REDLEGG

MANAGED SECURITY SERVICES

WHAT IS SIEM?

TABLE OF CONTENTS

WHAT IS A SIEM?

Security Information and Event Management (SIEM) is a software and solution for logging, monitoring, alerting, anticipating, correlating and visualizing security-related events and information garnered from networked devices. Plainly, SIEM is a combination of both processes and tools, or products.

SIEM converges various cybersecurity practices with rich contextual information via an aggregated security data repository for network logs, correlation engines, event modelers with alarm customization, ticketing, predictive analyzers and a decision support system that can be augmented with big data analytics for on-demand reporting and compliance.

What is Cloud-based SIEM?
Cloud-based SIEM is provided as a service for organizations. The SIEM platform with its various tools are in the cloud. This means no hardware and lower operational costs across the board. Monitor, analyze, and update your SIEM from one cloud access point.

WHO USES A SIEM?

Although predominantly utilized by sectors like the government, finance, healthcare, manufacturing and law, any organization that is vulnerable to cybersecurity threats like malware, ransomware, zero-day exploits, cyber warfare and insider threats, should implement SIEM (preferably at the beginning or early stages of business expansion). Compliance requirements like GDPR, NIST, audits and log management are another reason.

Do startups need a SIEM?

Cyber attacks do target small businesses. However, many startups can do without a SIEM if data backup policies and general security best practices are followed well. As the business scales up, SIEM should definitely be considered.

SIEM DEFINITIONS

Depending on the service provider, a number of terms may be interchangeable, but here are a few you may come across.

Alarm

Anything that comes from the SIEM, IPS, or Endpoint solution that is notifying you of a potential threat, security risk, or operational problem.

Alert

A notification from which an analyst will determine if the Alert needs to be converted to a case, merged with an existing case, or closed as a false positive or "noise."

Analyzer

When an Observable is detected, analysts may run tools called Analyzers to automatically gather intelligence about that particular piece of data.

Breach

A verified incident that results in information being accessed, disclosed, or exposed.

Case

When an Alert requires investigation or work, the Alert is converted into a Case. Within a Case, tasks can automatically be generated within the Analyzer.

Event

An occurrence that may go against your company's security policy or result in unauthorized activity.

Incident

An event that does result in unauthorized activity or access.

Log

A recorded activity taking place in your company's cyber environment. Logs may originate from your security controls and network infrastructure. Essentially a record of every contact or touch made in your systems.

Observable

Key data points that are identified in an Alarm that allow an analyst to more quickly identify the nature of the activity in question. An Observable could be an IP Address, Domain, URL, or File Hash. IP Addresses are the most common Observable.

Parsing

A rule created to extract data from a log to common fields by the SIEM.

Risk

The likelihood of a threat to enact a certain amount of damage or harm.

Rules

A sequence of correlated logic from logs derived from one or more log sources that when those data points are observed the activity triggers an alarm or alert.

Threat

Event or activity with the potential to cause damage or do harm.

Tuning

Adjusting your alarms and rules to lessen the "static" or "noise" created by logs that do not need further review.

Use Case

A specific situation or scenario in which the product is used.

WHAT IS MANAGED SIEM?

Cybercrime, increasing complex attack vectors, growing hordes of threat actors, shortage of security professionals, and 24x7 readiness are many of the reasons organizations are moving towards managed security providers.

Managed SIEM may also be the first step in aggregating logs into one location, the SIEM. Many businesses may have a SIEM but no way to manage it or provide the workforce needed to review the SIEM's collected logs.

According to the 2019 SIEM Survey Report, 76% of enterprises say SIEM reduces the likelihood of a security breach and 30% of those enterprises also report a reduction in breaches overall.

While SIEM can be effective in reducing the likelihood of a breach, in helping to monitor the environment, and in detecting threats, 40% of enterprises say they lack expert or trained staff to manage their SIEM.

Overall, those who may benefit most from managed service are...

Businesses with a large environment but smaller staff.

Those who spend more time putting out fires than completing projects and whose engineers tend to operate in a reactive mode, not proactive.

Businesses lacking visibility into their environment.

There is limited or no central log collection, no predictable system upgrades or expansions, and likely blindsided by security or operational issues.

Businesses needing to focus staff efforts on innovation, not routine tasks.

Projects may drag on too long because routine and maintenance tasks tie up engineering hours.

Businesses wanting to optimize the value of their employees and focus on company objectives.

We'll discuss the varying options on the next page as there are many ways to achieve this goal within managed services.

