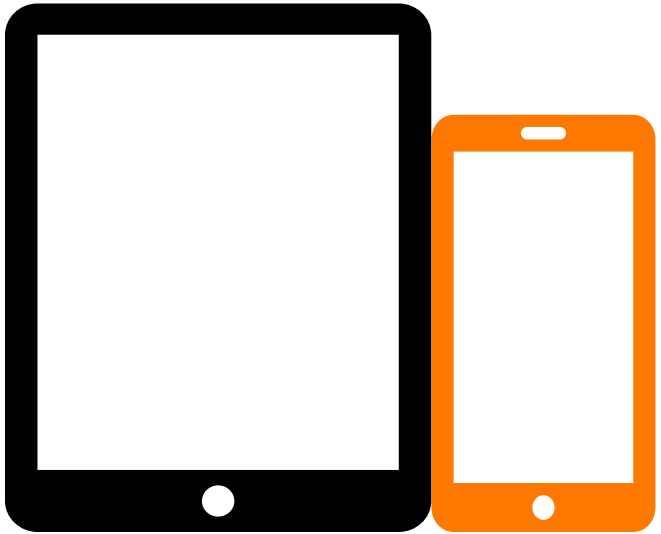
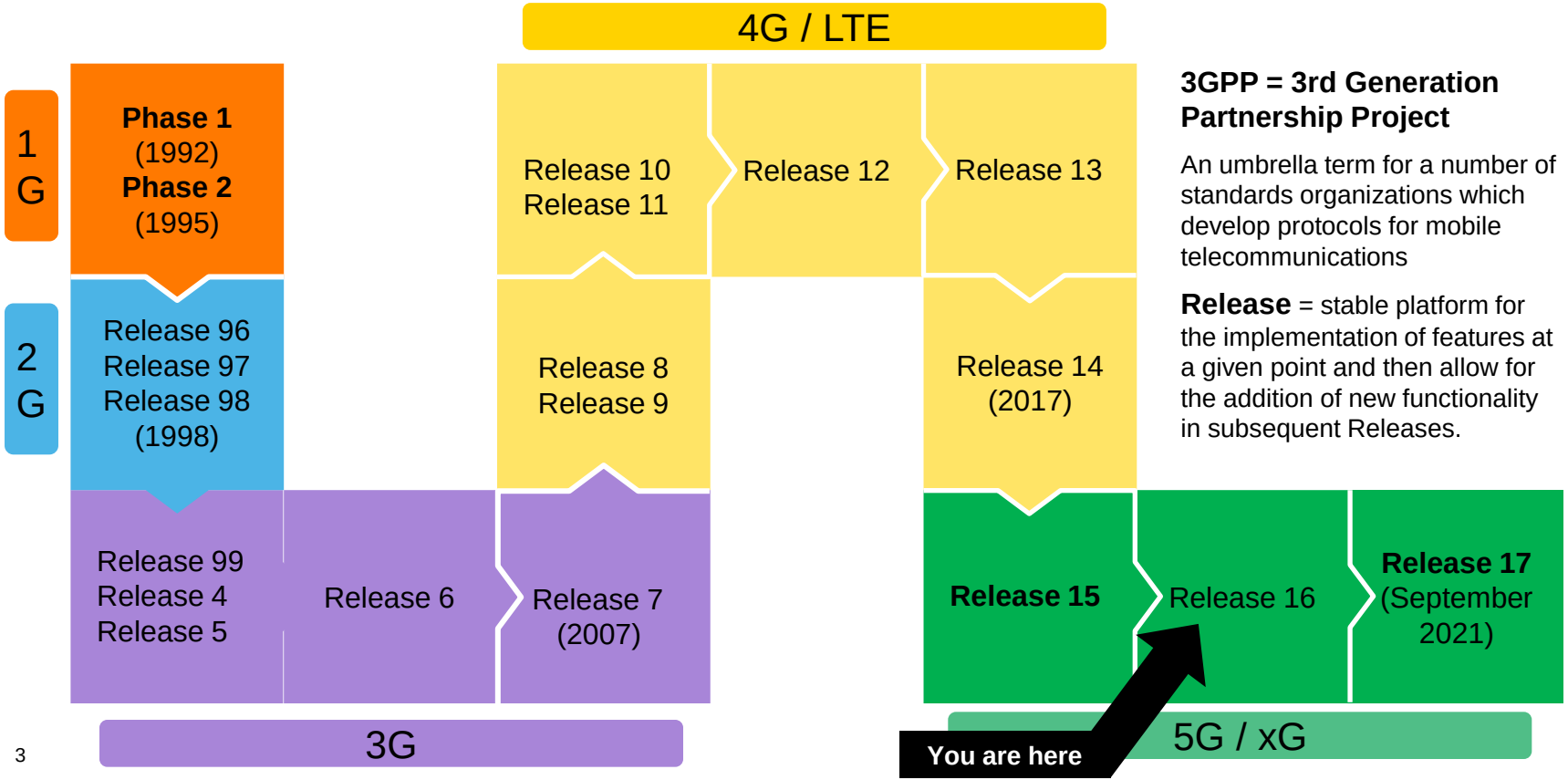
AI Driven Automated Security Orchestration in Heterogeneous xG Networks

