Security Information and Event Management

Whitepaper

2022

konnektable TECHNOLOGIES

Konnektable Technologies

Authored by:
Christos Angelidis

ENERGY SHIELD

Security Information and Event Management tool

IN A NUTSHELL

This white paper is about the Security Information and Event Management tool. SIEM tool is an open-source cybersecurity solution, adapted on the EnergyShield Project, in order to protect the EPES sector from any malicious activities. SIEM tool is considered as part of SCADA systems from the IT perspective.

It presents the combined tools that constitute the SIEM and its functionalities. Moreover, it illustrates demo scenario and how SIEM works.

Finally, it presents the exploitation plan of the SIEM in the upcoming period.

CONTEXT

SIEM tool aims to combine the security information management (SIM) with the security event management (SEM), forming a single collaborative security management system.

SIEM combines the most widely used network security tools, starting from:

- Wazuh
- OSSEC
- ELK stack (Elasticsearch, Filebeat, Kibana, Logstash, Beat agents, X-Pack)
- Suricata
- Virus Total Framework

SIEM tool is adapted on the EnergyShield Project, in order to protect the EPES sector from any malicious activities. SIEM tool is considered as part of SCADA systems from the IT perspective.

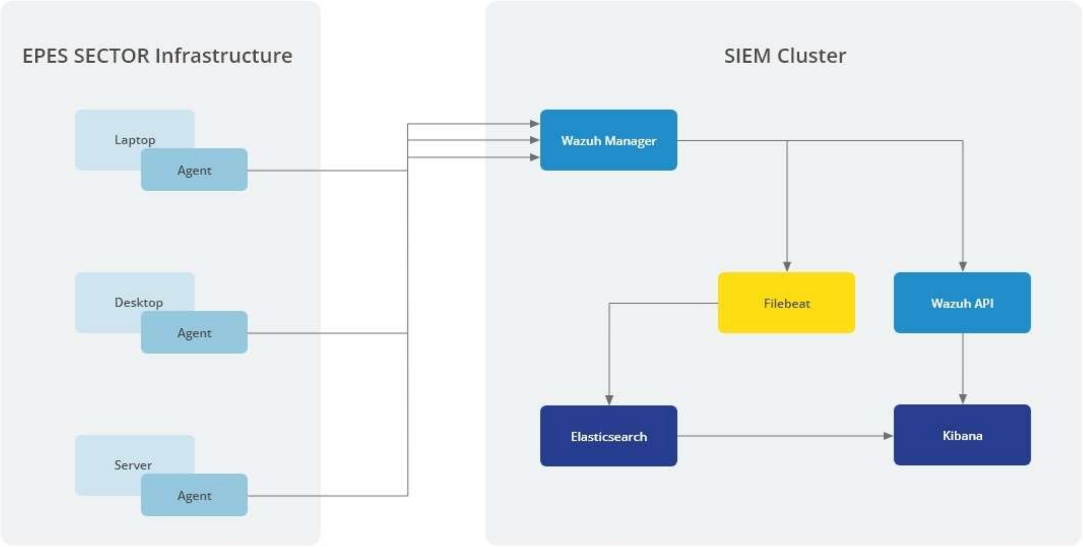
More specifically, SIEM will detect and monitor the infrastructure's endpoint activities. The endpoints, where the SIEM's agent can be

> “
>
> ***Our contribution in the adaptation of SIEM tool on the EnergyShield Project sets out our ambition to strengthen the cyber security and to propel an increasingly massive deployment and use of cyber security solutions in the EPES sector as well as to critical infrastructures and production lines.***
>
> *Konnektable Technologies Ltd*

installed, are Servers, VMs, laptops or Desktops. These endpoints must be linked to other assets involved in SCADA System (e.g., RTU, PMU etc.).

SIEM solution in detecting attacks being considered as an essential solution to protect the EPES sector against a variety of threat scenarios. It can identify anomalies in the system (SCADA systems etc.). As a result, alarms can be raised when a deviation is detected and valuable information is provided to the SOC Analyst that can help to mitigate and manage detected attacks. More key points of the value of SIEM are:

- Prevent a single security vulnerability from compromising the entire infrastructure
- Better adaptation to dynamic environments with fully-hosted security monitoring
- Monitor all layers of the environment: infrastructure, hosts, containers, and applications
- Discover security issues continuously or in real-time
- Monitor at least 100 endpoints of the infrastructure
- Powerful and easy to use tool for SOC analysts to monitor and prevent threats to their organization's IT infrastructure, and to assess security systems and measures for weaknesses and possible improvements



TECHNICAL DETAILS

SIEM, as a standalone solution, enhances the awareness and response by adapting features as the following:

Log data collection. This feature is the real-time process of getting logs and events generated by the monitoring endpoints, where the agents are installed. The purpose of this feature is the identification of system errors, mis-configurations, policy violations, intrusion attempts, among other security issues.The end users can view the analyzed logs through dedicated dashboards.