MANAGED SIEM OPTIONS

In-House SIEM

Organizations may recruit and train their own team to run an in-house Security Operations Center (SOC), fearing a Managed Security Services Provider's (MSSP) unfamiliarity with the business, risk of data exposure, and loss of control. However, this option can be three to five times more expensive and can result in alarm familiarity/noise, leading to important alarms being ignored. This option may be available for those companies further in their lifecycle and is often seen as an "end goal" for many security teams.

Co-Managed SIEM

An MSSP deploys SIEM from scratch or integrates it with an organization's existing security infrastructure and personnel to improve security posture. This ensures a wider security cover (knowledge of common issues across the industry) at lower cost and generally quicker deployment, depending on the customization. Co-managing also ensures the in-house team remains up-to-date and has access to state-of-the-art security tools.

This option is often seen as a partnership between a managed security services provider and the client security team, helping the client build their operations and manage long-term projects.

Multi-Tenant SIEM

This SIEM option can be compared to multiple renters living in the same apartment complex. A scalable, centralized SIEM, allows security management for multiple client instances (tenants that may be geographically distributed), allowing data segregation, role-based access, centralized upgradation, and lower costs due to shared resources. This option however, has the disadvantage of being a single point of failure that can have a cascading effect on all tenants.

WHY CO-MANAGED SIEM?

If you're hiring a company to help with your company's SIEM, you can normally choose from two options: co-managed and managed SIEM. While both solutions have their pros and cons, there's a strong internal debate in the security community on which option is the best choice.

Companies like to choose co-managed SIEM when they have a decent in-house IT staff but lack the bandwidth to monitor alerts constantly. Such organizations often use the co-managed solution to cut operational costs while they are smaller but look to move many of the functions in-house as they mature. Co-managed SIEM is also known to be a positive step toward building a SOC within your own IT team.

Co-Managed SIEM Advantages

When compared to other managed SIEM service options...

INTEGRATION

- Greater ROI when using the SIEM and accompanying platform with the in-house tools you already own, not just consuming the service.

CAPACITY

- Co-Managed Engineers can intervene and resolve operational issues on systems they have access to resulting in quicker problem resolution.
- Co-Managed Engineers can open and work on support issues with the manufacturer, saving you and your staff from being stuck on a potentially multi-hour support call. You're free to work on productive projects for your organization.
- Build your in-house security team at your pace.

EXPERTISE

- 24x7x365
- Better confidence in your security posture.

LOSSLESS TRANSITION

- If you outgrow MSSp, you don't lose everything that was developed or tuned as happens in other managed SIEM situations; however, some MSSp may have proprietary rules.

CUSTOMIZATION

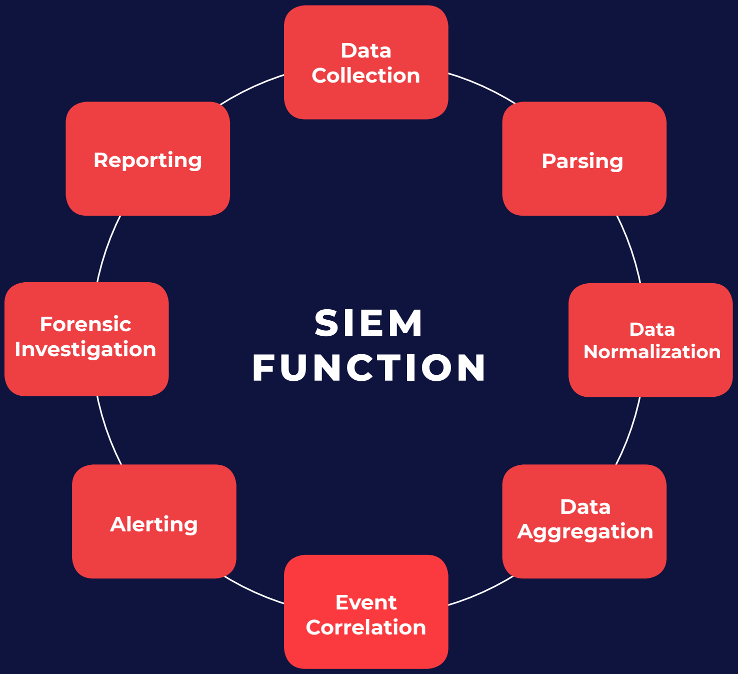
- Customized rules and tuning to your environment which can provide more accurate identification of threats and incidents.
- Co-Managed works with you to create custom weekly reports on the data you need, including ad hoc reports and investigations.
- Retain control and visibility.

