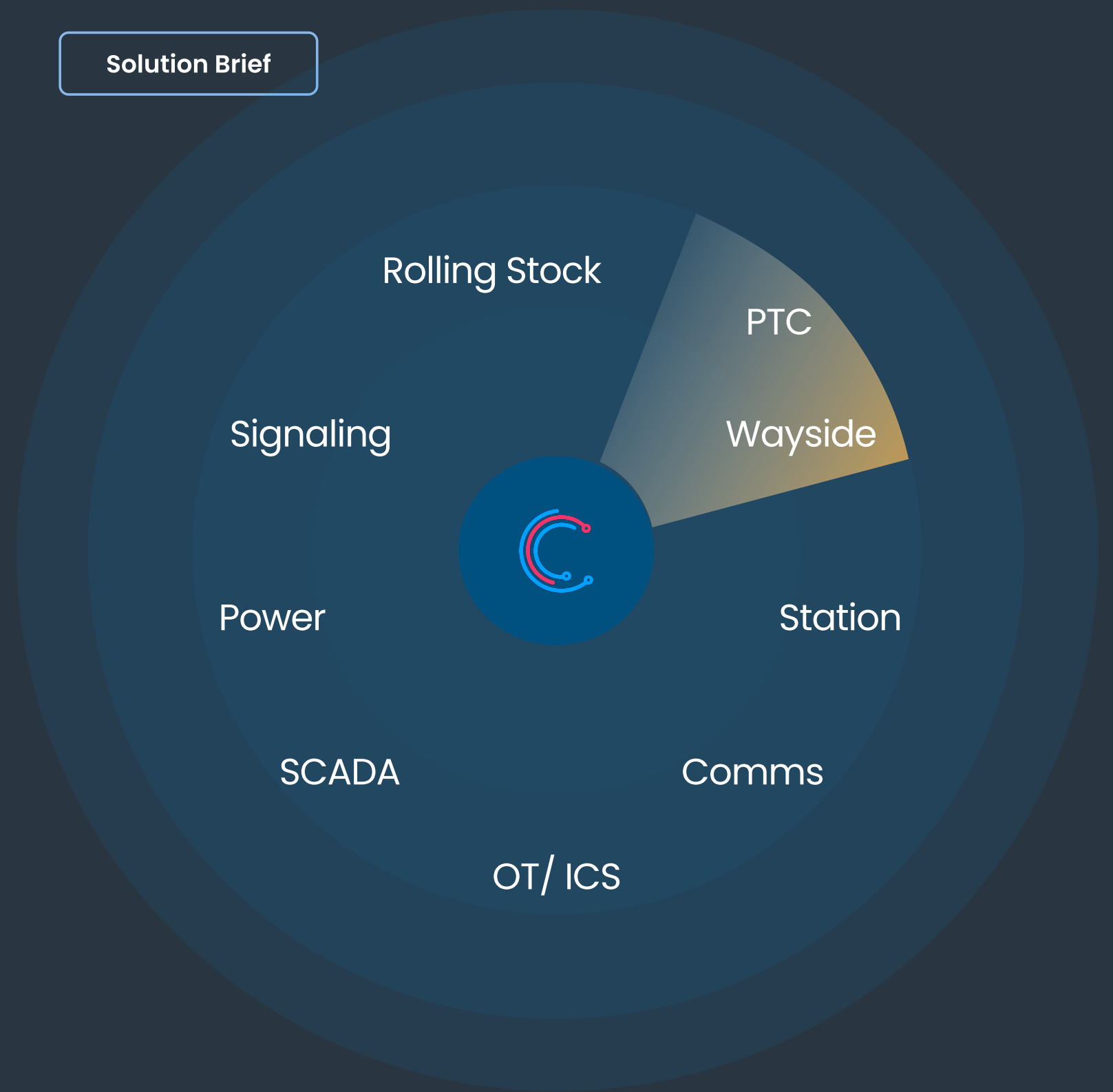
Cervello Platform - Rail-Specific Cybersecurity

Solution Brief



Addressing Today's Rail Cybersecurity Challenges

The Challenge: The rail industry is navigating an increasingly complex cybersecurity landscape. Digitalization, the integration of new technologies with traditional rail systems, and the large geographical reach of rail networks are challenging the industry's ability to manage its cyber risks. It is further magnified by the sector's requirement for high availability and security. Any disruption in service may not only cause significant economic loss but also risk public safety, turning the role of cybersecurity into a top priority. Furthermore, the dynamic nature of cyber threats means that what was secure yesterday may not be secure today and that regulatory demands are constantly evolving.

