Repenser l'architecture sécurité telecom à l'ère de la 5G

Alexandre De Oliveira – alexandre.deoliveira@post.lu
Telecom Security Expert
Fratel – Mai 2022

POST
CYBERFORCE
« Smart security enabling the digital society »

POST
LUXEMBOURG

L’expertise d’un opérateur, au service des opérateurs

- **Post Luxembourg** est le fournisseur de services télécom des clients les plus sensibles
  - Gouvernement du Luxembourg, institutions européennes, banques et fonds d’investissement

- Nous sommes **directement confrontés aux attaques télécom internationales**
  - Piratage, interception de communications, localisation de téléphones, fraudes & déni de service

- Pour protéger nos clients, nous avons conçu **notre propre système de défense**

Les réseaux télécom, des infrastructures stratégiques

- **Augmentation radicale** des **menaces** depuis 5 ans :

LightBasin: A Roaming Threat to Telecommunications Companies

- **Des attaques** aux **impacts majeurs** :

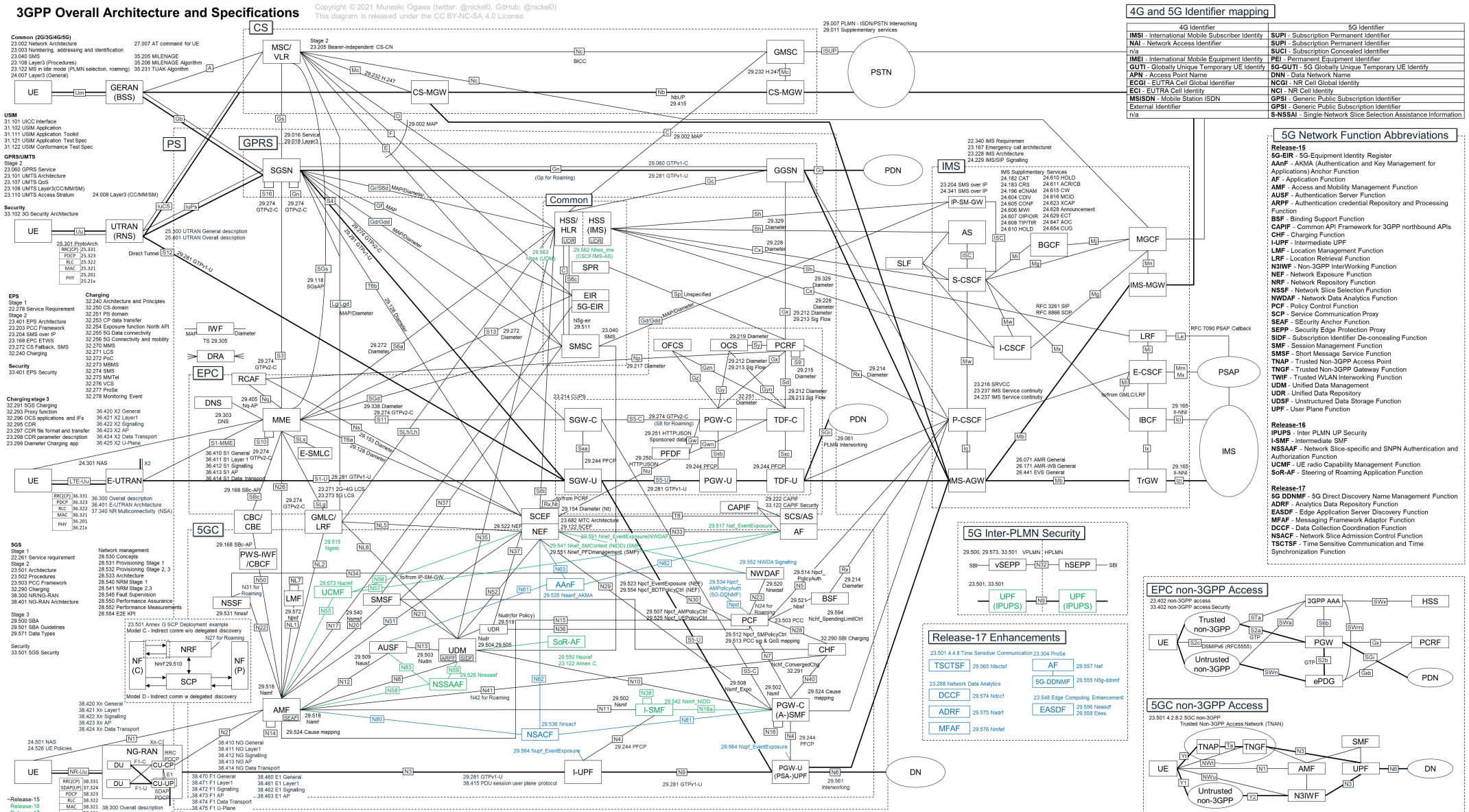
OPÉRATEUR PIRATÉ	DÉNI DE SERVICE GLOBAL	LOCALISATION DE TÉLÉPHONES	INTERCEPTION APPEL & SMS	FRAUDE & PHISHING SMS

