Automated security operations for railways

NetGuard Adaptive Security Operations: the Nokia SOAR suite

Application note

Abstract

Railway telecommunications and transmission assets serving critical infrastructure for railways and other mass transit organizations require a new set of capabilities, tools and procedures for efficient security prevention, analysis and resolution processes.

Considering the current threats in cybersecurity, this application note describes Nokia’s carrier grade and vendor independent security, orchestration, analytics and response (SOAR) suite. It allows rail operators to significantly improve operational efficiency with respect to real time monitoring and mitigation, central access management and configuration audits.

Contents

The security world is changing

The consequences of a successful major cyber-attack on a nation's rail infrastructure could be catastrophic. A metro transport system brought to a standstill for even a short period would cause city-wide havoc, damaging the local economy, harming the metro operator's bottom line, and making passengers doubtful about the future safety and reliability of transport services. Worse, a successful attack on a communications-based train control system could cause an accident, putting lives at risk.

Nobody in the industry wants any of that to happen. Yet, based on Nokia's experience, the risks of cyber-attacks occurring are often underestimated by rail operators. Unfortunately, some attacks have succeeded in the past, resulting in serious consequences in several countries.

Digital transformation in railway operations has ushered in new applications to monitor and control rail systems. These applications are typically based on IP technologies, generating a wide range of IP traffic flowing across the communications network. Examples of how digitization is being deployed more widely include train control, control of signaling, maintenance monitoring, video protection and passenger information systems.

As the cyberattack surface has grown, many of the technologies used to address it have contributed to the complexity of security management, often creating segmented data that requires an excess of time and resources to unify. Many conventional security management solutions only provide limited insight into the networks' actual security posture, failing to show the big picture, and react only to threats already present.

Threat and vulnerability data provide some of the underpinnings for answering the security state of your network but lack the scope and business relevance to put the data in context. Incident response technologies, such as traditional security information and event management systems (SIEM), are powerful for displaying current security events, but can overwhelm users with excess information while failing to provide context to the actual state of security. As a result, security teams are left with manually aggregating data from various sources to get a glance at the overall security state.

The ability of traditional security management system to detect and investigate unknown threats and exfiltration alone are insufficient. There is an important distinction between an intrusion (when unauthorized entities gain access to the network) and exfiltration (when a data breach occurs). Traditional systems such as SIEMs typically do not provide the contextual analytics necessary to identify potential threats, which may indicate exfiltration, nor are they able to determine post-incident what data may have been exfiltrated or which systems were compromised. They are typically deployed to look at the perimeter of the network. Outsiders that have already infiltrated the network, whether by stealing hardware or taking over an insider's account, can roam freely in a perimeter-centric security system. Malicious insiders pose a significant risk as well, as they are already inside the network.

As a result, there is a growing trend to implement cognitive security analytics systems as an enrichment to traditional existing SIEM solutions for advanced and context-aware detection and response provisioning. Security management enrichment with cognitive security software helps security teams achieve key strategic objectives including improving operational costs, regulatory compliance, and enabling and protecting new technology introductions.

Security teams need a better way to not only gather the supporting information about the security state from a wider range of sources, but also to automate security processes. Security operations, analytics and response (SOAR) can automate response workflow to gather and analyze security data from various sources and to make them available and consumable by different stakeholders. A platform that uses intelligent analytics and machine learning would continuously evaluate the risk posture and the state of the environment to enable informed decision making, and formalize and automate responsive actions in real time. Such cognitive analytical and automated technologies measure rather than monitor to provide formalized workflows and enable informed remediation prioritization.

To keep pace with the rapid rise in attacks, railway operators should consider shifting from legacy reactive security infrastructures (detection and response) to a proactive automated security strategy. Key capabilities to protect networks must include:

- Security analytics that encompasses business processes, incident response plans, regulations and policies
- End-to-end security that encompasses the operation of the network and its processes
- Security analytics to correlate security-related information from across the network, devices and cloud layers to spot suspicious anomalies and provide insight into threats
- Multi-layer encryption to protect network traffic.

Such a multi-layered and active security approach provides the right balance of costs with the in-depth protection needed to defend against today's security threats, while ensuring that railway operators are prepared to meet their compliance obligations.