The Solution: To address these risks, rail organizations must adopt a unified and comprehensive cybersecurity strategy that is specifically tailored to the unique dynamics of rail operations. Such a strategy is essential to effectively monitor and detect cyber threats in real-time, and to better understand the risks of each organization's specific environment.

Why Cervello? Cervello makes rail cybersecurity management simple and efficient. Instead of using multiple, non-integrated solutions for different purposes and for different environments, we provide one unified solution, dedicated to rail, to protect your entire operational environment with maximum precision. With Cervello, you become the master of your networks, gaining a deep and clear understanding that empowers you to achieve unparalleled control over your operations with minimum effort.

Cervello Platform

Cervello Platform is a multi-layered, end-to-end cybersecurity solution for rail.

Using passive, non-intrusive monitoring of network traffic, Cervello Platform detects, visualizes, and alerts on vulnerabilities, risks, and cyber threats across the entire rail infrastructure, including the IT, IoT, OT/ICS, Signaling, and Rolling Stock. The platform provides comprehensive security against internal and external cyber threats for railways. Its acute and industry-specific level of detail on incidents and risks includes the precise location of affected assets and the potential rail operational impact. Cervello leverages its unique understanding of rail operations and cybersecurity to create strong operational insights based on the entire rail network traffic. This enables a faster and more precise response to incidents.

Defend Your Rail Operations with One Platform

Cervello introduces an eight-layer approach to rail cybersecurity protection.
From in-depth visibility to incident response, Cervello provides the tools and information security teams need in order to resolve issues more efficiently.

- Discovery & Visibility
- Asset Management & Virtual Segmentation
- Vulnerability Management
- Misconfiguration Management
- Threat Detection & Mitigation
- Risk Management & Reporting
- Investigation & Response
- Automated Compliance Monitoring

Eight Layers - Key Functionalities

Asset Visibility and Virtual Segmentation

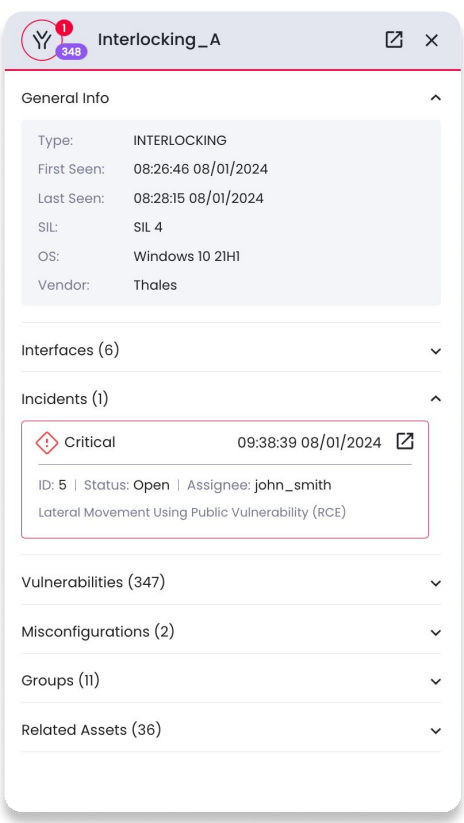
Knowing the network's cybersecurity posture and having 360-degree visibility of the rail's infrastructure is critical in ensuring the safety of the business and operations. Cervello Platform provides in-depth visibility of the rail network, displayed in different views for better management. By identifying each asset based on its traffic behavior from both rail and network perspectives, Cervello provides a comprehensive mapping of assets and their responsibilities. This mapping enhances the understanding of the entire asset landscape.

In-Depth Asset Insight

The platform delivers real-time information about network assets categorized into network, rail, and cybersecurity.

- Network information: IP, MAC, OS, connections, and commands, etc.
- Rail information: SIL, location, station, line, rolling stock, cab, etc.
- Cybersecurity information: Vulnerabilities, misconfigurations, and security incidents.

