



The Definitive Cybersecurity Solution for Railways

Israel Baron, VP of Customer Relations

israel@cervello.security

February 2022

About me

From a Cybersecurity Specialist to a Railway CISO



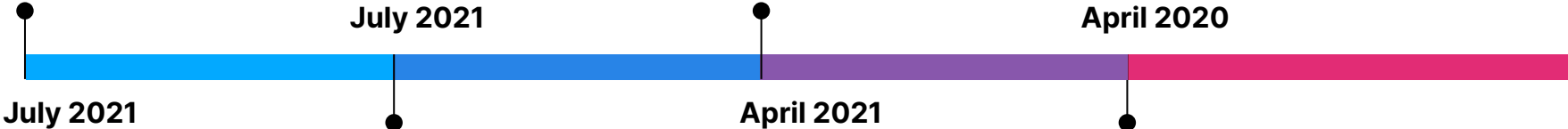
The recent string of cyberattacks

Iran's National Railway System

July 2021, cyberattack hits Iran's transport ministry and railways.

New York Transit Agency

Hackers with suspected ties to China penetrated the New York transit agency's computer systems (3rd breach).



Transnet Port Terminals (TPT)

Transnet Port Terminals (TPT), South Africa's state-run ports operator and freight rail monopoly, had its rail services disrupted after a hack by unknown actors.

April 2020

Amtrak

The National Railroad Passenger Corporation (Amtrak) has disclosed a data breach that may have resulted in the compromise of customer personally identifiable information (PII).

The recent string of cyberattacks

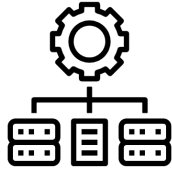
Europe

Hacking group claims control of Belarusian railroads in move to 'disrupt' Russian troops heading near Ukraine



A train station in Minsk, Belarus. (Dan Kitwood/Getty Images)

