



SECURITY ASSURANCE & EVOLUTION OF INTERNATIONAL STANDARDS

Marie Royce, Vice President Public Affairs, Alcatel-Lucent

Rao Vasireddy, Director Bell Labs Security Group, Alcatel-Lucent

September 15, 2014

AGENDA

The Importance of International Cybersecurity Standards

International cybersecurity standards provide a basis for planning and deployment of sound security solutions and build trust among those creating and using those solutions throughout the globe. These standards provide a common language to communicate security requirements and ways of implementing them that are common and accepted. Cover examples of national priority and international efforts

INTERNATIONAL CYBERSECURITY STANDARDS

Enterprise security policies
Industry specific requirements
Security Frameworks
NIST Cyber security framework, ETSI, etc

Global Standards Organizations & Forums

ITU-T, 3GPP, 3GPP2, ETSI, ATIS, IETF, IEEE, OMA, TIA, NIST, ISO/IEC, CSA, SwA, NERC-CIP, TSDSI, ...



Security thought leadership

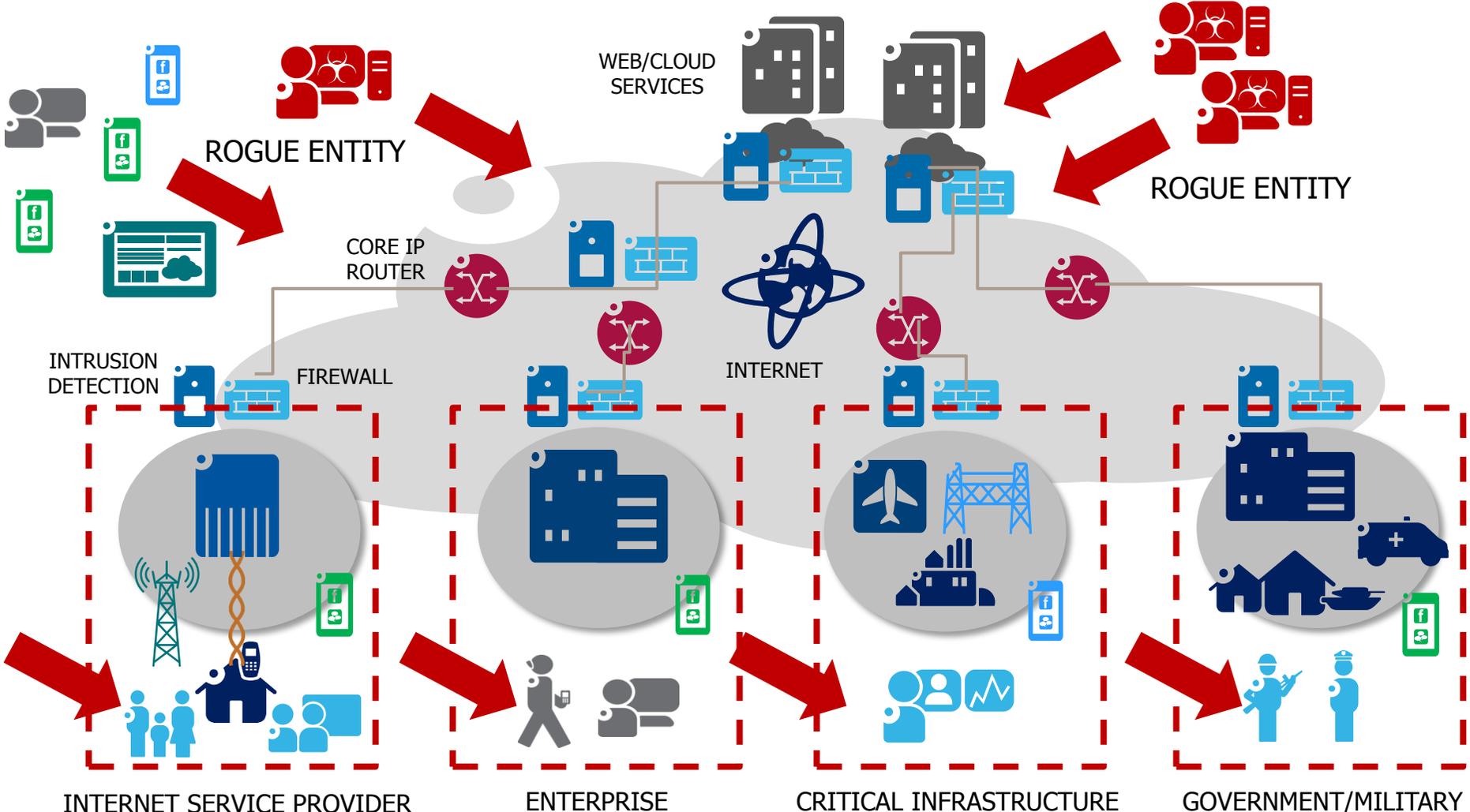
Adaptability, innovation and usability

Program Integrated into product & service life-cycles

Interoperability
User acceptance
Trust

International cybersecurity standards provide a basis for planning and deployment of sound security solutions and building trust

