Security Information & Event Management

AEC

Do you know what's happening in your infrastructure?

The diversity of technologies in infrastructure is growing every day, the number of administrators is increasing and some elements are often administered by external organizations. This „weakens" awareness of the security situation, with the absence of a subsequent overall view. Most IT staff only deal with information in the log after a non-standard situation is reported. Events are not monitored minute by minute, twenty-four hours a day, seven days a week. At the same time, any device connected to the infrastructure can hold important information that allows us to broaden our view of adverse situations.

The role of an SIEM solution is to provide an overall picture of the security situation in your infrastructure based on individual information.

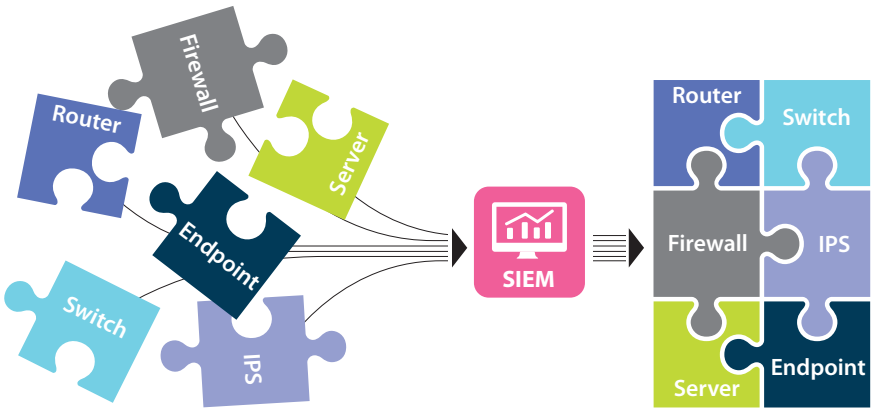
aec-security.eu

Security Information and Event Management is a solution that consolidates information about security events and incidents from many different sources distributed throughout the infrastructure in one central location. It stores the collected information in unchanged form as records (logs) for the detailed investigation of incidents, protects it from unauthorized modification, and creates logical links over data to distinguish real threats from false alarms. It thus provides security analysts and operators with access to information on security events and incidents in real time, but also retrospectively for in-depth analysis.

Key benefits of SIEM solutions

- Collection, normalization, categorization, storage of events and other information for investigation, in-depth and forensic analysis and to thus enable compliance with regulatory requirements.
- Analysis of information, processed in real time, i.e., to detect targeted attacks, advanced threats, infrastructure security breaches in time and to respond to them in a timely manner.
- Reporting deviations from regulatory requirements and thereby drawing attention to emerging deficiencies and the development of the security situation.

Security Information & Event Management



How is a SIEM solution from AEC implemented?

Analysis
A detailed analysis of all the links and specifics of the organization, its business model, technologies and processes must be performed at the very beginning of the project. This analysis is an integral part of deploying the SIEM solution. Analysts use risk analysis, which documents potential risks and their impacts. They also focus on threat modelling and an analysis of customized applications and their ability to provide the necessary information. They evaluate what legislative requirements are placed on the customer and define how to ensure compliance management.

Selection of optimal solution
Based on the information and requirements gathered in the analysis, we will propose a suitable solution that corresponds to the organization's specific conditions, including a detailed summary of the advantages and disadvantages of individual options.

Implementation and configuration
We will implement all components of the SIEM solution, integrate them with systems in the customer's infrastructure and help connect log sources, their parsing and categorization.

Optimizing evaluation
This involves optimizing the collection and evaluation of obtained data and creating your own/unique detection and correlation rules, which reflect situations identified by risk analysis or threat modelling.

Pilot operation
We provide staff training and test the delivered solution in cooperation with the customer during pilot operation. We also offer verification of detection capability in the form of penetration tests simulating a real attack.

Handover of the solution
At the end of pilot operation, we hand the solution over to the customer for full operation, which it can either undertake at its own expense or it can choose the option of professional security management in the form of a service. AEC offers the services of its AEC Cyber Defense Center, which monitors, detects and escalates security incidents.

Technical support
We provide technical support for the delivered solution, in the context of which we also handle the system's further modification and development and training new employees, as required.

Certification

Our security specialists hold the following professional certificates:

IBM Certified Associate Administrator
IBM Certified Deployment Professional
IBM Certified SOC Analyst
IBM Certified Associate Analyst
RSA Certified Analyst
RSA SE Professional
RSA SE Master
RSA Certified Administrator

Benefits of the solution

- Reduction of the response time to an incident (increased efficiency), i.e., mitigating the impact of a security incident (reducing recovery costs).
- Centralization of security information in one location.
- Overview of the current security situation of protected infrastructure.
- Minimization of the possibility of operator error (security automation) thanks to predefined procedures for dealing with security incidents.
- Coverage of a comprehensive portfolio of security threats (through the integration of multiple sources and creation of correlations). Reflection of known and zero-day threats.

Why AEC?

- We have experienced and certified specialists in the field of SIEM solutions, as well as other areas of information security.
- We have experience with dozens of successful implementations of SIEM solutions.
- We work with leaders in the field of SIEM solutions. We are not limited to a specific manufacturer; we look for the best solution for each specific case.
- We don't install servers and applications; we create solutions that really help customers.
- Our implementations reflect legislative requirements, such as the Cybersecurity Act, ISO, PCI DSS, and more.
- Our work doesn't end with implementation, we continue to maintain and develop the solution.

Prague – AEC a.s., Voctářova 20a, 180 00 Praha 8, tel: +420 226 229 133
Brno – AEC a.s., Veveří 102, 616 00 Brno, tel: +420 541 235 466
Bratislava – AEC s. r. o., Prievozská 6, 821 09 Bratislava, tel.: +421 254 410 283