Today's cybersecurity challenges



Unsupervised railway
operational systems



Lack of railway-specific
cybersecurity solution



Cybersecurity awareness

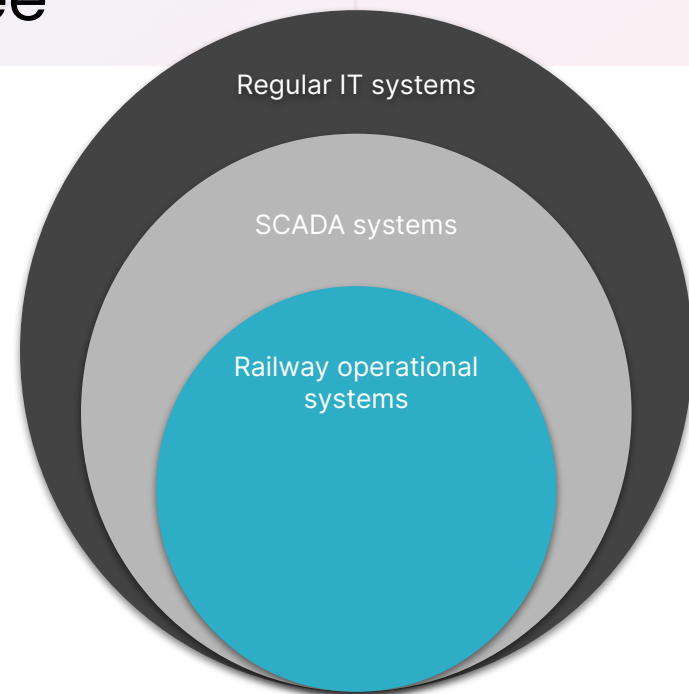


Digitized connected Devices

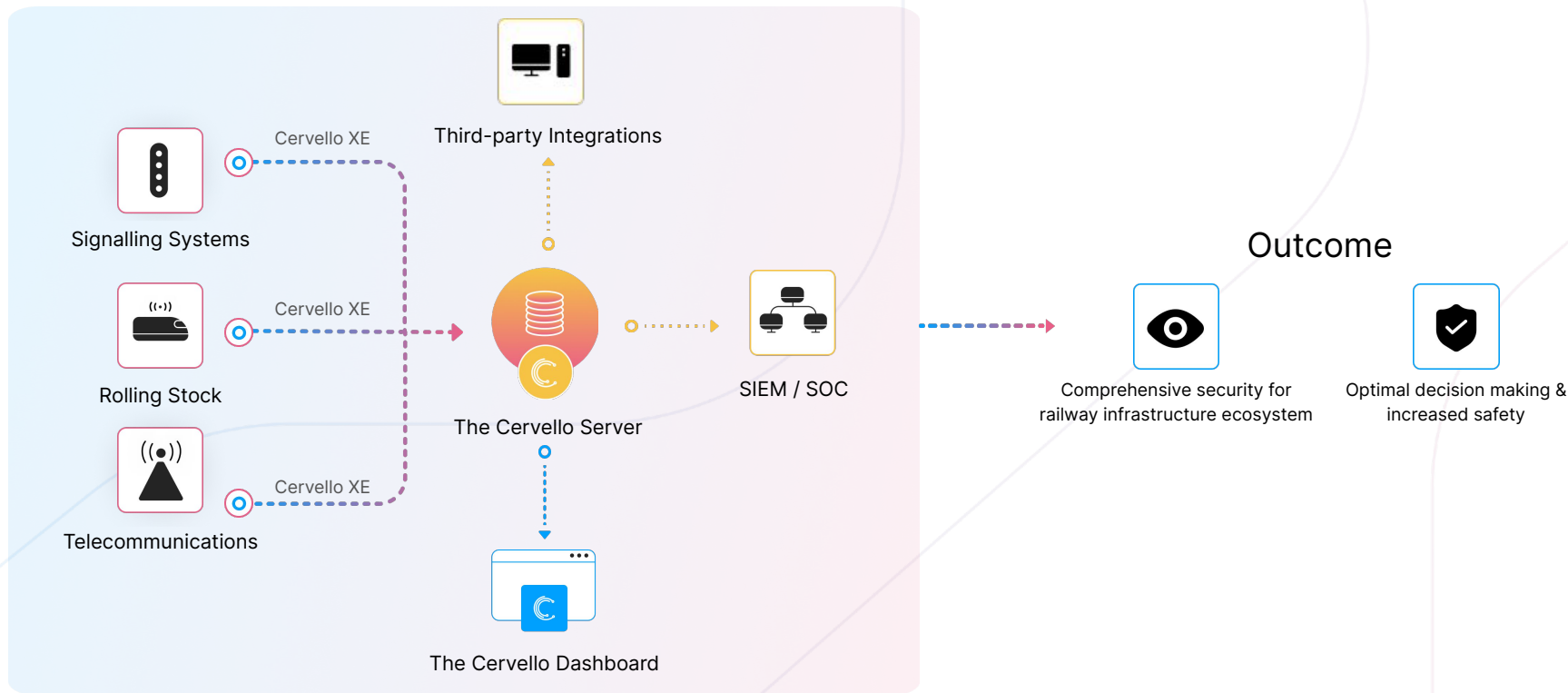
You can't protect what you can't see

With good intentions, railway organizations adopt standard solutions for protecting enterprise systems and data, such as firewalls, proxy servers, and other methods of perimeter defense.

Such generic solutions were not originally built with the railway industry in mind — they are not equipped to adequately identify, contextualize, or investigate the unique threats that railway systems face in their everyday workflows.



Providing railways with comprehensive protection, complete visibility, and coverage of the entire operational network and infrastructure, from signalling systems to telecom and rolling stock.



The Cervello Cybersecurity Platform

Trusted by railway operators, infrastructure managers, and OEMs globally, the Cervello platform is a railway-centered cybersecurity solution that combines a patented zero-trust yet fully passive authentication mechanism, nation-state grade threat intelligence, and actionable remediation guidance — Enabling maximum security of both legacy and modern railway systems to ensure safe, reliable transport and maximum productivity.



Incident Response, Forensics
and Threat Remediation

Automated Asset Discovery
and In-depth network Visibility

Contextual Risk Assessment
and Vulnerability Management

Advanced Analysis and
Network Segmentation

Railway operators and infrastructure managers use Cervello to ensure safe and reliable transport

What Makes Cervello Different?

- ✓ **A simple connection is all you need**
With flexible deployment and zero down-times, Cervello begins delivering significant value within hours after you passively connect Cervello to your operational environment backbone.
- ✓ **We don't assume, we verify**
Cervello analyzes your full signaling stack through patented authentication and validation technology - without relying on previous experience and pre-known, sensitive information.
- ✓ **Improving your safety**
Cervello combines the functionalities of vulnerability management, visibility, access control, traffic management, incident response, and context-aware threat detection into a single unified platform that continuously correlates safety and security risks.

Leading the Shift to Railway-Centered Cybersecurity

The Challenge



Transmission of critical operational data cannot be fully interpreted.



Unable to assess the operational impact of cyber-events.



Manual intervention is needed to inventory and map assets.

Cervello's Solution



A patented passive zero-trust authentication mechanism identifies misleading commands.



Produces a contextual view of the affected assets and operational impact.



Automatically discovers and segments all assets and devices into defined zones.

Customizable for the Industry's Unique Needs

- ✓ We are **100% compatible** with any rail infrastructure and signalling equipment
- ✓ We **ensure compliance and alignment** with industry-specific regulations, standards and safety measures (including IEC 62443 and TS 50701)
- ✓ We **seamlessly integrate into existing rail operational environments** including SIEM/SOC, security tools and admin. systems
- ✓ We deliver a **fully agnostic service** to all industry technologies, proprietary protocols and customized systems
- ✓ We run with **low latency architecture** through the existing bandwidth or out of band, with zero system downtimes or changes
- ✓ We **cover all industry segments** including mainline, urban, light and freight
- ✓ We are **experts on all rail operation standards and components** including ERTMS, CBTC, ETCS, GSM-R, IXL, FRMCS, RBC, PTC and OBU



"We are pleased to be partnering with the leader in the rail and transport industry to help secure critical transportation infrastructure systems with OT and ICS visibility and security."
SVP of Business Development and Alliances, Nozomi Networks

Offering An Ongoing Operational Tool

Value Added: Cost Savings and Improved Service

The Cervello Platform created clear annual impact within weeks



Prevents Disruption & Delays

Eliminated potential delays and service disruptions totalling hundreds of hours.



Mitigated Thousands of Vulnerabilities

Automatically detected, prioritized, and mitigated thousands of vulnerabilities throughout the network.



Saved Millions of Dollars

Avoided exorbitant costs of downtime and regulation non-compliance.



Identified Hundreds of Inactive Assets

Discovered inactive assets according to responsibilities and connections.



Let's Get in Touch



cervello.security



82 Yigal Alon Street, Suzuki Tower,
Tel Aviv, Israel



info@cervello.security



IL: +972 77 408 0307 | CH: +41 79
108 4000 | DE: +49 30 8319 7173