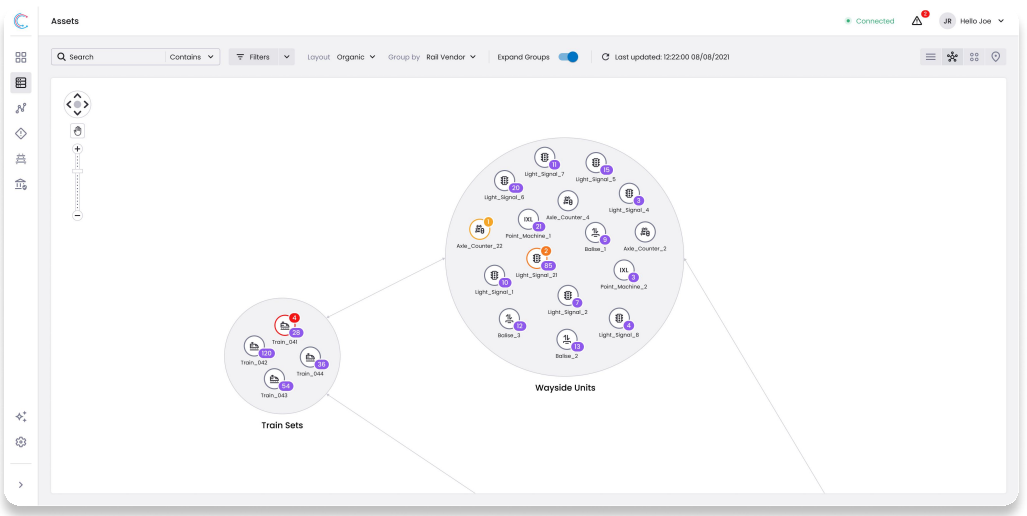
In addition, the platform detects when new assets are connected to the network and displays the change accordingly. This level of visibility provides a complete and up-to-date understanding of the rail network status.



Virtual Segmentation

Once the network is physically segmented and the assets are grouped into their corresponding geographical locations per its communication function, organizations need to ensure that this architecture is operating according to their specifications. Cervello implements virtual segmentation using various criteria such as location, subnet, and TS 50701. The platform provides a comprehensive virtual map of the current segmentation of the assets, with details such as station location, security zones, control centers, lines, cars, trains, Rolling Stock, etc.

Additionally, organizations are able to customize the virtual segmentation according to their own needs. This gives rail organizations an enormous advantage which is, to understand, in real time, if the communication between their assets is taking place as intended, and if they are not, what the operational risk is and how to resolve it.



Regulation and Standardization

With Cervello, organizations are able to stand in full compliance with leading industry frameworks. Among the many standards that require proof of secure network segmentation are the TSA Security Directive, NIS2, and the TS 50701. Cervello Platform gives stakeholders an accessible path to compliance with these requirements and the ability to provide proof to auditors and other relevant stakeholders through automated reports.

Vulnerability & Misconfiguration Management

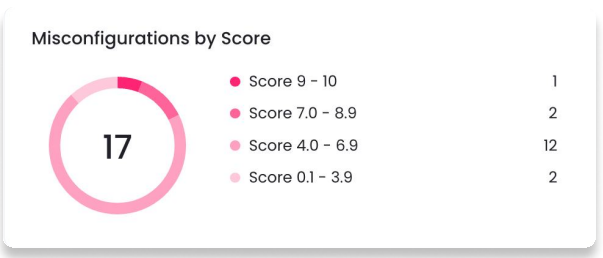
Cervello detects, categorizes, assesses, and prioritizes a wide variety of known vulnerabilities (CVEs) and misconfigurations, including rail-specific ones. Based on the vendor and the characteristics of each rail component, we are capable of identifying the specific vulnerabilities and misconfigurations within each component. The platform generates action steps to remediate all security weaknesses.

Detailed Vulnerability Management

Cervello monitors each rail network asset for vulnerabilities, providing critical insights such as CVE scores, detailed vulnerability descriptions, patch management, and potential impact. Signature-based detection methods are used to identify the exploitation of a CVE, which triggers instant alerts and guidance for immediate response. Users are able to generate reports at the click of a button and deliver the reports to relevant stakeholders and vendors. The result is an unparalleled level of vigilance and precision, ensuring our solution aligns with the need to alert and remediate known vulnerabilities.

Comprehensive Misconfiguration Management

Cervello automatically and passively detects misconfigurations in network traffic. The platform prioritizes an asset based on its vulnerability and the impact it has on the system, including safety and network responsibility. Remediation guidance is automatically delivered with precise, actionable next steps. By fixing the misconfiguration, organizations receive maximum value and function from the asset while minimizing potential cyber risks.