THE FUTURE OF ICT : COMMON CLOUD NETWORKS WITH MASSIVE IP ENDPOINTS



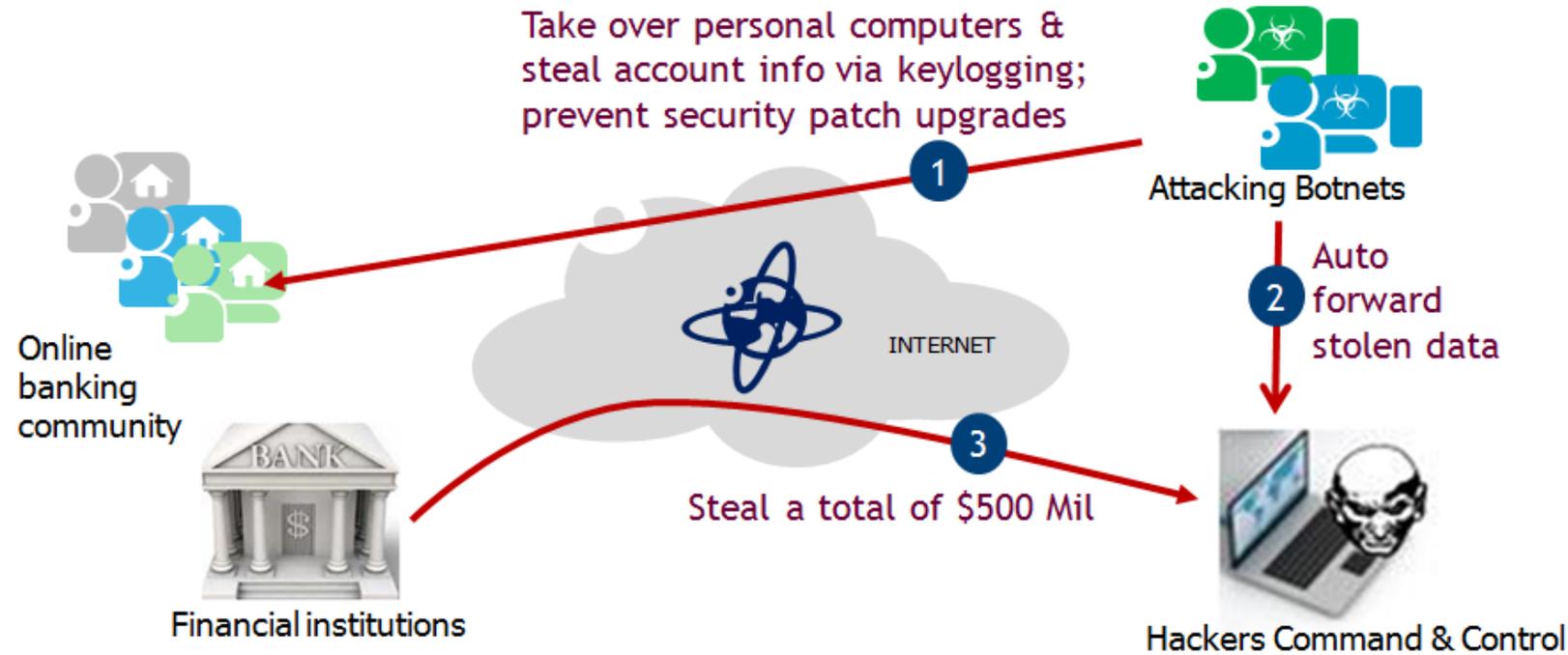
SIGNIFICANT CYBERTHREATS TO ICT

'Cloud' networks with Internet and own IP devices and Cloud Services as multiple (large scale) points of entry → unforeseen increase in attack surface

CYBERSECURITY PROBLEM IS BOUNDARYLESS

STRATEGY TO ADDRESS ICT THREATS: TECHNOLOGY INNOVATION, AUTONOMICS AND STANDARDS

TACKLING THE ICT ATTACKS



CITADEL: AN EXAMPLE OF & GLOBAL PREVENTION

- **1000+ botnets in 80 countries attacked 5 million Victims**
- **Botnets were ultimately shutdown as a result of public private partnership** (Collaboration between Microsoft, financial institutions, FBI and law enforcement in 80 countries)

COORDINATED PUBLIC-PRIVATE PARTNERSHIPS INCREASINGLY KEY TO FUTURE OF CYBERSECURITY TO SAFEGUARD
NATIONAL AND INTERNATIONAL INTERESTS