Ioan Constantin
Orange Romania



Contents

Beyond 5G and Networks of the Future



3GPP = 3rd Generation Partnership Project

An umbrella term for a number of standards organizations which develop protocols for mobile telecommunications

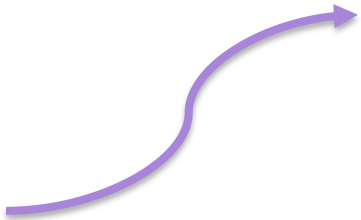
Release = stable platform for the implementation of features at a given point and then allow for the addition of new functionality in subsequent Releases.

Moving from 5G to the Networks of the Future

Heterogeneous, Multi-domain networks and their security challenges

5G

- Common Composable Core
- Software Defined Networks & NFV
- Virtual-*everything*
- Slicing
- Management & Orchestration



xG

- Iot - RAN – EDGE – Core – Cloud Continuums
- A.I.-enabled Man & O, A.I. driven self-healing
- Hyper-scalability, Hyper-integration
- Medium-agnostic, platform-agnostic
- 100x SLAs

Challenges in beyond-5G Networks Security Orchestration

Multi-domain

Assets might roam through multiple operators

Control plane(s) and **datapaths** are extended beyond 5G-land to (private)clouds and the Internet

Multi-vendor

Each provider (telcos, cloud, security, data, services) operates their own stack of multi-vendor tech

Massive IoT

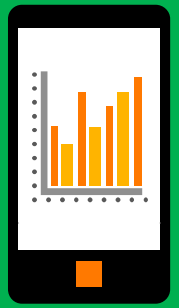
Multiple Billion connected devices by 2030

Fragmentation

SOAR models, methods, playbooks are fragmented. Only recent endeavours have targeted common schemas but adoption is (s)low

Performance

Multi-domain / multi-vendor has a toll on end-to-end performance due to overhead of integration

