Automating Service Self-Healing and Security Management

Davide Cherubini

Cloud & Automation CoE

ONAP Roadmap

R1 AMSTERDAM
December 2017

R2 BEIJING
June 2018

R3 CASABLANCA
December 2018

R4 DUBLIN
June 2019

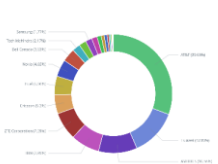
ONAP & Openness

- Modularity
- Flexibility (seamlessly integrate with existing deployment & 3rd party systems)
- Promote adoption of standard interfaces and APIs - **internal and external**
- Avoid proprietary interfaces
- Consistent implementation

Vodafone Contributions to ONAP

ONAP R3
Casablanca
Dec 2018

CCVPN Use Case
cross-technology, cross-domain, cross-operator
E2E Service fulfillment and assurance

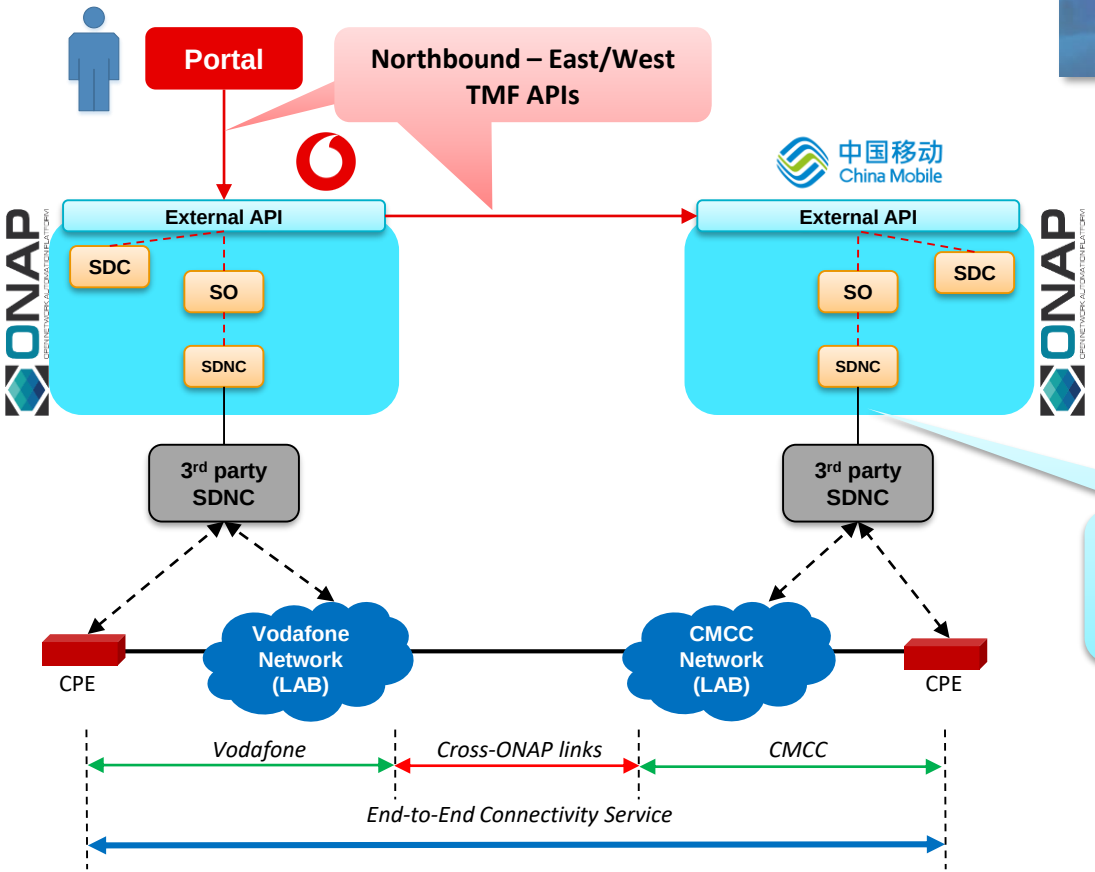


ONAP R4
Dublin
June 2019

CCVPN Extension
5 sub-use cases
(MP2MP, VAS+AI, DR, L0/L1)