SECURITY ASSURANCE ↔ MULTIPLE DEGREES OF COOPERATION

☆☆☆ Public-private partnerships

☆☆☆ Cross-border cooperation

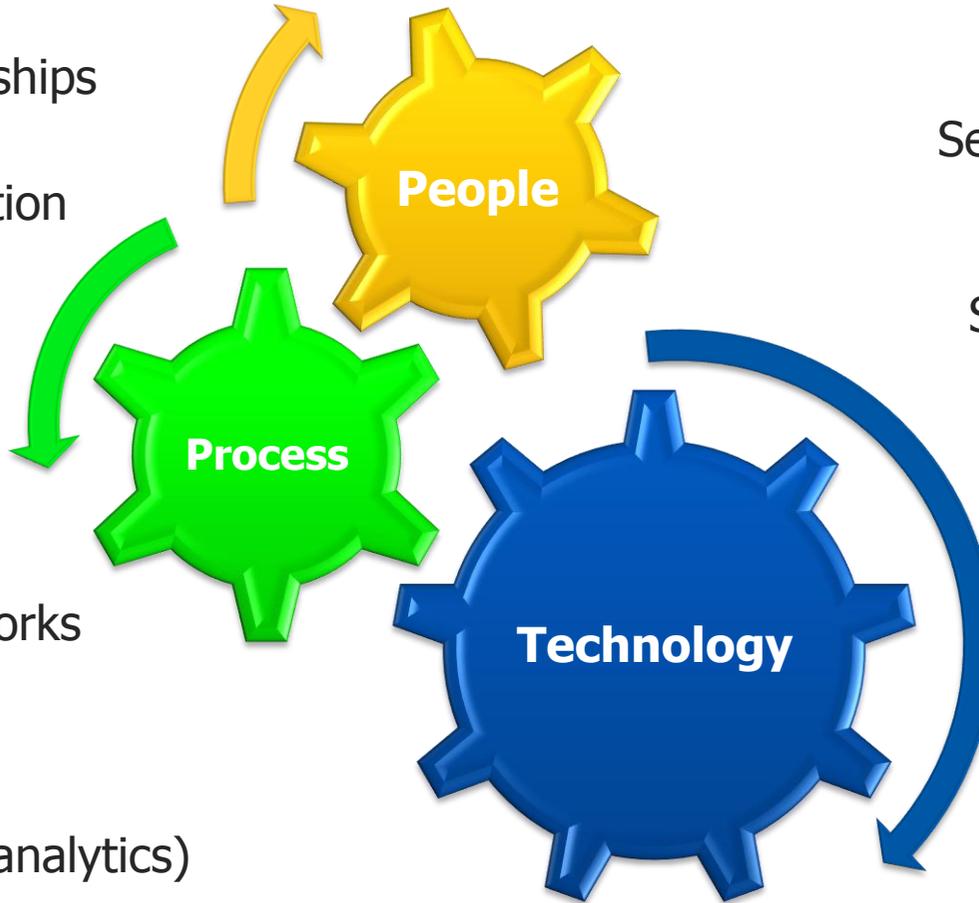
☆☆☆ Supply-chain integrity

☆☆☆ Standards evolution

☆☆☆ Cybersecurity frameworks

☆☆☆ Hardware security

☆☆☆ Security intelligence (analytics)



