Case Study

Fortifying CBTC Infrastructure Security for a Major Metro

Metro

North America

In today's digitally interconnected world, where technology drives efficiency and connectivity, urban metro lines serve as vital arteries of modern cities. Communication-Based Train Control (CBTC) revolutionized metro transportation, optimizing schedules and ensuring passenger safety. However, the digitalization and growth of metro networks has also made them a more appealing target for cyber threat actors.

As a result, many metro operators find themselves caught between the complexity of modern CBTC systems and the lack of adequate cybersecurity measures able to protect against the widespread and sophisticated cyber threats we see today.

In this case study, we outline the challenges faced by our North American customer, a leading metro rail operator in North America who could no longer safely operate without adequate cybersecurity protection. We demonstrate how Cervello Platform proved to be the comprehensive solution the organization needed to fulfill its security objectives.

Challenges:

- Enhance efficiency and service availability without impacting or interfering with the safety integrity levels (SIL) of the critical operational networks.
- Communicate efficiently and safely within their network as well as with vendors using proprietary protocols without documentation.
- Navigate a complex, multiple-network environment across the Operational Control Centers (OCC), station levels, and trains.

Key Metrics:

- **6K** Monitored Assets & Interfaces
- **5.6 TB** OCC traffic monitored (in 24h)
- **1K+** CVE & Misconfiguration Discoveries
- **250** Stations Covered

Solution:

Having completed an in-depth assessment of the rail operator's network framework and understanding the client's immediate challenges, a strategic decision was made to begin with protecting the operator's Supervisory Control and Data Acquisition (SCADA), Communication, and Signaling systems. Cervello Platform began monitoring and analyzing network traffic immediately after deployment, providing contextual insights on every security alert or warning. The implementation stage included utilizing our patented, passive and non-intrusive capturing mechanisms that instantly mirrored all traffic and sent all discoveries to Cervello Platform for further analysis. We were able to solve our client's main challenges in four steps:

1. **Passive Monitoring of Metro Operational Critical Network Traffic**

It was imperative to the organization that all monitored traffic be completely passive so as to not interfere with the SIL of their critical operational network. Cervello Platform analyzed all real-time data via a mirror port and data diode, ensuring no queries or data were sent back to the monitored network. Capturing data in this manner allows Cervello Platform to continuously monitor the system and provide non-intrusive guidance for incident remediation.

2. **Real-Time Monitoring of Proprietary Protocols and Advanced Threat Detection**

The combination of new, sophisticated threats and highly motivated threat actors is a growing worry to all industry stakeholders. From the organizations themselves to government officials understanding the catastrophic potential of an attack to national security, taking a serious step to strengthen cybersecurity preparedness is of everyone's interest.
Cervello Platform proved to deliver safe network communication and operational continuity with full visibility and understanding of network traffic, automated distribution of assets into respective groups, aggregation and network segmentation based on safety levels and cybersecurity policies, and continuous, Zero-Trust monitoring and threat detection that assure early incident warning. Immediate monitoring of the CBTC system included monitoring for CVEs, misconfigurations, and authentication failures. Following the TSA Security Directive guidelines, Cervello Platform ensured continuous monitoring and creation of cybersecurity detection policies to detect cybersecurity threats and to correct anomalies that affect Critical Cyber System operations.

3. Advanced Threat Detection

During our deployment, we were able to prove the effectiveness of Cervello's flexible architecture by integrating Cervello XE, our passive, proprietary software collector, throughout different selected points in the network. This served to immediately provide a reliable source of intelligence to perform high-functioning threat detection and analysis in real-time.
In the case of an incident or if a safety level is hurt, per one of their main concerns, Cervello Platform is able to immediately detect the problem area and allow our metro rail client to quickly remediate any damage, interruption, or prevent lateral movement. Cervello Platform is one of the only solutions capable of monitoring a CBTC network for threats, understanding rail-specific protocols and automatically capturing anomalous behavior in the rail context.

Our ML-based behavioral analysis and deep understanding of rail networks allows us to enforce virtual segmentation and micro-segmentation, then monitor our client's proprietary environment and traffic with state-of-the-art cybersecurity policies that permits them to quickly and proactively prevent unauthorized connections, access control, movement authority, and operational commands, in real-time.

4. Customized Playbook Guidance Tailored to a Metro Operational Network

As many experts have warned, a cyber attack is not a matter of 'if', but of 'when'. Our mission is to give our customers the tools and information they need to defend the integrity of their critical rail infrastructure. Cervello holds the rail industry's most comprehensive cybersecurity playbook guidance, based on numerous customer case studies around the world. We worked closely together with our US metro rail client to learn and understand their specific operational challenges, regulatory requirements (in this case, the TSA Security Directives), existing CBTC system infrastructure, and internal policies and protocols, to craft tailor-made cybersecurity playbooks that provide the precise guidance to fortify the network against potential threats, reduce the risk of exploitation of unpatched systems, and become an integral part of its operational workflows. One of the pivotal challenges faced by our client revolved around its increasingly complex, interconnected, and multi-network rail environment within its OCCs, station levels, and trains. Metro networks are subject to stringent regulations, so we ensured our automated and customized playbooks aligned with every regulatory requirement and guaranteed compliance while enhancing security measures.

Results:

We achieved transformative results in addressing our client's cybersecurity challenges. Our platform's unparalleled visibility and CBTC-specific, contextual insights into cyber activities gave our metro rail client an enhanced level of security, catching the attention of the entire organization. We were able to provide a deep level of insight into the metro line's rail operational activity without compromising the safety and integrity of its service.

Sophisticated monitoring mechanisms and understanding of rail networks and behaviors enabled the immediate translation of security activities into concrete operational impact, and the triggering of alerts in the case of suspicious activity.

Our client was able to compile the necessary evidence with detailed insight, including geo-location of impacted field elements or wrongly connected systems to quickly remediate with its vendors and suppliers.
Furthermore, our US metro rail client is today in full control and compliant with the most recent cybersecurity regulatory standards in North American, and fulfills the necessary requirements to maintain all respective SIL ratings.

In an era of growing competition within the global transportation industry and increasing dependency on public transport, the imminent chance of cyber attacks requires the strengthening of cybersecurity measures. The importance of protecting cyber-physical systems from cyber-security threats cannot be overstated, especially in the case of a critical infrastructure. Connected critical rail systems have now also become extremely vulnerable. Cervello is committed to provide tailored solutions that empower our clients across the world to proactively fortify their networks and protect the integrity of their mission-critical systems. The unmatched efficacy of our platform has proven itself in the face of these challenges, and stands as a shield against the risks threatening rail operational integrity.

Cervello redefines rail cybersecurity with cutting-edge solutions designed to protect and empower rail networks globally. Cervello Platform offers holistic protection across IT, OT, IoT, Rolling Stock and Signaling systems, ensuring maximum safety and operational integrity for rail networks. Cervello Platform is used by industry-leading transit operators and infrastructure managers as their go-to tool for risk management - delivering comprehensive visibility, deep asset and threat intelligence, and proactive operational resilience capabilities.
Recognized by top business magazines such as Fast Company and Forbes, Cervello's dedication to innovation and excellence positions us as the global leader in safeguarding the future of rail transport.

Visit our website *cervello.security* or contact *info@cervello.security* for more information.

cervello