Confidentiel – ne pas diffuser sans accord de Post Luxembourg et d'ACMS Consulting

Challenges pour les opérateurs

- Un empilement massif de technologies
  - De la 2G à la 5G, des vSAT, FTTH, IPTV
- Passage du tout **analogique** au tout **IP** et maintenant au **cloud**
- Changement de paradigme, des ingénieurs télécoms devenant des devOps ou ingénieur logiciels
  - Spécialités Kubernetes, Dockers, OpenStack, OpenDayLight…

Un réseau devenu massif



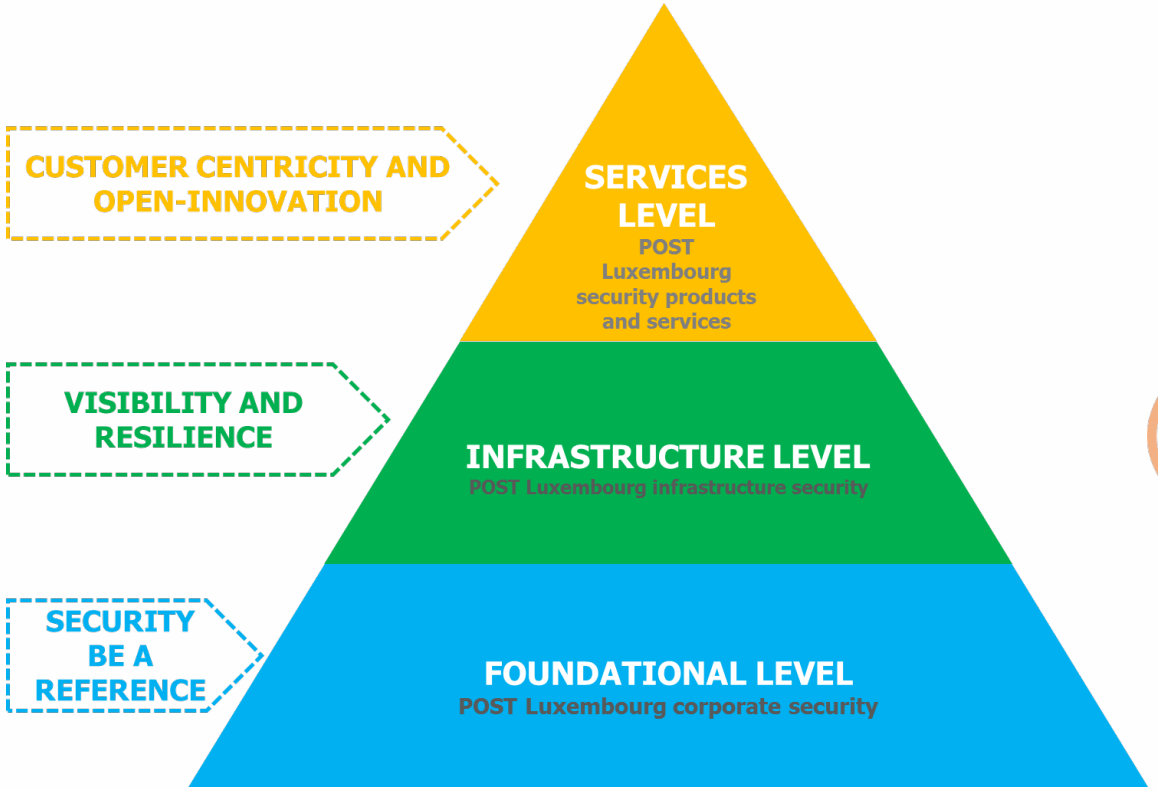
4G Identifier	5G Identifier
IMSI - International Mobile Subscriber Identity	**SUPI** - Subscription Permanent Identifier
NAI - Network Access Identifier	**SUPI** - Subscription Permanent Identifier
n/a	**SUCI** - Subscription Concealed Identifier
IMEI - International Mobile Equipment Identity	**PEI** - Permanent Equipment Identifier
GUTI - Globally Unique Temporary UE Identity	**5G-GUTI** - 5G Globally Unique Temporary UE Identify
APN - Access Point Name	**DNN** - Data Network Name
ECGI - EUTRA Cell Global Identifier	**NCGI** - NR Cell Global Identity
ECI - EUTRA Cell Identity	**NCI** - NR Cell Identity
MSISDN - Mobile Station ISDN	**GPSI** - Generic Public Subscription Identifier
External Identifier	**GPSI** - Generic Public Subscription Identifier
n/a	**S-NSSAI** - Single-Network Slice Selection Assistance Information