Nokia's response to increasing cybersecurity threats

Railway telecommunications and transmission assets serving critical infrastructure, such as railways and other mass transit organizations, require a new set of capabilities, tools and procedures for more efficient security prevention, analysis and resolution processes.

Considering the current threats in cybersecurity, this paper describes Nokia's carrier grade and vendor independent SOAR suite. It allows rail operators to significantly improve operational efficiency with respect to real-time monitoring and mitigation, central access management and configuration audits.

Implementing a SOAR suite results in the following cybersecurity benefits:

- Measure security compliance in real time
- Automate network-wide configuration compliance for incorrect, outdated, and vulnerability-introducing errors
- Manage, control, analyze and audit user activity
- Identify threats and mitigate rapidly using machine learning algorithms and analytics mechanisms
- Empower security teams with reports across endpoints, servers and networks to detect insider threats.

The above can be covered by the Nokia NetGuard Adaptive Security Operations suite.

Security orchestration, analytics and response (SOAR)

Many standards relating to security are available, such as IEC 62443(-2-4), ISO 2700x. There is also a wealth of best practices from mission-critical networks around the world, most of which advocate an active and adaptive security management approach with automation and continuous improvement.

The traditional approach to security is largely based on manual and often reactive processes without a centralized management system. This is still a reasonable approach for some organizations, but the increasing sophistication of attacks and growing regulatory complexity mean this will not be realistic in the medium term. An expanded security management solution would support workflow management and automation, analytics and reporting. This would enable security operations teams to automate and prioritize activities and report data to inform better business decision making.

General targets

- Operation of the railway mission-critical infrastructure with a highly available, scalable and extendable active security solution
- Support daily operations with a SOAR platform with network element integration
- Seamless integration with a railway operator's existing infrastructure from an interface — e.g., existing SIEM systems, OSS (operational support system), LDAP (lightweight directory access protocol), ticketing, storage and virtual resources perspective.

Monitoring and mitigation

- A customizable dashboard with powerful search and reporting capabilities optimized for the individual needs of the technical experts and management
- Advanced analytics capabilities for precise security risk and root cause identification ensuring real-time alerts with reduced lead time for the execution of target mitigations
- Pre-defined and automated mitigation workflows selected and recommended for occurring incidents to relieve security experts and accelerate mitigations.

Access management

- Improved security standards, unified access security policies across the network infrastructure, and increased network uptime through enhanced accountability to users
- Implementation of comprehensive video/text logging and integration within the security management center to ensure a high compliance to key security specifications such as auditing capabilities
- OPEX savings using automated management workflows as well as password rotations with a centralized access management for the whole eco-system
- Elimination of account and password sharing
- Clearly defined access rights to groups of employees
- No direct access to tools' and equipment's login credentials.

