NOKIA

Mission Critical security overview

NOKIA Security Strategy overview

Faris Al-Katib

April 2019

- Security challenges in critical networks
- NOKIA security strategy
- Key solution highlights
- Evolution of security strategy

NOKIA

- Security challenges in critical networks
- NOKIA security strategy
- Key solution highlights
- Evolution of security strategy

NOKIA

Security Challenges in Critical Networks

NOKIA

Who are we up against?

Daily Business

Only few but critical Incidents

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

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

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

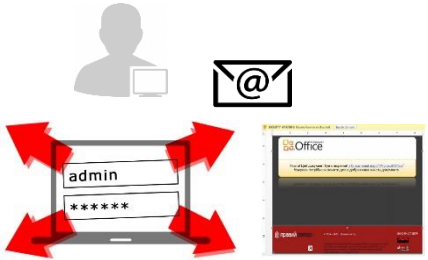
- Offensive capability
- The acquisition of trade secrets and other intellectual property
- Espionage

What are the potential consequences?

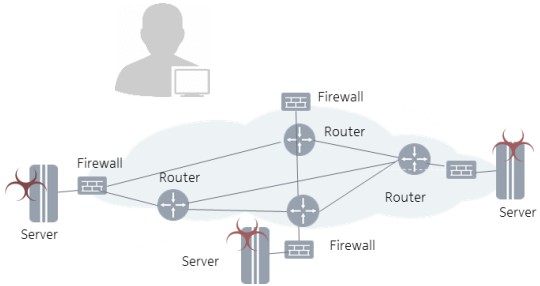
- **DATA** THEFT
- **EXTORTION**
- OPERATIONS/SERVICES **DELAY**
- **DAMAGE** TO FREIGHT/PHYSICAL SYSTEMS
- PASSENGER **INJURY/LOSS**

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.

NOKIA

- Security challenges in critical networks
- NOKIA security strategy
- Key solution highlights
- Evolution of security strategy

NOKIA

NOKIA Security Portfolio Domains

Security Operations

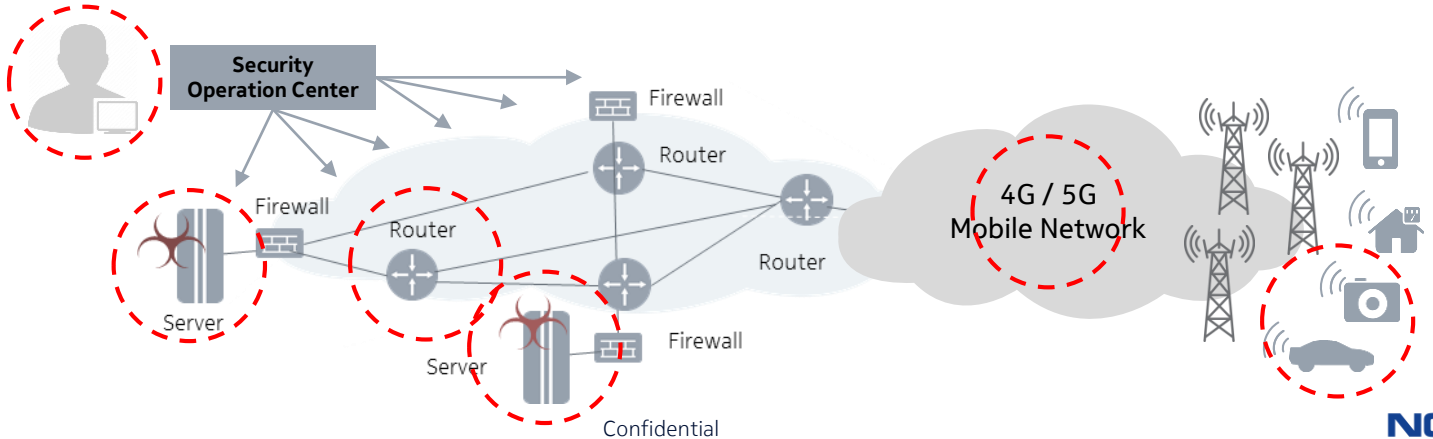
Monitors, controls and orchestrates to perform proactive actions with machine-learning analytics

Network Security

Pervasive infrastructure protection against external attacks and malicious intrusion

