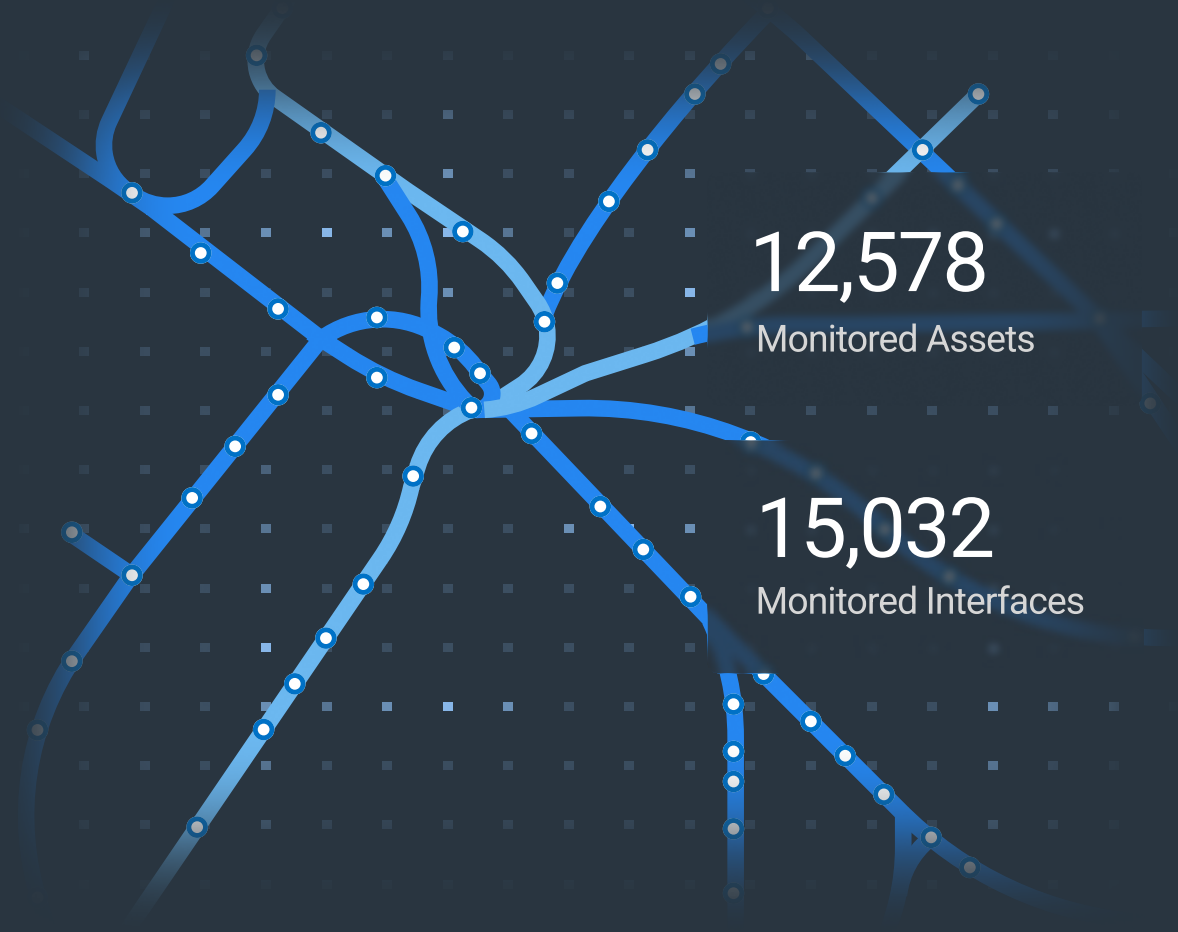
cervello

CASE STUDY

Enhancing Cybersecurity for a National Rail Infrastructure



Europe

In an era where digital threats loom large, the rail industry stands at the crossroads of innovation and vulnerability. The merging of real-time operations and critical data networks demands a robust cybersecurity approach.

This case involves a leading rail organization and a pioneer in rail innovation who was presented with the same challenges all rail operators face today, security in the face of digitalization.

Transporting over one million passengers and hundreds of thousands of tons of cargo a day demands a level of efficiency that can only be achieved with a greater application of digital technologies.

Adding to an already complex network that must operate with the highest regard for safety and security, the newly formed reliance on technology and interconnectivity posed an even greater challenge.

We delve into the challenges faced by the organization and how Cervello Platform completed the task of enhancing the security and operational integrity of this top-tier operator by monitoring its Signaling and OT systems for cyber threats.

