Logsign

Migrating Your Legacy SIEM to Logsign Next-Gen SIEM

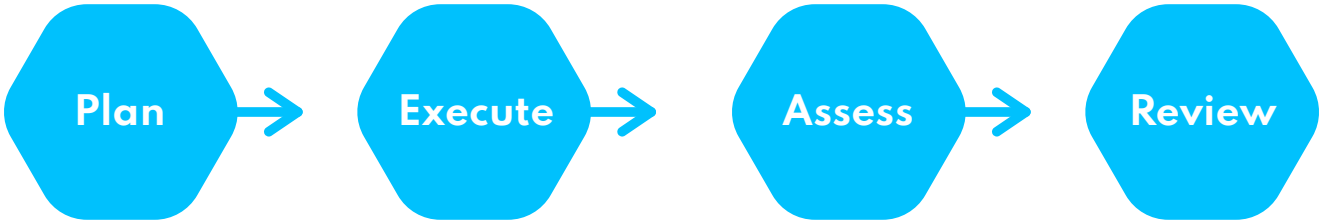
Contents

Migrating Your Legacy SIEM to Logsign Next-Gen SIEM

When organizations strive to achieve the highest level of security possible, it needs to accept that it faces risks from every corner. Irrespective of whether you have a dedicated Security Operation Center (SOC) or not, logging and monitoring will play a crucial role in your security operations. However, as your business expands and grows in size, so does your IT infrastructure. In enterprise networks, there can be hundreds of connected devices and assets that continuously generate logs. In a short period, your team may deal with millions of log events daily. While there is no denying that human beings cannot deal with this amount of log alerts daily, legacy SIEM solutions often falter due to lack of automation and scalability.

One of the primary objectives of a SIEM solution is to assist your team in detecting security threats across the network and respond to them without any delays. As the performance of legacy SIEM solutions continuously downfalls, it becomes imperative for organizations to migrate from their legacy SIEM solutions to platforms such as Logsign. Considering the pivotal role of a SIEM solution in SOCs, SIEM migration is not a simple task. If you or your team has already started discussing the migration, you would know that it would not be a trivial security operation.

The first step in SIEM migration is to choose a service provider that can offer you seamless migration support. In this white paper, we discuss Logsign's four-phase approach to SIEM migration: plan, execute, assess, and review. We compile our learnings from the last few years in our engagements involving migration of legacy SIEM solutions to Logsign's SIEM platform. As organizations look forward to incorporating automation and machine learning in their security ops, we strongly believe in a successful enterprise-level partnership as you switch to a new SIEM solution.



Migrating From a Legacy SIEM Solution: WHY?

As a security solution, SIEM platforms have been around for more than fifteen years now. Legacy SIEM solutions are often hard to configure and complicated. As new technology continues to develop, legacy SIEM platforms become redundant and difficult to scale. In 2020 and beyond, organizations require SIEM solutions that are flexible, scalable, advanced, and analytics-driven. While there are plenty of options to collect and store log data, next-gen SIEM solutions are capable of turning incoming log data into actionable intelligence. Operational hurdles posted by legacy SIEM platforms decrease the efficiency of your security team, and they are not able to focus on high impact and high-risk alerts.

Migrating to Logsign SIEM platform comes with the following benefits for your security operations.

Smartly Designed Big Data Environment

- Big data infrastructure based on Hadoop & NoSQL
- Unlimited scalability for petabyte-level experience
- Fast and easy deployment
- Massively parallelized system with flexibility to add any number of users, notes, or sources
- Continuously active with zero performance loss
- Unlimited log storage
- Long-term data retention

Create Your Own Data Lake

- 250+ built-in integrations and vendor-free integration capabilities
- Unstructured data parsing with free plugin service
- Limitless data collection from any source from any environment
- Real-time data enrichment with real-time threat intelligence
- Flexible data policy manager

Find the Hiddens

- Search functionality with Logsign's drill-down, full-text search
- Accelerated incident investigation
- Uncovering threats, anomalies, and IOCs using the MITRE ATT&CK framework

Heighten the Visualization

- 200+ built-in alerts, dashboards, and reports with easy customization
- Easy-to-use wizards
- User delegation with increased focus on visibility and responsibility

