USE CASE

RazorSecure™

Security Monitoring

Continuous cyber security monitoring of onboard networks and system behaviour to identify issues and security threats

SECURITY MONITORING DEFINED

Security monitoring is the process of continuously monitoring networks, and systems, to gain forensic insights, real-time and historic, into cyber security threats, across the full IT or OT environment.

As a proactive approach to cyber security, security monitoring is a crucial part of cyber risk management for rail, enabling operators to detect cyber-attacks early, and respond to them before the incident can affect operations and availability.

RAIL CYBER SECURITY RISKS

As cyber attacks become increasingly sophisticated, the rail industry needs to implement appropriate proactive, rather than reactive, security practises. While preventative cyber security technology is capable of known signature-based threats, cyber security threat monitoring is required to identify more sophisticated threats that evade these controls.

MALICIOUS INSIDER THREATS

The belief of a security perimeter, with trusted actions on the "inside", and untrusted on the "outside", is no longer valid. Many attacks now come from within the network, and from those who already have access. Rather than just protecting the edge, it is now essential to monitor within the network perimeter as well.

UNKNOWN ZERO-DAY ATTACKS

A zero-day attack is the constant threat of an unknown security flaw on a system, that an attacker takes advantage to stay undetected and spread throughout the network. By nature of the attack, rail networks may not have the detection mechanisms in place, meaning it can take days, weeks, or even months before the attack can even be discovered and investigated.

CYBER RISK BLIND SPOTS

The attack surface of rail is increasingly growing. Networks have been proliferated with new digital devices and systems. With an inability to continuously monitor the location, status and configuration of every system across a fleet, then you are unaware of the true scale of the present cyber risks.

DELAYED RESPONSE ACTIONS

In cyber security, speed defines the success of both the defender and the attacker. The severity of cyber attacks can vary, but it can directly correlate to the length of time an attacker has access to their target systems. There is a considerable difference in impact of breach that is detected and remediated within two hours, versus two days.

COMPLY WITH INDUSTRY STANDARDS

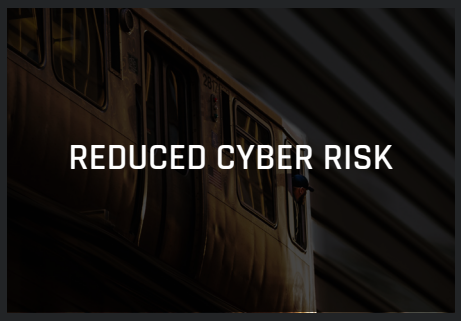
Continuous security monitoring is a key requirement of current rail cyber security standards and regulations such as TS50701, IEC62443, the EU NIS Directive and the NIST Cyber Security Framework. Cyber security programmes that use continuous security monitoring, facilitate essential ongoing awareness of threats and vulnerabilities to maintain the security of critical systems, over time in highly dynamic environments of operation.

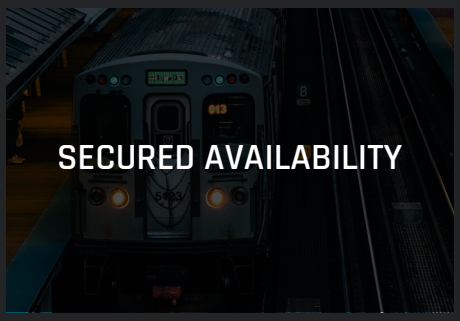
RazorSecure Delta continuously monitors the behaviour of individual systems and traffic across the full network in real-time, to quickly detect, alert and respond to malicious activity and security violations that are outside of normal operation patterns.

DETECTING THE TRUE SECURITY AND OPERATIONAL UNKNOWNS

RazorSecure Delta uses machine learning to build a baseline of 'normal behavior' for each individual system on rolling-stock, and identify patterns of activity, to provide the best possible data to protect each system individually, even when considering intrusion anomalies across a rail fleet with hundreds of similar assets.

- Aggregate and analyse data from processes, configurations, network ports, network traffic and system logs.
- Build a baseline metric and understanding of how each system behaves in normal operations.
- 24/7 continuous monitoring for behavioural anomalies that go against established behaviour patterns.
- Ensure effective protection for the life of the asset, without the reliance attack signatures.





REAL-TIME AWARENESS OF THREATS

By understanding what is 'normal' behaviour for the network and each individual system, we gain a better understanding to know when activity is suspicious, in real-time, as it deviates from the system's normal behaviour patterns.