Key Metrics

6K Monitored Assets & Interfaces

1K+ CVE & Misconfiguration Discoveries

5.6 TB OCC traffic monitored (in 24h)

250 Stations Covered

Challenges

- Improving security posture and patching vulnerabilities without interfering with sensitive data and real-time operational traffic
- Immediate protection against new kinds of unknown threats brought by digitalization and interdependency
- Navigating a complex network of multiple, interconnected environments within the OCC, interlocking, and station level
- Complying with regulatory requirements

Solution

Following an extensive learning phase and in-depth risk assessment of the rail operator's network framework, strategic decisions were made to protect the trackside infrastructure and operational technology. Immediately after deployment, Cervello Platform began real-time network monitoring and deep packet inspection providing contextual insight to every security risk.

Customized access controls and network segmentation, as well as proprietary protocols were used in forming and automating cybersecurity policies and incident response guidelines for our client. Four solutions were utilized to meet the operator's main challenges:

01

Passive, Zero Trust Monitoring of Critical Infrastructure Environment

To bolster the organization's security defenses and address vulnerabilities without disrupting sensitive data flows and real-time operational traffic, Cervello Platform uses a mirror port to passively monitor and analyze rail network traffic for vulnerabilities, misconfigurations, and anomalous behavior.

Our flexible implementation capabilities allowed immediate integration into our client's existing workflow and Splunk SIEM system.

02

Immediate Deployment and System-Agnostic Integration

One of the pivotal challenges faced by our client revolved around the intricacies of managing a complex multi-network rail environment each with its unique specifications, functions, risks, and policies.

Cervello Platform's system-agnostic deployment and implementation process, which includes seamless network implementation on-prem or on a private cloud, as well as its state-of-the-art asset management solution with immediate asset discovery and classification capabilities laid the foundation for a unified, secure, and streamlined operational framework that the client was able to use to quickly and efficiently safeguard its critical systems.

03

Regulation-Compliant Rail Cybersecurity

A railway can no longer responsibly operate without implementing the security measures dictated in leading cybersecurity frameworks such as the TS 50701 or the IEC 62443. Cervello's 8 layer platform solution ensures rail organizations stand in line with their regional regulation requirements, strengthen their resilience and cybersecurity preparedness, and maintain their safety integrity levels intact. Our solution to our client encompassed multifaceted compliance strategies, including network segmentation and micro-segmentation, continuous monitoring, and stringent access control measures that aligned with industry requirements, ensuring their operations were not only secure but also fully compliant with the regulatory landscape.

04

Translation of Proprietary Protocols into Cybersecurity Policies

One of the pivotal challenges faced by our client revolved around the intricacies of managing a complex multi-network rail environment each with its unique specifications, functions, risks, and policies. Cervello Platform's system-agnostic deployment and implementation process, which includes seamless network implementation on-prem or on a private cloud, as well as its state-of-the-art asset management solution with immediate asset discovery and classification capabilities laid the foundation for a unified, secure, and streamlined operational framework that the client was able to use to quickly and efficiently safeguard its critical systems.

Results

In addressing our client's cybersecurity challenges, our strategic approach yielded transformative results, setting new standards in rail cybersecurity. With unparalleled visibility into cyber activity risks within the context of rail, the operator achieved enhanced security for its entire rail environment. Real-time monitoring mechanisms and a sophisticated understanding of rail networks and behaviors enables the immediate translation of security activities into their direct operational impact on rail services. This deep understanding allows for precise threat prioritization, swift responses, and proactive measures, ensuring enhanced security while preserving the integrity of rail operations.

A cornerstone of our success was the meticulous compilation of cybersecurity evidence. Through detailed Packet Capture (PCAP) data, PDF-based incident reports, and a comprehensive timeline of events, we provided our client with a thorough collection of evidence. Our operational security insight not only facilitates forensic analysis but also serves as a powerful tool our customer can use in communicating cyber incidents to auditors, rail vendors, OEMs, and suppliers.

Our efforts not only ensured compliance with the necessary cybersecurity regulatory standards, but also seamlessly integrated these regulations into the core of our client's operations. By aligning every aspect of their cybersecurity measures with these standards, we were able to meet legal obligations and demonstrate a full commitment to industry best practices. This proactive approach fortifies their position in the regulatory landscape and builds trust among stakeholders.

A rapidly digitizing rail industry presents a growing threat of cyber attacks, making it imperative to enhance security without disrupting sensitive data flows and real-time operational traffic. Even the largest and most secure rail organizations are looking for immediate protection against novel threats. Cervello provided the solution and expertise our client needed to navigate proactively securing a complex and interconnected network in a way that met stringent regulatory requirements. Cervello Platform proved to be the most comprehensive solution in the market able to handle these challenges head-on and achieve remarkable outcomes.

About Cervello

Cervello is the world's first rail cybersecurity platform protecting the entire rail operational environment (OT/ICS, IoT, Signaling, and Rolling Stock) from cyber threats. Using patented, state-of-the-art technology, Cervello Platform delivers comprehensive visibility, deep asset insight, and proactive risk management capabilities, giving security teams the contextual understanding to efficiently detect abnormal behavior and threats, and take action to protect critical rail operations.

https://cervello.security | info@cervello.security