

Measure the positive economic impact of your SIEM solution on the basis of three metrics:

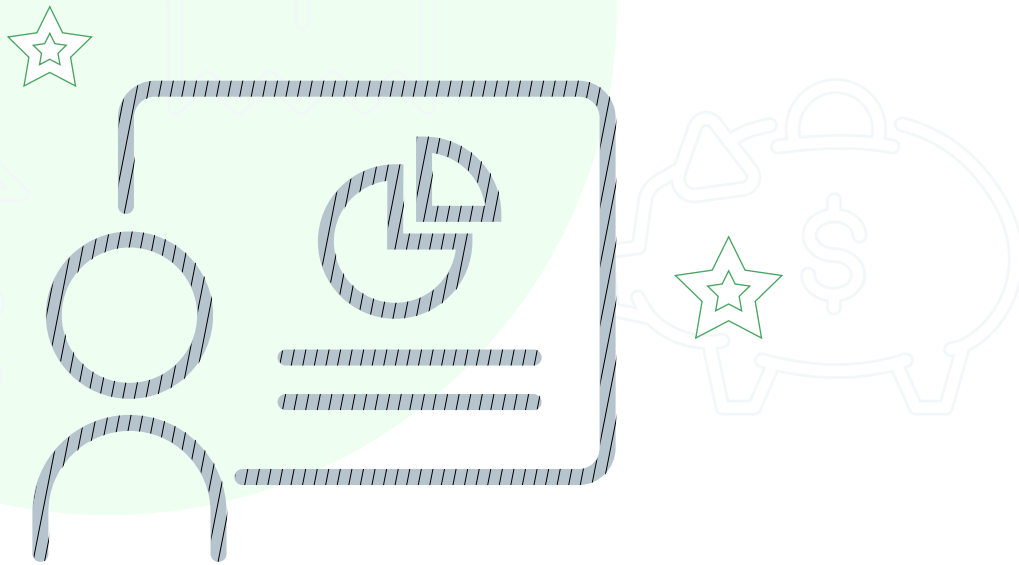
- ▶ Compliance reporting
- ▶ Operational efficiency
- ▶ Breach impact mitigation



How to calculate the

COST
SAVINGS

from your SIEM implementation



INTRODUCTION

Cybersecurity is often perceived as expensive. But in the face of increasingly severe attacks and data breaches, it is clear that we cannot afford to be complacent. By understanding the potential cost savings due to your SIEM investment, you can make the right choices in your cybersecurity spending.

In this white paper, we will discuss:

- ✔ Why measure cost savings for a SIEM deployment?
- ✔ How to quantify the benefits of a SIEM
- ✔ Three perspectives of cost savings: Compliance reporting, operational efficiency, and impact mitigation
- ✔ How to calculate cost savings for a SIEM deployment by illustrating through an example




WHY MEASURE COST SAVINGS FOR A SIEM DEPLOYMENT?

A security information and event management (SIEM) solution, without a doubt, is an essential component of your security architecture, supporting threat detection, compliance, and security incident management through the accumulation and analysis of security events (both near real-time and historical). Modern SIEM solutions combine threat intelligence, machine learning-based anomaly detection, and rule-based attack detection techniques to identify sophisticated attacks and offer security orchestration and automation capabilities for effective remediation of threats.

If you are a CISO or a decision maker looking to bring value to the table, cost savings is a language that you easily understand. Measuring the monetary benefits of your SIEM investment helps you understand financial blind spots and plan a budget for your security department. Additionally, understanding cost savings is critical because most organizations build their security operations centers (SOCs) around their SIEM solution. In short, calculating cost savings helps enterprises make better spending decisions.