Threat Detection

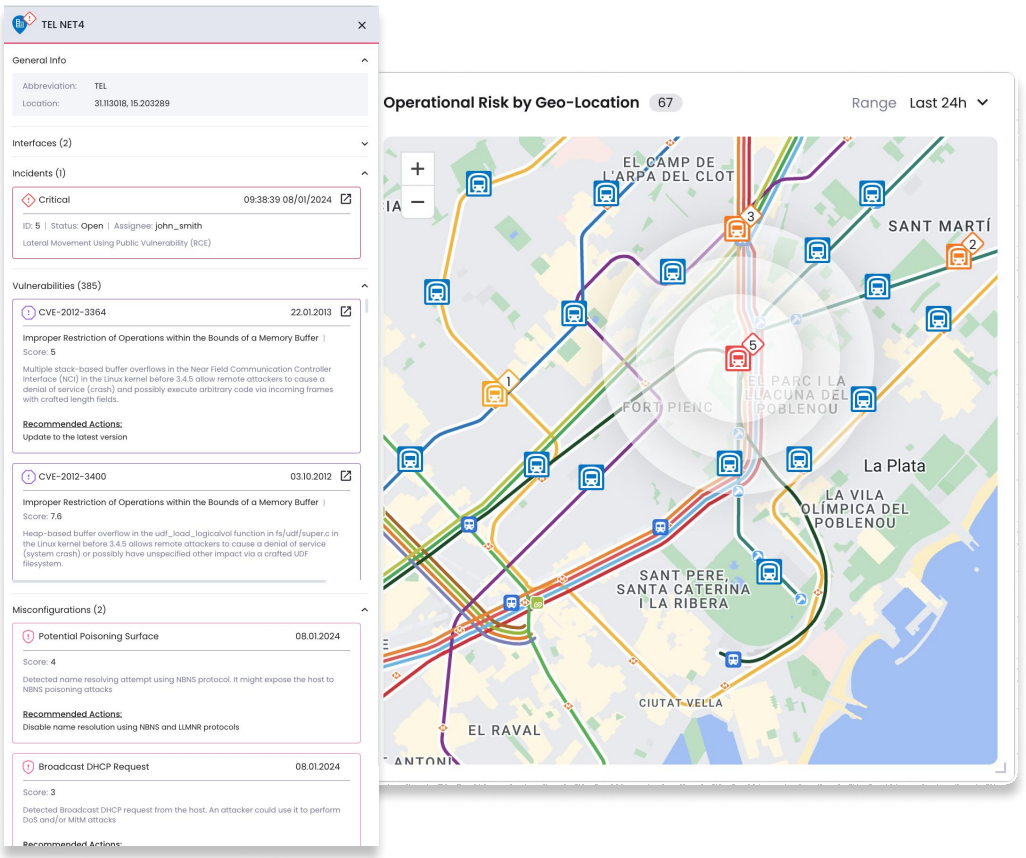
Cervello Platform uses patented threat detection algorithms and advanced machine learning techniques to identify and alert suspicious behaviors and potential threats in real-time. Users can adapt and customize the cybersecurity detection model to fit their network and needs.

Advanced Rail Threat Intelligence

Cervello's rail cybersecurity research team is dedicated to continuously analyzing rail hacking techniques and methodologies across a wide array of equipment and services. The platform provides insight based on the unique operational characteristics of each rail network. It uses a Zero Trust approach, AI, and other advanced technologies to gather the most up-to-date, rail-specific threat intelligence.

Rail-Specific Anomaly Detection

Cervello's deep understanding of rail-specific protocols, applications, roles, data flow patterns, and behaviors, allows it to effectively identify anomalies, vulnerabilities, and cyber threats. By employing a Zero-Trust approach and integrating insights from the MITRE ATT&CK model, Cervello Platform protects critical rail infrastructure from known and zero-day attacks.



Threat Prioritization

Time is of the essence during a cyber incident. Cervello Platform analyzes and prioritizes alerts based on their potential rail operational impact. The platform's dashboard classifies incidents and events according to characteristics such as the Safety Integrity Level (SIL), rail asset type, responsibility, and more, enabling risk prioritization with a rail-centric context.