Security training, skills ☆☆☆

Security-as-a-Service ☆☆☆

Secure cloud infrastructure ☆☆☆

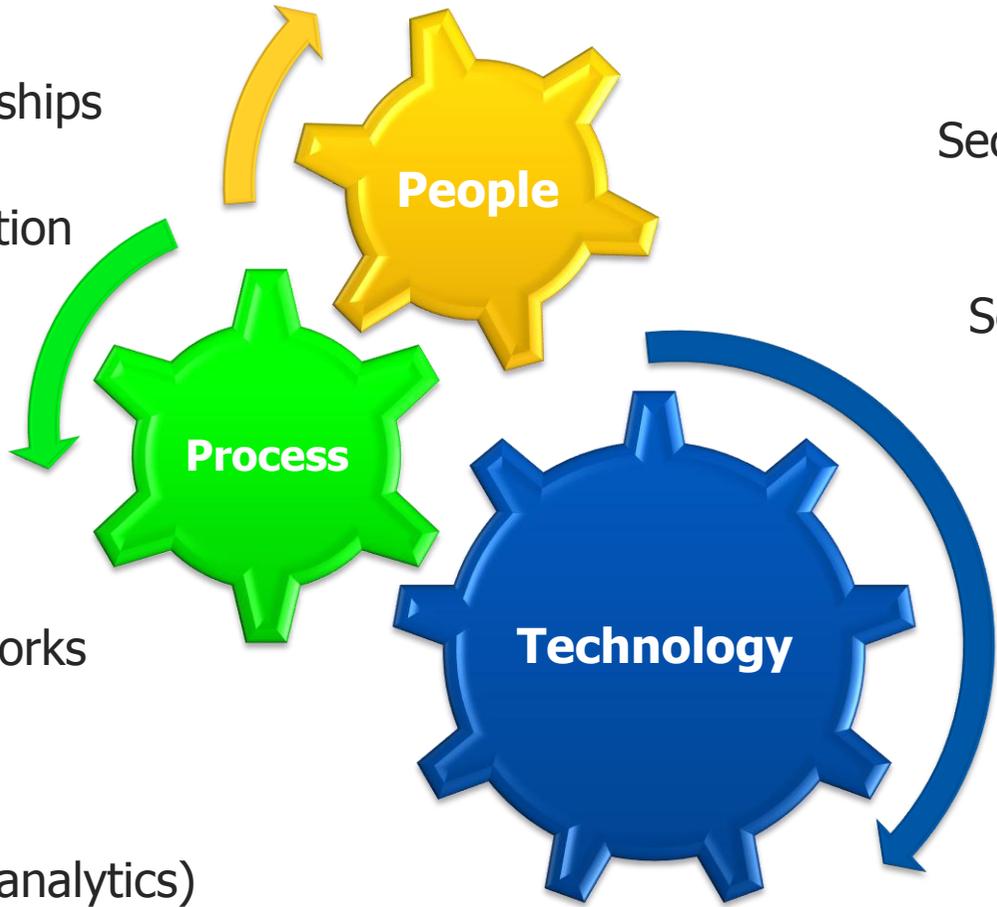
Scalable security appliances ☆☆☆

Biometrics ☆☆☆

THE TOOLS ARE INCREASINGLY DEFINED, BUT MUCH REMAINS TO BE DONE

SECURITY ASSURANCE ↔ MULTIPLE DEGREES OF COOPERATION

- ★★★☆☆ Public-private partnerships
- ★★☆☆☆ Cross-border cooperation
- ★★★☆☆ Supply-chain integrity
- ★★★★☆ Standards evolution
- ★★★☆☆ Cybersecurity frameworks
- ★★★☆☆ Hardware security
- ★★☆☆☆ Security intelligence (analytics)



- Security training, skills ★★★☆☆
- Security-as-a-Service ★★★☆☆
- Secure cloud infrastructure ★★★☆☆
- Scalable security appliances ★★★☆☆
- Biometrics ★★★☆☆

THE TOOLS ARE INCREASINGLY DEFINED, BUT MUCH REMAINS TO BE DONE

GLOBAL AND REGIONAL REQUIREMENTS

Common Criteria (ISO 15408), TL9000, FIPS 140-2, ISO27K , NERC CIP, 3GPP SECAM (evolving), etc ...

US guidance

- Banking, finance
- Energy, Healthcare (NERC CIP, HIPAA)
- NIST
- PCI, SoX
- FIPS, FISMA

APAC

- Australian Privacy, Business Continuity Management Guide
- India National Cyber Security Policy
- Japan Handbook on the Protection of Personal Data
- JSOX System Management Standards, Singapore Corporate Governance
- Korea Act on the Promotion of Information Communication Network Utilization Information Protection

EU

- EU Directive on privacy and electronic communications
- EU Data Protection Directive 95 46 EC
- EC ECNS DPP Regulations
- UN Guidelines for the Regulation of Computerized Personal Data Files
- EU Safe Harbor US European

Other International

- Cloud Security Alliance
- IIA GAIT, GTAG
- ISO/IEC
- COBIT
- Computer Security Incident Handling

EVOLUTION OF INTERNATIONAL STANDARDS

SECURITY ASSURANCE - JOINT 3GPP AND GSMA ACTIVITY



3GPP SA3

- Launched SECAM activity in 2012
- 3GPP specifications cover interfaces and protocol security
- SECAM adds test cases for 3GPP network equipment security assurance