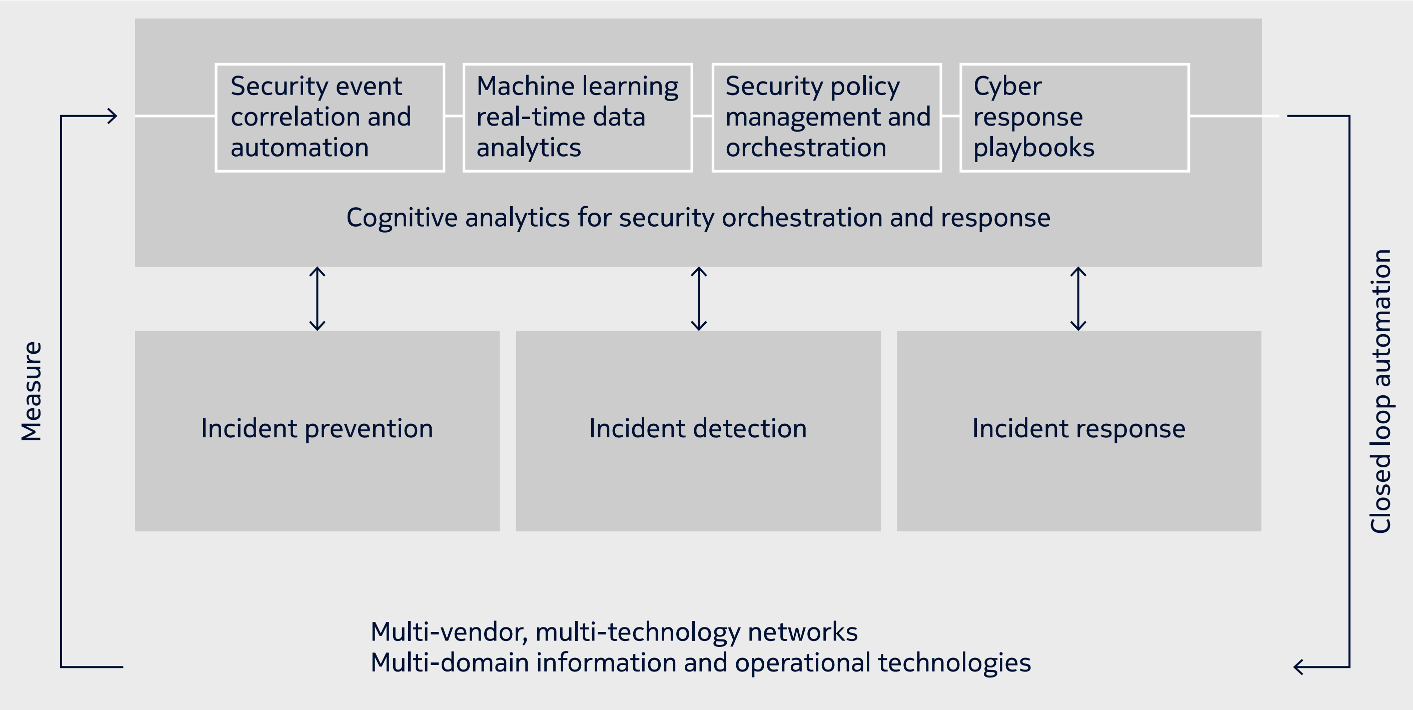
Configuration audits

- Fully automated error identification of attribute values, eliminating time consuming manual processes/scripts, which is also useful for troubleshooting support
- Misconfigurations eliminated, thus assuring network configuration compliance, detect configuration caused vulnerabilities, improve quality, and reduce service outages or degradation
- Continuous monitoring of network hardening configuration to ensure that no security loop-holes are inadvertently introduced
- Review audits before/after an upgrade to ensure that changes have been made correctly and advise engineers of potential service-affecting impact before equipment goes live.

