Reformo NETWORKS

Kyberturvallisuus rautatieoperaattoreille

Traficom

Raideliikenteen kyberturvallisuuden seminaari

3.12.2024

Railway cybersecurity

Challenges and importance in OT, IoT and IT systems

Agenda & Summary

- Two types of cyber attacks that matter
- Significant Cyber attacks
- Improving cyber security against rail transportation
- Latest cyber events
- Safety systems
- Access control systems
- Testing systems

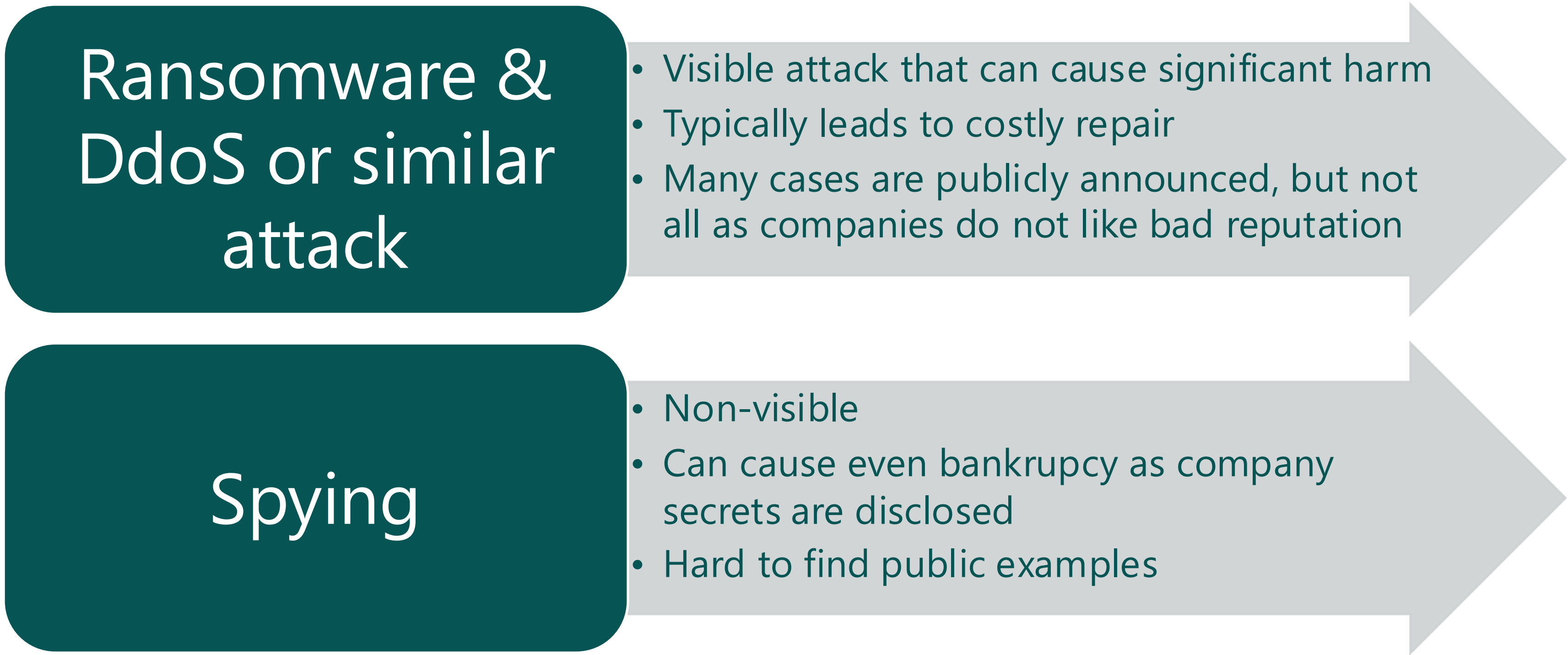
Introduction

Cyber attacks against companies

2 main types of attacks

Attacks against OT infrastucture

To simplify it can be stated that there are basically two Cyber attack types against OT infrastructure:



Ransomware & DdoS or similar attack

- Visible attack that can cause significant harm
- Typically leads to costly repair
- Many cases are publicly announced, but not all as companies do not like bad reputation

Spying

- Non-visible
- Can cause even bankrupcy as company secrets are disclosed
- Hard to find public examples

In both types the outcome is severe. Actually typically more severe than if it would have been an attack against the IT-infrastructure. Also, the most severe IT-outages often lead to shutting down Operations (= OT infrastructure).

And, in many cases the OT-infrastructure is actually **critical infrastructure**.

Attacks against OT infrastucture – visible

DdoS and Ransomware type of attacks are making the news. They are typically announcements from the company itself, or news that came public due to some reason.

