

Mission Critical security overview

NOKIA Security Strategy overview

Faris Al-Katib

April 2019

- 
- A nighttime aerial view of a city, likely Toronto, featuring the CN Tower prominently in the background. The city lights are visible, and a river flows through the foreground. The image is overlaid with a semi-transparent blue rectangle containing a list of bullet points.
- Security challenges in critical networks
 - NOKIA security strategy
 - Key solution highlights
 - Evolution of security strategy

- 
- A nighttime aerial view of a city, likely Toronto, featuring the CN Tower prominently in the background. The city lights are visible, and a river flows through the foreground. The image is overlaid with a semi-transparent blue rectangle containing a list of bullet points.
- Security challenges in critical networks
 - NOKIA security strategy
 - Key solution highlights
 - Evolution of security strategy

Security Challenges in Critical Networks



Who are we up against?

Daily Business

CRIMINAL

Hacking has become a big business - Target the digital assets that can be sold

- Personal information
- Credit/debit card information
- Intellectual property

Only few but critical Incidents

MALICE

Technical ability and motive combine, those with ill-feelings towards an organization

- A disgruntled employee
- Untargeted malicious code
- Random selection
- Proof of ability

TERRORIST

Hacking of critical infrastructure represents an appealing option for terrorist

- Disruption to infrastructure
- Economic consequences
- Damage to property
- Loss of life

STATE

Most sophisticated and technically capable threat

- Offensive capability
- The acquisition of trade secrets and other intellectual property
- Espionage

What are the potential consequences?

DATA THEFT

EXTORTION

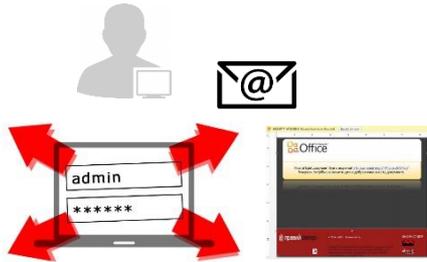
OPERATIONS/SERVICES DELAY

DAMAGE TO FREIGHT/PHYSICAL SYSTEMS

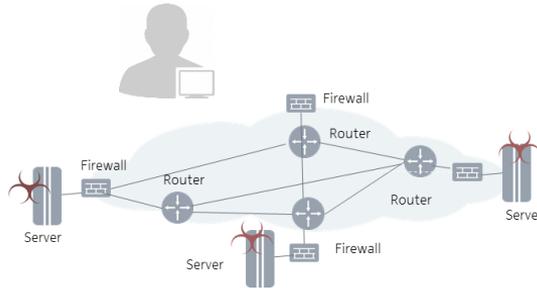
PASSENGER INJURY/LOSS

Example complex security threat

Anatomy of an Advanced Persistent Threat (APT)



1. Spear-Phishing targeting employees.
2. Employee opens email and malicious attachment, infecting endpoints.
3. Attackers collect data and steal credentials.



4. Using stolen credentials, hackers modify network configurations.
5. Malware bombs implanted on critical servers.



6. Malware is detonated, substations taken offline.
7. Operators are locked out, preventing a response.
8. Servers wipe clean preventing timely recovery.



Cyber Kill Chain

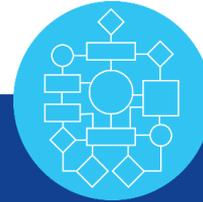
- 
- A nighttime aerial view of a city, likely Toronto, featuring the CN Tower prominently in the background. The city lights are visible, and a river flows through the foreground. The image is overlaid with a semi-transparent blue rectangle containing a list of bullet points.
- Security challenges in critical networks
 - NOKIA security strategy
 - Key solution highlights
 - Evolution of security strategy

NOKIA Security Portfolio Domains



Security Operations

Monitors, controls and orchestrates to perform proactive actions with machine-learning analytics



