Cyber Security for Railways

Protecting the communications network

EBC Workshop, February 2023

Nokia Solutions & Networks G.K.

The cybersecurity world is changing

Security operations teams are drowning from a deluge of data

Technology shift

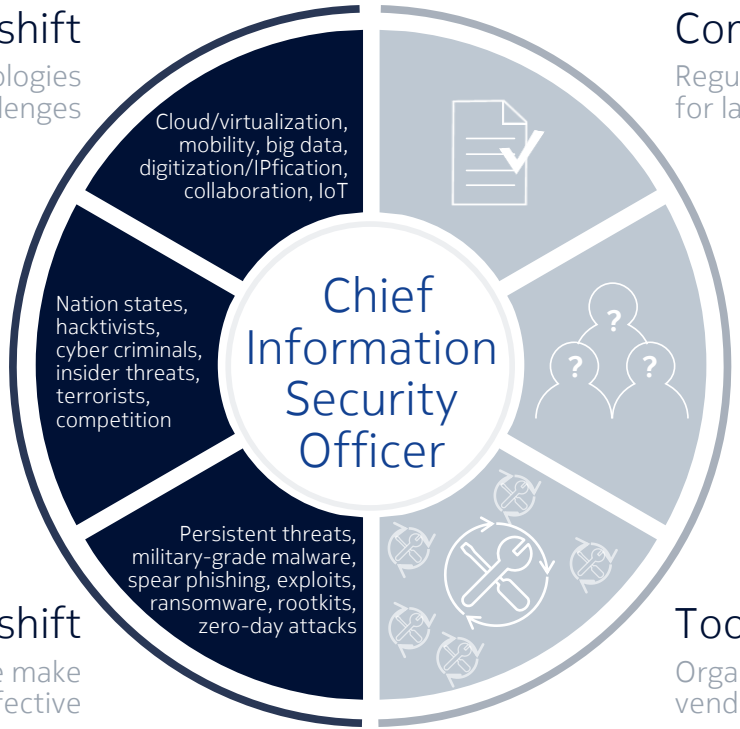
Adoption of new technologies introduces new security challenges

Attacker shift

Cyber criminals are better organized and financially motivated

Threat shift

Major deterioration in threat landscape make traditional security measures ineffective



