Case Study

Protection of Digital Train Fleets

Northern Rail use RazorSecure to ensure new digital fleet is compliant with NIS cyber security regulations

Background

Northern Rail were in the process of procuring a new digital train fleet for one of their franchises. Prior to the delivery of the fleet, it was identified that there would be new regulations related to cyber security that were in the process of being implemented by the EU, these are now in force as the NIS Directive.

This new fleet formed part of a wider digital train programme across the organisation, involving new CCTV systems, passenger information and other devices that had not previously been connected.

Arriva were looking for a single pane of glass view across their digital trainfleet, both new and refurbished trains.

What our customer says:

> *"RazorSecure's products are an effective part of our security in depth approach. We consider their solutions to be unique and ideally suited to work in a distributed and often isolated environment."*

Marc Silverwood,
Digital Trains Project Manager, Northern Rail

northern

Industry

- Rail

Environment

- Train Operating Group - UK and Europe

Requirements

- Solution adaptable to all trains across the fleet
- Must adhere to NIS Directive regulations
- An alternative to outdated signature based detection
- Customised reporting of cyber security programme

The Challenge

As the operator, Northern Rail realised that they would be accepting not only the operation of the new train fleet, but also the risk attached to the connected systems onboard the train.

The train builder was able to supply information regarding the design of the onboard networks, but were in the early stages of implementing a cyber security programme themselves.

Icomera had been engaged as the onboard connectivity supplier for the digital services, and introduced RazorSecure to the team at Northern Rail.

Working with RazorSecure, the team at Northern Rail quickly identified that the Icomera X6 gateway represented a key point of aggregation within the network. The gateway represented the main point of traffic ingress/egress to the train, as well as a key convergence point for passenger, CCTV, passenger information and operational traffic onboard. through machine learning and anomaly detection.

The Solution

After following the application of the RazorSecure Process and identifying the Icomera X6 gateway as a key system, RazorSecure proposed to introduce RazorSecure Delta to the Icomera X6 gateway.

RazorSecure Delta is designed to deal with key points of aggregation within an onboard network, by learning "what is normal" for key systems. Going beyond network traffic and looking at over 700 points of key data including running software, installed software, listening network ports, system logs and critical files onboard.

Importantly RazorSecure Delta does not rely on signatures but instead focuses on the behaviour of devices. This ensures that the software remains effective for the life of the asset. The team at Northern Rail began with an initial fleet of 16 trains, before rolling out across their new digital trains. The software was remotely installed by the Icomera engineers.

The RazorSecure team also worked with the Digital Trains team at Northern Rail to develop customised reporting for their management team, to demonstrate the ongoing value of the cyber security programme they had put in place

Outcome

Once installed it became clear that RazorSecure software could also identify operational anomalies, helping the Icomera team to quickly identify and remediate issues that would have been challenging to otherwise diagnose.

They used the software to compare across the fleet of digital trains, quickly identifying differences in software versions, security patches and configuration. Ensuring compliance across the fleet and preventing configuration drift.

Once installed, RazorSecure Delta was quickly able to identify passengers performing vulnerability scans against network systems, and provide a continuous view of risk to Northern Rail. This was provided through monthly threat reports and regular review calls.