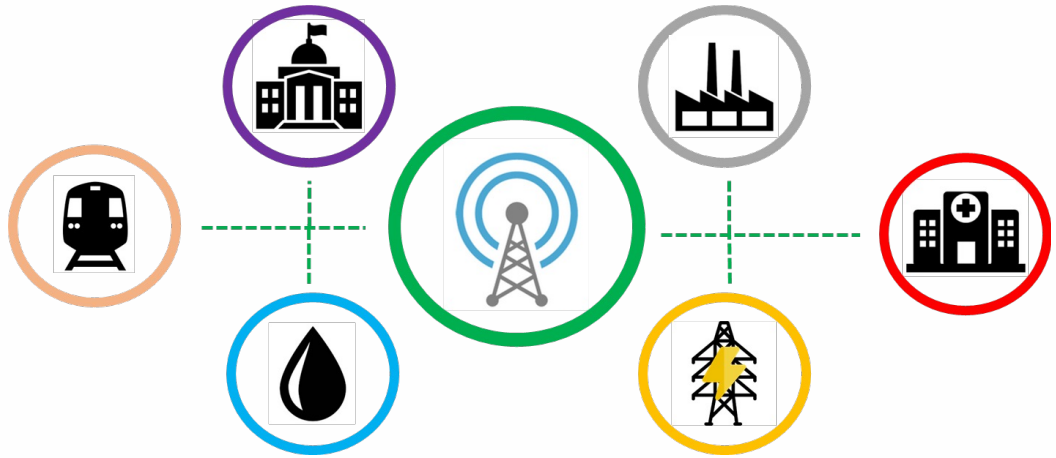
Release-15
5G-EIR - 5G-Equipment Identity Register
AAnF - AKMA (Authentication and Key Management for Applications) Anchor Function
AF - Application Function
AMF - Access and Mobility Management Function
AUSF - Authentication Server Function
ARPF - Authentication credential Repository and Processing Function
BSF - Binding Support Function
CAPIF - Common API Framework for 3GPP northbound APIs
CHF - Charging Function
I-UPF - Intermediate UPF
LMF - Location Management Function
LRF - Location Retrieval Function
N3IWF - Non-3GPP InterWorking Function
NEF - Network Exposure Function
NRF - Network Repository Function
NSSF - Network Slice Selection Function
NWDAF - Network Data Analytics Function
PCF - Policy Control Function
SCP - Service Communication Proxy
SEAF - SEcurity Anchor Function.
SEPP - Security Edge Protection Proxy
SIDF - Subscription Identifier De-concealing Function
SMF - Session Management Function
SMSF - Short Message Service Function
TNAP - Trusted Non-3GPP Access Point
TNGF - Trusted Non-3GPP Gateway Function
TWIF - Trusted WLAN Interworking Function
UDM - Unified Data Management
UDR - Unified Data Repository
UDSF - Unstructured Data Storage Function
UPF - User Plane Function

Release-16
IPUPS - Inter PLMN UP Security
I-SMF - Intermediate SMF
NSSAAF - Network Slice-specific and SNPN Authentication and Authorization Function
UCMF - UE radio Capability Management Function
SoR-AF - Steering of Roaming Application Function

Release-17
5G DDNMF - 5G Direct Discovery Name Management Function
ADRF - Analytics Data Repository Function
EASDF - Edge Application Server Discovery Function
MFAF - Messaging Framework Adaptor Function
DCCF - Data Collection Coordination Function
NSACF - Network Slice Admission Control Function
TSCTSF - Time Sensitive Communication and Time Synchronization Function