Compliance mandates

Regulatory fines can cost billions for large global companies

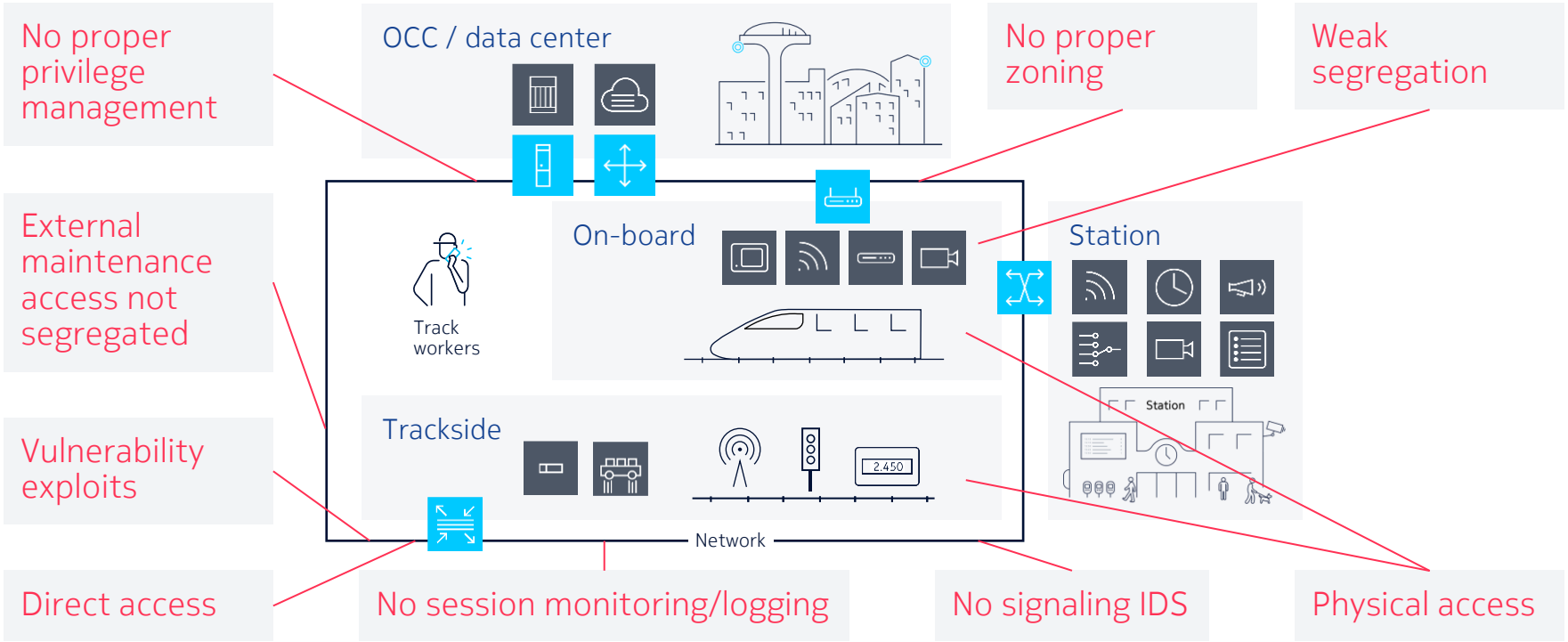
Skills shortage

1.8 million unfulfilled cybersecurity positions in 2022

Too many tools

Organizations are using many vendors with different tools

Cybersecurity threats for critical railway infrastructure



Protecting the railway network with security automation

What is required?

1

Secure architecture & processes

Secure by design principles

Compliance mandates

Defense in depth

Zero trust

Adaptive security architecture

2

Security configuration management

Integrity & visibility of configuration parameters

Prevention of configuration manipulations

3

Vulnerability management service

Faster vulnerabilities triaging and prioritization

Automation operations and dashboards

4

Identity & access management

Increase in number & type of accesses

Full visibility on privileged identities and actions

5

Real-time threat detection & response

Managed detection & response (SOAR)

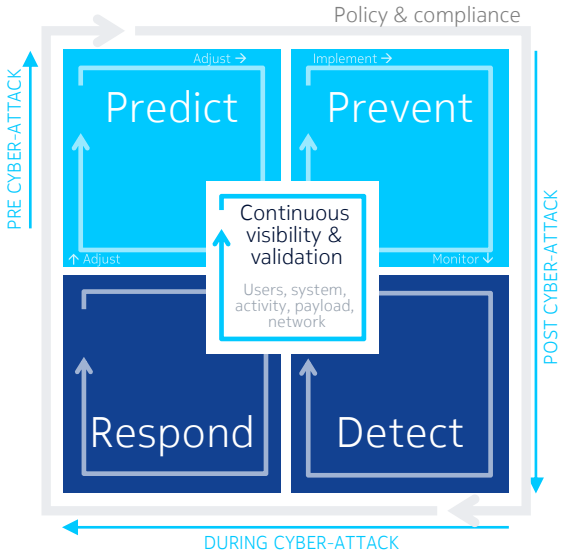
XDR/MDR enabled

Integrated and automated approach

Secure architecture & processes

Network and data protection & secure operations

- Risk-prioritized exposure assessment
- Anticipate threats/ attacks
- Baseline systems and security posture



- Harden systems
- Isolate systems
- Understand your own vulnerabilities
- Prevent attacks