HOW TO QUANTIFY THE BENEFITS

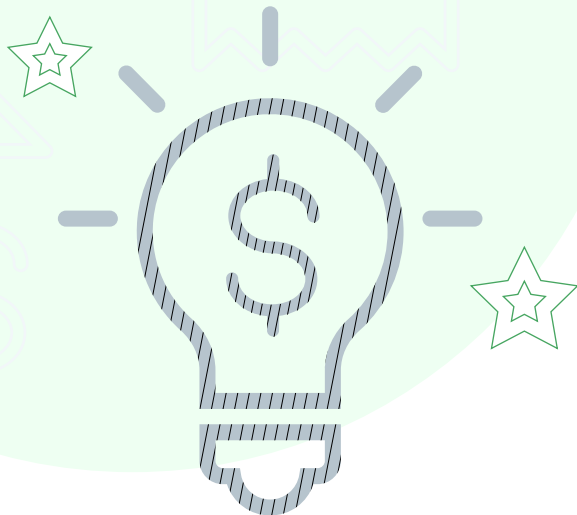


As the saying goes, a penny saved is a penny earned. Returns from a SIEM investment can be realized by saving time and work while avoiding unnecessary costs. Many benefits of investing in a SIEM tool are hidden in blind spots that one might not realize are costing their organization money. Organizations are losing money due to delayed threat detection and response, regulatory fines, and wasted analysts' time.

While these tangible metrics are usually measured, there are numerous intangible benefits to investing in SIEM as well. Implementing SIEM can improve visibility and confidence over the network, enhance team efficiencies, and ease workforce challenges.



Moreover, not having to purchase separate tools that perform different functions in silos—viz-a-viz investing in a single comprehensive SIEM solution—is also a key consideration. Using one comprehensive SIEM solution can help a small yet dedicated team work more efficiently.



THREE PERSPECTIVES IN MEASURING COSTS SAVED USING A SIEM SOLUTION

Compliance

Organizations must conform to stringent and complex compliance requirements to protect the data they hold. Compliance standards tend to be highly prescriptive and regularly require several person-hours in collecting logs, updating statuses, and maintaining reports.

There is also a considerable amount of time spent liaising with auditors and giving them the information they seek. Failure to comply or any standard violation may result in hefty legal fines. Of course, compliance requirements are there for a reason, so not adhering to them can also lead to lax security controls that attackers can exploit.

Here are some of the compliance standards that organizations (depending on their industry) must conform to:



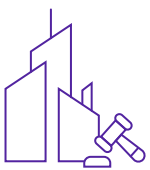
GDPR: General Data Protection Regulation (GDPR), enforced by the European Union (EU), applies to any enterprise handling the data of European citizens. This concerns how enterprises manage individuals' digital privacy. GDPR requires organizations to notify about personal data breaches within 72 hours and submit a compliance status report. Organizations may need to generate security event reports on user logons, privilege changes, and file access, among others, for the required period.



PCI DSS: Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards that protect payment card information from security breaches. PCI DSS emphasizes logging and reporting events related to network devices, web applications, firewalls, user logons, object access, etc.



ISO 27001 ISO 27001 is the international standard for securing information assets from threats. It provides requirements for holistic information security management.



Sarbanes-Oxley Act (SOX): In the United States, all public companies, accounting firms, and private organizations on the verge of IPO must comply with SOX regulations that mandate the accuracy, integrity, and security of the financial information the companies handle.



HIPAA: The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law in the United States designed to refine the movement and continuity of health insurance coverage in individual and group markets.



NERC CIP: North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) is a regulatory framework designed to ensure the reliability of the North American bulk power system by protecting critical infrastructure, known as Bulk Electric System (BES) cyber assets, from cyberattacks. This requirement states that each instance of access to end-point devices, firewalls, and web servers should be documented.



FISMA: Federal Information Security Management Act (FISMA) mandates that federal agencies in the United States and organizations dealing with government information establish a formal security program and conduct annual audit reviews to ensure continuous network security.



Cyber Incident Reporting for Critical Infrastructure Act of 2022: This act makes it compulsory for organizations in the United States to report any cybersecurity incidents to the Cybersecurity and Infrastructure Security Agency (CISA) within 72 hours and report all new information pertaining to an incident until it's fully resolved. Organizations are required to submit reports on events such as unauthorized access, zero-day vulnerabilities, threats detected, and more.



CCPA: Under the California Consumer Privacy Act (CCPA), businesses must put adequate measures in place to defend against data breaches and identity theft, and penalties are imposed upon violation.

All compliance standards discussed above mandate documenting and reporting on various network and security events. Considering the average time of about 10 minutes to manually generate one AD change audit report, the amount of working time needed for compliance reporting becomes untenable when using tools that lack out-of-the-box compliance templates.