Detect Complicated Threats

- Comprehensive correlation of data
- Risk-score based incident triage
- Advanced detection with minimum noise

Safeguard Your Data

- Automated incident response
- On-time incident notification
- Automated remediation actions for threats and vulnerabilities

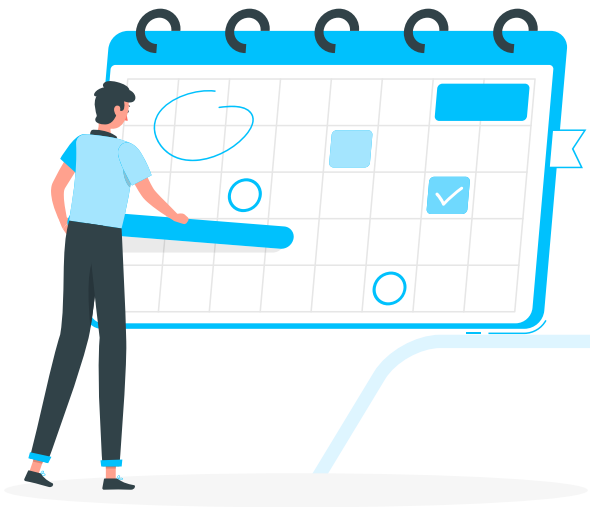
As a result, your storage costs for log entries decreases due to big data architecture. Before big data architecture was adopted for enterprise applications, venders' costing models often relied on the amount of data ingested for calculating the total costs. With an easy to understand cost model and predictable costs, Logsign SIEM also provides long-term data retention capabilities. Another outstanding benefit for your security team can be the utilization of threat intelligence (TI) feeds and behavior analytics. Legacy SIEM platforms only relied on correlation rules to identify suspicious activities within your network.

However, due to the increasing complexity of attacks, our experts encountered many incidents where legacy SIEM solutions were not able to detect an attack. Further, it requires a dedicated individual from your team to continuously update and modify correlation rules. With drill-down full-text search functionality and accelerated investigation features, Logsign's SIEM platform uncovers threats and anomalies in line with MITRE ATT&CK framework.

With over 250+ integrations and 200+ built-in dashboards, reports, and alerts, next-gen SIEM platforms like SIEM offer heightened visualization of your security posture in real-time. With a legacy SIEM solution in place, they are chances that your team may not be able to determine the full extent of an alert due to limited insights. However, with on-time incident notifications and advanced detection capabilities with negligible noise, modern SIEM solutions take your security operations to an altogether different level.

Phase 1: Plan

SIEM migration is often a strategic decision. Considering that it may impact your business operations, the top management's support is crucial. The first phase should start with setting up a dedicated team to look after SIEM migration right from day 1. In the initial meeting itself, all the roles and responsibilities should be defined and conveyed. An ideal team will consist of individuals from the executive team as well as the security team(s). This dedicated team must be familiar with business requirements and organizational priorities. It will help them in identifying the assets and systems with highly sensitive data. This can include critical systems/ applications, security devices, customer information, trade secrets and intellectual property, employee information, financial information, etc.



Once the dedicated team starts functioning, they should request the following information:

i. Risk management framework and the results of the last risk assessment;

ii. Relevant legal, contractual, and regulatory requirements; and

iii. Needs and expectations of interested parties.

In our experience of previous engagements, we have come across various clients who do not entirely replace their existing SIEM solution. Instead, they incorporate next-gen capabilities on top of their legacy SIEM solution. At this point, it becomes necessary to decide how the migration would actually take place. For example, you can adopt a phased-approach or a total replacement. Our expert recommends running both the SIEM solutions in parallel for a while before turning off the legacy solution altogether. An important consideration is also in terms of how you will deploy a SIEM platform: entirely in the cloud as SaaS, on-premises, or hybrid.

After mutual agreement among the stakeholders and top management, the dedicated team should now document the problems that you aim to solve with the migration of your SIEM platform. These problems must relate to security use cases and focus on people, process, and technology. It is also advisable to prepare a network map and identify the sources of log data. In our engagements, we often share a list of in-built use cases with our clients so that they can find out the areas where maximum improvements are required.