IDENTIFY SOFTWARE MISCONFIGURATIONS

When systems are tampered with, it may produce unwanted or unpredictable results. Changes in a system's operating patterns or configurations may be done to mask attack behaviour or any malicious activity.

RAPID RESPONSE AND REMEDIATION

With awareness of real-time anomalous behaviour, that hasn't yet become a cyber security incident, we can zoom in to investigate the attackers capabilities, what their potential attack plan is and how we can prevent it escalating.

CYBER SECURITY METRICS AND INSIGHTS

Gain live data that offer a full view of your security posture, compliance, cyber risks and vulnerabilities. Accurate insights enable informed decisions when addressing and prioritising additional security measures and actions.

RAZORSECURE.COM

SALES@RAZORSECURE.COM

REPORTING

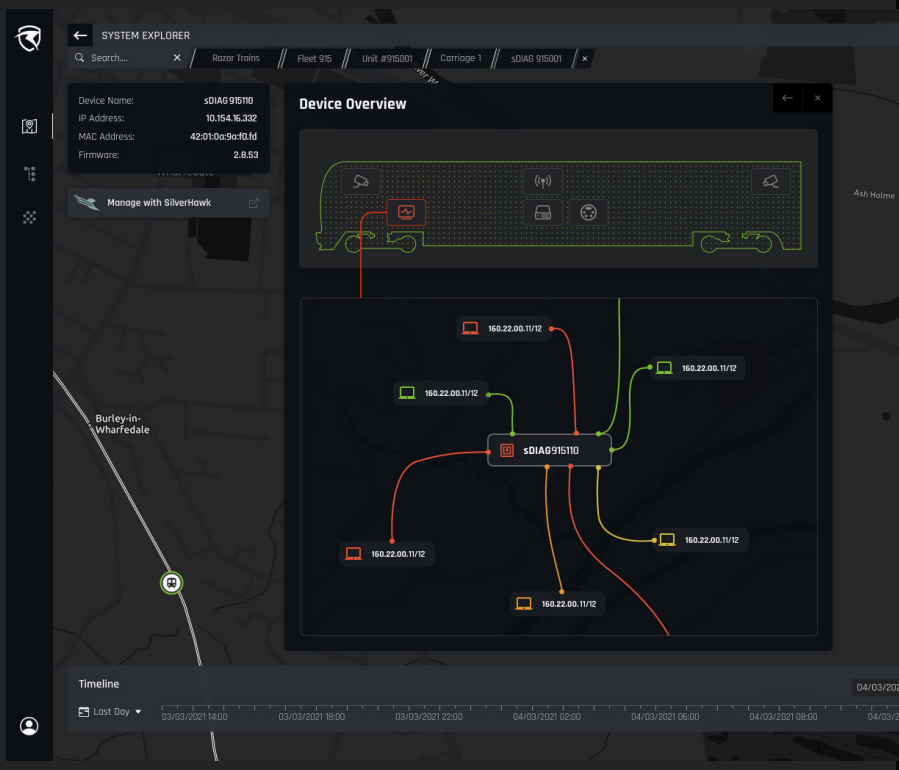
SECURITY MONITORING SERVICE

RazorSecure also offers a full monitoring service for organisations that don't have resources to run their own SOC in-house. Our fully managed monitoring services help our customers see more, know more and take the right action, with a dedicated team of experienced cyber security experts that provide up-to-date threat intelligence and expert analysis of activity in your environment.

SECURITY DASHBOARD

Developed with leading train operators, the RazorSecure security dashboard is a full feature managed platform that presents high-level overviews and granular data leveraged from all systems, devices, and segmented networks within your fleet.

With clear, consistent reporting and in a single pane of glass view, the dashboard will help clarify, and prioritise, your fleet's cyber requirements and operational risks with clear, understandable data and alerting.



INTEGRATION WITH EXISTING SIEM

Data from the RazorSecure platform can be integrated into leading SIEMs via Common Event Format (CEF) feeds and REST APIs.

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 offers products and services to enhance railway cyber security by monitoring and protecting networks and their key systems. We deliver this through our flexible approach to cyber security, designed specifically for rolling stock, signaling and infrastructure systems.

RazorSecure™

RAZORSECURE.COM

SALES@RAZORSECURE.COM