# BOMBARDIER TRANSPORTATION AND POSITIVE TECHNOLOGIES ACCELERATE CYBERSECURITY OF THE RAIL CONTROL SYSTEM

Bombardier Transportation is a global leader in the rail industry. The company offers an extensive and diverse portfolio of products and solutions including rolling stock, hauling gear, rail control solutions, as well as design, integration, and maintenance services. Bombardier Transportation's focus is on the maximum security possible around transportation processes. Its automated microprocessor rail control and signaling systems are successfully utilized in over 50 countries around the world.

## THE CHALLENGE

A vast variety of solutions for mainline rail employ the computerized interlocking system EBILock 950, including the ones used in radio-based train separation systems. EBILock 950 components are utilized for high-speed trains, metros, light rail vehicles, and trolley buses.

Modern systems of railway transportation rely heavily on IT solutions, which makes them vulnerable to cybersecurity threats. That is why Bombardier Transportation and Positive Technologies joined their efforts to raise the security level of the EBILock 950. The team of experts from Positive Technologies, which had previously discovered over 250 zero-day vulnerabilities in various ICSs, faced a new challenge to meet the client's requirements.

The specialists began their research by analyzing a testbed environment that precisely copied the train control architecture. These tests revealed a number of vulnerabilities. The team produced full threat models for these weaknesses and recommendations for urgent remedial action. As Positive Technologies always takes a responsible approach towards their projects, during phase one the experts conducted an audit to guarantee that a resulting solution would be able to provide full protection to the system while taking into consideration its protocols, business operation, and logic, as well as counteract all relevant security threats.

Phase two saw the specialists from Positive Technologies working in close collaboration with the Bombardier Transportation team. Detected flaws were eliminated thanks to Positive Technologies expert advice and follow-up control. The key restriction was not to disrupt the usual workflow of EBILock 950 components as they manage critical processes. The solution should passively monitor the EBILock 950, detecting unfolding cyberattacks and security incidents, and instantly report them to responsible parties.

## THE SOLUTION

Positive Technologies presented PT Industrial Security Incident Manager™ (PT ISIM™) as a solution to the challenge. Unlike any other product, not only does PT ISIM™ support industrial protocols and logs security accidents but it also visualizes attack development in time across the whole infrastructure. Also, a customized visualization interface was developed to display all incident stages on the object's schematic designed to replicate the monitoring screens in the control room.

All additional requirements concerning integration in the operation infrastructure were also met.

PT ISIM™ doesn't require recertification of the equipment as it uses a one-way flow of data and there is no risk of interference with the rail control technology and its processes. The industrial version fully complies with the operating conditions of the protected object.

### BOMBARDIER TRANSPORTATION

**Industry:** Transportation, manufacturing of railway products

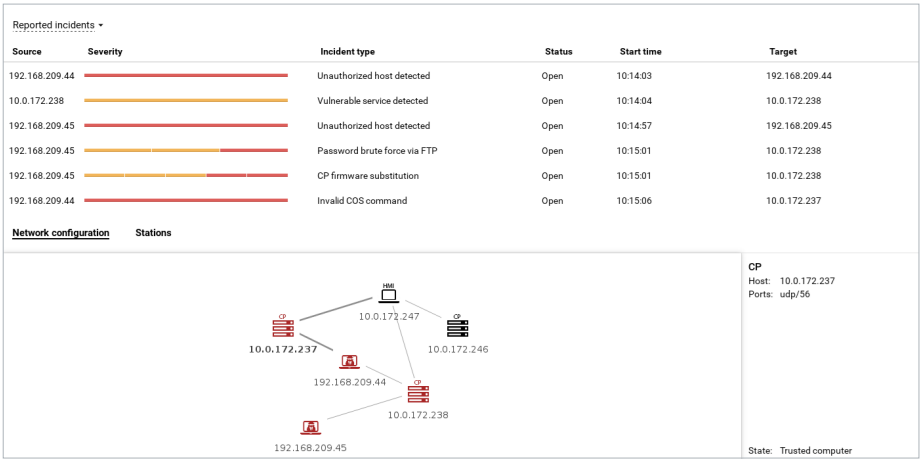
**Challenge:** Detect new cyberthreats for the microprocessor-based industrial control system EBILock 950 and upgrade its protection

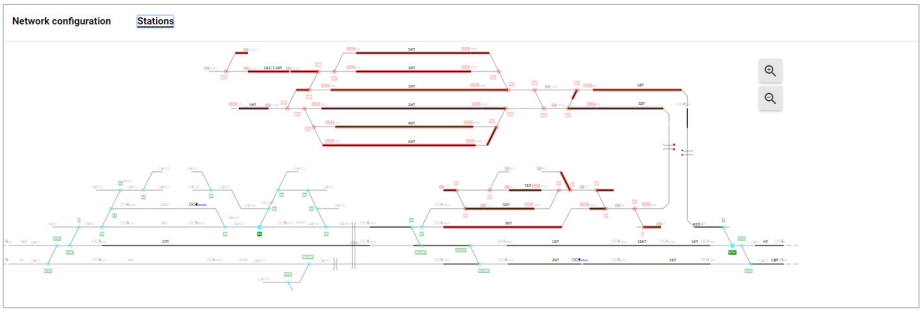
**Solution:** PT Industrial Security Incident Manager™ (PT ISIM™)

**Result:** The EBILock 950 system is protected against new cyberthreats and hacker attacks.

## KEY FEATURES

- Visualization of unfolding attacks as a chain of events
- Attack visualization on the organization's schematic based on the equipment data and business logic
- Data collection with no risk of interference with the rail control processes
- Incident investigation without interrupting the system
- Alerts and instructions for urgent remedial action at all levels




## RESULTS

Following a successful pilot project, PT ISIM™ is being rolled out across multiple railway stations with heavy traffic flow. The level of expertise and the technology solutions provided by Positive Technologies managed to meet the high standards of Bombardier Transportation and proved that PT ISIM™ is capable of maintaining ICS security in rail control systems of any scale.

## About Positive Technologies

Positive Technologies is a leading global provider of enterprise security solutions for vulnerability and compliance management, incident and threat analysis, and application protection. Commitment to clients and research has earned Positive Technologies a reputation as one of the foremost authorities on Industrial Control System, Banking, Telecom, Web Application, and ERP security, supported by recognition from the analyst community. Learn more about Positive Technologies at ptsecurity.com.



POSITIVE TECHNOLOGIES

info@ptsecurity.com ptsecurity.com