Une approche globale de la sécurité



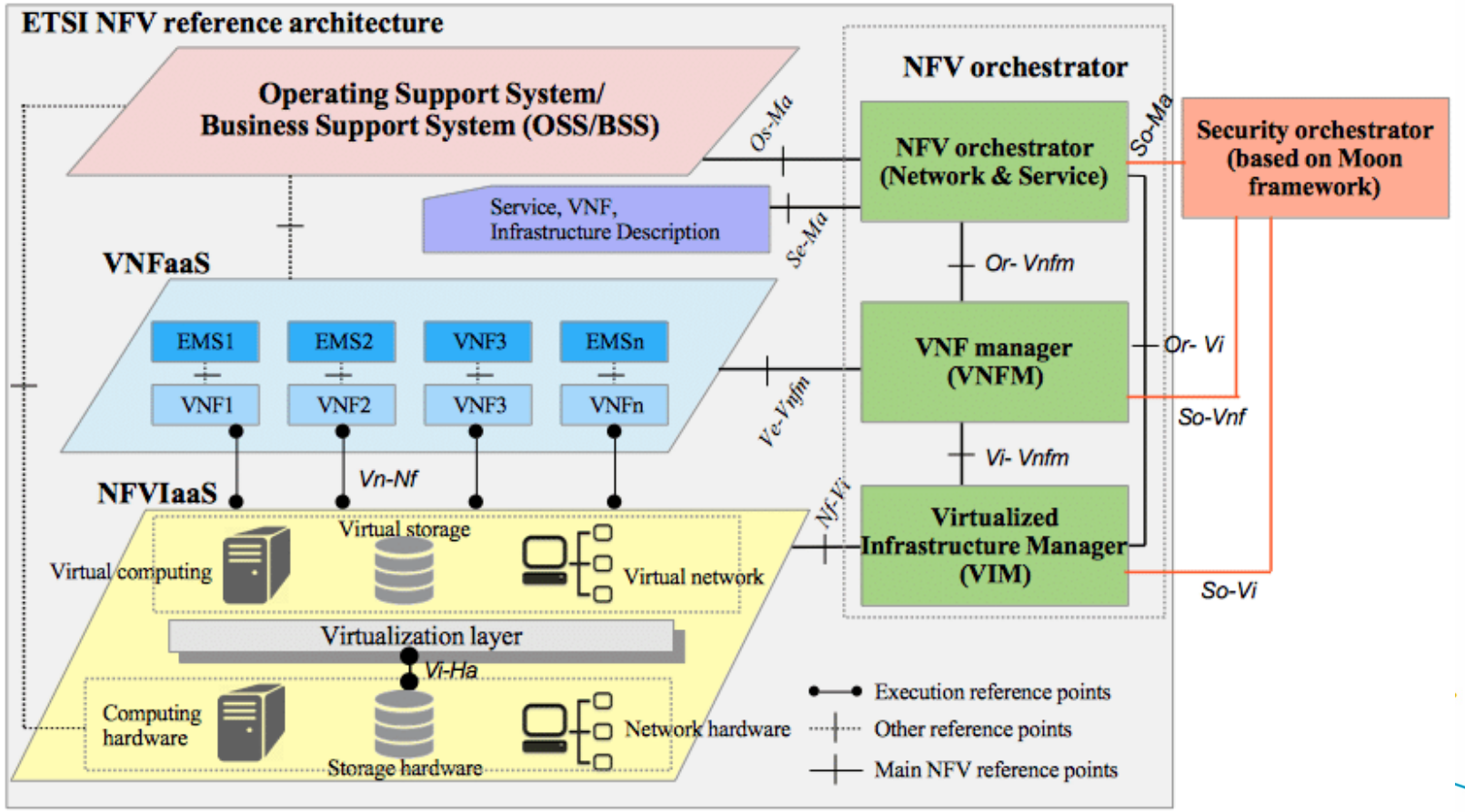


Infrastructure Virtuelle / NFV complexe

- API Security
- Container Security
- Software Lifecycle
- Segmentation
- Autoscaling