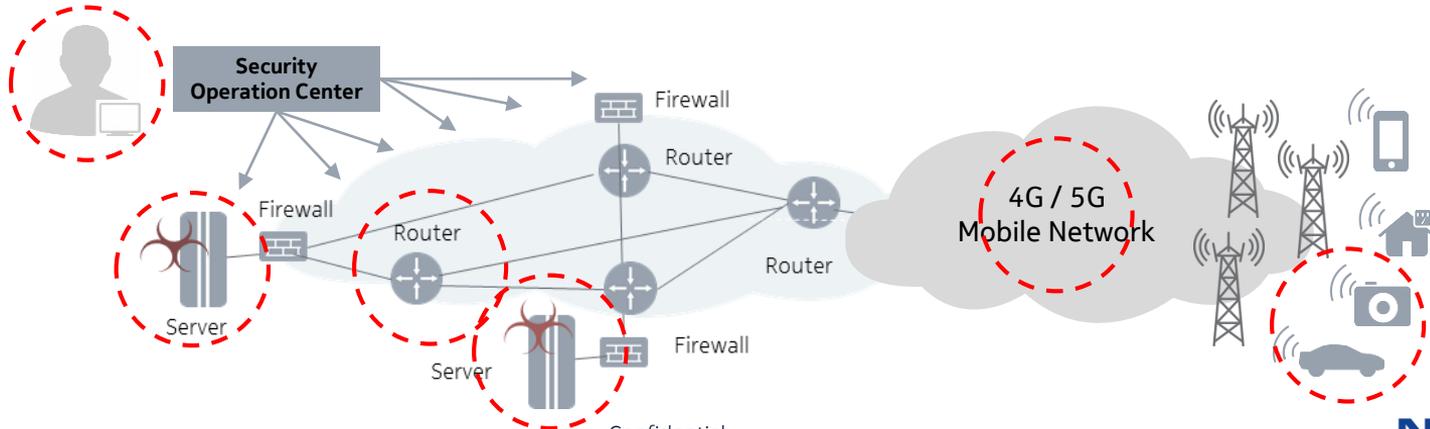
Network Security

Pervasive infrastructure protection against external attacks and malicious intrusion