July 2021. Security researchers detect a spike in hacking attempts against **IoT devices in Finland** during the run-up President Trump’s summit with Vladimir Putin in Helsinki. The majority of attacks originated in China. (significant cyber attacks report)

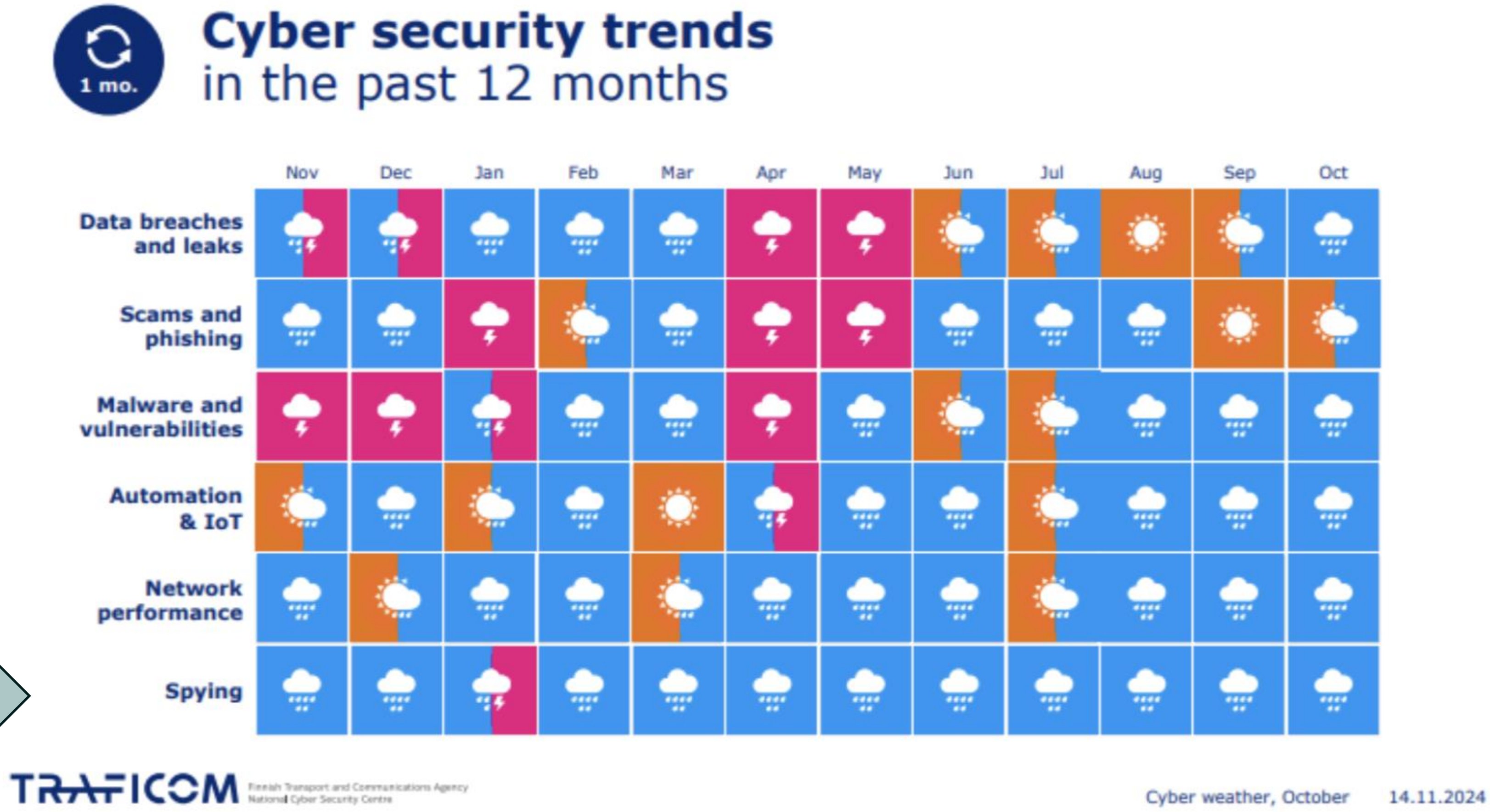
May 2021. On May 6, the **Colonial Pipeline**, the largest fuel pipeline in the United States, was the target of a ransomware attack. The energy company shut down the pipeline and later paid a $5 million ransom. The attack is attributed to DarkSide, a Russian speaking hacking group.

***May 2021.* LineStar Integrity Services**, a pipeline-focused business, was hit by a ransomware attack the same time as the Colonial Pipeline, with 70 gigabytes of its internal files being stolen. (significant cyber attacks report)

November 2022. Hackers damaged **Danish State Railways**’ network after targeting an IT subcontractor's software testing environment. The DDoS attack shut down train operations for several hours. (significant cyber attacks report)

Attacks against OT infrastucture – Type spying

Spying type of attacks are not making the news in real-time. They are typically after thoughts and can be found in statistics, such as “significant cyber attacks” or in Finnish Transport and Communications Agency’s monthly “cyber security trends” report.



1 mo.