Distributed Data Storage. SIEM provides a distributed data storage by using Elasticsearch. SIEM uses Elasticsearch to store the log data. Its distributed architecture makes it possible to search and analyze huge volumes of data in near real time. It allows you to start with one machine and scale to hundreds. Elasticsearch makes it easy to run a full featured search cluster, though running it at scale still requires a substantial level of expertise.

Integrity Monitoring. The File Integrity Monitoring is located in the monitoring endpoint via the Wazuh agents, where periodic scans are running inside specified directories, in order to trigger alerts when these files are modified. The end-user can see graphs of generated alerts, alerts by agents, rule that fired, among other things in the FIM dashboards.

Vulnerability Detection. Wazuh is capable to detect vulnerabilities in the applications installed in agents using the Vulnerability Detector module. This software audit is performed through the integration of vulnerability feeds indexed by Canonical, Debian, Red Hat, and the National Vulnerability Database.

Secure Authorization. EnergyShield's SIEM uses Role-based access control (RBAC) in order to secure the system. Role-based access control (RBAC) refers to the idea of assigning permissions to users based on their role within an organization. It provides fine-grained control and offers a simple, manageable approach to access management that is less prone to error than assigning permissions to users individually.

The user-role and role-permissions relationships make it simple to perform user assignments since users no longer need to be managed individually, but instead have privileges that conform to the permissions assigned to their role(s). With X-Pack plugin users can:

- Create reports based on Kibana dashboards
- Protect their stored data
- Keep their finger on the pulse of their Elastic Stack through monitoring

The main goal of RBAC is adding to EnergyShield's SIEM the capability to control access to different endpoints and resources through API based on privileges to users.

Compliance. SIEM tool provides necessary security controls to become compliant with industry standards and regulations. These features, combined with its scalability and multi-platform supp, help the EPES sector meet technical compliance requirements.

- MITRE attack framework. This feature allows the user to customize the alert information to include specific information related to MITRE ATT&CK techniques. MITRE ATT&CK

framework stores all possible attacks that can be made and what to do to mitigate and detect them.

- National Institute of Standards and Technology. The Wazuh platform provides necessary security controls, such as intrusion detection, log analysis, among others, to meet compliance requirements. In order to achieve this, SIEM rules have been mapped against compliance requirements. Within this approach, when an alert is generated, it automatically includes compliance information to detect violations of NIST security controls. As a result, when an alert is generated, Wazuh tags it with the related security control, thanks to the NIST ruleset.
- General Data Protection Regulation. When initiating a GDPR compliance process, a certain preparation must be performed for it to be successful. It is crucial, to take into consideration the place where personal data are stored since it is highly correlated with the whole process of indexing information. This process is a technique that is advised to be used whenever personal data are stored, since Elasticsearch, by indexing, can execute a full-text search in a matter of seconds.Furthermore, Wazuh offers extensive support for GDPR compliance.

Incident Response (Countermeasures). Following the attack as it unfolds to take immediate countermeasures to minimize its impact and gather forensic information for sharing & coordination with CERTs and other value chain actors.

SIEM has enabled the Active Response on well-known attacks. Furthermore, the collected information on the incidents firing a rule triggers an Active Response (e.g., host-deny, firewall-drop, etc.). The end-user can view these actions in UI. In addition, a mechanism was developed to send email reports on the occurring threats. SIEM solution adapted more countermeasures, in order to actively respond in any possible threat.

Alerting. Alerting let us take action based on changes in our data. It is designed around the principle that, if someone send a query in Elasticsearch, he/she can alert on it. Simply define a query, condition, schedule, the actions to take, and alerting will do the rest. Alerting can be enabled when configuring the cluster. Alerting could run on separated clusters, if needed.

The main purpose of alerting is to detect anomalies, spikes, or other patterns of interest from data in Elasticsearch.

Visualization. The Visualization component of SIEM, based on Kibana, provides an advanced way to visualize and analyse SIEM alerts stored in Elasticsearch. Statistics per agent can be obtained, search alerts and filter by using different visualizations. It integrates with the SIEM API to retrieve information about manager and agent's configuration, logs, Ruleset, groups, etc. A number of different graphs provides convenience to the user to present the data in the most desirable way.