Customizable Rulesets & Policies

Following a learning phase of the organization's network, Cervello creates sets of policies that are based on: best practices, the network's architecture, and a specific set of assets. The platform provides a dynamic and user-friendly interface for the customization and creation of cybersecurity policies. By allowing users to define and modify these policies, Cervello Platform ensures that its cybersecurity measures are always aligned with the evolving security landscape and our client's specific needs. These policies empower the platform to continually refine and augment its surveillance and defense mechanisms. Additionally, it offers the capability to engineer and deploy sophisticated rulesets based on signatures, heuristics, or behavior, including but not limited to YARA, Snort, Suricata, and BroIDS/Zeek frameworks.

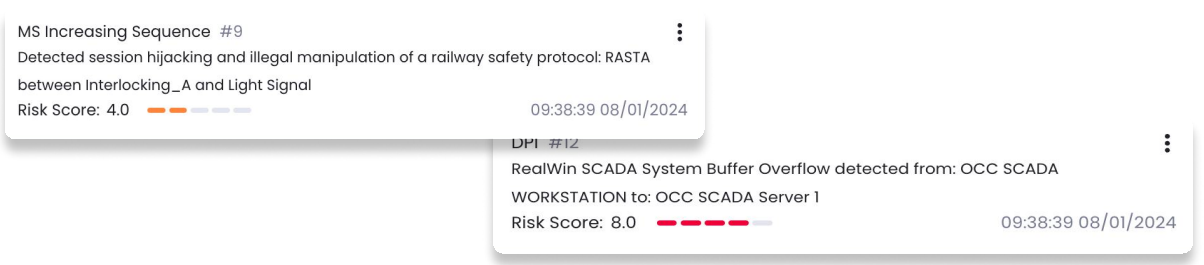
Risk Management, Incident Investigation, & Response

Following the detection of a cyber incident, Cervello Platform synthesizes the events data (sequence, attack vectors, techniques utilized). It delivers risk analysis and information at a high level of rail detail so any relevant stakeholder can easily and quickly follow. In addition to illustrating the cascading effects of an attack, the platform also reveals the path the attack can take to spread throughout the network, along with its operational impact. This gives organizations tools to stop an attack before it escalates.

Cervello powerfully communicates its deep risk insights in ways that can be understood and translated across the rail organization through various visual methods, including: geo-maps (per line or station), network maps, a graphic anatomy of the train, and general risk assessment pages of each particular asset. Cervello also provides playbook guidance as a layer of support for quick threat remediation.

Detailed Risk Visualization

We display the network risks by providing their overall context and potential consequences from different perspectives for more effective management. The displays include "the network perspective", which means a map of assets and their risks, their connections, and how each risk creates an impact on others, and "the station perspective". The station perspective is created by taking the exact geo-location of each asset and producing a visual map of the stations, trains, cars, lines, the connections between them, and each asset associated with the rail's infrastructure components, to have a better view and understanding of the risks.



Automated Incident Sequencing

Following the identification of a cybersecurity incident, Cervello Platform immediately issues an alert. The incident is classified according to its severity, and an incident case is then generated with all the relevant details. The information of the incident includes which policy has been breached, PCAP file of the traffic, the problematic packet, and more. The incident case receives a comprehensive threat profile which includes: the affected systems and assets, their connections and related stations, the attack sequence in detail, and the operational implications. This allows organizations to find the origin and method of the attack surface, critical for both remediation and future prevention strategies.

Prioritization and Impact Assessment

By assessing each asset's criticality, safety level, and role, our solution intelligently prioritizes remediation activities, so that the most critical risks are addressed first. In addition, Cervello Platform uses predictive analytics to forecast the potential consequences of security incidents and suggest remediation actions. This foresight allows operators to evaluate the implications of their decisions on operations and safety.

Optimized Response Playbooks and Enhanced Team Collaboration

An incident is triggered when an unexpected action takes place against the network's policies. Cervello offers a customizable playbook tool for incident-handling. Playbooks can be seamlessly integrated into existing workflows. The playbook includes a set of clear, actionable steps, so security teams can act according to the rules of the organization. Organizations are able to create their own playbooks according to different scenarios, levels of criticality, groups of assets, etc. They can also use Cervello's own suggested guidelines. The platform automatically generates the relevant playbook when an incident is detected.

Automated Compliance Monitoring

Cervello Platform's automated compliance monitoring capability helps organizations align with leading regulatory security frameworks. The platform simplifies adherence to regulations such as NIST, TSA directives, IEC 62443, and TS 50701. With advanced monitoring and reporting tools that automate the assessment and auditing processes, organizations can significantly reduce the effort and time required for compliance checks. Rail organizations can be ready for audits and internal assessments in minutes with Cervello's detailed and customizable Compliance reporting option.