Cyber security trends
in the past 12 months

	Nov	Dec	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct
Data breaches and leaks	🌧/⛈	🌧/⛈	🌧	🌧	🌧	⛈	⛈	🌦	🌦	☀	🌦	🌧
Scams and phishing	🌧	🌧	⛈	🌦	🌧	⛈	⛈	🌧	🌧	🌧	☀	🌦
Malware and vulnerabilities	⛈	⛈	🌧/⛈	🌧	🌧	⛈	🌧	🌦	🌦	🌧	🌧	🌧
Automation & IoT	🌦	🌧	🌦	🌧	☀	🌧/⛈	🌧	🌧	🌦	🌧	🌧	🌧
Network performance	🌧	🌦	🌧	🌧	🌦	🌧	🌧	🌧	🌦	🌧	🌧	🌧
Spying	🌧	🌧	🌧/⛈	🌧	🌧	🌧	🌧	🌧	🌧	🌧	🌧	🌧

TRAFICOM Finnish Transport and Communications Agency National Cyber Security Centre

Cyber weather, October 14.11.2024

Introduction

Cyber attacks against companies

Significant cyber attacks

Collected from 2021-2024

Report from CSIS

https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

- Records significant cyber incidents that have occurred since 2006. However, in this statistics we concentrate on incidents since 2021
- The focus is on cyber attacks on government agencies, defence and high technology companies or economic crimes with losses superceding a million dollars

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

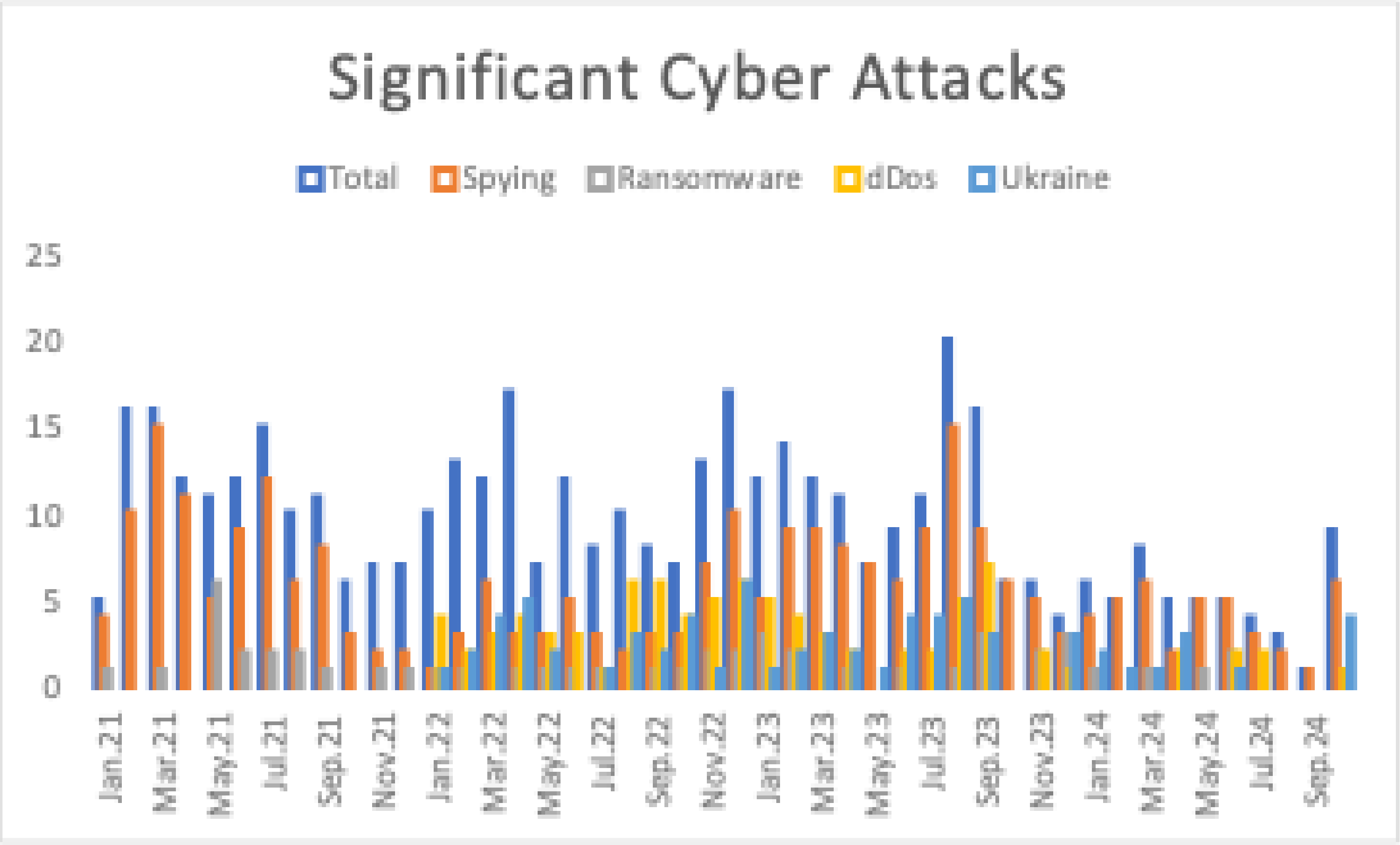
Statistics January 2021 – January 2024

Ransomware is here to stay.