Nokia NetGuard Adaptive Security Operations suite

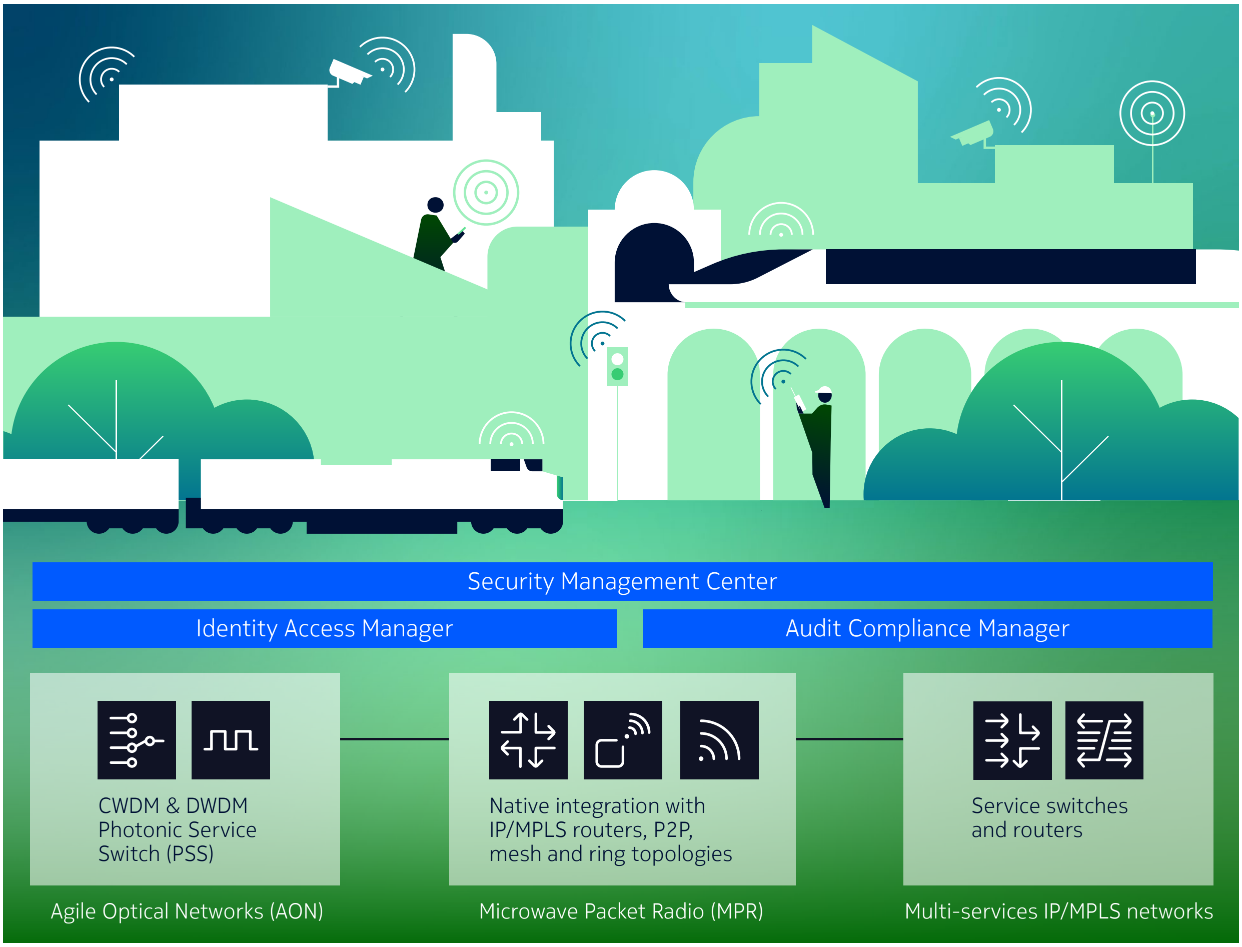
Nokia's NetGuard Adaptive Security Operations suite provides a contextual view of security posture across the complex, heterogeneous, and diverse operational environments railway operators face. It spans physical, virtual, software-defined and traditional networks and seamlessly extends between operational and information technology. It delivers reporting capabilities and real-time monitoring to provide contextual security issues alerts that help to reduce attack surface and time. By using these automations, it enables security operation teams to become more effective.