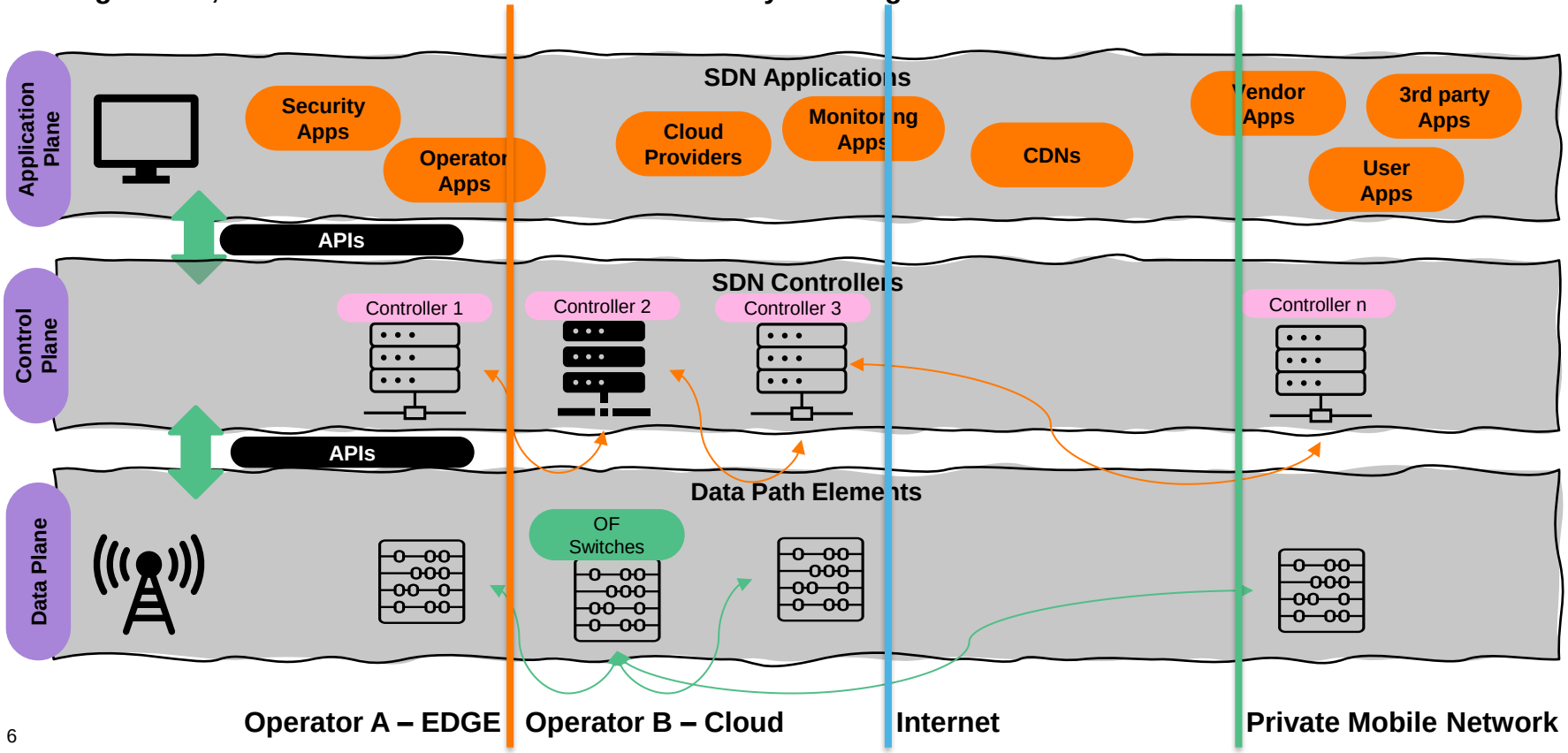


Regulatory & Compliance pressure

Telco-world is heavily regulated. Compliance is costly and TCOs are extended to multiple years