MANAGED SIEM TOOLS

A Few Known Platforms and Devices

- LogRhythm’s NextGen SIEM
- IBM’s Qradar SIEM
- Splunk’s Analytics-Driven SIEM
- Exabeam's Security Management Platform

SIEM FUNCTION



SIEM SERVICE FEATURES

SIEM and SIEM Service features are dependent on each provider.

- Data Aggregation and Correlation
- Content and Offense Rules
- Packaged Use Cases
- Advanced Intelligence
- Incident Response & Forensics Service
- Managed Detection and Response (MDR)
- Endpoint Detection and Response (EDR)
- Unified Threat Management/Firewall (UTM)
- Advanced Threat Detection (ATD)
- Intrusion Detection and Prevention Systems (IPS/IDS)
- Threat Intelligence Service Feeds (TI)
- Security Orchestration, Automation, and Response (SOAR)
- Service Desk Integration
- Dashboarding Visualization
- Reporting

Other co-managed SIEM features may include...

- Complementary skillsets and certifications of Engineers and Analysts
    - Python
    - Powershell
    - Regex
- SIEM Capability Build Out

COMMON SIEM MANAGEMENT FEATURES

These management and monitoring features are often offered by the co-managed service, to be performed by the co-managed service's staff. Some fully managed service providers will vary.

Real-Time Analysis

Real-time analysis is performed on critical alarms generated from the SIEM's log correlation. Correlation is performed by the SIEM as logs are inspected to look for relationships, patterns, and trends across all log hosts to identify activity that may be malicious in origin. Actionable events will be investigated and escalated via the ticketing system and pre-determined escalation path.

Health and Performance

Monitoring of appliance health and performance.

Tuning and Configuration

Ongoing tuning to keep up with network changes as well as adding new log sources.

Detailed On-Demand Reporting

On-demand reports detailing statistics and analysis of the activity of the hosts reporting in to the service may be available. Many of the reports are tailored to meet security or compliance requirements.

Patch and Software Updates

When new software updates or patches are available, the co-managed team will schedule a maintenance window to perform updates.

Data Aggregation

As a function of the SIEM itself, logs from your environment are gathered into one central location and displayed together to provide full context to host activity

COMMON SIEM MONITORING FEATURES

Once the SIEM is fully deployed, or if the co-managed team is taking over monitoring of an existing SIEM deployment, monitoring features may then include...

Integrated Ticketing System

When actionable events are identified by the co-managed team or an automated alert is generated, all information is submitted into the ticketing system for investigation, tracking, and auditing purposes.

Log Queries and Investigation

When suspicious activity has been detected or an investigation of the activity of a host is required, the co-managed team can perform custom queries in the SIEM Log Database to retrieve event information from a designated date and time.

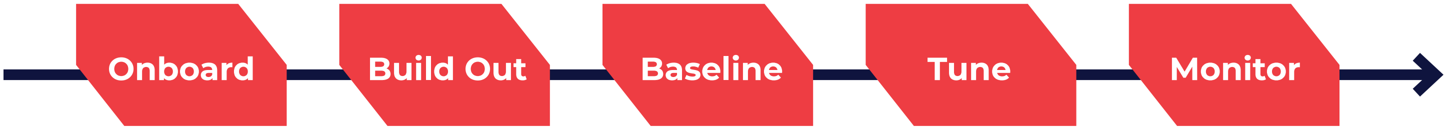
Availability and Outage Notifications

Availability of the equipment is monitored 24x7. In the event that the device, becomes unreachable, an investigation will take place.

HOW IS SIEM CO-MANAGED?

This is an example workflow that details the beginning and ongoing stages of co-managed SIEM. Further ongoing activities are listed in the management and monitoring features.

We've used the RedLegg process as the framework here. Other co-managed and fully managed services may differ in their processes.



PHASE 1: KICKOFF AND ONBOARDING

The co-managed team holds a kickoff call with you and the assigned personnel for the engagement:

- **Deployment Engineer** – Assists with conducting a SIEM health check when taking over an existing SIEM installation, as well as building the appropriate alarms and rules to maximize the capabilities of the system.
- **Support Engineer** – The assigned lead engineer for the account who will handle upgrades, patching, and making sure the SIEM is running at optimal efficiency.

During the kickoff and onboarding phase, the co-managed team discusses your needs and the service team's capabilities for providing the best service. This includes...

- Reviewing your business and security operations
- Assigning the main project contact
- Determining the secondary client contact
- Creating initial escalation documentation
- Reviewing relevant co-managed processes and procedures

PHASE 2: MANAGED SECURITY SERVICE CAPACITY BUILDING

During this phase, the co-managed service team assists in reviewing current log collection and, if needed, collecting additional required log sources from the network. This process helps eliminate unnecessary "noise" and provides the best information to be ingested into the SIEM. This is a significant amount of work designed to help you get the most of your SIEM installation.