VSP Compliance [SDC]
VNF/CNF Certification + Testing

CCVPN Use Case

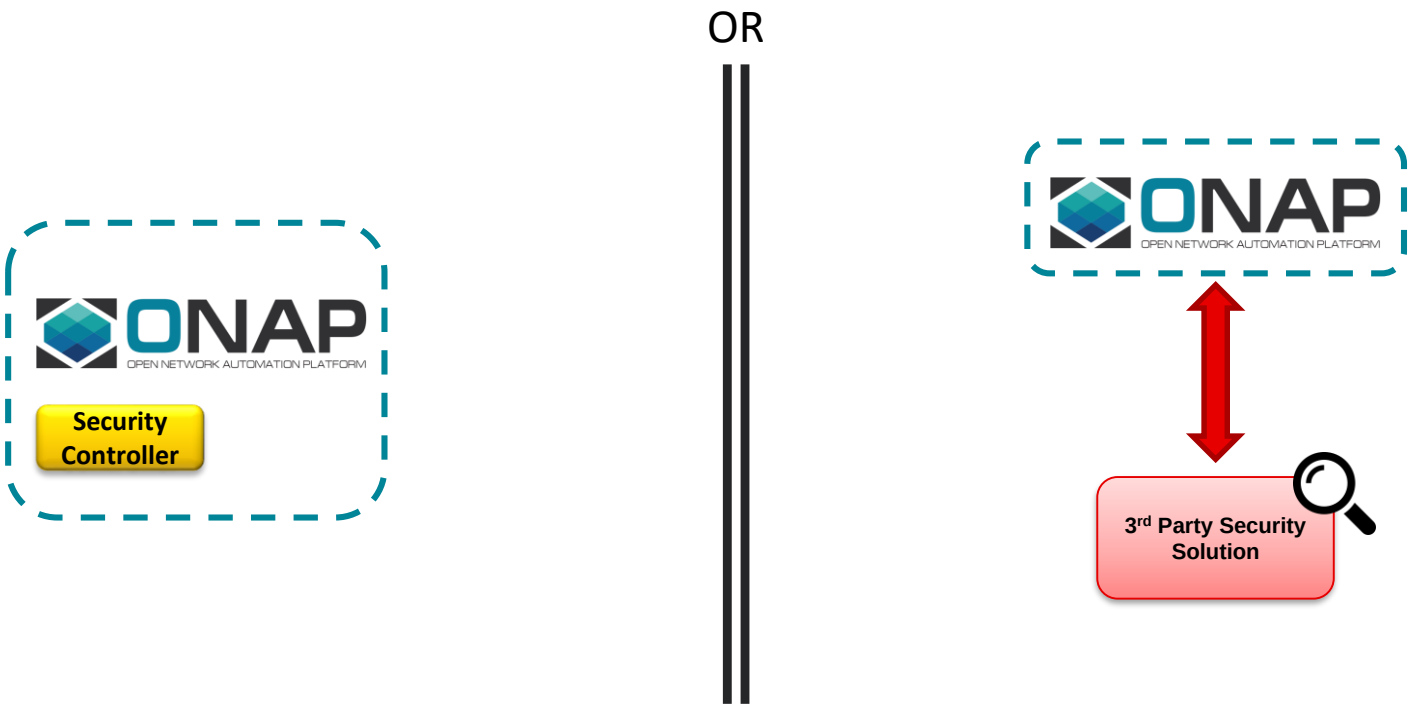


ONAP R3
Casablanca

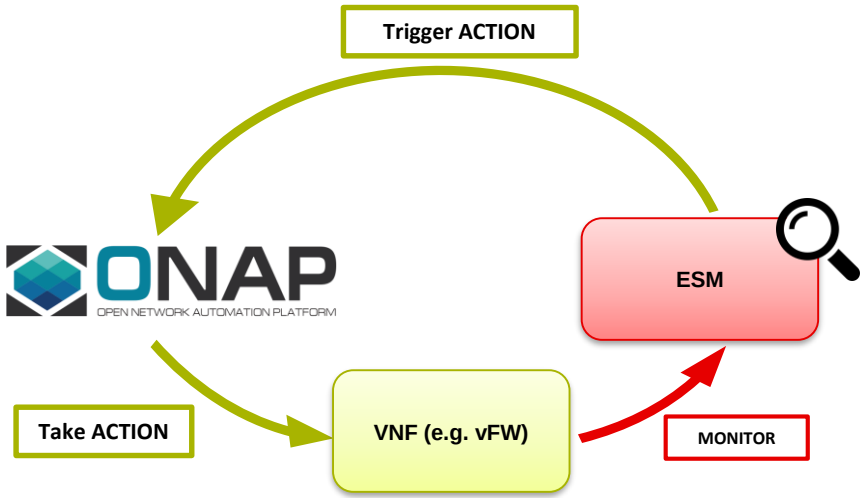
ONAP Security Considerations

- Enhancing ONAP security
  - Projects (security by design)
  - CII badging
- ONAP used to enhance Service security