Audit-ready templates and violation alerts can ease compliance reporting for analysts by effectively reducing manual work in report building and event monitoring. Moreover, secured log archival is also critical for retaining logs, as tampering or deleting can result in larger trouble and hefty fines from the concerned authorities.

Operational efficiency

The operating efficiency of your SOC is a great metric that not just offers you financial benefits but helps reduce alert fatigue and analyst burnout by saving time and effort involved in alert triaging and response operations.

Security teams are often overwhelmed with alerts, with false positive alerts incorrectly indicating that a vulnerability is present. While some of these alerts are false positives, others might be true positives that are overlooked. Investigating alerts takes most of the analysts' time, as it may involve the manual triaging of each alert and taking individual response measures. When alerts start stacking up and don't get dealt with promptly or at all, important issues may go unnoticed and spiral out of control, resulting in a huge breach.

With increasing alert volume, hiring more analysts may not always be the right approach as it will not bring down the volume or offer you more context. Focusing on refining your alerts, reducing false positives, and automating investigation and response could be the long term solution. It is imperative to improve the SOC teams' efficiency to reduce the time spent on standard, repetitive response measures and dedicate more time to higher-value activities.

When it comes to efficiency, out-of-the-box templates that bring in all security events from across the network are a significant enabler. It makes investigations easier and faster, and keeps all the relevant information in one place. Reducing false positives while expediting the triage and investigation of legitimate alerts ensures SOCs focus on their KPIs. Triggering response workflows for known alert profiles improves the number of threats automatically mitigated. As more threats become blocked at the initial phase, the less likely they are to result in a breach.

Mitigating the impact of a breach

Many organizations underestimate the risk of a breach. A breach is inevitable; however, the severity matters. It is essential to note that your SIEM investment doesn't just reduce the likelihood of a data breach but also the impact and potential fallout of a breach.

From a financial aspect, the cost of a single breach (single loss expectancy) includes the cost of lost business, costs due to system downtime, regulatory fines, and the cost of response and investigations, which includes hiring outside experts.

Two important metrics to measure the effect of a breach are MTTD (mean time to detect) and MTTR (mean time to recovery).

MTTD is the average time it takes to discover a potential security threat. In many cases, attackers might have access to your network long before a breach. It might be through a phishing campaign carried out a few months back followed by slow lateral movement across the network to gain access to more resources until the final act of data exfiltration. They try to leave little or no indicators of a data breach, making it harder to detect. Monitoring all devices, users, and visibility over the network—with more contextual information about a suspicious event or incident—is critical. Doing this effectively can help bring down the MTTD.

MTTR is the time it takes to contain, remediate, or eradicate the threat once it's been discovered. It entails response measures, investigation, escalation, threat forensics, data audits, and tracking incidents timelines.

The lower the number of days it takes to detect and repair, the lower the cost of the breach.

Table 1 below shows the associated costs from 3 perspectives and how a SIEM solution helps.

Metrics	Associated costs	How a comprehensive SIEM helps
Compliance	<ul style="list-style-type: none"> • Legal costs. • Regulatory fines. • More compliance analysts are required to manually pull records during audits. This leads to higher wage costs. • Hiring outside experts to undertake incident investigations. 	<ul style="list-style-type: none"> • Audit-ready templates and reports are available at any time. • Real-time compliance violation alerts. • Secure archiving ensures that a tamper-proof log is available for forensics and audits. • Advanced threat analytics to aid in forensic investigation. • Records can be easily retrieved for audit preparation.
Operational efficiency	<ul style="list-style-type: none"> • A high proportion of false positives wastes analysts' working time. And extra working time leads to higher costs. • More analysts and working hours are required to investigate any influx of alerts. • High manual work to evaluate, analyze, and respond to each alert, which can lead to alert fatigue and burnout. This also leads to more time being spent on alerts and therefore higher costs. 	<ul style="list-style-type: none"> • Easy alert triaging: Dynamic threat intelligence feeds for quick information on indicators of compromise (IOCs), with reputation scores and geolocation details. • The number and variety of incidents to investigate is reduced with automated playbook-based response workflows.