Endpoint Security

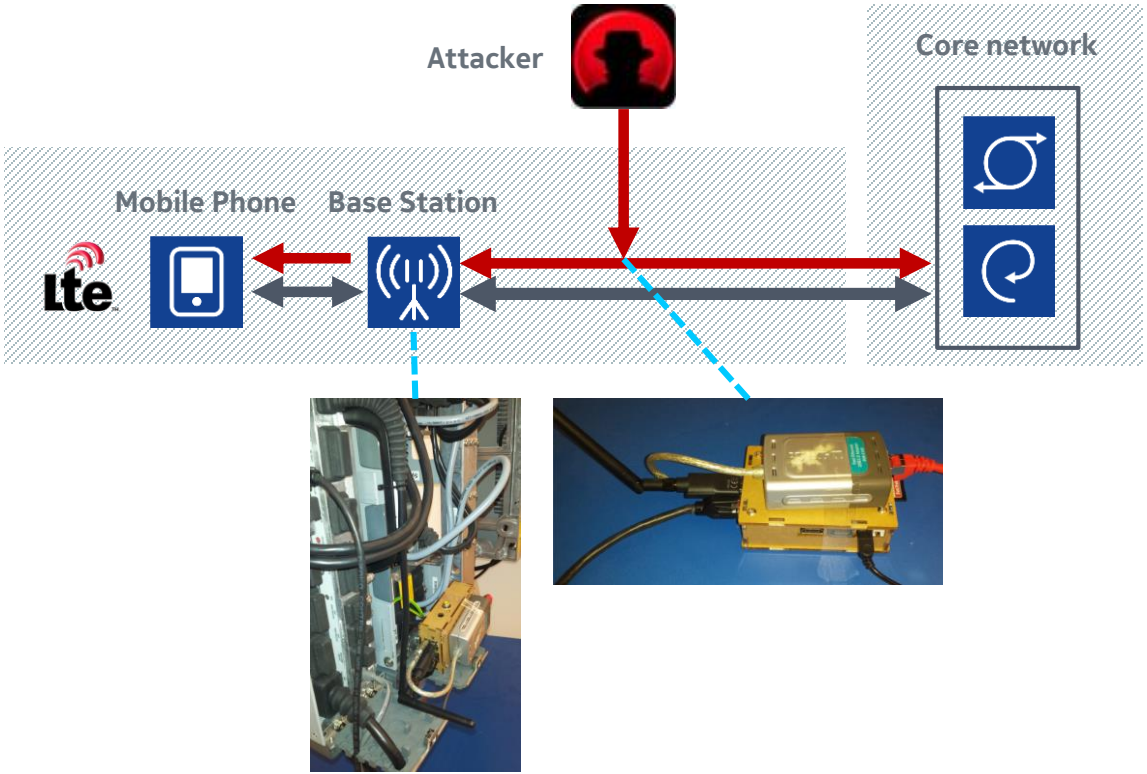
Network based malware, botnet and threat detection & digital identity authentication of endpoints



NOKIA


• Security challenges in critical networks
• NOKIA security strategy
• Key solution highlights
• Evolution of security strategy
NOKIA

NOKIA 4G/5G Public Safety



Threats:

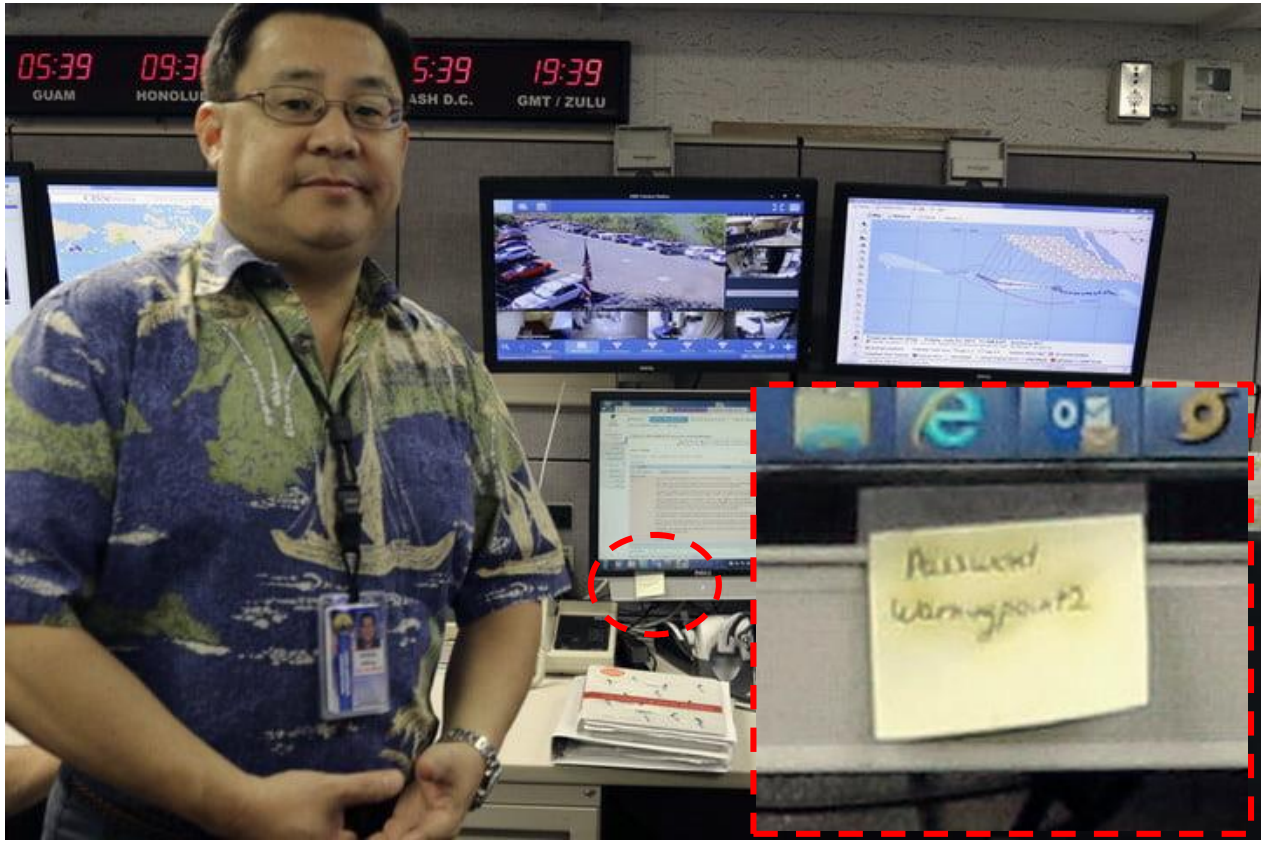
- Eavesdropping on subscriber data and voice
- Injection of malicious traffic (signaling and user plane)
- Unauthorized access to operator network, base station and mobile
- Denial of service attack against core network