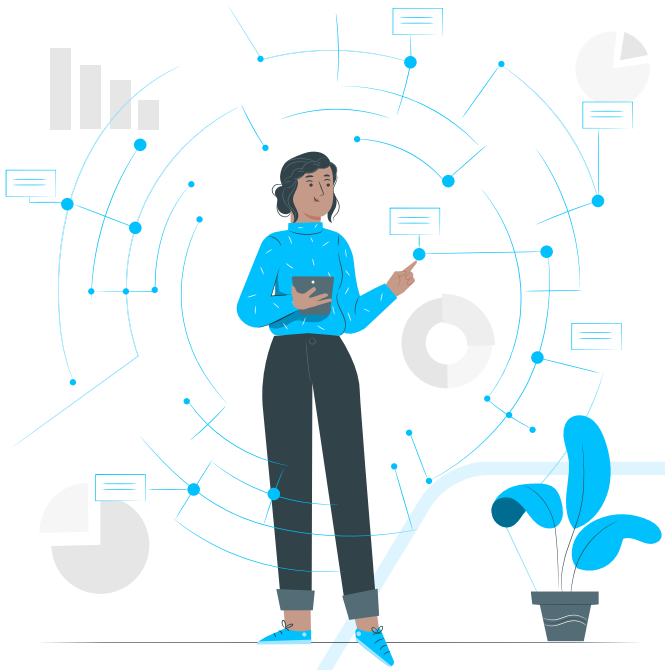
It is also possible that your security team is used to dealing with hundreds of use cases and correlation rules in the existing legacy SIEM platform. Enhanced correlation rules and increased automation features can effectively eliminate the need to look after a large number of static use cases. Frameworks like MITRE ATT&CK can be a good starting point for your organization to identify common attacks and use cases. The main point of focus in this phase should be on the identification of use cases which are critical to business operations. Over time, use cases with less priority or less potential impact can be implemented as your security program looks to attain maturity.

Based on our previous engagements, the duration for this phase may vary between 1 to 2 months. This variation in the time is observed because of the different maturity levels of our clients' security programs before they partnered with us.

Phase 2: Execute

A SIEM solution, whether legacy or next-gen, is useless without log data. Considering that your organizational network will have hundreds of sources of log data, the correct configuration of data sources will be pivotal to the working of your SIEM solution. Typical sources of data include

- Servers for application, database, network, VPN, and email;
- Applications and information services;
- Network devices such as routers and gateways;
- Operating systems; and
- Security tools and techniques such as data loss prevention, mobile device management, firewalls, TI feeds, mobile device management, anti-virus/anti-malware application, etc.



While an organization may prefer configuring their data sources, we always recommend closely coordinating with your SIEM vendor while setting up your SIEM platform and adding log data sources. Ideal SIEM solutions come with inbuilt support for an exhaustive range of data sources and require negligible manual parsing of log data. The dedicated team can also match the existing data sources with use cases from Phase 1 to understand how log data is flowing through.

Though the configuration process is straightforward in theory, it is relatively complex in terms of technology. The dedicated team should start with the ingestion of log data from available sources. This is followed by a SIEM platform's capability to identify every data field correctly. Logsign's SIEM platform comes with over 250+ data sources that you can configure while setting it up for your organization. Our support team also accepts requests from our clients to create new parsers, apart from regularly assisting in the configuration of data sources. Some vendors may charge you an additional fee for providing dedicated support for configuration of log sources.

Once all the required parsers are in place, the next challenge is to shift the existing database from legacy SIEM to next-gen SIEM. If the dedicated team decides to run a new SIEM platform in parallel with the legacy solution before permanently switching it off, both SIEM platforms will require data from log sources at the same time. While identifying data sources is one part, storage is another consideration that often complicates the functioning of a SIEM platform. Next-gen SIEM solutions offer storage options in dedicated data lakes for efficient search results. Most of legacy SIEM solutions prescribe a charge based on data volume; the costs increase with an ever-increasing number of log alerts. However, modern SIEM platforms like Logsign offer a flexible pricing model to meet your business requirements within the available budget.