ENERGYSHIELD DEMONSTRATOR

A demonstration scenario is described below to highlight what Wazuh agent provides to SIEM environment. In this scenario, the following infrastructure elements are included:

- Server
- Laptop (Windows, Linux)

More specifically, the steps to build this instance are the following:

- Installation of a Wazuh agent into an internal server which is the endpoint, the SOC analyst wants to monitor. This server will be replaced with an endpoint given from the infrastructure, in order to test SIEM functionalities in the EPES sector. For the sake of a real adaptation on the EPES sector, the endpoint must be connected and monitor assets such as PMUs, RTUs, etc. in infrastructures like hydro plants. As shown in the following instance and chapters, SIEM aims to protect this endpoint from malicious actors. If access is gained to this endpoint, the attacker will be able to monitor the rest of the assets in the sector (PMU, RTU, etc.).

  There are also agents can be installed in laptops for testing purposes, in order to highlight their adaptation to different OS environments (e.g., Linux, Windows), but also to different types of hardware (e.g., Servers, VMs, Desktops, Laptops). These endpoints have to participate in the SCADA System (they have to be connected to Energy Sector's assets).

- Deployment of the SIEM environment (Wazuh, ELK stack) into another server.

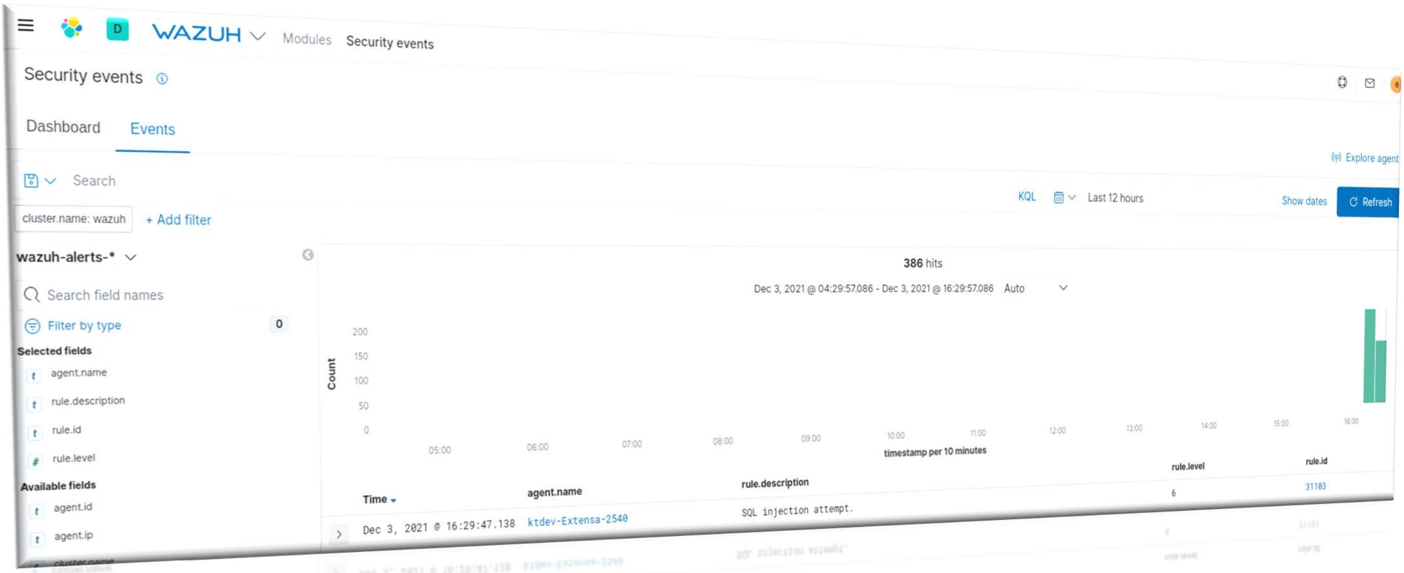
  Automatically receiving log entries from the endpoint with the installed agent to the SIEM cluster via Filebeat, Elasticsearch stores and classifies the logs into indices and finally, Kibana visualizes the outcome to dashboards.

  In the current instance, the SOC analyst has the administrator role of the SIEM Cluster. The goal is to detect any abnormal behaviour from the endpoint, that is monitored.

SQL Injection. An SQL attempt has been made in one of the monitoring endpoints, the Linux-based laptop of the infrastructure, named "kt-dev-Extensa-2540".

This attack was created by providing the following command from the attacker's side: curl -XGET "http://web_server_address:80/?id=SELECT+*+FROM+users";

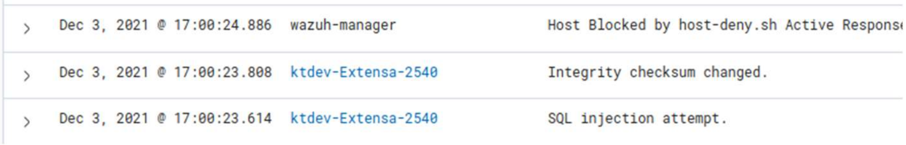
In simple words, the attacker aimed to retrieve hidden data in order to modify the SQL query and get additional results of the monitoring endpoint.



