
RazorSecure
Improving Cybersecurity on Legacy Trains through Retrofit

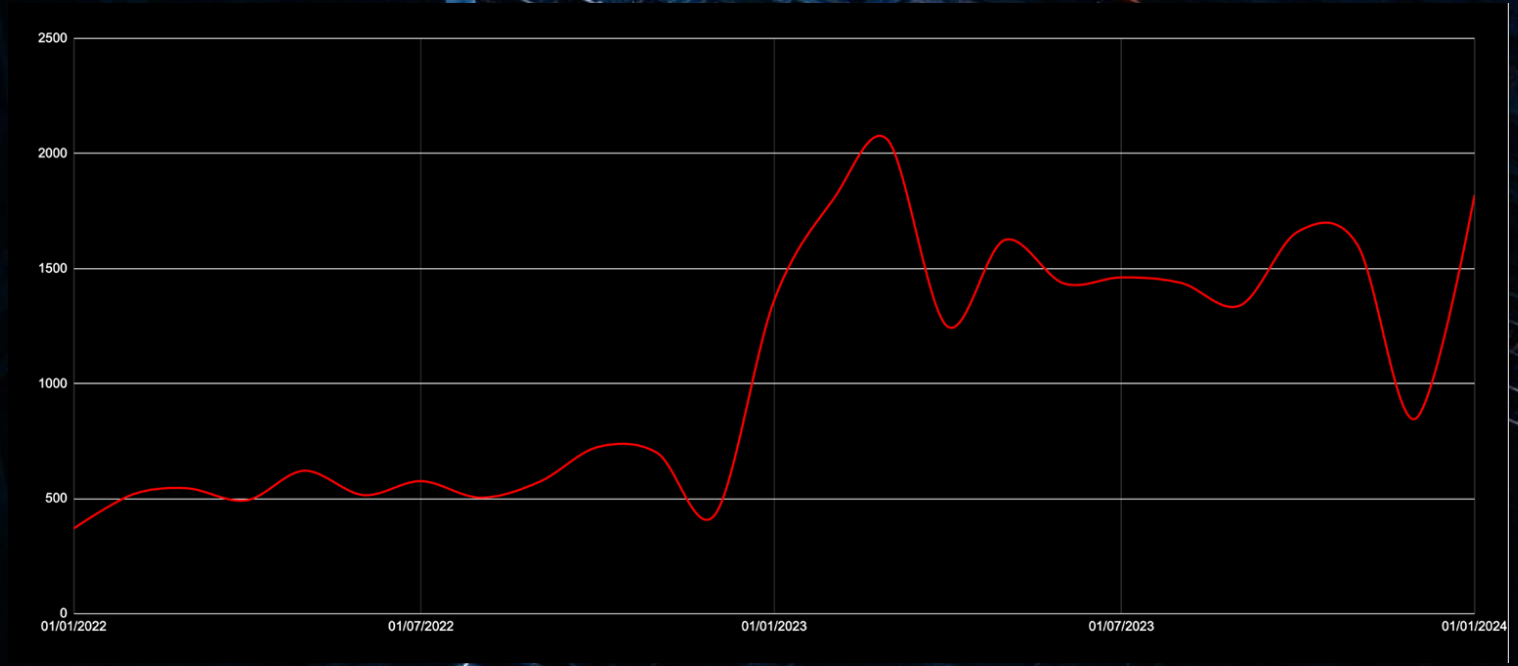
Independent Rail Cyber Security Specialists

9 Active Operators

Projects with 5 Train Builders

6 Years Production Deployment

Cyber Security Threats In Rail



391%
Increase

Portscans + Denial of Service Comparison 2022-2024

Threats recorded on trains protected by RazorSecure

Introduction – NS Security Appliance

Overriding aim – to realize a solution in our Rolling Stock, designed to optimally protect this Rolling Stock against Cyber Security threats.

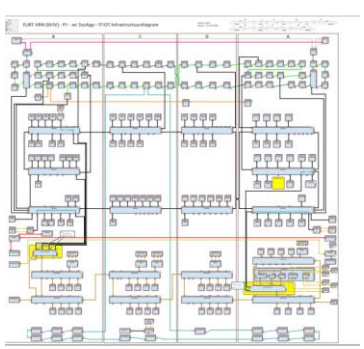
Fleet wide Risk Analysis exercise led to the insight that certain rolling stock is vulnerable to cyber risk more than we initially anticipated.

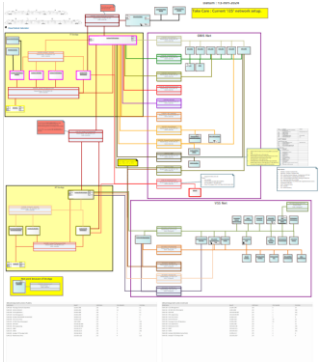
- The solution must make it possible to segment the network in the train and to inspect traffic between these segments.
- The solution must ensure that only inter-segment network traffic occurs that has been previously allowed (configured).
- The monitoring capability monitors that this traffic is legitimate and is not consisting of network traffic that carries malicious data or elements (intrusion detection, deep packet inspection, anomaly detection).
- The solution must be able to handle a large number of deployments (~1200 in total)
- The setup needed to be interchangeable (no vendor lock-in, vendor agnostic stack)