Alignment with Leading International Cybersecurity Frameworks

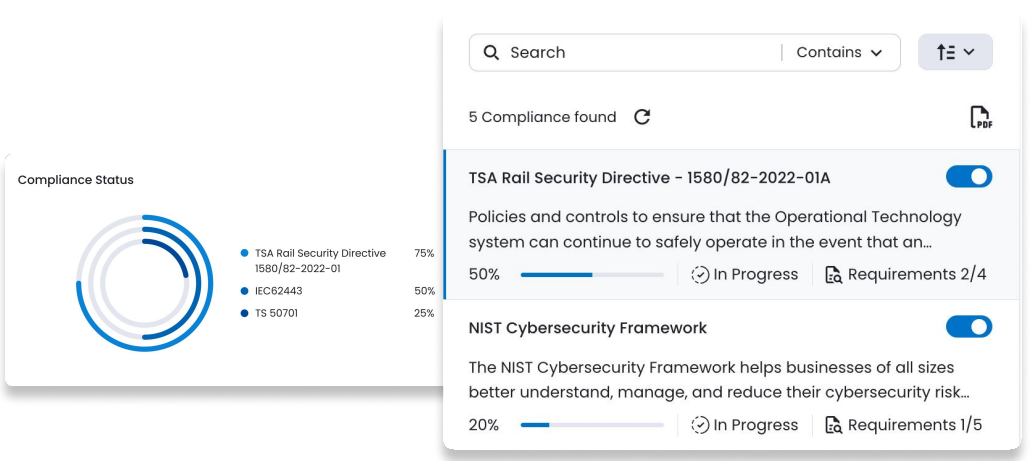
Cervello's integration of global and regional compliance and regulatory frameworks make it easier for organizations to follow their compliance status and make the relevant changes to meet the requirements. The breakdown of each requirement and the platform's ability to analyze and advise on the correct steps to meet the relevant requirements significantly simplifies a usually complicated process.

Automated Compliance Assessments and Customizable Reporting

The platform conducts automated compliance assessments to quickly identify organizational gaps and areas of non-compliance. This saves stakeholders significant time and resources by eliminating the need for manual compliance checks. Cervello's customizable compliance reports provide detailed evidence and context for each security incident and indicate how well an organization complies with the relevant compliance standard for its region - an invaluable tool for audits and internal assessments.

Actionable Compliance Guidance

Cervello provides actionable next steps for addressing compliance gaps, tailored to the specific regulatory needs of each region. This feature guides organizations toward full compliance, enhancing their overall security posture and operational integrity.



How Cervello Approaches Rail Cybersecurity

Zero Trust
Cervello's Zero Trust model for monitoring and threat detection ensures no implicit trust is granted. Every digital interaction is continuously validated to prevent unauthorized access and actions. By leveraging passive authentication and real-time traffic validation, the platform identifies vulnerabilities, monitors connection behaviors, and correlates these with assigned roles to maintain operational trust.

AI-based Behavioral Analysis
Cervello Platform tailors its analysis using Artificial Intelligence (AI) capabilities, to each unique rail network, continuously monitoring data to detect anomalies and unusual traffic patterns. It ensures the authenticity of signals across vulnerable channels and validates the origin and destination of safety-critical commands, aligning seamlessly with rail cybersecurity policies and safety protocols.

Threshold Analysis
Cervello Platform logs each activity detected in the network traffic and utilizes its patented scoring mechanism to rank the security factors of each activity. In case the activity's risk exceeds predefined thresholds, an alert is triggered.

Deep Packet Inspection (DPI)
DPI is a network traffic analysis method that goes beyond conventional packet filtering by examining the contents of packet payloads. At Cervello, it is enabled by the deep knowledge of rail protocols. While traditional packet filtering inspects primarily packet headers, DPI identifies, classifies, and manages packets based on specific data in the payloads that standard methods do not detect.

Unified Security
The power of Unified Security in Cervello lies in its ability to monitor various types of networks with one platform – SCADA, Signaling, Rolling Stock, IT, OT/ICS and more. This unified approach minimizes the need for various solutions and integrations.

In addition, Cervello strongly believes that sharing data between these systems is critical for achieving the best possible security and maximum value from operational data. Having all the information analyzed in one platform allows for greater operational insights due to the cross-referencing of different networks and their impacts on each other.