Possible Service Security Scenarios for ONAP



ONAP ⟷ Ericsson ESM Demo



- 3 Use Cases demonstrated
  1. Misconfiguration detection
  2. Threat detection & Self-Healing
  3. Forensics & Root Cause Analysis

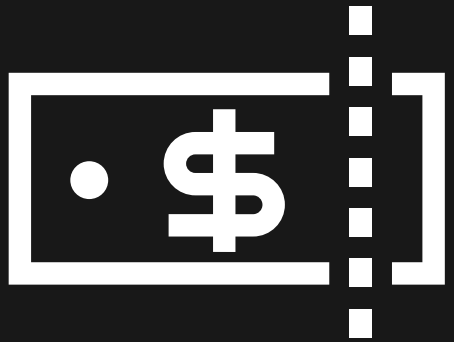
Automating service self-healing and security management

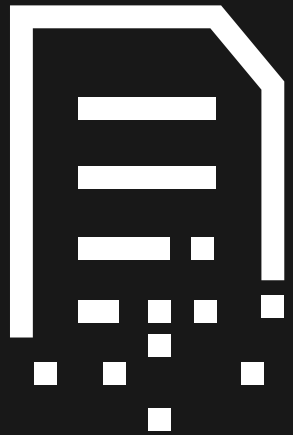
Open Networking Summit
North America
April 2019