Solution:

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

NOKIA

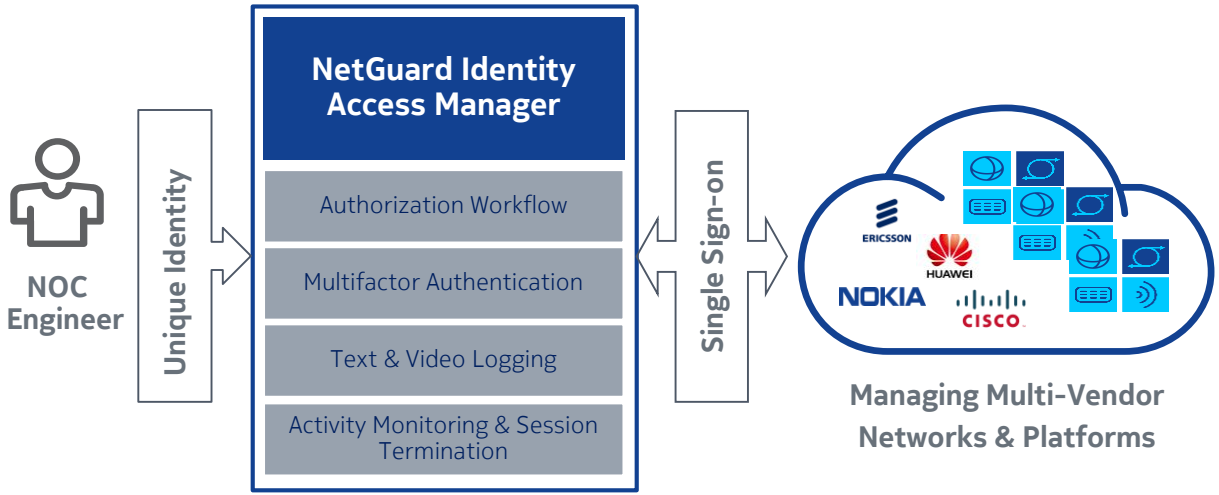
Threat: access control



Access to the network

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

NOKIA Identity Access Management System

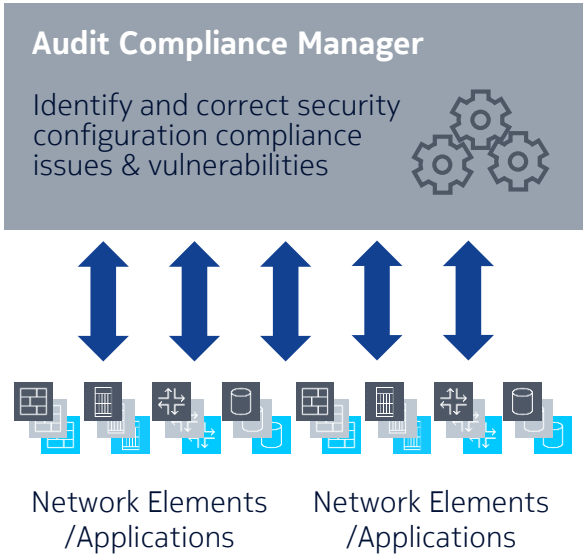


Enhanced network access management for multisite and multivendor network management

Identity access control Mitigation:

- Separate people from credentials.
- Full real time overview of activity on al network elements
- Full audit trail based on identification of individuals not rolls
- 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

- Security Challenges in Critical networks
- NOKIA security Strategy
- Key solution highlights
- Evolution of security strategy

NOKIA

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:

NOKIA

SOAR

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

NOKIA

Copyright and confidentiality

NOKIA