Spying reports are made when they are discovered. This report shows more how they are discovered – than WHEN they occur.

The share of Distributed Denial of Service attack is decreasing, but “thanks to Ukraine campaign” they still occur.

The Ukraine War is very visible in the Cyber world. Both parties are doing Cyber war.



Reformo NETWORKS

Danish Railways – 3-7.11.2022

November 2022. Hackers damaged Danish State Railways' network after targeting an IT subcontractor's software testing environment. The attack shut down train operations for several hours.

- ✓ DDoS attack that caused servers to be out of service.
- ✓ A third-party IT service provider shutting down its servers resulted in a complete standstill on Denmark's railways.
- ✓ The company developed software called the Digital Backpack 2 that delivers operationally critical information to DSB's drivers.

Source: cybernews.com

Incident 1: DSB Train Cancellations (October 2022)

Danish operator DSB faced sudden train cancellations.

- A critical test environment provided by Supeo caused vital interfaces to fail.
- Investigation revealed a single system failure cascaded into multiple systems.
- Risk assessment for third-party supplier was inadequate.

Incident 2: Emergency Stop Messages in Poland (August 2023)

20 trains were halted due to emergency stop messages.

- The issue disrupted many services and took six hours to resolve.
- Cause: VHF train radio system, an open channel with no encryption.
- Documentation was easily accessible, and risks of external access were underestimated.

Incident 3: Software Malfunction in Poland (December 2023)

- Supply chain software malfunction caused a denial of service.
- Train services were significantly affected.
- Manufacturer was aware of cyber threats but software underperformed.
- Lack of awareness about software state; additional interfaces worsened the situation

Cyberattacks on Transportation & Logistics are Increasing

WORLD ECONOMIC FORUM

The Global Risk Report 2020
January 2020
Cyberattacks on critical infrastructure— rated the fifth top risk in 2020—have become the new normal across sectors such as transportation.

AP Associated Press

Christmas Ransomware Attack Hit New York Airport Servers
January 2020
An upstate New York airport and its computer management provider were attacked by ransomware over Christmas, officials said.

SECURITYWEEK INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

Railway Vehicle Maker Stadler Hit by Malware Attack
May 2020
The Swiss manufacturer announced that what appears to be a professional threat actor was able to compromise its network with malware and to exfiltrate an unknown amount of data.

The New Zealand Herald

Toll Says Data Stolen in Second Ransomware Attack Within Months
May 2020
In a statement, the transport and logistics giant said data was stolen during its second ransomware attack of the year, with hackers accessing a server containing private information.

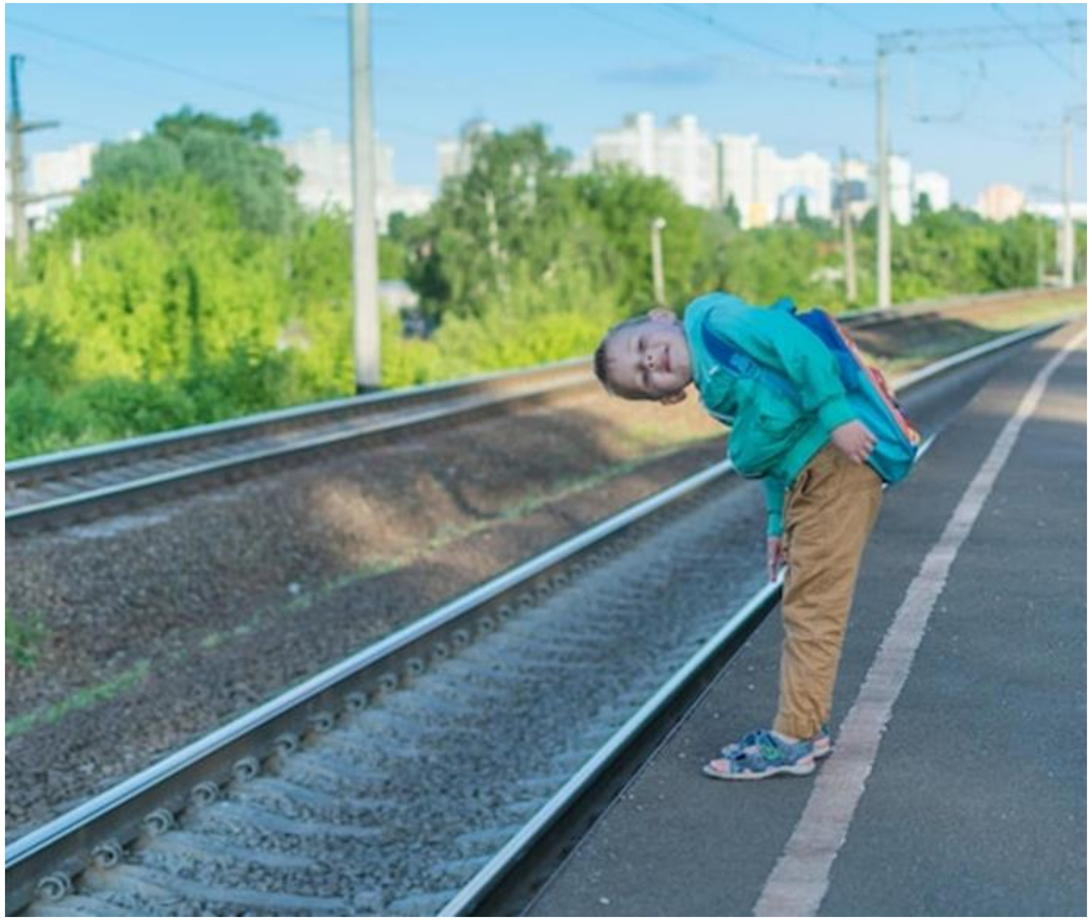
Improving Cybersecurity for Rail Transportation

