CASE STUDY

IBM QRADAR

POWER AND DISTRIBUTION

SOITRON*

With a SIEM system, large critical infrastructure company has its cyber risks under control

> "The success of the project was clearly due to the people in the implementation team, both on the customer's side and on our side as the implementer. What helped us was thorough preparation and commitment and the customer's cooperation. In this project, we fully utilized our long-term experience with IBM QRadar technology and once again proved our competence in IT and OT environment security."

Maroš Rajnoch
Soitron, Security Solutions Architect

1. BACKGROUND

- The client is responding to the growing **threat of cyberattacks**, which in extreme cases may result in a complete shutdown in power supply.
- The company **did not have a tool to collect logs** important for evaluating security risks and operation issues.
- **They lacked the ability to correlate** different **events**, analytics, and incident investigation and audit trails.
- **Compliance with new legislative requirements** imposed by the Cybersecurity Act was hard to achieve.

2. SOLUTION

- **The QRadar system** for recording, evaluating, and managing security incidents (SIEM).
- **An analysis and the integration of QRadar with the IT and OT infrastructure** for comprehensive log collection.
- **The development and setup** of dozens of different **customer-specific security and operational scenarios** for the SIEM system to respond to.
- **The implementation of the Watson artificial intelligence** add-on to support the aggregated data correlations and analysis.

3. BENEFITS

- **Increased protection against cyber risks** and **the elimination of operational issues** that could result in service outages.
- **An easier job** for administrators and security specialists.
- **Automated risk alerts** derived from the infrastructure data and event analysis.
- **The secure storage of logs** with the ability for retrospective evaluation, auditing, and reporting.
- Establishing prerequisites for **compliance with legislative requirements.**

CASE STUDY

IBM QRADAR

POWER AND DISTRIBUTION

The client has always taken great care to assess and manage all types of risks. In recent years, they have paid more attention to cyber threats, which, in extreme cases, could result in disruption to the supply of electric power to customers.

The government is also trying to prevent such worst-case scenarios by imposing a number of cyber security-related obligations on selected organizations – including energy companies – which are commonly referred to as "essential service providers".

These obligations include the systematic recording, evaluation, and reporting of cyber security incidents to a central early warning system.

Background

The customer used to record logs (audit trails of information system activity) in a technology infrastructure environment; however, the data was collected in multiple databases, and there was no analytical tool that would allow these basic reports to be put into context and thus allow for the identification of relevant security incidents.

This made investigating suspicious incidents and identifying security and operation risks difficult, and the company was unable to effectively meet the new legislative requirements.

The company's management therefore decided to deploy a technologically advanced and comprehensive Security Information and Event Management (SIEM) solution, which allows for the real-time collection, analysis, and correlation of selected log records from the infrastructure and the ability to report on any discrepancies with security policies.

Solution

The choice was IBM's QRadar – this is one of the most widely used SIEM systems, and it has been ranked as one of the market leaders by Gartner analysts for the twelfth time in a row.

QRadar allows data recording from IT infrastructure as well as from the "OT environment" – i.e. from operation technologies. In addition, with the Watson add-on, it can leverage elements of artificial intelligence that can assist in the investigation and evaluation of incidents and automate multiple routine manual tasks, thus preparing detailed reports for decision-making by experts and freeing up their hands for more sophisticated work.

A high-quality SIEM tool is in itself an important prerequisite for effective cyber protection and achieving compliance with legislative requirements; however, the key to maximizing benefits and added value is to have a high-quality implementation and detailed customization of the entire solution.

Deployment

Our customer relied on the integration services of Soitron, who have extensive experience with infrastructure-building projects and various system interconnections and with securing technology and data against cyber risks. Our subcontractor in this project was Axenta s.r.o. With their support, Soitron was able to speed up the implementation of the overall solution.

An essential part of the project was a comprehensive analysis, which was particularly important due to the large variety of technological infrastructure, including custom-developed software systems. The analysis was followed by the integration of QRadar with network and security devices, servers, operating systems, applications, and other various IT and other systems.

Although QRadar has a number of built-in predefined scenarios, each organization is specific; it is therefore always necessary to customize SIEM to individual needs and conditions. For this customer, Soitron added dozens of additional relevant scenarios that QRadar responds to. The responses include alerting the person in charge to a potential risk as well as automated actions, such as the blocking of suspicious communication.

This detailed customization and integration of multiple systems was the reason why Soitron's experts worked on the project for more than a year. The technological environment of a large energy distributor is constantly changing, so perhaps it can never be considered completely finished; however, to fulfil its mission and meet customer expectations, this is not essential.

> "The client´s security department correctly assessed the risks in their industrial control systems environment, and therefore the project also included the collection and evaluation of security incidents from the OT environment. The customer's ICT systems environment is extensive and diverse. When, on top of that, a SIEM implementation project covers both IT and OT, especially in a big organization, it is to be expected that this requires time and the involvement of staff from multiple IT/OT disciplines."

Maroš Rajnoch
Soitron, Security Solutions Architect

CASE STUDY

IBM QRADAR

POWER AND DISTRIBUTION

Benefits

The detailed setup of data collection from the IT and OT environments to QRadar, the definition of dozens of scenarios that could potentially result in operational or security issues, and the helping hand of artificial intelligence have all raised the cybersecurity of firm to a new level. At the same time, they have helped the company to easily meet its legislative obligations, such as the detailed recording and reporting of incidents.

The integration performed by Soitron played a key role in the project. This is because the functionality of any SIEM system is largely limited to log aggregation when it lacks the added value of fine-tuning and fitting to the organization's environment. Rather than making the job of administrators and security specialists easier, it may make it even more difficult by overwhelming them with data.

With a well-deployed SIEM system IT teams get a tool that gives them an invaluable bird's-eye view of what is happening in their entire technological and industrial infrastructure. This allows them to better identify security and operational risks and configuration errors that might lead to unnecessary service outages. QRadar has also become a secure central repository for all logs, making it easier to investigate any past incidents and prevent their recurrence. The implementation of the SIEM solution, including technological and processes integration at the customer's site, was carried out in multiple stages. This allowed for an effective use of human resources and the completion of each separate functional unit even in the large and complex infrastructure operated by the customer. The customer started to intensively use the IBM QRadar SIEM platform during the implementation process. With the growing risk of cyber threats in Slovakia in 2021 and 2022, additional ICT systems were connected and the detail of audit logs gradually increased as well. As extending the licences under the original licensing programme became cost prohibitive, the customer took advantage of migrating to the new IBM Cloud Pak for Security licensing programme. With the IBM QRadar SIEM solution, we were able to evaluate over 10x more events than originally envisaged, while allowing the solution performance to scale with no licensing restrictions. The IBM Cloud Pak for Security includes a stack of security applications that significantly complement and extend the scope of the SIEM solution. We also used the IBM QRadar SOAR platform to automate the solution and significantly upgrade the system.

SOITRON, s.r.o., member of SOITRON Group

Soitron is a Central European integrator operating in the IT market since 1991. The company's philosophy is to constantly move forward, and that is why it is a leader in implementing unique technologies and innovative solutions. It offers its clients products and services in the field of robotization and process automation, artificial intelligence, the Internet of Things (IoT), IT infrastructure, communication and cloud solutions, IT security, IT services and outsourcing, IT advisory and applications, and IT department digitalization. Its product portfolio includes smart police car solutions – Mosy and cyber security services – Void Security Operations Center. Soitron, s.r.o. is a part of the Soitron Group and employs more than 800 international experts. The group brings together professional teams in Slovakia, the Czech Republic, Romania, Turkey, Bulgaria, Poland, and the UK.