- Once the proper log sources are being fed into the SIEM, the co-managed service team builds out the roles for their support and security to send operational and security alarms.
- To build out the operational alarms, the Deployment Engineer goes into the operational rules, copies each applicable operational rule, and creates a customized alert. This is done to prevent the rules from being erased during updates to the SIEM solution. These rules are then installed in the system. The operational alarms allow the co-managed service team to monitor the performance of the SIEM to make sure it is operating at its peak efficiency. Once the Deployment Engineer is sure the rules are operating correctly, alerting of these rules is turned on and monitored and is then handed off to the Security Analysts.
- While Phase 3 is in progress, the Deployment Engineer will work with you to build any additional use case alarms, custom parsers, or dashboards, or upon your request, customizing what you want to monitor and then building it.
- Some customizations may result in additional cost. The Deployment Engineer will advise whether any additional charge is necessary, and then will update and validate the escalation documentation to move the service into Phase 3.

PHASE 3: BASELINING

During Phase 3, the co-managed service's Security Analysts monitor the initial alerts coming into the SIEM and perform initial tuning. This helps to ensure that the alarms are operating properly, that the suppression thresholds are properly set to avoid too many alarms, and that there is no duplication. This is one danger area of SIEM installations, as the initial baselining and operational turning can be overwhelming for many organizations monitoring alerts. During this period, the co-managed service team will work with you to finalize the escalation paths and re-align the escalation plan if necessary. During Phase 3, all alert monitoring and response is performed outside of the SLAs.

PHASE 4: OPERATIONAL TUNING

Phase 4 features the bulk of the tuning of the SIEM. Along with Phase 3, this is one of the danger areas of a SIEM, as the operational tuning can be overwhelming. During Phase 4, the co-managed service's Security Analysts will be monitoring the alerts and investigating them. Real events will be handled according to the escalation procedure. False alarms will be tuned appropriately. During this process, the co-managed service team may be tuning down duplicate alerts, ensuring that the rules fire correctly and that the alerts are sending relevant information, and then verifying what the alarm is forwarding.

PHASE 5: ONGOING MANAGEMENT AND MONITORING

As the false alarms subside and the SIEM alerts stabilize, the environment now has a fully functioning and tuned SIEM. The co-managed service team will continue to monitor security alerts and conduct investigations, while ensuring that the SIEM is running at peak performance. During this time, the co-managed service team will begin running quarterly business reviews, offering suggestions to help improve the services and the overall security posture.

CO-MANAGED SERVICE TEAM STAFFING

When partnering with a co-managed security service, the service may provide staffing for three areas of the SIEM management and monitoring process.

Managed Security Services Staffing

Security Team	Operations Team	Deployment Team
Meet SLAs for all Security Alarms	Customer SMEs	Product Subject Matter Experts
Recieve support calls and tickets		Advanced Product Support
24x7 On-Shift Presence		Deployment Lead Engineers
Threat Analysis		
Basic Troubleshooting and Configuration		

- Your service may provide a team of Information Security engineers. You may be assigned a lead engineer and a team of operations engineers. We will also have a deployment lead as part of our onboarding assigned to the project.
- The service may assign a dedicated Customer Success Manager as well. The Customer Success Manager will be responsible for ensuring that you have a successful project and for delivering our quarterly briefings.
- Co-managed service team members may have multiple certifications. A co-managed service may provide individual tracks for all engineers that include peer-to-peer training, industry certificates, vendor training and certificates, as well as general purpose and customer service training.

HOW REDLEGG CO-MANAGES SIEM

RedLegg offers a co-managed SIEM service to empower your company to achieve its business and security goals as well as build your in-house staff and their capabilities. The security landscape is always changing, and high-level security architects are hard to come by. Products are helpful, but it is the mapping with the products, technology and organizing business politics, policies, compliance requirements, current teams, and objectives that matter. Information Security needs to be done correctly, quickly, and professionally to meet individual your individual and specific needs.

We are expert guides in a complex terrain. As your partner we offer...

- **Personable service and ongoing, open communication**
- **Expert analysts and engineers with complementary skillsets**
- **24x7x365 service in your US-based time zone**

Our expert team members use SOAR/Automation as the engine to our service in order to increase incident response speed and effectiveness. You can read more about the platform online or by giving us a call.

REDLEGG

MANAGED SECURITY SERVICES

CONTACT US

Geneva, IL 📍
877.811.5040 ☎
dotell@redlegg.com ✉
redlegg.com 🌐