- Remediate
- Design/ model policy change
- Investigation & forensic analysis

- Detect incidents
- Prioritize risk
- Contain incidents

Defining different and complementary security tools/solutions in layers

Each part of the network is protected independent of the other parts

A zero-trust architecture uses identity and context to manage trust decisions

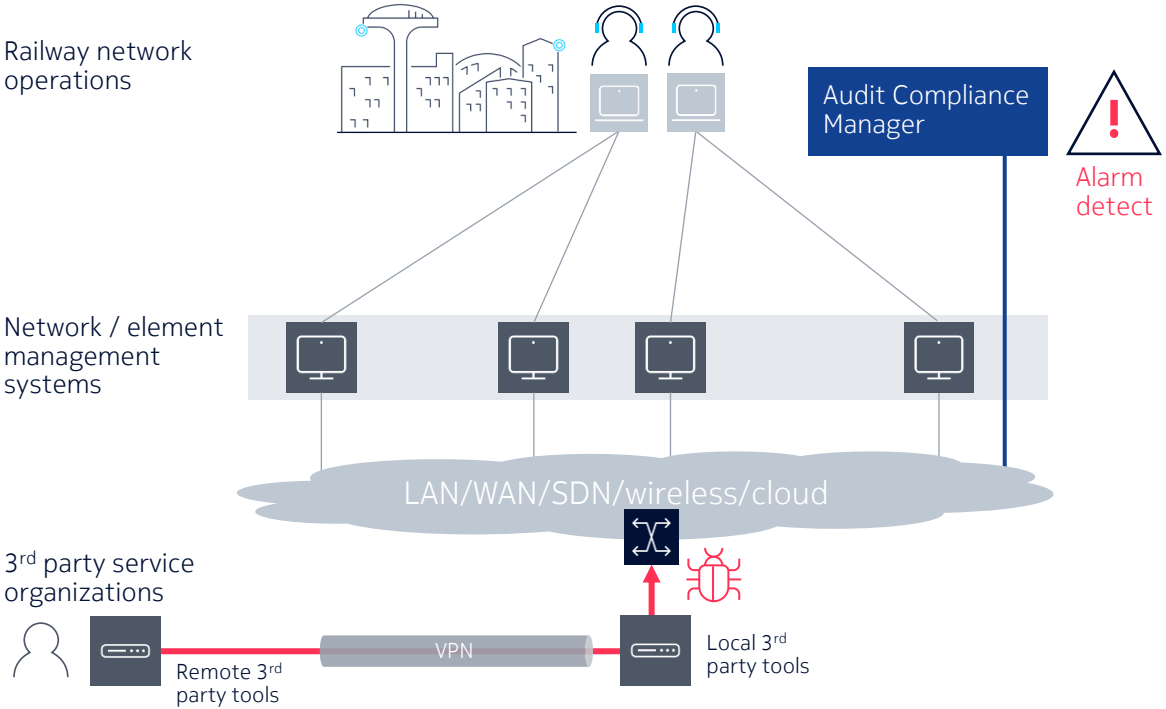
Defense in depth network access control and data protection

Adaptive security model

NOKIA

Security configuration management

Configuration control with Audit Compliance Manager



Compares configuration parameters against industry standards: CIS, ISO 27001, NERC CIP…

Automated audits and optional reconciliation: Security hardening, change management, compliance

Pre-integrated with Nokia 4G/5G core and radio

Multivendor support

NOKIA

Vulnerability management service

Faster vulnerabilities triaging and prioritization

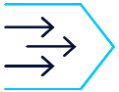
Manage & operate

Fully automated operations for vulnerability assessment, mitigation and remediation

Advanced vulnerability assessment (e.g., VAMS) and design of telecom-specific mitigations for vulnerabilities (w/o fixes)

Monitor & automate

Fully automated dashboards for the monitoring of organization's vulnerability and security posture



Design, build & deploy

Coverage: 2G-4G infra (OSs), 5G NFs, cloud and containerized infra vulnerabilities, OT

E2e VM lifecycle design with Nokia and/or 3rd party tools (SOAR, trouble ticketing, VA scanners, assets inventory, etc.)

Risk mitigation specific to telecom and OT

Pool of security & telecom SMEs

Automation operations and dashboards

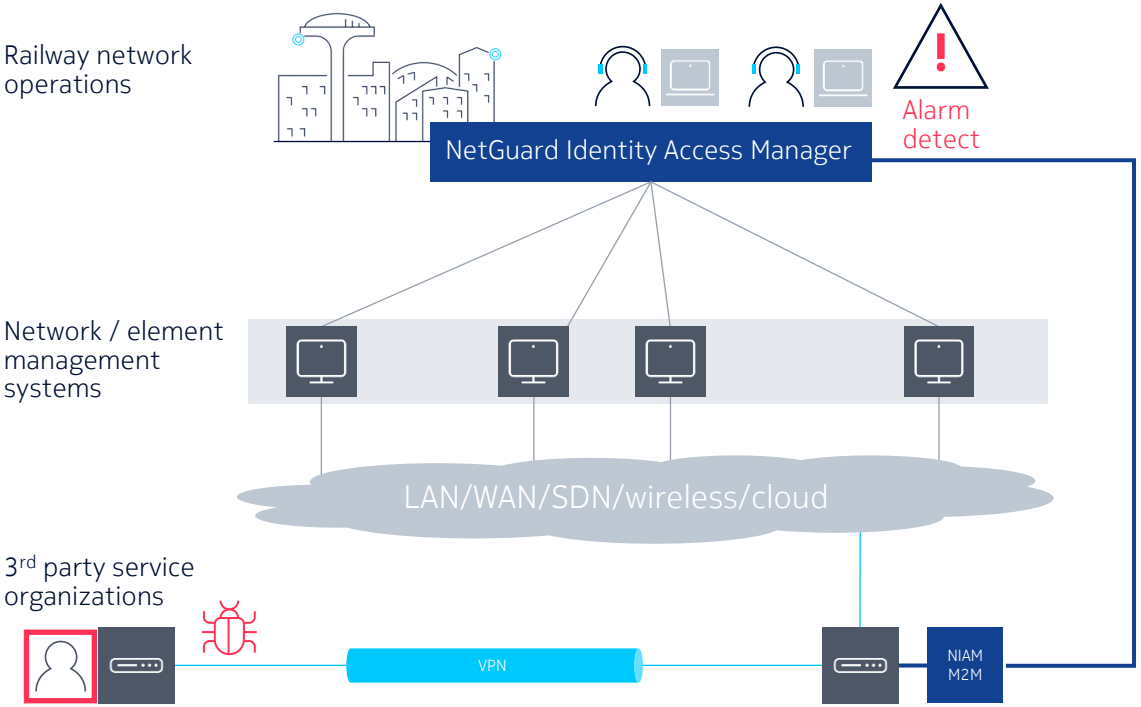
Global SIOCs (8x5 or 24x7) in India and Romania