	<ul style="list-style-type: none"> Missing or having a slow response to alerts can spiral into a significant breach. A breach leads to costs associated with business downtime, loss of reputation, legal fees, and compliance penalties. 	<ul style="list-style-type: none"> Reduced false positives using anomaly detection and correlation rules-based alert profiles with risk prioritization.
Mitigating the impact of a breach	<ul style="list-style-type: none"> Financial exposure: Business disruption, extended system downtime, and lost customers due to higher MTTD (mean time to detect) and MTTR (mean time to recover). Response activities: Hiring investigation, forensics, and auditing services. Legal costs and regulatory fines. 	<ul style="list-style-type: none"> UEBA: Anomaly detection using seasonality and peer-group analysis can ensure no threats go unnoticed. Dashboards enable better network visibility. SOAR: Playbook-based automated response workflows initiate as soon as alerts are triggered. Quick reaction time reduces the attack window before further data can be affected. External ticketing to probe into incidents and track repair progress easily. Reduced SLAs minimize business disruption.

Table 1: The table depicts the costs associated with compliance reporting, operational efficiency, and the impact of a breach, as well as the various capabilities of an effective SIEM solution

Calculating cost savings through an example

In this section, we will illustrate the cost savings due to a SIEM implementation through the example of a hypothetical company called Legacy Corporation. Understanding how Legacy Corp's CISO would calculate cost savings using various metrics can provide a better picture of the financial advantages of a comprehensive SIEM. We will also assume that Legacy Corp has 7,000 employees; this will help us make some informed assumptions as we do our calculations.

Organization: Legacy Corporation

Size: 7000 employees

Story: Legacy Corp. is based in the United States with over 7,000 employees. It has been using a basic log collection tool for compliance management and network monitoring. Due to increased incidents of data breaches and the looming fines associated with non-compliance, Legacy Corp has been hiring more analysts for its compliance and IT teams to conduct a greater number of compliance audits and hopefully detect more threats in its network.

However, despite analysts working round the clock and an increase in spending, this enterprise is unable to reach its goals. The security tool they use lacks modern SIEM features such as:

- ✔ Audit-ready templates.
- ✔ Incident forensics.
- ✔ Correlation engine with ML and AI capabilities.
- ✔ Security automation and response.

Legacy Corp's CISO wants to invest in a unified and comprehensive SIEM solution that will alleviate the organization's challenges. But before he gets the necessary budget approval, he needs to calculate the possible cost savings of this implementation.

Here is an example of how Legacy Corp's CISO could compute the financial benefits of a SIEM solution by **forecasting** cost savings based on the three metrics: Compliance reporting, operational efficiency, and impact mitigation.

Compliance reporting		
	Basic tool (present tool)	After SIEM implementation
Number of employees who work in compliance reporting	5	3
Salary of one employee who works in compliance reporting*	\$78,686	\$78,686
Total yearly compliance reporting cost	\$393,430	\$236,058
Savings		\$157,372
*Average salary of an compliance analyst in USD obtained from glassdoor.com		

This computation is based on cost overhead with respect to the number of employees required to work on compliance reporting.

The CISO assumes a 40% reduction in headcount with respect to compliance reporting as a SIEM implementation can provide out-of-the-box reports and alerts on compliance violations in real time. The basic tool required more hours of analysts' time as they had to manually conduct audits. Using a SIEM tool, the analysts will likely no longer have to waste time on searching through logs, filling records, and maintaining documents.

Operational efficiency		
	Basic tool	After SIEM Implementation*
Monthly alerts	5,000	
How many are false positives	1,500	750
Total alerts to attend in a month	5,000	4,250
Total alerts to attend in a year	60,000	51,000
Minutes spent on each alert	30	15
Total hours spent working on alerts	30,000	12,750
**Security analyst salary calculated by the hour	\$40	\$40
Total spend	\$1,200,000	\$510,000
Savings		\$690,000
<p>*After SIEM: Values when using an effective SIEM tool with advanced detection and incident response capabilities. **Security analyst salary obtained from glassdoor.com</p>		

The existing tool used by Legacy Corp generated 5,000 alerts a month or 60,000 in a year, of which 30% were false positives. With event correlations, rule-based alert profiles, and anomaly detection that employs seasonality and peer group analysis, a 50% reduction in false positives is assumed after SIEM implementation.

