

EWA is relying on advanced technology to protect against cyber-attacks

Elektronikwerk Amberg (EWA) is boosting its security against attacks – thanks to *tailor-made monitoring services* and *Totally Integrated Automation*.

Customer

Elektronikwerk Amberg

Location

Amberg, Germany

Project

Implementation and operation of a *security information and event management* solution as part of *Industrial Security*

Implementation period

Since February 2, 2015

Scope of service

- Installation of SCALANCE security modules
- Security configuration of S7-1500 and SCALANCE S with TIA Portals
- Integration of EWA's computer systems
- Monitoring of security-relevant events by the Siemens *Cyber Security Operations Center (CSOC)*
- Monthly status reports on plant security
- Recommendations on ways to optimize the level of protection

The challenge:

Comprehensive protection of products, processes and data in a networked automation system

Elektronikwerk Amberg is a prime example of a digital factory. The factory uses cutting-edge technologies to produce approximately fifteen million SIMATIC products each year. All of the highly sensitive processes are IT-controlled. From production and manufacturing data to coordinates for placement machines, production figures, downtimes and inventory levels, the fully networked automation environment ensures a consistent, end-to-end data flow and extensive database.

The results are maximum quality, freedom from errors and unique delivery reliability exceeding 99 percent. However, the EWA is also facing growing challenges when it comes to protecting against industrial espionage, manipulation and hacker activities. The Amberg factory management was therefore seeking a reliable solution to monitor the security level of their production facilities and to quickly identify security incidents. They chose *Security Information and Event Management (SIEM)* as part of *Industrial Security*.

The solution was developed based on a Holistic Security Concept.



Comprehensive monitoring measures are needed to fully network the digital factory

“Considering our extensive network, which multiplies the number of possible points of entry to our IT infrastructure, we cannot assume that yesterday’s solutions will protect against today’s potential threats. Since introducing SIEM, we have much higher transparency about the effectiveness of our measures to protect against cyberattacks.”

EWA CEO Dr. Gunter Beitinger



“SIEM solution was optimally customized to the factory’s needs in order to implement a comprehensive, reliable monitoring process.”

(Stefan Woronka of EWA’s Plant Security Services)

Innovative protection with Network Security Monitoring

EWA was the first factory in the world to be equipped with a SIEM system from Siemens. The hardware and software were implemented first. This included configuring SCALANCE S security modules, which are directly engineered in the TIA Portal automation project. In parallel the security functions for access and know-how protection of the S7-1500 CPUs were configured in the same engineering project. As a result the network security and the system integrity could be implemented based on the Defense in Depth security concept. Due to the integration in the automation solution future modifications can be easily and cost effectively integrated by the EWA. In addition the computer systems of the EWA were also integrated into SIEM. In the future, SIEM will continuously monitor all critical routers, servers, SIMATIC controllers and communication interfaces in production - as defined by Totally Integrated Automation.

Thanks to the monitoring system, industrial security specialists from Siemens can identify security-relevant events such as cyber-attacks on the automation network and EWA’s factory IT and initiate effective countermeasures as quickly as possible, SIEM uses many different mechanisms to automatically collect and process all security-relevant information generated by existing network users, such as firewalls, routers, switches and automation devices.

This approach makes it possible to identify suspicious events, risks as well as typical attack patterns and issue corresponding alarms.

Every month, threats detected in this manner are summarized in a detailed report, to which are added clear recommendations for protective measures. In urgent cases, the management is also informed so as to initiate countermeasures before damage occurs.

Security from the very beginning – 24/7

Thanks to SIEM, EWA now receives sound, substantiated security information. Since the factory is monitored around the clock without interruptions, the system also identifies incidents that occur outside of normal business hours. Moreover, recommendations for protective measures show ways to continuously optimize the security concepts.

“Monitoring with SIEM is an essential part of our strategy to protect and monitor our investment,” says EWA CEO Dr. Beitinger. “After installing the system, we were able to quickly and efficiently identify potential security vulnerabilities and establish state-of-the-art countermeasures. These are activities one would expect of a modern web security solution, making us secure and allowing us to focus on our essential tasks.”

Publisher

Siemens AG 2016

Digital Factory P.O. Box 32040
91050 Erlangen | Germany
E-Mail: pds.industry@siemens.com

Article no.: DFCS-B10069-00-7600

Printed in Germany

Dispo 21639

GB 160082

Subject to modifications and errors. The information provided in this document contains descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract.