Bayer AG | Global | Manufacturing

Bayer brings its manufacturing operations' OT security up to date

Client profile

Bayer AG, headquartered in Leverkusen, Germany, is a listed chemical and pharmaceutical group with over 100,000 employees at more than 170 locations worldwide. The operating business is managed through three divisions: Pharmaceuticals, Consumer Health and Crop Science.

What technologies?

- Guardian appliances from Nozomi Networks
- Central Management Console (CMC) from Nozomi Networks

Which services?

- Technology Infrastructure Services
- OT/IoT services
- Project management
- Design, delivery, implementation and transition (including SOC connectivity)
- Training

What partners?

- Nozomi Networks

> "We need to be able to constantly detect attacks and anomalies in our production network as early as possible in order to prevent a system failure.

Jürgen Focke, Global Program Manager Manufacturing IT Security, Bayer AG Division Pharmaceuticals

Summary

Bayer AG wanted to improve the visibility and transparency of the complex Operational Technology (OT) environment in their Pharmaceuticals Division, which is spread across the company's 15 largest sites worldwide. The goal was to increase asset availability and protect critical infrastructure from potential cyberattacks. The chemical and pharmaceutical company selected Guardian appliances and the Central Management Console from Nozomi Networks. Our security experts designed, implemented and rolled out the solution globally.

Business need

Bayer wants to protect its critical infrastructure from interruptions

In the development and construction of a production plant, the functional requirements are the first and foremost priority. Availability around the clock is of the utmost importance so that production does not come to a standstill. However, the integration of the corporate network increases the need to protect such OT systems against cyber risks. Companies that are considered operators of critical infrastructures need to protect themselves through the latest technologies so that they can respond at the earliest signs of attacks and anomalies within the network.

Bayer AG's Pharmaceuticals Division also faces this challenge. While Bayer already had well-established security policies and protocols in place, in light of the rapid increase in cyberattacks they wanted to better protect themselves against new threats, as well as prevent data from being compromised or from intellectual property falling into the wrong hands. For Bayer, the issue of product safety – and therefore patient safety – is a top priority. Since the company's supply chain is spread across several production sites and countries, the transparency and security of OT processes and networks required further optimization. Although Bayer had an overview of the number of individual devices in its networks, the IT team was not able to identify how they communicate with each other and where vulnerabilities and risks lie. Meanwhile, those responsible were faced with the challenge of standardizing security processes across IT and OT.

The new solution, as an additional building block in securing production facilities, was intended to help Bayer Pharmaceuticals find weak points and detect and respond to attacks at an early stage. Additionally, Bayer wanted a uniform management level to consolidate global risk monitoring and OT visibility across all sites in order to optimize workflows.

Transformation

Advanced detection capabilities identify potential cyberthreats and vulnerabilities in the plant

Bayer selected us to implement the Guardian solution with Nozomi Networks' Central Management Console (CMC). To begin the project, a Guardian appliance and virtual management console were initially installed at a selected production site as part of a proof of concept (PoC) to demonstrate the solution's features and capabilities. Nozomi Networks' Guardian appliance automatically tracks OT and IoT assets and monitors communications and device behavior to gain insight into the network and its activity patterns. In this way, it detects anomalies in behavior as well as attacks and identifies the respective vulnerabilities with the appropriate priority. In doing so, the CMC consolidates OT and IoT visibility and risk monitoring across all sites to streamline workflows and accelerate incident response. The results of the PoC impressed those in Bayer's inhouse OT security team: Guardian not only automatically creates a comprehensive asset inventory, but also creates full transparency of all operations in the company's own network, which supports optimized network configuration. The security team is thus able to reduce manual troubleshooting and forensic efforts, speeding up the response to potential vulnerabilities.

NTT's security experts handled the design, implementation and global rollout of the solution at all production sites in close coordination with Bayer. NTT's tried-and-tested project method was chosen for the implementation, in which eight so-called work packages were "worked through" step by step. The project started with a kick-off and the general design of the architecture. This was followed by an initial inventory and a rough design for each individual site, defining where the appliance would be inserted into the network and what data traffic would be monitored. The next step was configuration and – as soon as the number of alarms had been reduced and all false alarms had been fished out – final fine-tuning, including activation of the protection mode. All further measures were then implemented, including real-time reports, dashboards, audits, integration into the central Security Operation Center (SOC) and final training sessions for the security managers at Bayer.

Outcomes

Bayer now has visibility of its complex, globally distributed OT environments

With the new solutions, Bayer AG has the capability to optimize its network security in a highly targeted manner. Network communication and behavior are constantly monitored in order to detect anomalies and possible attacks, which allows for a swift response to potential incidents before they can disrupt operations. Advanced threat intelligence capabilities identify cyberattacks as well as production risks early. The included threat intelligence service continuously updates Guardian appliances with the latest data and analysis. The pharmaceutical company is thus always kept up to date on emerging OT and IoT threats and can promptly detect and prevent the spread of potential infiltrations across its networks. This allowed around-the-clock availability of the production plants, which is essential for the pharmaceutical sector. The central console at the main site in Leverkusen also gives Bayer's managers a consolidated overview of all production sites around the world, providing company-wide transparency. With the help of our experts, the systems were also configured in such a way that false alarms and operating costs are reduced to a minimum.

> "As a major supplier in the pharmaceutical sector, providing patients with their medications is our top priority. An intrusion detection system is an essential component of our strategy, which we have successfully integrated, together with our partner NTT.
>
> **Jürgen Focke**, Global Program Manager Manufacturing IT Security, Bayer AG Division Pharmaceuticals

Learn more about NTT DATA
services.global.ntt