Minutes spent on each alert includes time to review, analyze, and respond. With a SIEM tool, dynamic threat intelligence feeds can offer quick information on indicators of compromise (IOCs), with reputation scores and geolocation details for faster analysis. Also, analysts do not have to worry about the immediate response measures as automated response workflows can be set. Hence, the CISO estimates that analysts will spend 15 minutes on average to work on each alert after SIEM implementation.

Considering that Legacy Corp can save 57.5% of its workforce's total hours spent working on alerts, this corresponds to a yearly savings of up to \$690,000.

Mitigating the impact of a breach		
	Basic tool	After SIEM Implementation
MTTD (number of days)	239	212
MTTR (number of days)	85	77
Total number of days	324	289
Average daily cost of a breach	\$6,546	\$6,546
Total cost of a breach (Single loss expectancy)	\$2,120,904	\$1,891,794
Number of breaches per year (Annual rate of occurrence)	1	1
Total cost of breaches (Annualized loss expectancy)	\$2,120,904	\$1,891,794
Savings		\$229,110
MTTD, MTTR, and daily cost of breach data obtained from Ponemon institute Cost of a Data Breach report.		

The lower MTTR and MTTD after SIEM implementation are assumed by weighing various security AI and automation features such as user and entity behavior analytics (UEBA) and security orchestration, automation and response (SOAR). Incident management and ticketing also aid in faster resolution. By lowering the total number of days needed from 324 to a conservative estimate of 289, the total cost of the breach can be brought down with savings of up to \$229,110.

We obtained the total cost of a breach by multiplying the average daily cost with the total number of days. The annualized loss expectancy is the product of cost of a single breach and the number of breaches in the year.

The total estimated cost savings of a SIEM implementation would then be the sum of the cost savings due to better compliance readiness, operational efficiency, and breach impact mitigation. This is shown in the table below.

Metrics	Savings
Compliance reporting	\$157,372
Operations efficiency	\$690,000
Impact of a breach	\$229,110
Total	\$1,076,482

Note:

Implementing a SIEM solution is a continual activity rather than a one-time purchase. It is a combined exercise that involves following the best practices in cybersecurity, training the teams to stay up to date, and optimizing processes constantly. Though real-life conditions may be different, this is to be taken as an illustrative example of how much one stands to gain by computing the cost savings at *Legacy Corp.*

You can get an estimate of how much Log360, a comprehensive SIEM solution, costs [here](#). Please note that the cost of Log360 given here is an approximate value. The final price may vary.

ABOUT THE AUTHOR



Varun currently works as a product marketing specialist for IT security solutions at ManageEngine. He has authored various blogs on the latest trends in cybersecurity. His favorite themes include security information and event management (SIEM), cloud security, and security orchestration, automation and response (SOAR).

ABOUT LOG360

Log360 is a unified SIEM solution with integrated DLP and CASB capabilities to detect, investigate, and respond to security threats. It brings threat intelligence, machine learning-based anomaly detection, rule-based attack detection, event correlation, log forensics, cloud security monitoring, and incident management to address complex security use cases of organizations. Log360 ensures the security of different on-premises, hybrid, and cloud network components such as Active Directory, perimeter devices, workstations, databases, business-critical applications, cloud services, and more through continuous monitoring.

The user interface is simple to understand and use. With its intuitive dashboards and advanced security analytics capabilities, a security analyst will immediately know if a threat is lurking anywhere in the network. With alerts and contextual responses, they can also resolve a problem before it turns into a major security incident.

For more information about Log360, visit manageengine.com/log-management.

\$ Get Quote

↓ Download

REFERENCES

1. https://www.cisco.com/c/dam/m/sl_si/events/2017/cisco-connect/pdf/ConnectSLO_What-can-you-lose_Security_2015-03-16-v3.pdf
2. <https://www.ibm.com/au-en/security/data-breach>
3. <https://securityintelligence.com/how-business-continuity-management-boosts-value-in-your-security-program/>
4. https://www.glassdoor.co.in/Salaries/us-security-analyst-salary-SRCH_IL.0,2_IN1_KO3,19.htm?clickSource=searchBtn
5. <https://solutionsreview.com/security-information-event-management/3-ways-to-mitigate-false-positives-in-your-siem/>