Given that this phase involves highly complicated activities, it may take between 3 to 6 months for an organization to move onto the next phase. Total duration is proportional to the number of use cases and data sources. If you are also adding new use cases in the migration process, it will require additional time to figure out appropriate log data sources and visualize those use cases in action.

Phase 3: Assess

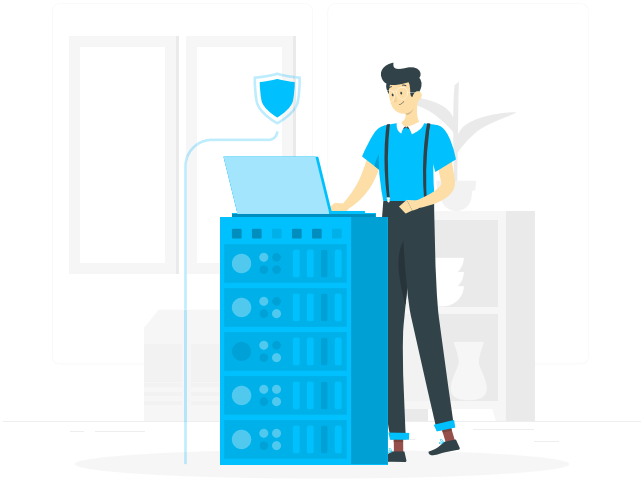
SIEM migration is not completed as soon as your team starts using the new SIEM solution. If your organization had been using a legacy SIEM platform for a considerable amount of time, there are chances that your team is heavily reliant on correlation rules and alerts. On the other hand, modern SIEM solutions use behavior analytics and various machine learning algorithms for providing accurate results and swift detection. This results in a quick and appropriate response to security incidents.

As the new platform sets in motion, your security team will require assistance for effective operations. Your SIEM vendor may conduct a series of training sessions for your team to get familiar with the working of their platform.

The dedicated team is also responsible for ensuring that dashboards, reports, and alert configuration on the new SIEM platform are in line with their defined use cases. This is why we share a list of inbuilt use cases on Logsign SIEM platform so that the onboarding process for organizations gets simplified. If the team comes across instances where a dashboard or report or alert needs to be configured, they should make the relevant changes at this stage.

One important consideration here in this phase is the fulfilment of compliance requirements. An organization is bound by several regulatory, legal, and contractual security obligations. Fulfilment of compliance requirements has been one of the most popular advantages of SIEM platforms. Based on the industry segment you operate in and your geographical location(s), exact requirements may vary. The dedicated team can seek assistance from the legal/ compliance team to understand requirements pertaining to security operations. Following this, you can discuss with your vendor and analyze whether your compliance requirements are being fulfilled.

When your team switches to use the new SIEM platform for their daily activities, they will be dealing with a new platform and user interface (UI). The chances of learning a new language are on the lesser side as next-gen SIEM solutions have a point-and-click interface that replaces the command line interface. Variation is also observable in how alerts are generated and responded to. Your security team will observe an exponential decline in the number of false positive alerts, and this will directly reduce your team's workload.

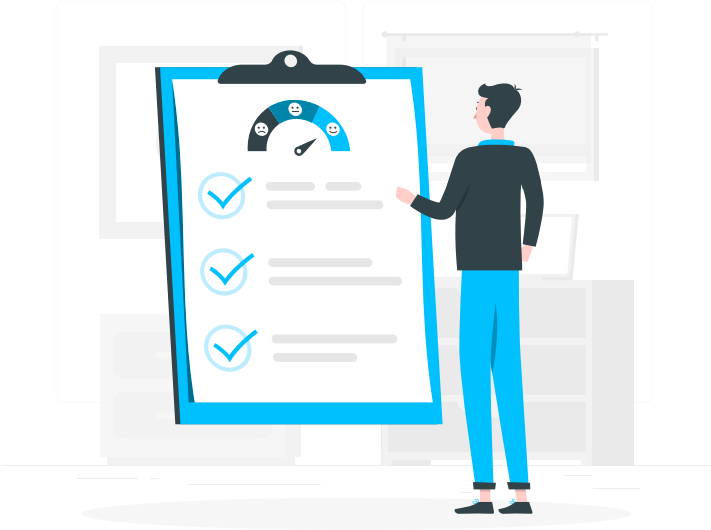


With the adoption of a new SIEM platform, you may need to redefine your productivity expectations from the security team. In legacy SIEM platforms, it may take hours to execute a search query and get the desired results; while next-gen SIEM platforms can present the results in a few seconds or minutes. With automation in the picture, your security team can focus on high priority issues for your organization; instead of mundane and repetitive tasks.