Time	agent.name	rule.description	rule.level	rule.id
Dec 3, 2021 @ 16:29:47.138	ktdev-Extensa-2540	SQL injection attempt.	6	31103

The SIEM tool fires a predefined rule for this attack and then the attacker’s IP will be denied by the whole infrastructure.

Finally, the end-user can see in WUI, the following:



```
>  Dec 3, 2021 @ 17:00:24.886  wazuh-manager         Host Blocked by host-deny.sh Active Respons
>  Dec 3, 2021 @ 17:00:23.808  ktdev-Extensa-2540    Integrity checksum changed.
>  Dec 3, 2021 @ 17:00:23.614  ktdev-Extensa-2540    SQL injection attempt.
```

In the above figure, the attacker has been blocked by the whole infrastructure.

BEST PRACTICES & LESSONS LEARNED

The overall aim of Konnektable Technologies Ltd. is to exploit the results of EnergyShield project as part of its core strategy in the marketing and selling of industrial projects and services. Through its participation in EnergyShield and other European projects, KT strengthens its core business value which is enabling the users and creating connections utilizing technological solutions and data-driven insights. The practical application of research and the acquired knowledge will be incorporated to the business department, increasing its capabilities and the possibility of offering enhanced products and services during the project, with the aim of strengthening cyber security for EPES sector, critical infrastructures and production lines; propelling an increasingly massive deployment of cyber security solutions and an increasingly intense use of those solutions in their respective fields.

The results will strengthen KT’s competence and will be transferred into industrial use via contract R&D projects and consultancy services and as plug-inns to the commercial platforms of the company.

Furthermore, KT will actively contribute to the overall Business activities of EnergyShield Technology itself is just a few interesting results if the business orientation is not considered. In this path the technologies are valorised, the risks are mitigated, the exploitation strategy is defined and, finally, a business plan is produced. The business activity path ends with a “mixed” activity, partially technological, focused on the commercialization of the technology which is one of the core objectives of the company.

SIEM in EnergyShield project is dedicated to EPES sector but its structure is universal and can be adapted in other sectors with the suitable configurations and the customer’s requirements.

This project has shown us that we can achieve more by working with specialist partners having a common goal to prevent threats in various organizations IT infrastructures, while assessing security systems and measuring for weaknesses and possible improvements.

DISSEMINATION & COMMUNICATION

Published papers

- Sklavidis, I., Angelidis, C., Babagiannou, R., Liapis, A. (2021) "Enhancing SIEM Technology for protecting Electrical Power and Energy Sector," 2021 IEEE International Conference on Cyber Security and Resilience (CSR), 2021, pp. 473-478, doi: 10.1109/CSR51186.2021.9527944.]

Dissemination events

- International Conference on Cyber Security and resilience which took place in Rhodes, Greece between July 26–28, 2021.

ABOUT THE COMPANY

Konnektable is a technology research and development firm based in the Republic of Ireland, with offices located also in Greece and the USA.

KT combines Internet Technologies with the application of Research and Development, aiming to build software products that are powered by data-driven insights, utilizing machine learning algorithms, advanced data mining techniques semantics, data aggregation, data analytics and IoT technologies to connect disparate systems, enabling users to manage a specific process or system efficiently. We apply these technologies in a series of operational domains such as energy, healthcare, transport, creative industries, maritime, water, manufacturing, cybersecurity and emergency management.

For more details: https://konnektable.com/about-konnektable-technologies or info@konnektable.com and via social media

Facebook: https://www.facebook.com/konnektable/, Twitter: https://twitter.com/Konnektable, LinkedIn: https://www.linkedin.com/company/konnektable-technologies-ltd

Instagram: https://www.instagram.com/konnektable/

This project has received funding from the European Union's H2020 research and innovation programme under the Grant Agreement No. 832907

SIMAVI
Software Imagination & Vision

PSI

SIGA
OT Solutions

foreseeti

L7DEFENSE

konnektable
TECHNOLOGIES

TechInspire
Inspire for innovation

KTH
VETENSKAP OCH KONST

ΕΘΝ. ΜΕΤΣΟΒ. ΠΟΛΥΤΕΧΝΕΙΟΝ

CITY
UNIVERSITY OF LONDON
EST 1894

iren

ESO EAD

РАЗПРЕДЕЛЕНИЕ

K3

SC Software Company Ltd
Developing quality software solutions since 1996

MIG23
turnkey engineering

GOLDLINE

HPP LENISHTA

Website: www.energy-shield.eu Twitter: @EnergyShield_

LinkedIn Group; https://www.linkedin.com/groups/8831159/

Youtube channel: https://www.youtube.com/channel/UCtNRIf0uXvDsxVCSo1NfF_Q

E-mail: EnergyShield@siveco.ro