Cervello Platform is tailored to meet the specific needs of rail organizations by utilizing its flexible architecture and integrations with other systems. For example, our agnostic integrations with SIEM and SOC systems bring missing operational data and contextual security information into IT infrastructure. In this way, Cervello Platform acts as a centralized information source that contains information from all environments and can be easily shared across departments.

Furthermore, Cervello Platform emerges as the sole solution seamlessly integrating diverse layers of protection. From visibility and vulnerability management to threat detection, investigation, and automated compliance monitoring, it encompasses them all as an ultimate operational risk management, all in one platform.

Comprehensive Protection With Scalable Security

The high numbers of assets and subsystems in a rail infrastructure demand a scalable and flexible solution. Cervello is distinguished by its elegant and simple scalability; it can start with monitoring a single aspect and expand per the customer's needs. This means there's no need to commit to monitoring the entire network to gain value.

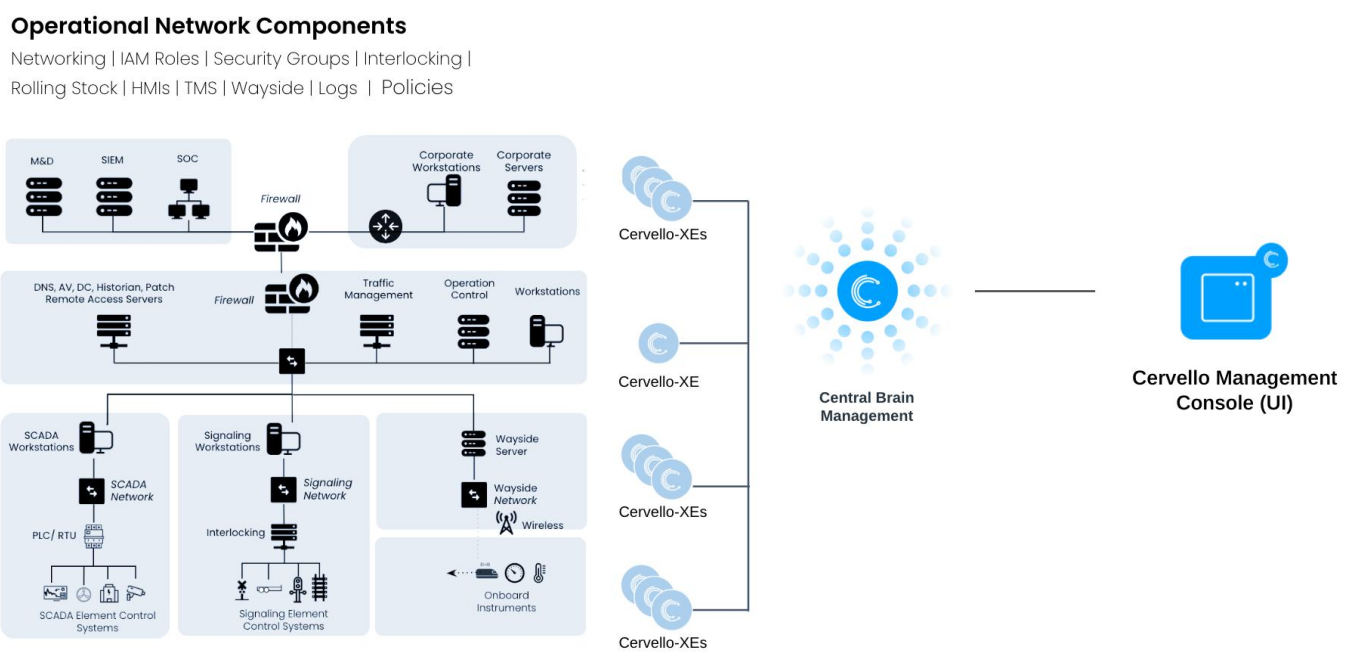
Moreover, we understand that forwarding all network traffic to one central point is challenging, which is why our XE solution is deployed in various locations to locally monitor network traffic and forward only the relevant information to the central system (the Brain).

The extensive range and flexibility of Cervello-XE (our software collector) facilitates the integration of any rail subsystem into your security solution in a quick and simple manner. This results in a consolidated, single view of the risk and visibility across all the rail environment, with reduced complexity and cost.

Tailored for Rail

Our solution is software-only and hardware-agnostic, tailored specifically for rail environments. Cervello Platform understands the unique requirements and challenges associated with the rail industry. By providing specialized protection and monitoring capabilities tailored to the railway industry, it addresses the complexity of control systems, signaling networks, and passenger information systems.