Importance of Cybersecurity for Railway operators

- 🛡️ Safety: Prevents accidents caused by cyberattacks.
- 🔄 Continuity: Avoids service disruptions.
- 🔒 Trust: Protects personal data.
- ✅ Regulatory Compliance: Ensures compliance with standards like ISO/IEC 27001 (e.g., EN 50159).

Key Cybersecurity Challenges

- Low digital and cybersecurity awareness.
- Reconciling safety and cybersecurity.
- Digital transformation of core business.
- Long lifecycle of equipment leaves systems outdated.
- Diverse supply chain and technologies add complexity.



Why Railway Systems Are Targets

- Distributed architecture increases attack surfaces.
- Diverse supply chain and technologies add complexity.
- Increased digital connectivity exposes critical systems to cyber risks.

Challenges Facing Rail Networks

It is not just the train, or the tracks, or the safety systems...

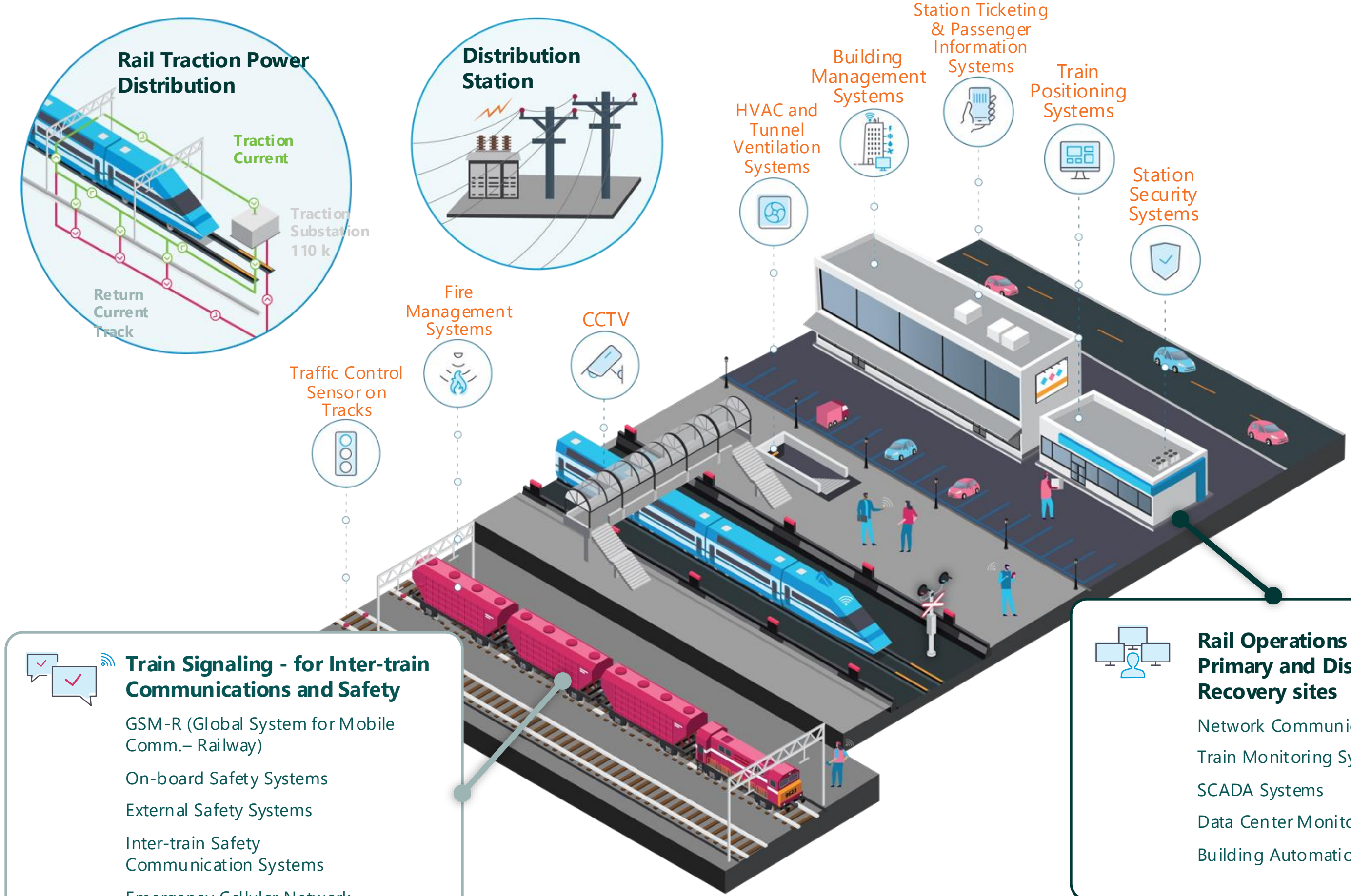
OT

Need advance warning of failing equipment or **end-of life** software in order to act before problems impact operations

Need faster and more resource-efficient **troubleshooting** of OT incidents with insightful forensic tools

Need **real-time visibility** of OT infrastructure assets, including those managed by third-party asset infrastructure service providers.

Need **actionable intelligence** to prioritize vulnerabilities and threats to expedite response and minimize downtime



Rail Traction Power Distribution
Traction Current
Traction Substation 110 k