Kari-Pekka Perttula Ericsson Security Solutions

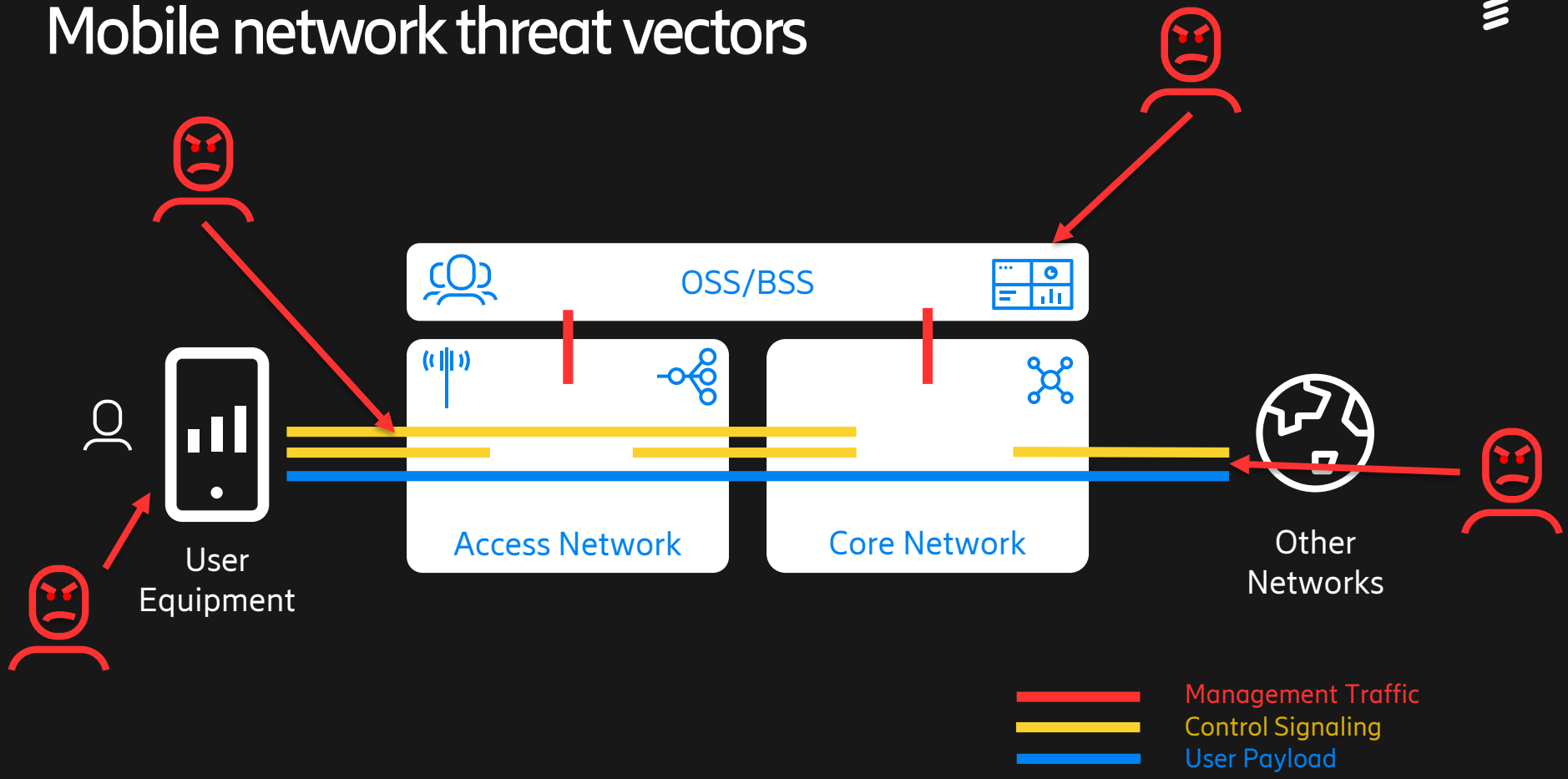
2019-04-05

Assets at risk



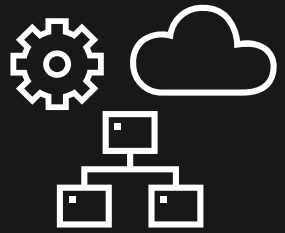


Mobile network threat vectors



Most common issues resulting in security breach or incident

Security policies are not enforced or monitored



Lack of hardening
Insecure configurations of the network

Current operational procedures prone for mistakes

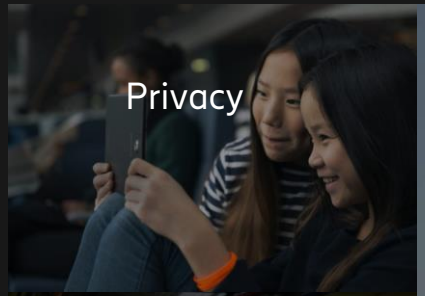
Lack of visibility, control and continuous monitoring

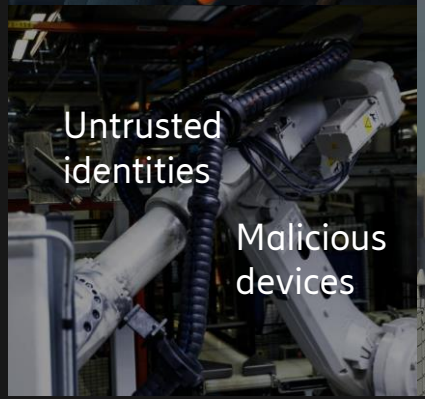
"Through 2020, 80% of cloud breaches will be due to customer misconfiguration, mismanaged credentials or insider theft, not cloud provider vulnerabilities."

