Professional article

How companies find the right solution

The five most important aspects of a successful SIEM implementation

Security Information and Event Management (SIEM) provides crucial added value for corporate information security in the detection of IT security incidents. This can significantly shorten the time it takes to identify a threat and thus increase the level of IT security. The prerequisite: the choice and implementation of the solution are well planned.

Cyber criminals do not sleep: last year, there were more attacks on companies, NGOs and governments worldwide than ever before. It is not just the sheer volume that poses a challenge, but also the increasing professionalism of the attacks. Whether it's ransomware, phishing, drive-by downloads or social engineering, hackers are leaving no stone unturned to compromise networks, gain access to corporate data and extort ransoms.

With the plethora of daily threats, enterprise cybersecurity teams need to be able to respond quickly and efficiently to threat situations. This is where Security Information and Event Management (SIEM) comes in: It combines components of security information management (SIM) and security event management (SEM). A SIEM solution collects enterprise-wide log data from underlying sources such as servers, endpoints, firewalls, intrusion detection and prevention systems (IDS and IPS), and applications. In a central management station, the data is aggregated, processed, and correlated and visualized on dashboards. Based on previously defined use cases, anomalies and rule violations can now be detected automatically. IT security incidents can thus be identified at an early stage by cyber defense analysts - in areas that conventional IT security solutions do not take into account. This offers IT security teams a decisive advantage - because the time required to identify an acute threat (mean time to detect) can be significantly reduced by a SIEM. This makes the work of IT security specialists more effective and significantly increases the level of IT security.

The prerequisite is that the relevant aspects are taken into account before implementation. After all, SIEM is much more than a product. The introduction must be well planned to avoid disappointed expectations and late cost explosions. Here, it is first elementary to define the specific company requirements. It makes sense to create a SIEM concept that forms the basis for the introduction and subsequent operation. Five aspects are central to implementation.

Integratability

SIEM solutions usually come with interfaces for common systems, but these do not necessarily match the systems used in the company. If interfaces are missing, the implementation time is significantly extended because connectors have to be developed manually. This leads to additional investment costs. For a SIEM system to offer relevant added value in the fight against cyber threats, the solution must be tailored as well as possible to the existing IT infrastructure. Before implementation, it is therefore necessary to define which log data a SIEM solution must process.

Costs

The payment models for SIEM solutions differ significantly in some cases: they are billed according to data volume, the incoming number of events or the connected systems. Many system manufacturers also offer attractive discounts for extensive implementations, but this can be a cost trap for small and medium-sized enterprises (SMEs). If an SME processes ten gigabytes of data volume in its SIEM system every day, it will have to pay for it in full. Groups, on the other hand, benefit from scalability - if, for example, 250 gigabytes of data volume are used here, the final price is proportionally lower because of the discounts. SMEs should therefore also take a close look at the cost structure of the SIEM solution in terms of sales and profit figures.

Functional scope

In terms of functional scope, many SIEM systems are also designed for use in large corporations - for example, with granular rights management or client sharing for the parent company and the IT systems of sub-companies. This is often oversized and unnecessarily complex for SMEs. In addition, it has been shown that many companies only use the basic functions in the first few years after implementation. If a solution that is reduced in scope is optimized to meet the company's requirements, this is an economical and secure approach. However, companies often opt for a SIEM solution that is far too comprehensive. In the absence of experience, those responsible often make decisions based on the familiarity of a product and trust that it will do all the work for them. However, no product can do that - not even the one with the most comprehensive range of features. Before making a decision, it is therefore essential to define which functions are really needed. It makes sense to develop an initial SIEM concept.

Use cases and detection rules

Use cases as the logical element for detecting attacks and their detection rules as the technical implementation of the logic are the heart of a SIEM system. For almost all vendors, supplied use cases as practical "out-of-the-box" solutions are one of the central selling points. However, these ready-made rules usually add little value. On the one hand, they are generic and thus hardly fit the IT landscape or the threat situation and have to be adapted at great expense. In most cases, there is a lack of information about which logs or events are required by the IT system, as well as instructions for action for cyber defense analysts in the event of an alarm. The large number of rules also often leads to a veritable flood of alarms if they are activated extensively. The rules must be selected sensibly in advance. Both for this selection process and for the subsequent processing of the alarms from the use cases, it is also important that these have a direct link to known IT security frameworks such as MITRE ATT&CK. With this and the appropriate expert knowledge, the essential goal of use case selection can be achieved: to obtain the maximum coverage of known attack vectors with the smallest possible number of high-quality use cases.

SIEM consultants such as the experts at SECUINFRA therefore recommend the use of use cases whose documentation and recommended actions are comprehensive and whose detection rules are specifically adapted to the IT landscape. When selecting these, care should be taken to ensure a broad spread of detection mechanisms in order to identify attack behavior at an early stage. The principle here is: it is better to implement a few high-quality use cases than many rules that are prone to errors and work. This is the key to effective and economical SIEM operation.

Trained personnel

For a SIEM to be effective, users - typically SOC analysts - must understand attack scenarios and alerts and know exactly how to respond. SIEM solutions do the repetitive work, but analysts must put the resulting alerts into context. Companies often need expert support here: experienced cyber defense analysts can reliably identify attack patterns and complex contexts.

A SIEM system is only effective if it is optimally adapted to the existing IT infrastructure. By opting for SIEM consulting prior to or during the project, companies not only save time and money, but also avoid problems and stumbling blocks that often arise on the way to a successful SIEM operation. If these aspects are taken into account, SIEM is an extremely powerful tool in the fight against cyber threats.

Conclusion

Security Information and Event Management significantly accelerates the detection of attacks and relieves cyber defense from repetitive routine tasks. Customized detection mechanisms in SIEM solutions can significantly increase a company's cyber resilience - but only if the product can be tailored to individual needs. Those who rely on out-of-the-box solutions often end up paying twice, resulting in higher costs overall. To avoid making the wrong economic decisions and at the same time optimize the functionality of the SIEM system, it makes sense to seek support from experts in the early stages of decision-making.

Authors:

Norbert Nitsche, Senior Cyber Defense Consultant SECUINFRA

David Bischoff, Senior Cyber Defense Consultant SECUINFRA

Further information:

https://www.secuinfra.com/en/solutions/siem/

Press contact:

SECUINFRA GmbH
Svenja Koch
Stefan-Heym-Platz 1
10367 Berlin
Deutschland
Tel. +49 160 921 633 44
svenja.koch@secuinfra.com