Consistency

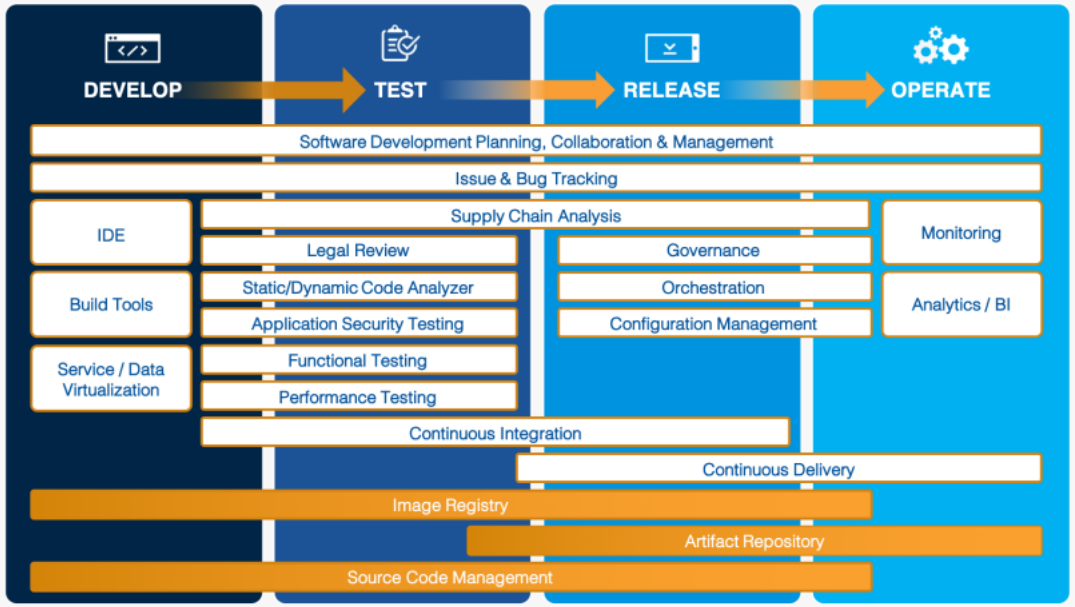
- Full IPv6



Le logiciel au centre des réseaux télécoms

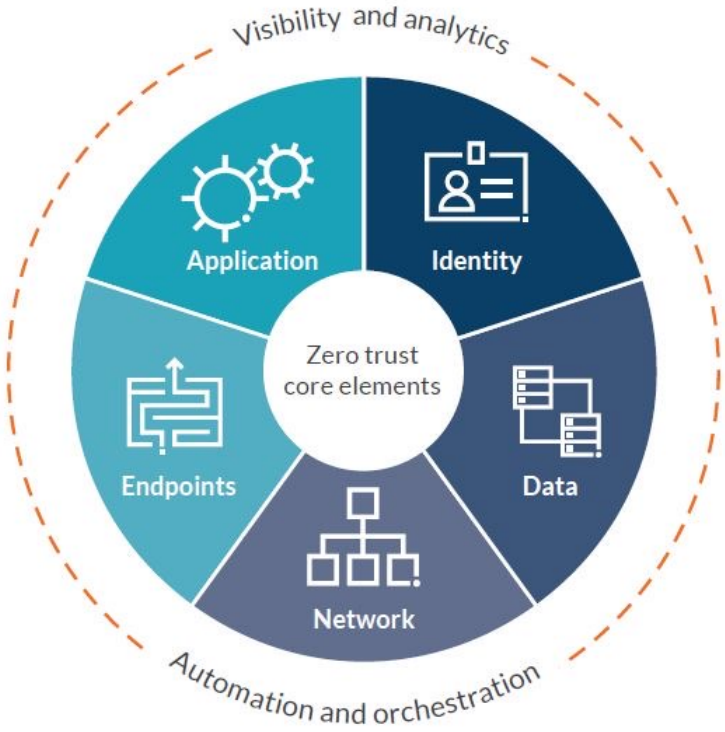
- Des mise à jours continues
- Une rapidité du cycle de vie des équipements télécom jamais vue
- Un manque de contrôle des équipes interne

- Quelle confiance envers les contructeurs télécom ?



Une approche Zero Trust

- Reconstruction d'un reseau de zéro
  - Deux datacenter Tier IV
- Une architecture totalement repensée
  - Assurer une étenchéité des zones
  - Réduire l'impact en cas de compromission
- Challenge de l'automatisation et ochestration d
  - Evolution constente du réseau
- Une intégration de la sécurité au coeur des réseaux
  - Revues d'architectures dès la conception
  - Tests offensifs réalisés avant et après la mise en production
  - Mise en place de SoC et contrôles internes et externes



Le choix d’un cloud souverain

- Choix de developper de zéro le nouveau réseau télécom de POST Luxembourg

- Consolider et faire grandir les connaissances de nos ingénieurs
  - Architecture Zero Trust, K8S, OpenStack

- Un soucis de souveraineté qui nous permet un meilleur contrôle
  - Multiplication des tierces parties (vendeurs, service à valeur ajoutée, paiement)

Une plus grande maitrise pour une plus grande sécurité

Se détacher des possibles contraintes géopolitiques
et conserver notre neutralité

Merci !

Alexandre De Oliveira – alexandre.deoliveira@post.lu