Implementation of Scadvance XP® in PKP Energetyka

CASE STUDY

PKP Energetyka has been operating in the Polish market since 2001, specializing primarily in the sale and distribution of electricity to rail carriers and other business customers. In addition, PKP Energetyka provides electricity services throughout the country and sells liquid fuels to railroad companies.

CHALLENGES

PKP Energetyka's development plan includes modernization of network infrastructure and introduction of new technologies for analyzing network traffic characteristics. Its main objective was to implement an effective tool for real-time identification of cyber threats in the OT network and ongoing analysis of the characteristics of object control and detection of anomalies in their operation. As a result, the system was to allow to increase infrastructure reliability and the level of protection against potential attacks. At the same time, an important requirement was to adapt the solutions to the technologies already implemented and used at PKP Energetyka, as well as to ensure the possibility of infrastructure audit and generation of reports in accordance with legal requirements.

To control industrial processes the company uses an unsupported BUSZ protocol. It is a unique protocol used only in the Polish power industry. Therefore, in the project aimed at increasing safety of the OT system, PKP Energetyka could not practically use universal, commercially available solutions and tools allowing monitoring of traffic and analysis of its characteristics.

SOLUTION

This problem, was solved without excessive costs by using an industrial network monitoring system called Scadvance XP® from ICsec, which is adapted to all types of networks and various protocols used in OT systems. The system consists of X1 probes responsible for "eavesdropping" on the OT network traffic and the Scadvance XP server, whose task is to collect data from the probes and analyze the traffic.

„We were looking for a vendor that would not only provide support for the BUSZ protocol, but also offer sniffers that would allow the network to be incorporated without changing its electrical parameters, such as resistance. Apart from that, the company has thousands of devices operated by dozens of external companies and therefore only control of the system at the lowest level allows for its effective monitoring and detection of irregularities which need to be addressed" says Wojciech Kubiak, Director of the ICT Security Office at PKP Energetyka.

Therefore it was finally decided to implement a pilot implementation of the Scadvance XP® solution adapted, among others, to support the BUSZ protocol. After detailed tests in two locations of PKP Energetyka it turned out that the solution meets all the requirements that were set for the provider. Among other things, it does not interfere or adversely affect the operation of the OT network, it ensures monitoring of the infrastructure and detection of practically all devices connected to the system in real time.

BENEFITS

Comprehensive testing of the Scadvance XP® system has shown that the system enables:

- monitoring and archiving actual traffic between PLCs,
- detection of anomalies and cyber-attacks in the monitored OT infrastructure,
- identification of transmitted commands controlling devices (among others, using the BUSZ protocol),
- presentation of information concerning data transmission between controllers and anomalies in the OT network,
- visualization of so-called nodes, i.e. all logical devices participating in communication.

"During the implementation, there were no problems or disruptions in the operation of the infrastructure, and this is of great importance, because railroad facilities are critical infrastructure requiring operational continuity. At the same time, in accordance with the manufacturer's assurances, it turned out that the X1 probes provide full visibility of the infrastructure by automatically detecting all devices connected to the network" Wojciech Kubiak says.

It is also worth noting that PKP Energetyka manages critical infrastructure for the state and is subject to the KSC (National Security System) Act. Therefore, it is also important that Scadvance XP helps in risk management and ensures support for incidents that occur, and their proper documentation and reporting in accordance with the requirements of national CERT organizations.

IDS for industrial networks

Scadvance XP® is a specialized IDS (Intrusion Detection System) for monitoring industrial automation networks and detecting potential threats and anomalies in the traffic between connected devices.
It is a comprehensive solution allowing for implementation of a system ensuring security and control of industrial networks using various protocols. It is based on advanced technologies, including mechanisms of machine learning and artificial intelligence.

Using the data provided by X1 probes, the software monitors networks and collects information not at the edges but directly from the center, analysing the entire traffic of packets transmitted in the network. The hardware interfaces developed by ICsec allow the system to be connected to virtually any type of industrial automation network, resulting in real-time visualization of all existing connections and devices in the network.

The software informs the network administrator about recorded events, indicates where they occurred, as well as points out to the target of the attack and its probable cause.
By using flexible AI/ML models, the system is prepared to support non-standard types of industrial networks and unique applications.

Basic functions and features SCADVANCEXP

- protocol support with deep packet inspection (DPI) and data extraction,
- NETFLOW/IPFIX analysis for IT protocols,
- real-time network audit,
- possibility of packet traffic recording,
- network map visualization,
- detection and presentation of information about devices connected to the network,
- mapping of connections between devices on the network,
- possibility of tracking traffic generated by external providers,
- automatic detection of anomalies, attacks and failures,
- automatic building of dedicated predictive-analytical models with a separate set of parameters for each detected logical connection using ML and AI engines,
- presentation of statistics on traffic in the protected OT / IT network and reports presenting network status.

ICsec S.A. is a leader on the industrial infrastructure security market, in particular for enterprises with industrial infrastructure. ICsec designed and built the Scadvance XP® system (IDS class intrusion detection system), intended for monitoring the OT network. The solution addresses the needs related to the monitoring of industrial automation networks, detection of potential threats and anomalies in the traffic between devices connected to the network.

ICsec S.A. | Wichrowa 1A, 60-449 Poznan, Poland | GSM +48 506 931 953
biuro@icsec.pl | www.icsec.pl