Benefits of NetGuard Adaptive Security Operations suite

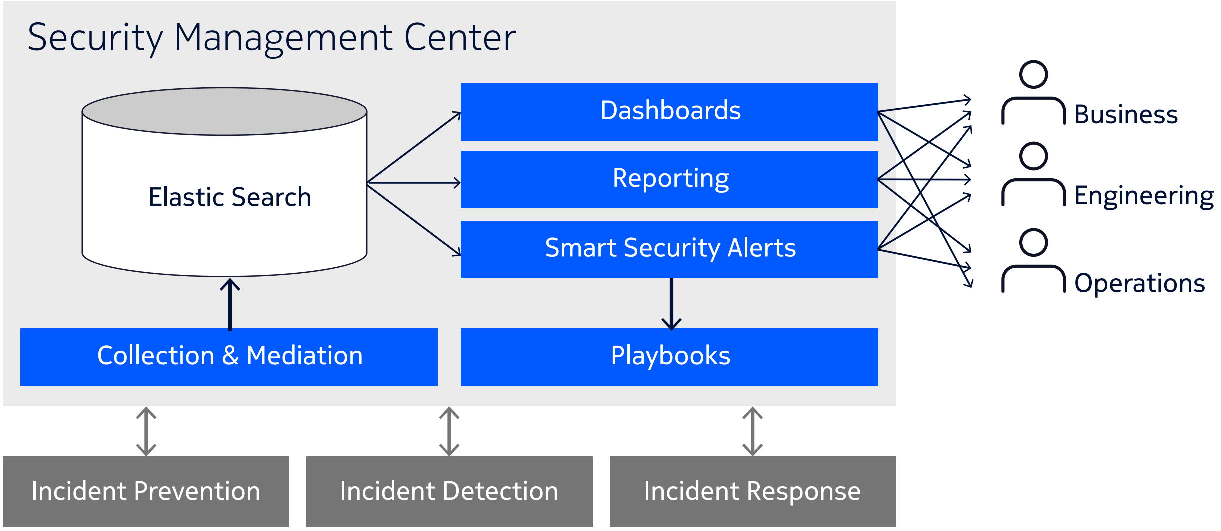

Security event correlation and automation
Machine learning real-time data analytics
Security policy management and orchestration
Cyber response playbooks
Cognitive analytics for security orchestration and response
Incident prevention
Incident detection
Incident response
Measure
Closed loop automation
Multi-vendor, multi-technology networks
Multi-domain information and operational technologies

- Security management with **end-to-end visibility** spanning device, network, and cloud layers
- Ability to collect, correlate, and analyze data from multiple operational silos
- **Identify anomalous behaviors** that indicate compromise by using threat intelligence information across network, device, and cloud layers using analytics and machine learning
- Appropriate automated rapid response based on contextual knowledge about the IoT service and business value
- Ability to scale to meet the increasing challenges IoT creates while creating new value-added monetization opportunities using **automation** technologies