In this phase, the dedicated team should define new operational procedures for your security team. All such operational procedures should be documented and communicated to the interested parties. Overall, this phase may take between 1 to 3 months. Like the previous phase, the duration depends on the number and complexity of use cases.

Phase 4: Review

Without this phase, your organization does not have any way of knowing whether your new SIEM platform is giving the desired results. We recommend setting up a baseline for assessing the performance of the new platform. This baseline can rely on a percentage of false positives, event correlation scope, compliance requirements, etc. However, it must be in line with the standards or regulations your organization currently uses, for example, ISO 27001:2013.



Considering that a modern SIEM platform will continue to fine-tune its detection and response capabilities, it is crucial to adopt a well-defined baseline for precisely understanding its impact on security operations. A baseline can also help your security team in examining which use case has been appropriately implemented and where additional efforts are required.

In this phase, the dedicated team may hand over the responsibility to the organization's security team. To rest the efficiency of a SIEM platform in real-time, the security team can explore the possibilities of conducting a red team exercise. For this exercise, they may partner with a third-party vendor or outsource it entirely. Red team exercises will help in identifying possible issues with the existing use cases that are affecting the detection capabilities of your SIEM platform. Though a modern SIEM will continue to improve its detection capabilities, red team exercises will give comprehensive coverage.

Migration to a next-gen SIEM platform minimizes many requirements that were regularly required by legacy systems. This enables your security team to focus on developing new use cases as your business expands and priorities change. As far as inbuilt features such as use cases, reports, dashboards, and alerts are concerned, we have a dedicated team in place to review and update them. Similarly, your security team can undertake reviews to ensure that use cases are in sync with your business requirements.

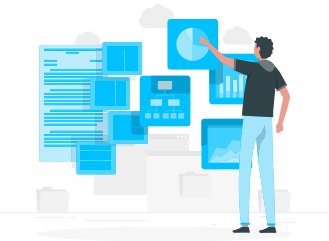
Modern SIEM solutions indeed simplify your security operations; your organization should not do away with the continuous improvement process. Just like other security operations, a SIEM solution should be continuously improved and modified for maintaining an adequate quality of security operations. Whether you follow a four-phase approach or six or eight, you should look at SIEM as a continuously improving component of your security operations.

Logsign Security Information and Event Management

Big data infrastructure with infinite scalability	Limitless log collection and storage	Detection of any complex threats	Fast and effective data protection
Rapid deployment & easy configuration in every environment	Collects every log from every environment with multiple, flexible pricing options	Comprehensive correlation of all your data	Mitigation & eradication of threats
Unlimited log collection & storage	Advanced parsing and indexing techniques	Accelerated, detailed incident investigation	Automated incident notification, response, and remediation
Massively parallelized, fault tolerant system	Easy-to-work with normalized, classified, and enriched data	Early detection of cybersecurity threats	Minimized response times excluding alert fatigue
Long-term data retention		Uncovered anomalies and IOCs	Early prevention of phishing and suspicious network traffic

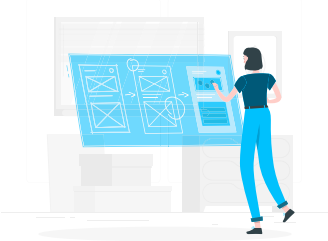
Why Logsign SIEM?

360-Degree Visualization



Visualization with hundreds of built-in security analytics-driven dashboards and reports

Smartly Designed UI



Easy-to-use platform and built-in modules, along with the flexibility to create new ones

Affordable Data Security

Calculating cost is simple with Logsign's multiple, flexible pricing options

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