Delivery model supports remote, on-site & hybrid

NOKIA

Identity & access management

Zero trust



- Centralized security for engineers, suppliers, machines
- Centralized credentials for all NMSs and vendors
- No shared accounts
- Automated password rotation
- Centralized and full audit-trail (CLI, video)
- Regulatory compliance

Real-time threat detection & response

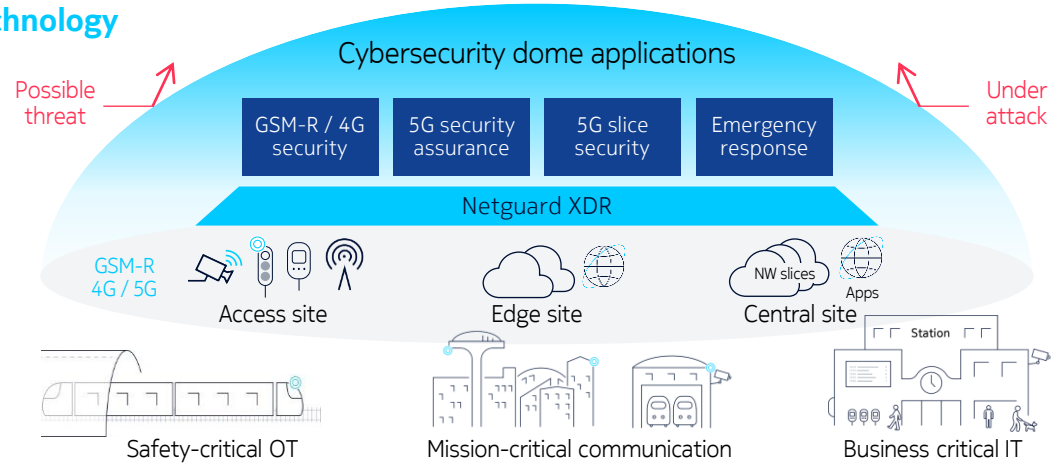
Security Orchestration Automation & Response (SOAR)

Services

Managed detection → | ← Managed response →

Use case and cyber playbook	Threat intelligence (TI)	Threat hunting	Security monitoring	Security incident mgmt.	Rapid response service	Investigation and digital forensics