- Agile and adaptive defense response using security operations workflow automation and orchestration (automation is the process of executing repeatable actions without human intervention, while orchestration is the concept of chaining these automated tasks into executed playbooks to perform workflows to **accelerate both investigation and mitigation**).

Nokia can provide NetGuard Adaptive Security Operations suite consisting of the following modules:


Security Management Center
Identity Access Manager
Audit Compliance Manager
CWDM & DWDM Photonic Service Switch (PSS)
Native integration with IP/MPLS routers, P2P, mesh and ring topologies
Service switches and routers
Agile Optical Networks (AON)
Microwave Packet Radio (MPR)
Multi-services IP/MPLS networks

NetGuard Security Management Center (NSMC)



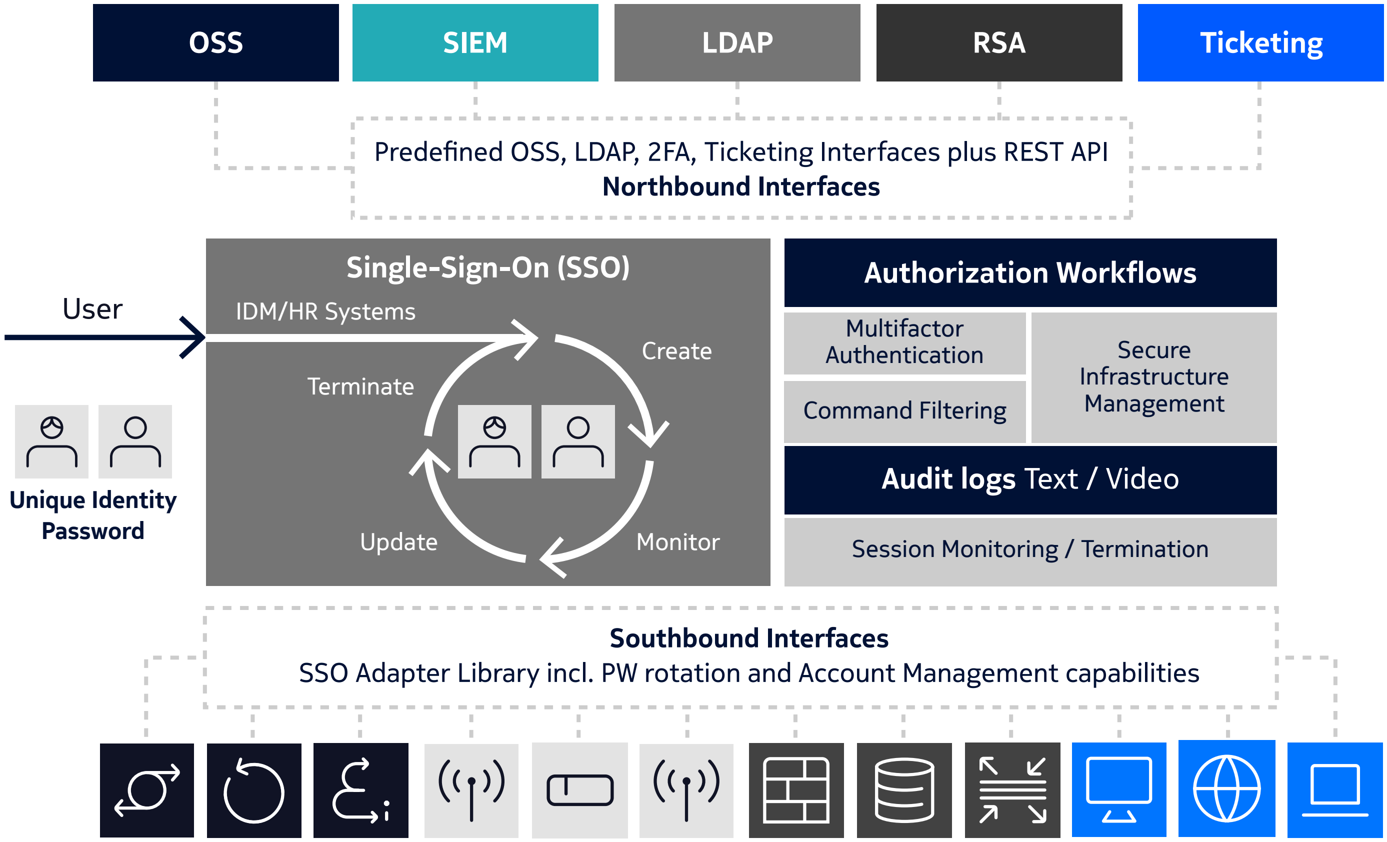
The key to high-performance and secure infrastructure operations lies in state-of-the-art, highly available and protected technologies. The systems environment has grown heterogeneously and demands a centralized Security Orchestration Engine with clear traceability.