Return Current Track
Distribution Station
Station Ticketing & Passenger Information Systems
Building Management Systems
Train Positioning Systems
HVAC and Tunnel Ventilation Systems
Station Security Systems
Fire Management Systems
CCTV
Traffic Control Sensor on Tracks

Train Signaling - for Inter-train Communications and Safety

- GSM-R (Global System for Mobile Comm.– Railway)
- On-board Safety Systems
- External Safety Systems
- Inter-train Safety Communication Systems
- Emergency Cellular Network
- Emergency Discharge

Rail Operations Center - Primary and Disaster Recovery sites

- Network Communications
- Train Monitoring Systems
- SCADA Systems
- Data Center Monitoring
- Building Automation Systems

IoT

Need comprehensive **visibility** of all IoT assets regardless of the vendor

Need clear **identification and prioritization** of the threats and risks that threaten security the most

Need **real-time monitoring** of building systems as well as above- and below-ground infrastructure, including rail signaling & positioning systems, electrical substations, tunnel ventilation, CCTV, and more.

Need to **reduce security risk** in a constantly changing threat landscape that includes targeted attacks

Comprehensive Cybersecurity Framework: Asset Visibility, Threat Detection, and Actionable Intelligence

Asset Visibility

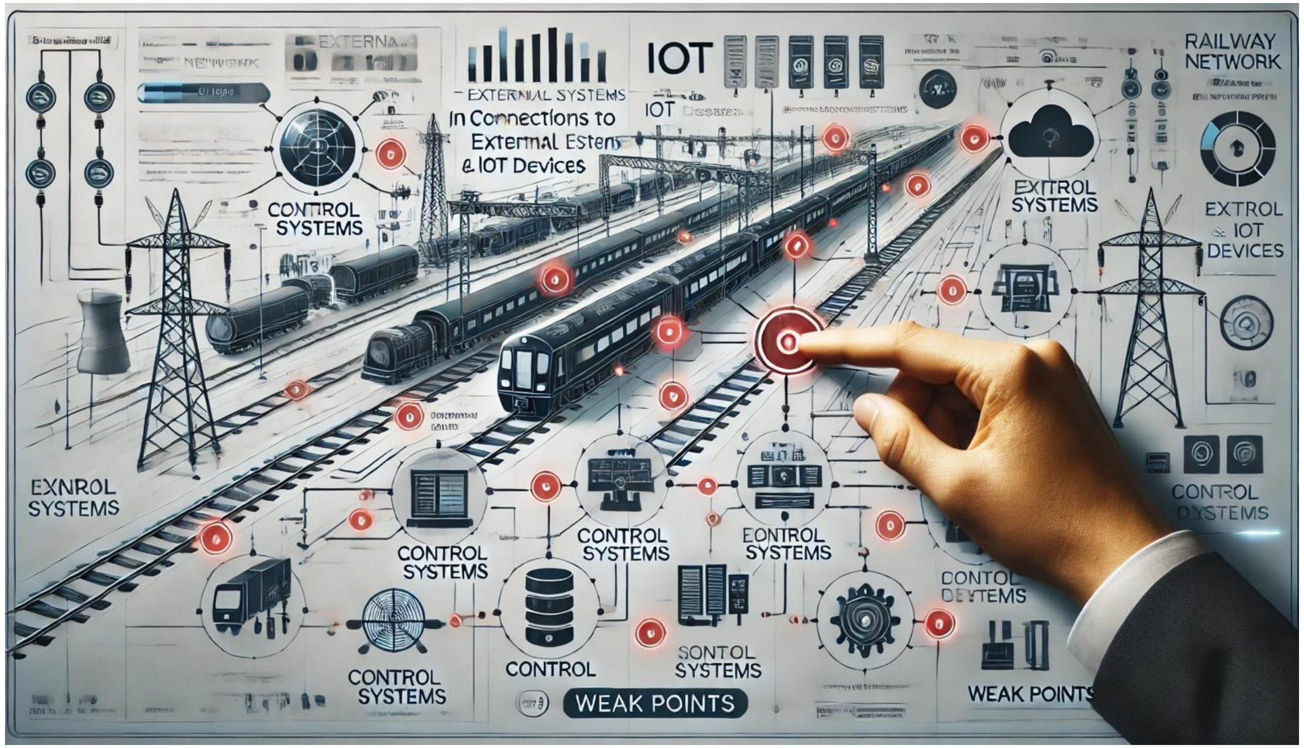
Knowing what assets are on your network is critical to managing risks and removing vulnerabilities