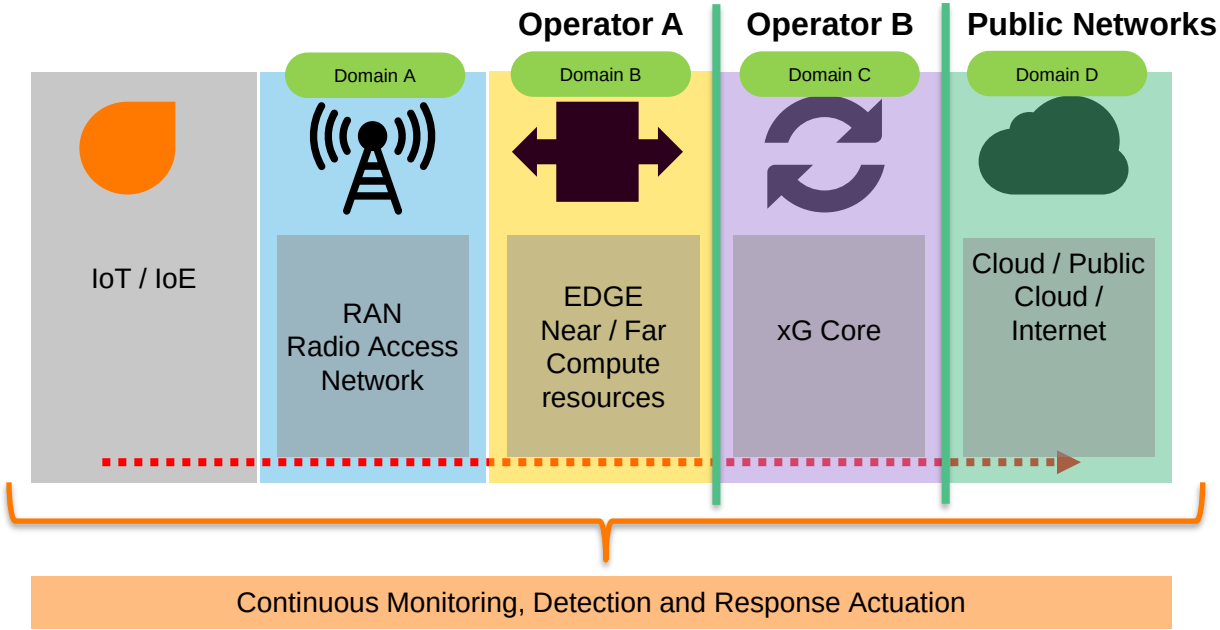
Beyond-5G Multi-domain Networks

Heterogeneous, Multi-domain networks and their security challenges



IoT-RAN-EDGE-Core-Cloud Continuums

Heterogeneous, Multi-domain networks and their security challenges



SoTA in 5G Security Orchestration

MANO

Management & Orchestration specifications defined by 3GPP;

Limited scope

Multi-domain

Current tools are multi-domain aware;

Cross-domain policies

Policy-based

SoTA is policy-based & uses various interposers / integrations as policy „translators” in multi-vendor, multi-platform settings

Vendor-specific

Limited open-source support;

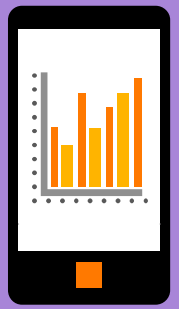
Limited platform integration methods & tools

Actuations

Difficult to integrate to heterogeneous domains

Fails-forward on vendor-locked methods;

MANO is opaque to most SOARs



Human-in-the-loop

Limited intent awareness

Limited SOAR integrations

RIGOUROUS: secuRe desIGn and deplOyment of trUsthwoRthy cOntinUum computing 6G Services

RIGOUROUS project aspires to **identify** and **address** the **major cybersecurity, trust and privacy risks** threatening the **network**, **devices**, computing infrastructure, and next generation of services. RIGOUROUS will address these challenges by introducing a new holistic and smart service framework leveraging new machine learning (ML) and AI mechanisms, which can react dynamically to the ever-changing threat surface on all orchestration layers and network functions.

