If a Security Information and Event Management (SIEM) solution is a part of your security operations, it will altogether streamline the process of recording metrics for various functions and processes. Besides, Security Orchestration, Automation, and Response (SOAR) capabilities will equip a security team with real-time insights into the entire network and automated detection and response capabilities. Using SIEM and SOAR, you can further track metrics such as:

i. Number of alerts closed per day by an analyst.

ii. Closure of alerts (Automated v. manual).

iii. Number of alerts marked as false positives.

iv. Alerts converted into security incidents.

v. Average time taken to detect a security incident.

vi. Types of alerts over a given period.

vii. Classification of alerts based on their source device.

In cases of large-scale organizations where security teams have multiple levels of analysts, security metrics can help to discover exciting insights into how analysts are interacting with each other. Consider that there are three levels of security analysts in a security operations center. Security metrics can help in understanding:

i. Types of alerts escalated to Level 2 from Level 1 analysts.

ii. Reaction time of security analysts responsible for responding to security incidents.

iii. Time taken for dealing with an alert at each level.

iv. Commonly used playbooks.

v. Most frequent IP addresses, users, and hosts involved in security alerts.

3.2 For Business Requirements

An organization hopes to perform its business operations without any disruptions. It adopts a detailed risk management framework to minimize the probability of the risks it faces. It may implement a dedicated business continuity management system to support its risk management initiatives. While it is true that every organization is prone to cyberattacks, risk management can significantly bring down costs in cases of successful cyberattacks. For example, if attackers can break into the organization's network, a tried and tested incident response plan would help in initiating the incident response process immediately. As soon as the incident is mitigated, the organization can resume its regular business operations.

When we discuss from the top management's perspective, a relevant KPI can be MTTD (mean time taken to detect). MTTD is the time taken for your security team to detect a security incident, either when it is in process or after it has occurred. MTTR (mean time to response) is the time taken for your security team to mitigate or remediate a security incident after it has been discovered. Trends in MTTD and MTTR over a period can help in understanding the detection and response capabilities of the security team. These two metrics can also give an idea of the duration for which the attackers had unrestricted access to the organizational network. During this period, the attackers can perform various actions that can directly impact your organization's security posture.

For the top management, the knowledge of alert fatigue may help them in deciding whether they need to invest in additional human resources for the security team. Addressing alerts one-by-one can result in alert fatigue, and as a result, the overall productivity of the security team decreases. However, if solutions like SIEM and SOAR are a part of your organization's security operations, the chances of alert fatigue decrease. With the help of automation, low-risk alerts are automatically addressed with the use of playbooks. High-risk alerts are enriched with contextual information and can be assigned to security analysts for manual verification.

Other metrics for business requirements that must be considered are:

i. Percentage of false-positive alerts per security tool

ii. Risk level-wise distribution of alerts and incidents

iii. Most common origins of security alerts and incidents

iv. Number of incidents that impacted business operations

v. Productivity of security analysts across various levels in the security team

4. What Next?

Manually collecting data for metrics may turn out to be a tedious process. The security team should explore various possibilities of how data collection, analysis, and report presentation can be automated. Once security metrics start getting collected, you can generate reports that demonstrate how variation has occurred over time. These reports can be sent to the top management to explain to them the progress as well as existing gaps in your security program. Problems like these are solved by default when an organization relies on SIEM and SOAR solutions. These solutions minimize the inconsistency in data, streamlined data reporting process, predictability in reports delivery, and promote acceptable data hygiene practices.

Maintaining a baseline will demonstrate changes over time, positive as well as negative. The security team should give an equal amount of attention to both negative and positive changes. Adequate attention to negative results will help in gaining the top management support for the long run. So, instead of focusing excessively on short-term results and positive changes, resources must be dedicated to ensuring that instances of negative changes are minimized.

At the end of the day, security metrics will provide detailed insights into the performance of your security program. As the level of automation increases for data collection, preparing reports after data analysis would take lesser time. If you are considering outsourcing your partial or entire security operations to a third-party service provider, your metrics program must account for this arrangement. There should be a designated point of contact (POC) to regularly communicate with your service provider and ensure that metrics for measurement of security operations are duly shared. It is recommended to specify expected performance levels in the form of a service level agreement (SLA).

Last but not least, a SIEM solution in combination with SOAR capabilities can certainly automate responding to security alerts to a greater extent. This automation can be either fully or partially automated requiring human intervention. With the help of these solutions, the manual efforts as necessary for alert management are substantially reduced. Further, as these solutions become part of an organization's security operations, the overall effectiveness of their security programs increases and the productivity of their teams improves consistently.

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