Threat Detection

Extensive database of known vulnerabilities and latest emerging malware threats

Actionable Intelligence

Actionable intelligence to address the problem with minimal costs and impact on operations



Emerging Threats

- Manage cyber risk **with a flexible and scalable solution to address OT/IoT security vulnerabilities**
- Make informed, prioritized decisions **with a clear picture of all rail assets and how they communicate**
- Get early warning **of possible disruptions across your entire rail transportation ecosystem**

The Nozomi Networks Solution Provides

Visibility

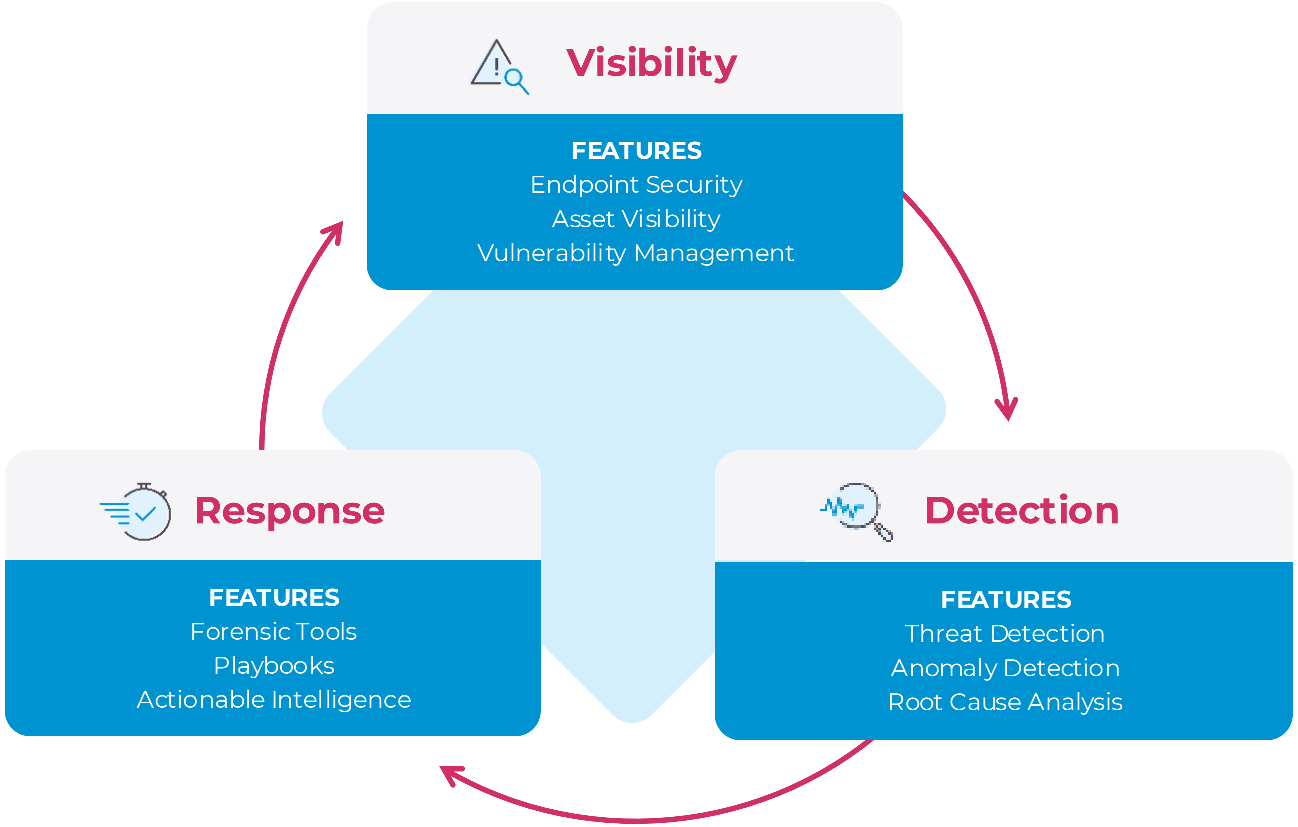
Gain visibility into security vulnerabilities and maintenance requirements to optimize operational processes

