Case Study

Protection of Passenger Wireless and Onboard Connectivity Systems

RazorSecure partners with Icomera, a leading provider of wireless internet activity for public transport.

Background

Rail operators are looking to add connectivity services to their train fleets for improving both passenger satisfaction and providing the ability to monitor and manage their fleets more effectively.

Connectivity is an enabler for a range of onboard services, powering a new type of passenger journey. Referred to by Icomera, the market leader in connectivity, as the Connected Journey.

What our partner says:

> *"At Icomera we believe wireless Internet connectivity has a very important role to play in making public transport a better, safer, more attractive option for passengers by enabling an ecosystem of onboard services and real-time data feeds.*
>
> *Integrated networks undoubtedly offer a vast range of benefits but as a provider of infrastructure, cybersecurity is a major concern for all public transport operators looking to keep passenger and operational data secure.*
>
> *We work with RazorSecure and their technology to mitigate the risks".*

Peter Kingsland, Managing Director of Icomera

icomera

A company of ENGIE

Industry

- Rail

Environment

- 25,000 connected vehicles
- Fleets in UK, Europe & NA

Requirements

- Visibility of the entire fleet, including performance
- Rigid bandwidth restrictions
- An alternative to outdated signature based detection.
- Flexible deployment due to challenging environment
- Accurate reporting of potential threats

The Challenge

Through the adoption of new cyber security requirements, Icomera began to see operators asking more detailed questions regarding security and how it was managed on their X-series router.

Operators had previously asked Icomera to perform penetration testing, which provides a good basis for understanding cyber security. However, they were beginning to see requirements around intrusion detection and cyber security monitoring.

They recognised that a different solution would be required to deal with onboard systems, having reviewed other solutions they quickly identified that:

- Bandwidth requirements for enterprise solutions excluded them from deployment onboard.
- A solution needed to operate independently of a cloud environment.
- Signature based approaches did not represent an effective solution because they require constant signature updates.
- Network based approaches would only provide limited protection, as they lack the insight into the core operating system of the device being protected.
- A significant number of false positives would lead to a high total cost of ownership for the system.

They were concerned that a solution would cause significant CPU usage and use a significant amount of resources on the X-series router. In addition, they see the opportunity to improve their operational monitoring through machine learning and anomaly detection.

The Solution

Icomera decided that cyber security would be a competitive strength and they undertook a programme to achieve ISO-27001 compliance. In addition, they engaged with RazorSecure to integrate the RazorSecure Delta software into the X-series IMP platform.

The RazorSecure team managed the integration process, dealing with minor differences between platforms and ensuring that the software would cover the device effectively. The RazorSecure team worked with the Icomera engineers to test the resource usage and ensure that it did not use more than the agreed upon resources.

Typically RazorSecure Delta uses less than 1% of the CPU on a system and up to 120mb of memory, however this can be tailored depending on the use case.

The deployment of the RazorSecure software was managed remotely by the Icomera Engineers, integrating into their existing deployment pipeline. To manage maintenance activities, the RazorSecure team integrated API calls to enable the maintenance mode of RazorSecure Delta.

Once maintenance is completed, the Icomera team receive a maintenance report with all activities recorded for future audit tracking and to ensure that no cyber security artefacts are left behind.

Outcome

Today the Icomera engineers use RazorSecure software to ensure that they have a complete view of fleets with transport operators in the UK, Europe and North America.

They work daily with the RazorSecure team to actively manage security threats to operators, investigating potential attacks quickly using the clear, easy to read alerts.

The Icomera support teams are empowered with visibility into the operational performance of their systems, using RazorSecure's anomaly detection to quickly identify units that are not performing consistently with the rest of the fleet.

RazorSecure's focus on learning behaviour and understanding "what is normal" for the Icomera IMP platform leads to low numbers of false positives, ensuring that the system is easy to manage

Belvedere House, Suite LG8, Basing View
Basingstoke, Hampshire, RG21 4HG

sales@razorsecure.com

RazorSecure™