Technology

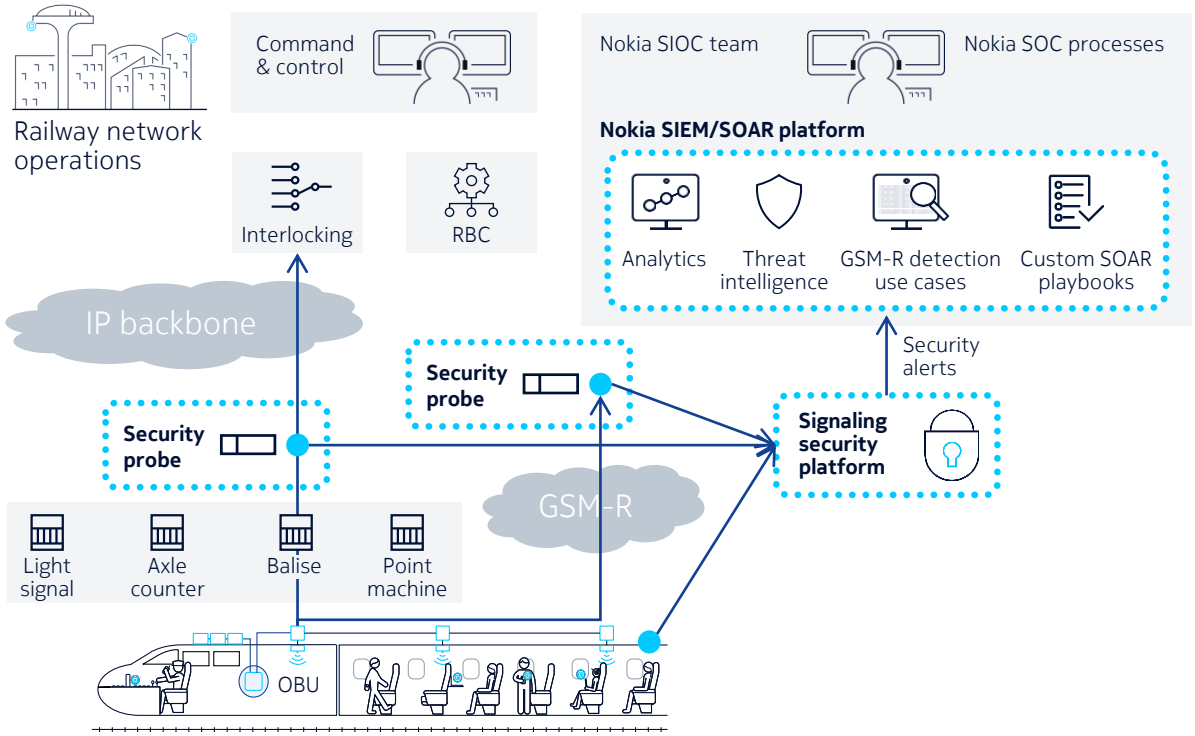


- 24x7 security monitoring of GSM-R and metro assets
- Real-time threat detection and mitigation
- Emergency response - automated business continuity for cybersecurity emergencies
- 5G security assurance - incident management and response capabilities
- Slice security - differentiated services depending on the slice/business

NOKIA

Real-time threat detection & response

Use case: Railway signaling security



24x7 security monitoring of
- GSM-R
- Trackside environment
- Onboard

Real-time threat detection and mitigation

Standard compliancy (IEC 62443)

Automatic & semi-automatic response

NOKIA

E2E security governance
What is required?

Security consulting

Security Assessment
Privacy & Security Risk Assessment

4G/5G Security Transformation
Security Compliance and Assurance Service

Security Operations
Workflow automation consulting,
Use-case definition

Security products

NetGuard Certificate Manager

NetGuard Certificate Lifecycle Manager

NetGuard End-point Security

Identity Access Manager

Audit Compliance Manager

Security Management Center/ CyberDome

7750 SecGW

Virtual Security Router

Deepfield

Nokia AAA

3rd party security controls

Managed Security Services

Managed Detection & Response
SIEM&SOAR operations, UC, workflows

Security Governance Risk & Compliance
Vulnerability management, MBSS

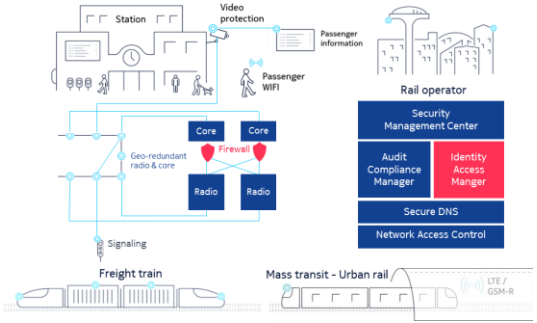
Security Infrastructure Management
Packet core firewall operations

White Label Security Services
B2B2B – SPaaP, SD-WAN, Security via slices

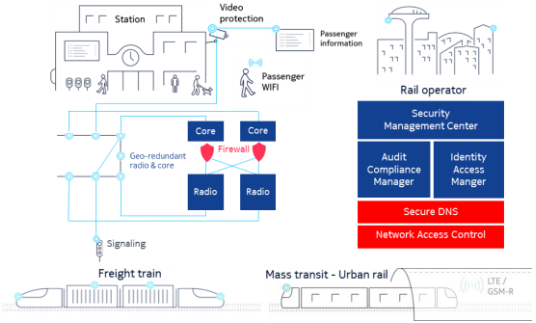
Security deployments

Increase emphasis on privacy, security and trust

Railway operators in Europe



Metro and railway operators in Europe/MEA/APJ



Nokia selected for U.S. Federal 5G Cybersecurity Project

NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Key takeaways

Security by design for any new deployment and to improve existing ones

Continuous Security monitoring to guarantee regulation compliancy

Recurring Risk assessment with any development/ change

Continuous vulnerability management and vulnerability treatment

Nokia and Railway operator tight collaboration to enforce OT and IT Security

NOKIA