Detection

Detect emerging security threats and process issues with AI-based analytics to reduce business risk

Response

Respond to the highest priorities with actionable insights and guided remediation efforts for maximum efficiency



Visibility

FEATURES
Endpoint Security
Asset Visibility
Vulnerability Management

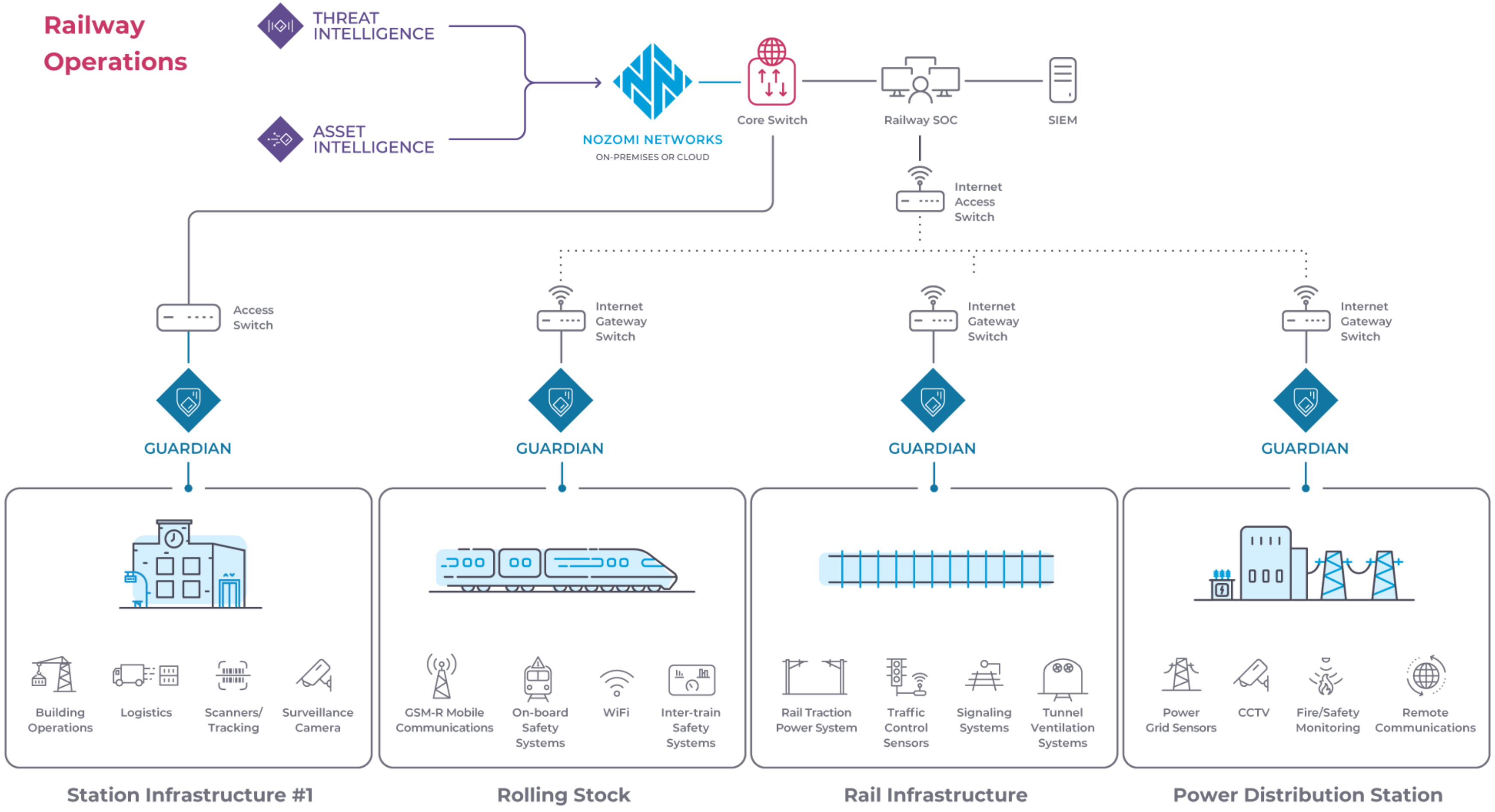
Detection

FEATURES
Threat Detection
Anomaly Detection
Root Cause Analysis

Response

FEATURES
Forensic Tools
Playbooks
Actionable Intelligence

Sample Deployment Architecture



Reformo
NETWORKS

Thank You - kiitos

reformo.fi