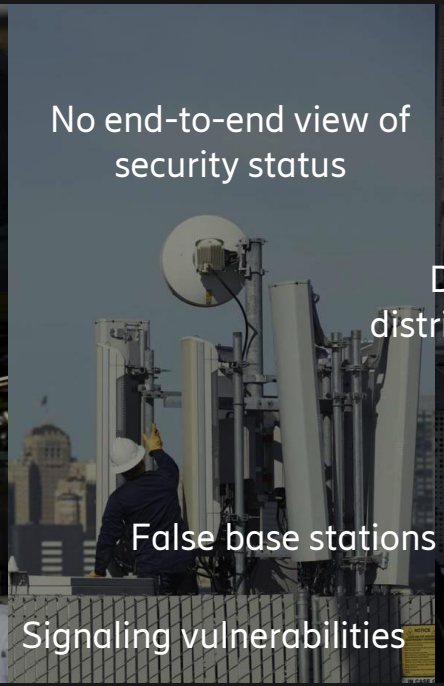
-Gartner

Service provider security challenges

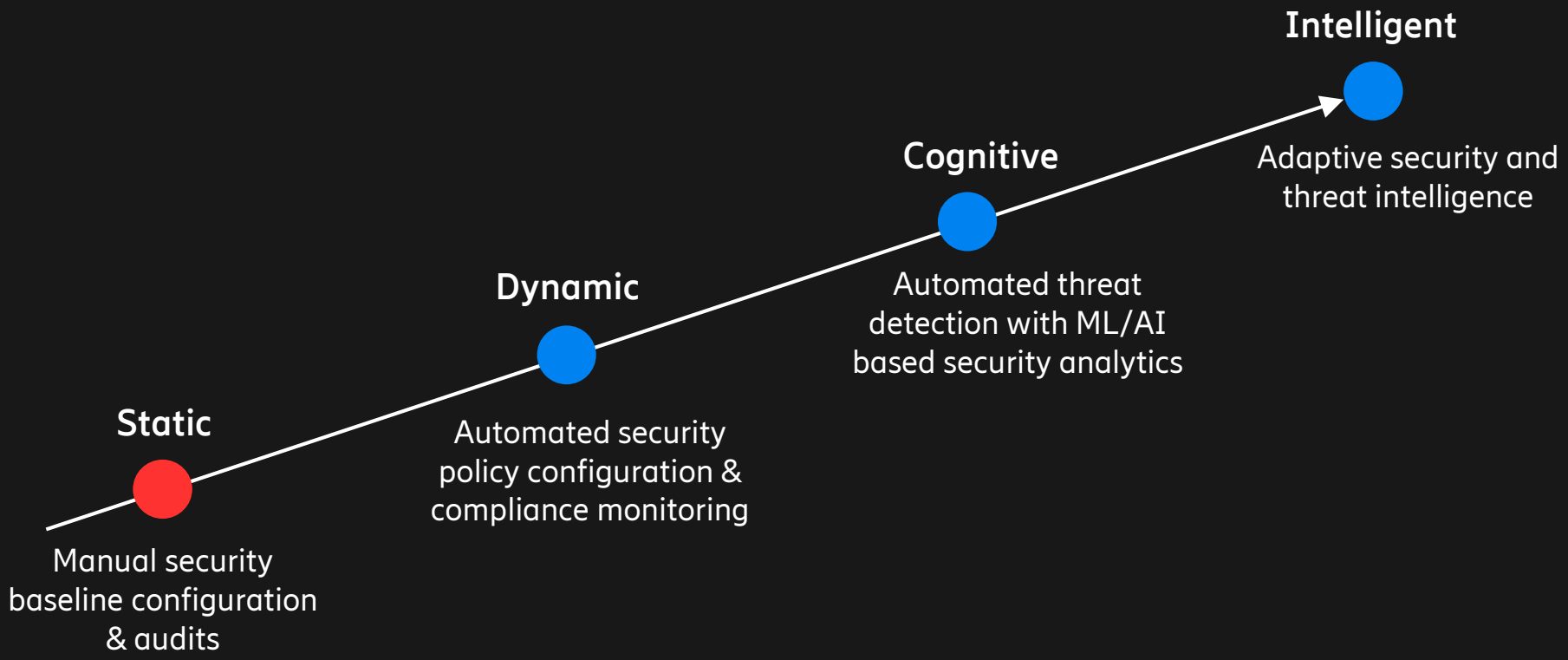
- Lack of end-to-end security visibility
- Security and privacy compliance
- Limited ability to detect and respond to threats
- Manual processes are not scalable







Journey towards intelligent security management

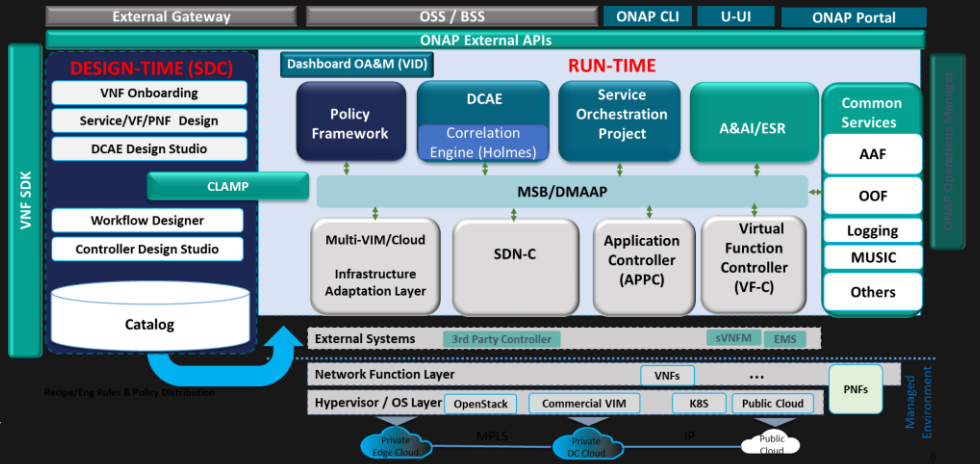


Security managent challenges with ONAP

— Security focus in the ONAP community is currently on the platform security and selected VNF use cases

— ONAP lacks security framework and APIs, that would facilitate connection to external security analytics and management tools

— These are needed to automate security operations use cases both for the NFs and the ONAP platform



Summary

— Security management is a challenge in current networks – lack of control and visibility

— Networks are becoming dynamic and distributed, at the same time new threats continuously emerge – manual security processes are not scalable and effective

— Automation of security use cases is an imperative for intelligent security management

ericsson.com/security