The operational insights that our platform is capable of providing, are made to the finest level of detail in rail context. Our platform knows everything in your network, analyzes it, and provides you with strong impact and consequence information. With Cervello's cybersecurity expertise and rail operational expertise, each component is examined at the system and operational levels in depth. Through its understanding of rail-specific protocols without requiring prior knowledge or assistance and the understanding of network behaviors, it can detect more cyber threats in real-time and direct you to the specific areas that need to be addressed. Whenever a protocol is not initially supported by Cervello, it is capable of learning and assimilation of an unfamiliar protocol into its platform for seamless integration. Operators receive precise, actionable insights, down to the finest details of their operations. This advantage leads to the most accurate, precise insights you can receive.



From Data Collection to Operational Insights - How We Do It

The strength of Cervello in creating the insights mentioned above starts from passively collecting pure traffic across the selected networks, including IT, OT, IoT, Signaling, Onboard, and Rolling Stock. Designed for flexibility, the platform can integrate and adapt to capture data from any part of the network, utilizing its versatile architecture to meet specific customer requirements.

The traffic is taken from systems across the following layers:

Operational Layers

The rail traffic management systems, which enable organizations to manage and control the entire infrastructure and operations.

Safety Layers

The physical and digital safety layer for train protection and remote control.

Element Control Layers

This transport layer acts as the communication hub, transmitting control signals and data across the railway via radio, fiber optics, copper cables, and cellular networks. It connects safety systems to field elements like signal heads and track sensors.

Field Elements Layers

The endpoint/edge components of the railway, such as signal heads, axle counters, level crossings, balises, and so on.

The Cervello Process from pure network traffic to operational insights -

Data Collection and Preliminary Analysis: **Cervello XE**
(Edge or Virtual, can be distributed to support unlimited scale)

This phase encapsulates the core functionality of Cervello-XE as it passively monitors, collects, and does an initial analysis of network traffic directly from the operational environment. It includes the critical steps of aggregating relevant data, which ensures that only essential information is forwarded to Cervello Brain for further analysis, thus optimizing bandwidth usage and focusing security efforts on genuinely significant threats and vulnerabilities.

- Tailored for Rail Networks
- Passive Monitoring
- Flexible Installation: Can be installed physically, virtually, via cloud or edge.
- Analyzes traffic locally and sends pertinent information to Cervello Brain (OMC/CMC) for further calculations and analysis.
- The pure data gathered and transmitted by the XE includes network interfaces, connections, insights, protocol commands, and events.

Security Intelligence Hub: **Cervello Brain -**

Cervello Brain acts as the central intelligence system, receiving and synthesizing data from Cervello-XE units distributed across the network. It analyzes the data and applies advanced patented security methods to assess and alert about cybersecurity threats based on its overall view of the various environments. This integrated system enhances threat detection capabilities and provides extensive visibility across the network's signaling and infrastructure components.

- Scalable architecture that allows it to handle and secure numerous assets, facilitating rapid and efficient response to security incidents.
- Seamless integration with SIEM/SOC systems and other administrative tools, improving operational coordination and efficiency.
- Cervello Management Console and User Interface offers streamlined and user-friendly access for managing cybersecurity operations, thus bolstering the organization's ability to maintain resilience against cyber threats.

Operational Command Center: **Cervello Management Console -**

The Cervello Management Console, hosted by Cervello Brain, serves as a central hub for comprehensive cybersecurity management across railway systems. It consolidates risk monitoring and visibility for OT/ICS, IoT, Signaling, Rolling Stock, and IT environments, providing real-time insights, asset management, threat detection, and compliance monitoring. The console's user-friendly interface brings together data from these various sources into a single, easy-to-navigate dashboard, setting a new standard for the user experience of cybersecurity in rail. This unified view ensures full control over rail operations and easily integrates with existing IT security and administrative systems. The platform's industry-tailored approach allows it to be seamlessly used across the organization, from operational personnel to cybersecurity specialists and CISOs, supporting streamlined workflows for fast threat response. Fully integrated with your existing security infrastructure, the Cervello Management Console enhances operational control, empowers you with tools to classify and manage risks, respond to incidents efficiently, and ensures robust protection against cyber threats, making it a pivotal element in enhancing global rail network security.

For more information, visit cervello.security or email info@cervello.security