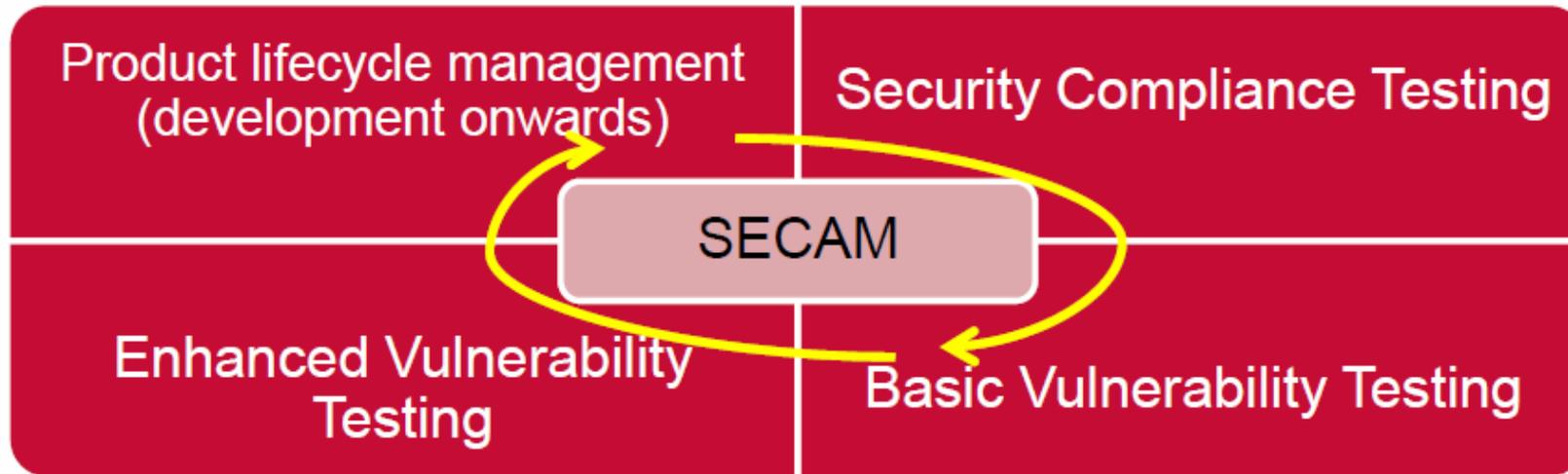


GSMA NESAG

- Established in Feb 2014
- Defines and governs security accreditation scheme for network equipment evaluation and conflict resolution
- Operates accreditation supported by third parties

3GPP SECAM AGREED UPON METHODOLOGY

- Security tests described per type of network equipment in **3GPP SCAS** documents



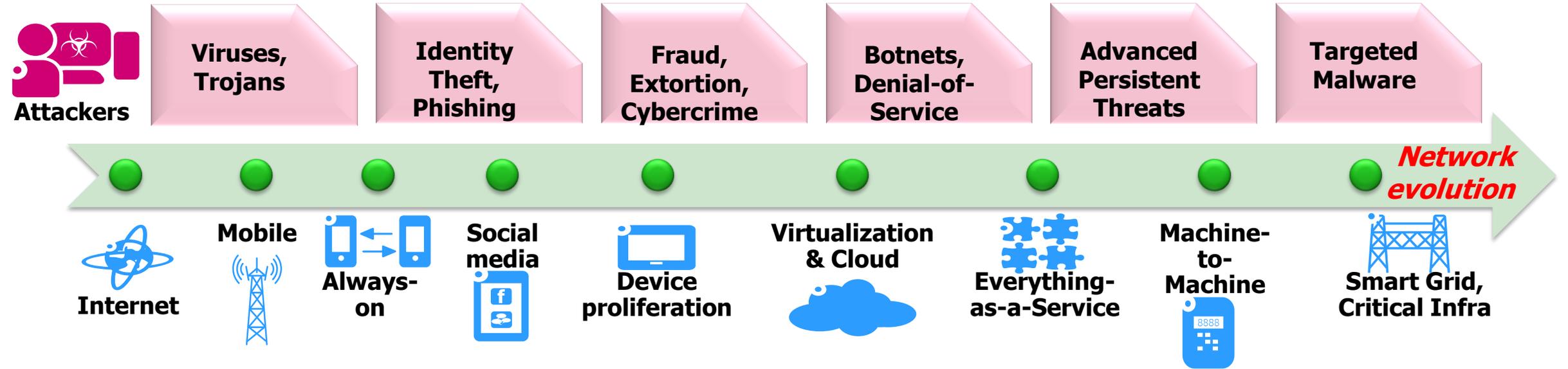
- **GSMA NESAG** takes care of accreditation and conflict resolution
- Tests are to be performed by an **accredited vendor or third party**
- **Mobile operator can still decide** whether to choose the product