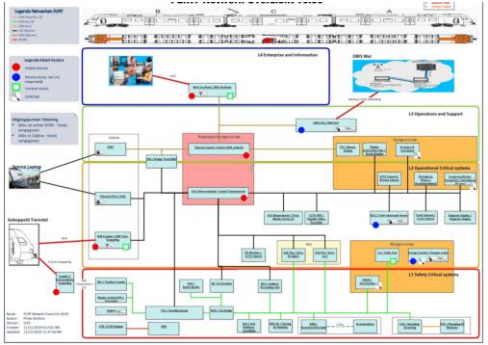
Introduction – NS Security Appliance

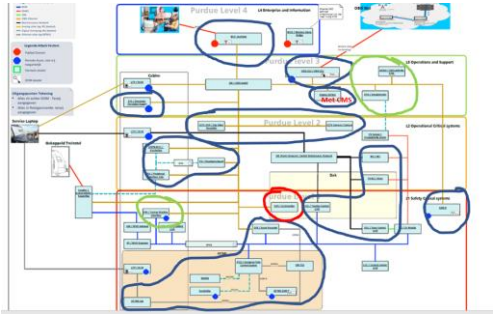
The solution design – from Asset analysis to network segmentation

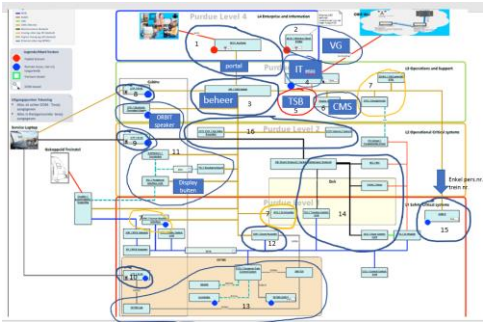
- The dirty work: it al starts by knowing what is out there
- Bringing the experts together to talk about it
- Draw, present, discuss
- Test











Dilemmas and concerns

Technology

- Do we select a combined HW and SW solution or do we separate them?
- Do we allow Operating system virtualization solutions or not?
- What host OS do we accept?
- Should we monitor MVB, CAM or other OT messaging busses?
- Is it one size fits all for all fleets or not?
- Implementing FW as Layer 3 device required a change to the entire network. Can this be handled?

Management

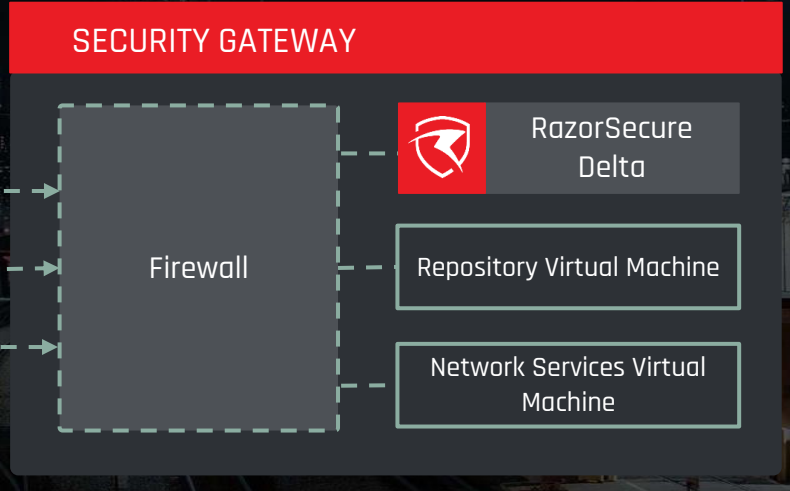
- Do we need an OT SoC or not?
- Do we allow IPS IDS to intervene (block) in network traffic or not?
- How to replace a device in the field?
- How to manage security incidents in our organization?
- How to prevent difficult homologation processes?
- How do we see if a device is failing?
- How do we manage 1200 devices?
- Do we allow cloud / SaaS managed solutions?

Some of these were classified as ‘hot potato’ and transformed in a steering committee decision memo.

Security Gateway Components

FIREWALL OPTIONS:

1. Open-Source Firewall
2. Open-Source Firewall + TRDP Protocol Filter
3. Next-Gen Firewall



Much effort was focussed to transforming the solution into a solid and low effort ‘field replaceable unit' that fits NS RS mechanics processes (auto detect and install).

First Fleet Install– Deployment and Challenges

Train build process

- Pre-try-outs (1), and 4 try-outs (build process)
- One train per day, 4 per week, 4 mechanics/ day
- Complex day scheme involving 7 new cables, OT and IT switch updates and WAP updates, 2 new devices, testing.

Outcomes (lessons learned)

- First fleet completed in 4-month time (final in august 2024)
- Daily available second line support team proved to be valuable in solving issues and making sure train was working correctly at e.o.b.d.
- 3 week delay because we encountered issues in IP plan with 4 coach trains (not revealed during testing)
- Inform stakeholders on a daily basis about progress proves very beneficial.

Three Top Tips

- Invest in a good test bench
- Invest the time to fully understand the onboard network
  - Physical, logical and traffic flows
  - This allows for good design in advance
  - Consider variations within a train fleet (3 vs 4 car)
- Be prepared to quickly solve problems during series production
  - Surprises occur on a daily basis that need to be acted upon swiftly
  - This is part of running a railway


RazorSecure