Nokia Security Management Center (NSMC) provides a contextual view of security posture across the infrastructure and delivers reporting capabilities and real-time monitoring, which enables security operation teams to become more effective and keep pace with the dynamically changing, digitalized environment.

- Ability to interact (collect/trigger) with multiple, vendor-independent technologies
- Analytics and machine learning offer complex correlations and detection capabilities based on pre-integrated and project specific use cases
- Customizable dashboards guarantee an effective presentation of key information
- Automated workflows allow the acceleration of the investigation and mitigation.

NetGuard Identity Access Manager (NIAM)

NetGuard Identity Access Manager (NIAM) centralizes security policy administration via a single application that seamlessly integrates into existing corporate identity management systems. It enforces robust and consistent security policies with automated network-wide security measures such as password aging and complex password requirements.

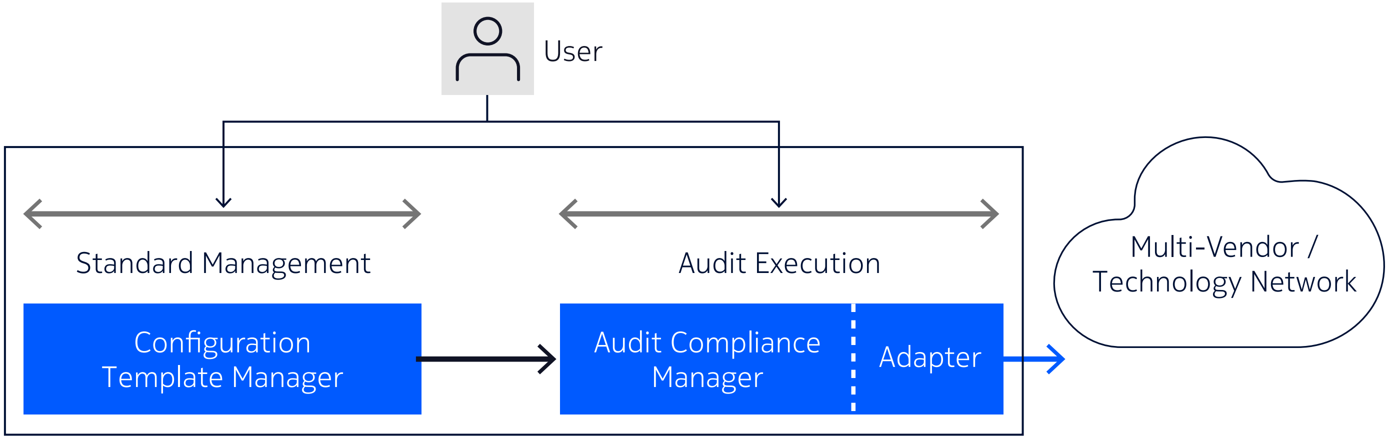

OSS
SIEM
LDAP
RSA
Ticketing
Predefined OSS, LDAP, 2FA, Ticketing Interfaces plus REST API
Northbound Interfaces
User
Unique Identity Password
Single-Sign-On (SSO)
IDM/HR Systems
Create
Terminate
Update
Monitor
Authorization Workflows
Multifactor Authentication
Command Filtering
Secure Infrastructure Management
Audit logs Text / Video
Session Monitoring / Termination
Southbound Interfaces
SSO Adapter Library incl. PW rotation and Account Management capabilities

Security privileges may be customized at the individual user level, assigned to a group or handled through automated processes using a flexible rules engine.

- Central management of user access and password policies providing single sign-on and separation of users from end systems
- Protection of network elements and EMS-related credentials (Enterprise Mobile Security from Microsoft)
- Logging of all user activities for text and video sessions
- Implementation of automated password rotation in line with the customer best practices.

NetGuard Audit Compliance Manager (NACM)

Nokia NetGuard Audit Compliance Manager (NACM) automates audit and analysis of parameters in physical and virtual networks. NACM extracts parameter settings from physical and virtual network functions and performs data integrity analysis by comparing results to gold-standards.



NACM analytics identify mismatches to help prevent service degradations and process inefficiencies.

- Eliminate service parameter misconfigurations, reduce outages or degradations
- Improve service assurance and troubleshooting processes by 60 percent
- Ensure continuous compliance to network hardening configuration
- Automate business processes, improve operational efficiencies.

The modular architecture of the NetGuard Adaptive Security Operations suite allows customizing the deployment of SW/HW and services to the railway's individual needs.

Conclusion

The recent increase in sophisticated, targeted security threats by both insiders and external attackers has increased the awareness and urgency of communications service providers, mission-critical network operators and utility and infrastructure enterprises for implementing comprehensive security strategies.

The ability of traditional security management system to detect and investigate unknown threats and exfiltration alone are insufficient. They are typically deployed to look at the perimeter of the network. Whereas outsiders that have already infiltrated the network and malicious insiders pose a significant risk as well, as they are already inside the network.

As a result, there is a growing trend to implement cognitive security analytics systems as an enrichment to traditional existing SIEM solutions for advanced and context-aware detection and response provisioning. Security management enrichment with cognitive security software helps security teams achieve key strategic objectives including improving operational costs, regulatory compliance, and enabling and protecting new technology introductions.

The NetGuard Adaptive Security Operations suite is a progressive, active and automated security management solution that seamlessly delivers a holistic view of security posture, vulnerabilities, threats and breaches using advanced threat analytics.

Deploying the right level of security is a high priority. While all mission-critical networks are different, sound security typically requires a move from manual processes to automation, the application of data analytics and machine learning, end-to-end encryption and a full lifecycle evaluation of cyber-security risks.

Nokia offers an advanced and comprehensive approach built on its long experience and in-depth expertise in both security and mission-critical network design and operations. In line with best practices and published standards, the Nokia solution can provide the highest levels of protection for railway communications.

About Nokia

At Nokia, we create technology that helps the world act together.

As a B2B technology innovation leader, we are pioneering networks that sense, think and act by leveraging our work across mobile, fixed and cloud networks. In addition, we create value with intellectual property and long-term research, led by the award-winning Nokia Bell Labs.

Service providers, enterprises and partners worldwide trust Nokia to deliver secure, reliable and sustainable networks today – and work with us to create the digital services and applications of the future.

Nokia is a registered trademark of Nokia Corporation. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.

© 2023 Nokia

Nokia OYJ
Karakaari 7
02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Document code: (June) CID207041