INFOSEC EXPOSED

Nov 2021

geevo® - delivering positive change!

INSIDE

Our contact details

Tel: +357 24 023203

Email: info@geevo.eu

Visit us: www.geevo.eu

NEW FINDINGS THIS MONTH

By Constantinos Andreou, Cyber Security Engineer and Vikentios Vikentiou, Cyber Security Consultant.

Cyber-attacks have increased dramatically in 2021 and according to the Security Magazine over 2,200 attacks occur daily. Most companies now deploy cybersecurity solutions such as SIEM and SOC to prevent such attacks.

SIEM and SOC are important concepts in Cyber Security. SIEM stands for Security Incident Event Management and is different from SOC, as it is a system that collects and analyzes aggregated log data. SOC stands for Security Operations Center and consists of people, processes and technology designed to deal with security events picked up from the SIEM log analysis. A SIEM solution consists of a number of components involved in Security Information Management (SIM) and Security Event Management (SEM) including the following:

- Data Aggregation
- Threat Intelligence
- Security Event Correlation
- Advanced Analytics
- SOC Automation
- Dashboards
- Threat Hunting
- Forensics

Speak to our data protection and information security experts!

A Security Operations Center (SOC) should be part of the security strategy of an organization and should be responsible for analyzing and protecting the organization from cyber-attacks. SOC provide two types of services, monitoring and incident management. Both of these services are an important part of how a SOC runs its day to day activities.

When you need it

SIEM-as-a-Service

- Reduce the time to identify threats and minimize the damages from potential threats.
- Offer a holistic view of your organization's information security environment, making it easier to gather and analyze security information to keep systems safe.
- Use it for a variety of use cases that revolve around data or logs, including security programs, audit, and compliance reporting, help desk and network troubleshooting.
- Perform detailed forensic analysis in the event of major security breaches.

SOC-as-a-Service

- Significantly reduce the cost of hiring internal IT security experts.
- Ensure live monitoring and remediations.
- Used for forensic investigations.
- Escalate potential suspicious threats.

What you will expect

SIEM systems have become commonplace with organizations as they have been seen to be an essential part of ensuring regulatory compliance.

In the world of the Cybersecurity, all security incidents are continuously examined for signs of a potential security incident. It might be helpful to consider the SIEM and the SOC solutions as a dedicated external IT department that focuses on security as opposed to network and server maintenance or other IT tasks. By constantly logging activities and reducing threats, organizations can work more efficiently and ensure high level of security.

THINK WE CAN DO THIS TOGETHER? GET IN TOUCH.