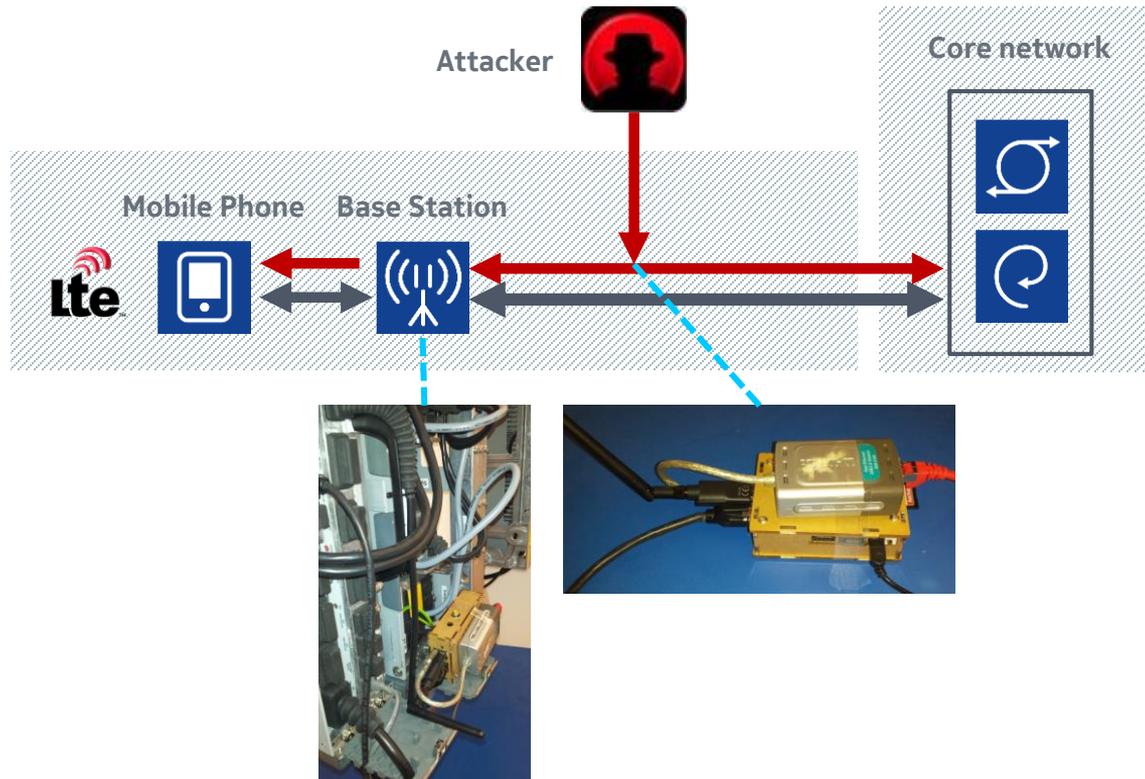
Endpoint Security

Network based malware, botnet and threat detection & digital identity authentication of endpoints



- 
- A nighttime aerial view of a city, likely Toronto, featuring the CN Tower prominently in the background. The city lights are visible, and a river flows through the foreground. The image is overlaid with a semi-transparent blue rectangle containing a list of bullet points.
- Security challenges in critical networks
 - NOKIA security strategy
 - Key solution highlights
 - Evolution of security strategy

NOKIA 4G/5G Public Safety



Threats:

- Eavesdropping on subscriber data and voice
- Injection of malicious traffic (signaling and user plane)
- Unauthorized access to operator network, base station and mobile
- Denial of service attack against core network

Solution:

- 3GPP standardized solution using IPSec
- Not deployed in all mobile operators - Risk vs. investment decision

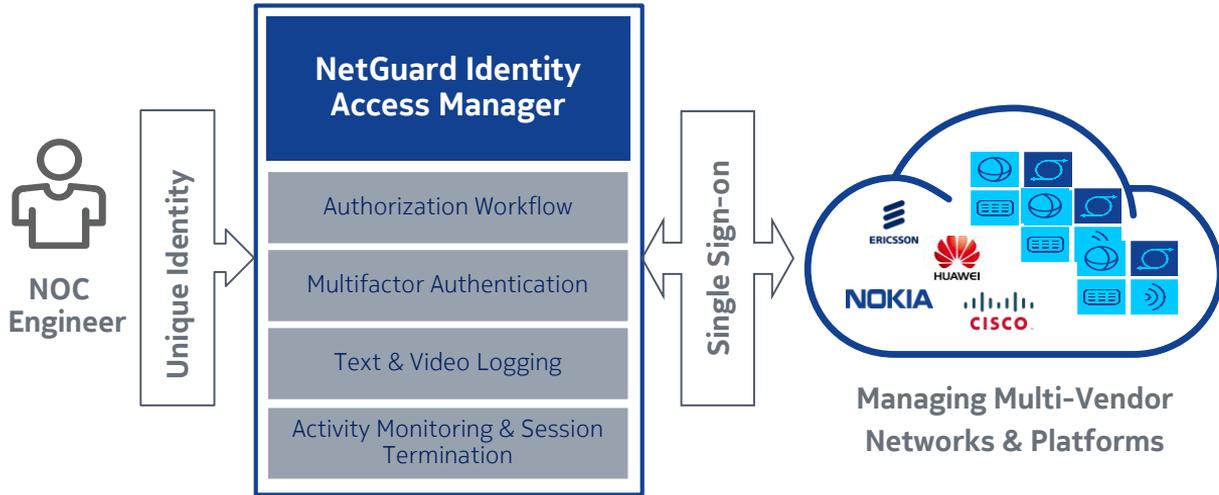
Threat: access control



Access to the network

- How to stop miss handling of credentials?
- How to protect network admins from social engineering?
- How to detect ATP attacks?