Security from product design onwards



SUMMARY

ADAPTABLE SECURITY FRAMEWORKS FOR ASSURANCE

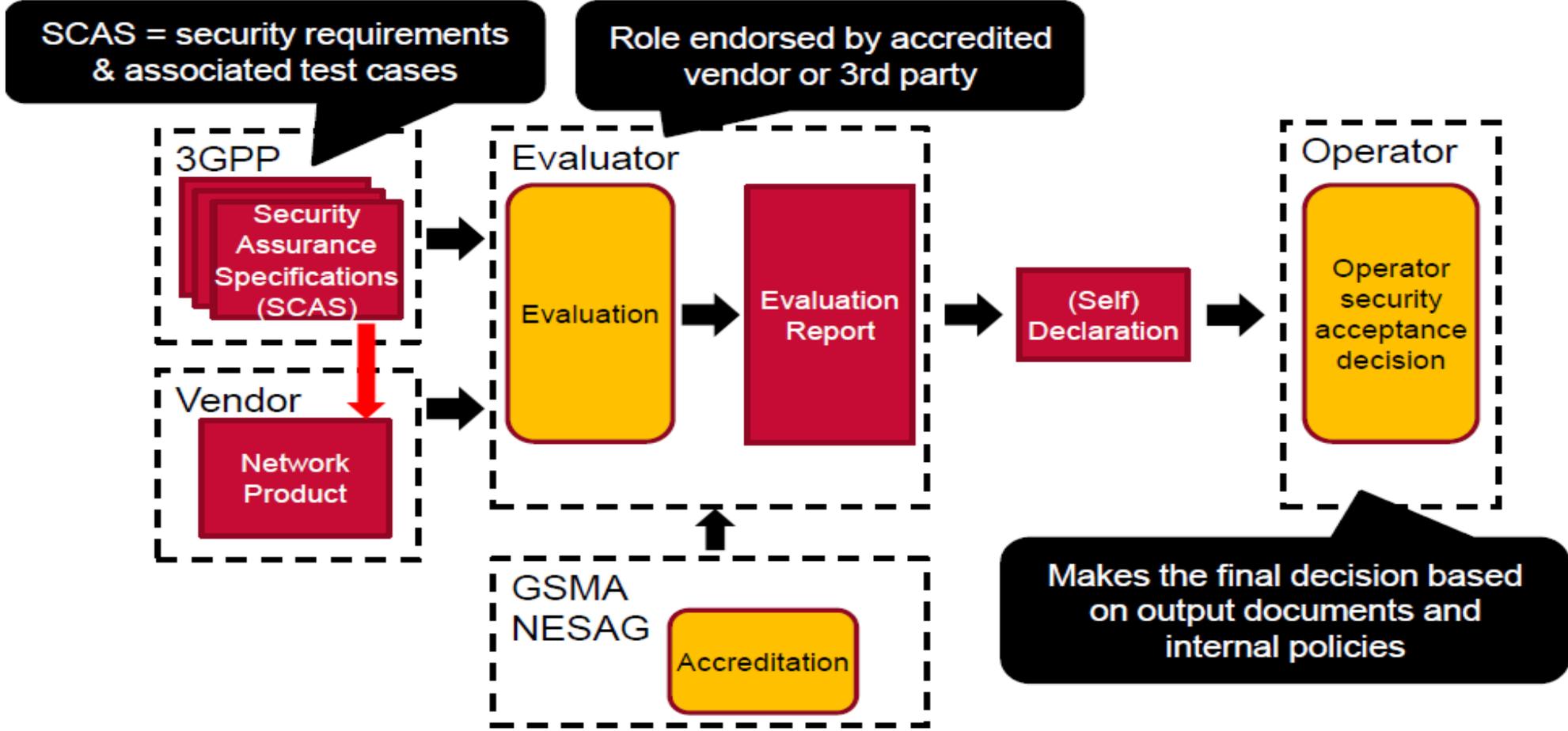


Network technology and applications are evolving rapidly

- Larger attack surfaces and sophisticated attack methods
- Security frameworks and policies should be able to adapt evolving standards and technology

REFERENCE SLIDES

3GPP SECAM OVERVIEW



Legend:



Unrestricted

SECAM: Security Assurance Methodology