SECUINFRA
Cyber Defense. Made in Germany.

Co-Managed SIEM

Working together to stop cyber threats

Security Information and Event Management (SIEM) is an effective tool for increasing cyber security, but for many companies, especially smaller ones, it is often an insurmountable hurdle. This is because implementation and operation require high resources: budget, time, but also expertise, not all of which are always available. This is where the co-managed SIEM approach comes in. Here, the SIEM is set up and maintained jointly with a service provider - companies can flexibly decide which services they want to provide themselves and which they want to have managed externally.

The digitization of all branches of business is progressing inexorably. However, the range of IT security threats is increasing at the same rate. Cyber criminals are constantly on the lookout for security gaps in IT systems and networks in order to access valuable data, sensitive company internals or confidential information. A SIEM (Security Information and Event Management) provides a decisive added value for the information security of companies: It enables them to comprehensively collect security-relevant data, consolidate it in a centralized repository and automatically detect anomalies and rule violations based on previously defined use cases. By using a SIEM system, IT security teams are able to react more quickly to cyber threats of all kinds. This is because the time required to identify an acute threat, the Meantime to Detect, can be significantly reduced. This is a decisive advantage, especially in the case of critical attacks on the IT infrastructure.

However, a SIEM implemented completely in-house is cost- and resource-intensive for companies and requires complex administration. Immense amounts of data have to be analyzed by internal IT security specialists on a daily basis. Companies often lack the resources that are indispensable for setting up and maintaining a SIEM - professional expertise, technical requirements or the corresponding manpower. The solution can be a co-managed SIEM approach, in which a SIEM is implemented in cooperation with an external service provider. For example, the service provider takes over the monitoring of SIEM messages, updates the solution with patches and provides reports and logs. Ideally, the service portfolio is modular and can be flexibly adapted to individual customer requirements.

The advantages of the co-managed SIEM approach

A partially or fully externally managed SIEM offers relevant advantages. After all, the more data is generated within a company, the more complex the detection of current threats becomes. The users of the system - usually SOC analysts - must be able not only to monitor the alerts from their SIEM solution, but also to analyze and evaluate them in detail and respond appropriately to actual threats. An external service provider with its expertise can often do this more professionally than the in-house team.

Another challenge in the operation of a SIEM lies in the staffing of the various roles: From monitoring log sources to developing SIEM content to incident response and threat hunting, the technology only works if all positions are ideally filled and mesh like a cogwheel. This can rarely be fully implemented by a company without the support of external cyber defense experts. Especially in companies with only a small IT security team, an internal SIEM system also carries the risk of capacity bottlenecks: This is because networks and systems need to be monitored around the clock,

365 days a year, in order for the SIEM to be used efficiently. With a co-managed SIEM, these tasks can be outsourced. The in-house IT security team then has sufficient freedom to respond quickly and efficiently to acute problems.

What's more, depending on the size of the company, an internal SIEM can generate costs in the six-figure range. The purchase alone is not enough - the SIEM must then be promptly implemented in the company's IT architecture. Training and education of the SIEM team costs time and money, and afterwards, stable operation with monitoring, utilization and maintenance must be guaranteed. An externally managed SIEM limits these initial costs. Expenses for training, maintenance and security patches are even completely eliminated.

Selecting the right partner for co-managed SIEM

Working with an external partner can result in a first-class SIEM if all these factors can be optimally served. When making a selection, companies should therefore take a close look at the offering of the respective cyber defense specialist. It is holistic if it covers the areas of security monitoring, incident response, content development and maintenance as well as platform operation and log source monitoring.

As part of security monitoring, the service provider's cyber defense experts analyze IT security incidents, qualify them and advise the customer on suitable countermeasures. Threat Hunting is used to review log data based on internal or external incidents or based on Indicators of Compromise (IOCs) or detected attacks by other customers. If security in-cidents are detected, the qualification of the incidents and recommendations for the incident response team for countermeasures follow. The IT security specialist SECUINFRA proceeds in the steps Level 1 and Level 2 analysis:

Level 1 includes the triage and initial analysis of SIEM alerts as well as the elimination of false alarms and duplicate reports. Relevant incidents are escalated to Level 2 analysis. Here, detailed analysis and evaluation of the detected events take place. A consultation with the responsible persons ensures a clear evaluation of the incidents. The resulting recommendations for action for the incident response team conclude the level 2 analysis.

The second important pillar is SIEM content development and maintenance. For this purpose, the SECUINFRA Cyber Defense experts define the required use cases depending on the security needs of the company and select them from the SECUINFRA Use Case Library. Alternatively, the use cases are developed individually for the customer - including log policy, SIEM rules, test routines and runbook. SECUINFRA's cybersecurity specialists have already developed more than 200 SIEM use cases based on the MITRE ATT&CK framework - including the provision of the necessary specifications for said log policy, test routines and runbooks. Subsequently, the "end-to-end SIEM use cases" are implemented, initially and later regularly tested and optimized. Continuous maintenance of the content is also important.

Last but not least, professional platform operation and qualified log source monitoring are the prerequisites for smooth SIEM operation. The former includes, among other things, release planning, i.e. testing and importing updates, checking the availability of the SIEM infrastructure, troubleshooting software problems in the infrastructure components, and regularly checking the license volume. Log source monitoring ensures the availability and quality of the connected log data. If necessary, adjustments to the

log policy are made or escalation to the person responsible for the log source is taken over.

It is ideal if a partner like SECUINFRA also offers an incident response as an option: This means that the cyber defense experts are also immediately available when an IT security incident actually occurs at the customer's site. After the compromised IT systems have been identified by means of a compromise assessment, forensic analyses are performed to clarify the course of events and to preserve evidence, and support is provided to restore IT operations as quickly as possible.

The necessary infrastructure

With SECUINFRA's flexible co-managed SIEM approach, any SIEM system and the required components can be installed and operated within the customer's network. The customer provides the operating system platform on which the expert team installs, configures and operates the SIEM system via remote access. Alternatively, it is also possible that the customer operates the platform independently and is only supported by individual modules from SECUINFRA. With this hybrid offer, data protection is guaranteed at all times. The data does not leave the ordering company and access to it is exclusively from Germany.

Conclusion

A SIEM system can significantly shorten the time it takes to discover an IT security incident and significantly increase cybersecurity. However, companies with small budgets and a lack of in-house IT security experts are often overwhelmed by this on their own due to a lack of resources. This is where a hybrid co-managed SIEM approach can provide flexible help. This makes it possible to set up and operate a SIEM individually and modularly

with services according to the modular principle. Companies can then decide for themselves which services they want to provide themselves and for which they need external support. Missing resources and expertise can thus be compensated for by adding a specialized partner.

Author: Ramon Weil, CEO & Founder SECUINFRA

Further Information: https://www.secuinfra.com/de/services/co-managed-siem/

Press contact:

SECUINFRA GmbH

Svenja Koch

Stefan-Heym-Platz 1

10367 Berlin

Deutschland

Tel. +49 (0)30 5557021 11

sales@secuinfra.com