NOKIA Identity Access Management System

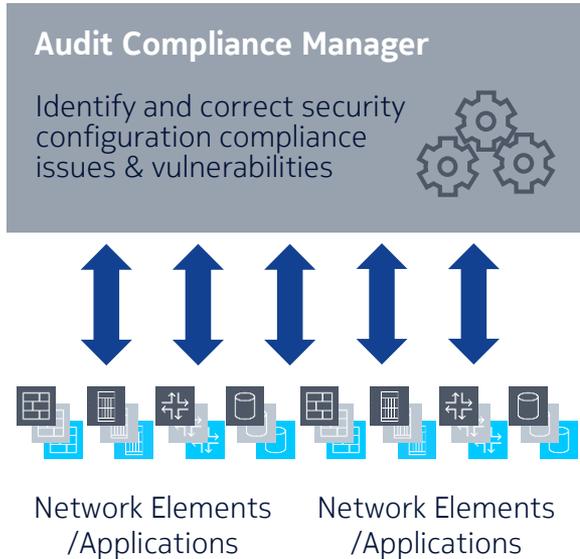


Enhanced network access management for multisite and multivendor network management

Identity access control Mitigation:

- Separate people from credentials.
- Full real time overview of activity on all network elements
- Full audit trail based on identification of individuals not roles
- Detection of any access bypassing the central system

NOKIA Audit Compliance Manager



Threats:

- How to detect anomalies / back doors in configurations?
- How to ensure the integrity of the configuration?
- How to evaluate this in near real time?

Audit Compliance management Mitigation:

- Ensure system configuration integrity
- Provide network wide overview in near real time
- Detect any anomalies on any network element configuration

- 
- A nighttime cityscape featuring a prominent tower with a red and white striped top. The foreground shows a multi-lane highway with long-exposure light trails from cars, including a bright red one. The background includes various city buildings and a river.
- Security Challenges in Critical networks
 - NOKIA security Strategy
 - Key solution highlights
 - Evolution of security strategy

Cyber attack strategy advancement demands a different approach

Cyber criminals are now using automation and artificial intelligence to attack companies and networks more efficiently. They're also exploiting an attack surface that's growing as companies embrace cloud, Internet of Things (IoT) and 5G technologies.

End-to-end security
for digital networks
and operations

Analytics that correlates
data from networks, devices
and cloud to spot anomalies

Automate security for
business processes,
regulations and policies

...to protect assets and interests:

SOAR

Security **O**rchestration **A**nalytics and **R**esponse



NOKIA

Copyright and confidentiality

The contents of this document are proprietary and confidential property of Nokia. This document is provided subject to confidentiality obligations of the applicable agreement(s).

This document is intended for use of Nokia's customers and collaborators only for the purpose for which this document is submitted by Nokia. No part of this document may be reproduced or made available to the public or to any third party in any form or means without the prior written permission of Nokia. This document is to be used by properly trained professional personnel. Any use of the contents in this document is limited strictly to the use(s) specifically created in the applicable agreement(s) under which the document is submitted. The user of this document may voluntarily provide suggestions, comments or other feedback to Nokia in respect of the contents of this document ("Feedback").

Such Feedback may be used in Nokia products and related specifications or other documentation. Accordingly, if the user of this document gives Nokia Feedback on the contents of this document, Nokia may freely use, disclose, reproduce, license, distribute and otherwise commercialize the feedback in any Nokia product, technology, service, specification or other documentation.

Nokia operates a policy of ongoing development. Nokia reserves the right to make changes and improvements to any of the products and/or services described in this document or withdraw this document at any time without prior notice.

The contents of this document are provided "as is". Except as required by applicable law, no warranties of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose,

are made in relation to the accuracy, reliability or contents of this document. NOKIA SHALL NOT BE RESPONSIBLE IN ANY EVENT FOR ERRORS IN THIS DOCUMENT or for any loss of data or income or any special, incidental, consequential, indirect or direct damages howsoever caused, that might arise from the use of this document or any contents of this document.

This document and the product(s) it describes are protected by copyright according to the applicable laws.

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.