RazorSecure

Case Study

PROTECTION OF DIGITAL TRAIN FLEETS

Northern Trains use RazorSecure to ensure their new digital fleet is compliant with NIS cybersecurity regulations

PROFILE:

Northern Trains is the largest UK train operator outside of London, and plays a vital role by connecting tens of thousands of people to work, leisure, education and more every day.

FACTS AND FIGURES:

- 100 million passengers every year
- Fleet consists of 355 trains
- Provides more than 2,500 services a day
- Trains call at nearly 550 stations

BACKGROUND

Northern Trains 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.

REQUIREMENTS

ADAPTABLE TO EVERY TRAIN IN THE FLEET

Northern Trains require a holistic approach to cyber security, with adaptable technology to cover new build and legacy vehicle requirements. When procuring a new digital train fleet for one of their franchises, Northern Trains 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.

ADHERE TO NIS REGULATIONS

Cyber security frameworks are essential components of understanding cyber risk and guidelines for the protection of railway assets. Northern Trains need solutions to align with the cyber security frameworks, whilst also supporting efficient ongoing operations.

NO USE OF SIGNATURE-BASED DETECTION

Traditional signature-based threat detection is no longer enough. Northern require anomoly-based threat detection to quickly expose threats from unknown sources to mitigate the risks of cyber attack.

CUSTOMISED CYBER SECURITY REPORTING

Northern Trains require a customisable, clear reporting of their fleet's real-time cyber security posture, allowing them to prioritise cyber requirements and operational risks with clear, understandable data and alerting.

THE CHALLENGE

With the new digital trains being delivered, Northern Trains, as the operator, realised that they would be accepting not only the operation of the fleet but also the risk attached to the connected systems onboard each 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 shortens the time to detect threats from unknown sources, and mitigate the risk from cyber attacks. RazorSecure Delta is in compliance with new NIS Directive regulations and has been fully tested, consistently demonstrated in production to maintain effectiveness for the full duration the asset is in service. 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 Trains to develop customised reporting for their management team, to demonstrate the ongoing value of the cyber security programme they had put in place.

RazorSecure Delta continuously monitors the behaviour of individual systems and traffic across the full network in real-time, to quickly detect, alert and respond to malicious activity and security violations that are outside of normal operation patterns.

RazorSecure Echo provides realtime monitoring or onboard IT and OT systems, giving a real-time accurate view of the status and availability of these systems and planning of effective maintenance.

RazorSecure Echo

The software was used to analyse the fleet of digital trains, quickly identifying differences in software versions, security patches, and configurations. This ensured compliance across the fleet and prevented configuration drift.

RazorSecure Delta

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.

"RazorSecure are always there, they're always at the end of the phone, they're always monitoring our systems, keeping our trains safe and secure. Any dynamic threat that may come our way, RazorSecure are always one step ahead in understanding what that could look like for Northern. We work very closely with them as a trusted partner and its important that we do observe their learnings. They're very highly skilled in the industry and that's why we've partnered up with RazorSecure to ensure that not only are we getting the best product that's out there, but also we have the trusted mechanism that Northern can operate its vast amount of passenger services every day knowing that RazorSecure's there, in our corner, fighting the cyber threats that we may face at one point."

Marc Silverwood, System Manager, Northern Trains

RAZORSECURE APPROACH

We recognise that each train fleet is different and may require a tailored approach due to differences in network design and levels of IP Connectivity. By understanding your network, we can advise on security best practises and the risks within your environment. We will then work with you to design, integrate, homologate and deploy the RazorSecure software across the key systems and network points we identify.

Our flexible approach is customised to manage the unique challenges and requirements of each customer. We will work closely with you to find a solution for any challenge you may have. The first step towards improved digital is simply to begin a conversation with us, and our team will be happy to guide you through the process.

ABOUT US

RazorSecure provides solutions to enhance railway cyber security by monitoring and protecting networks and their key systems. With over 500m passenger journeys and 23 distinct train fleets this proven approach ensures our solutions are designed specifically for rail, including rolling stock, signalling and infrastructure systems.

RazorSecure

sales@razorecure.com

razorsecure.com