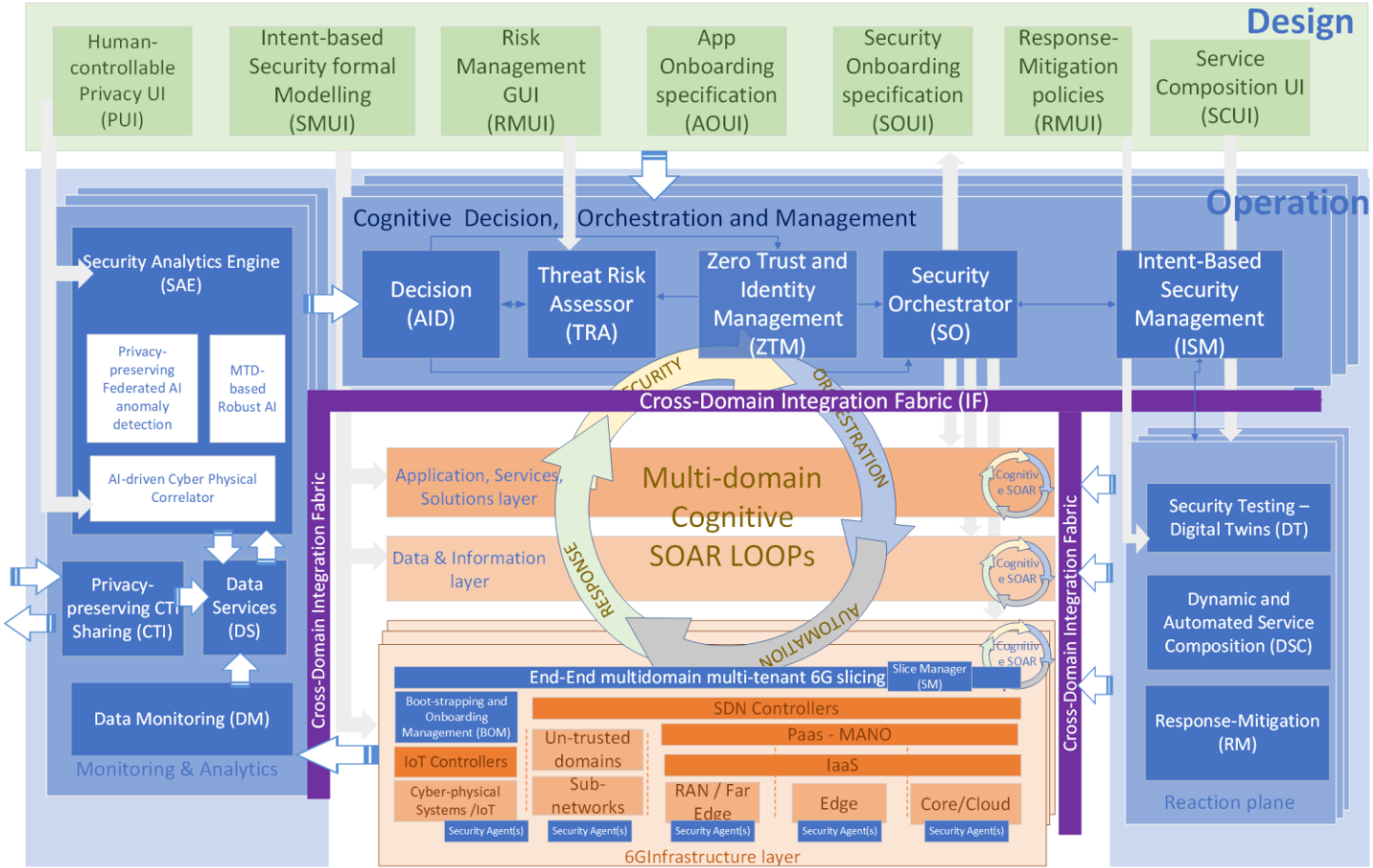
RIGOUROUS targets the following key objectives:

- Holistic Smart Service framework for securing the IoT-Edge-Cloud continuum lifecycle management
- Human-Centric DevSecOps
- Model-based and AI-driven Automated Security Orchestration, Trust Management and deployment
- Advanced AI-driven Anomaly Detection, decision and Mitigation Strategies
- Demonstration of a Set of Industrially Relevant Use Cases in Operational Environments

RIGOUROUS has received funding from the European Union's HE Research and Innovation Programme HORIZON-JU-SNS-2022 under Grant Agreement No 101095933

RIGOUROUS: secuRe desIGn and deplOyment of trUsthwoRthy cOntinUum computing 6G Services

RIGOUROUS



RIGOUROUS has received funding from the European Union's HE Research and Innovation Programme HORIZON-JU-SNS-2022 under Grant Agreement No 101095933

RIGOUROUS: Intent-based Security Management

Pushing past policy-based security management

Intent-based Security Management

Transforms abstract Protection Level and Security Level requirements into specific parameters for AI-driven Security Orchestrators. It provides a framework for defining Security Service Level Agreements (SSLAs), refines them into deployment-ready representations, enforces them in real time, and enables conflict detection.

Human Controllable Privacy

Assessment

Privacy Quantification Models assess the privacy levels of specified network services in real-time, and adopts a user-centric approach to comprehend associated privacy risks

Intent-based security formal modelling

Definition

Tools intended for DevSecOps to define, in a user-friendly way the security policies and intents aimed to rule the security operations in a multi-domain network

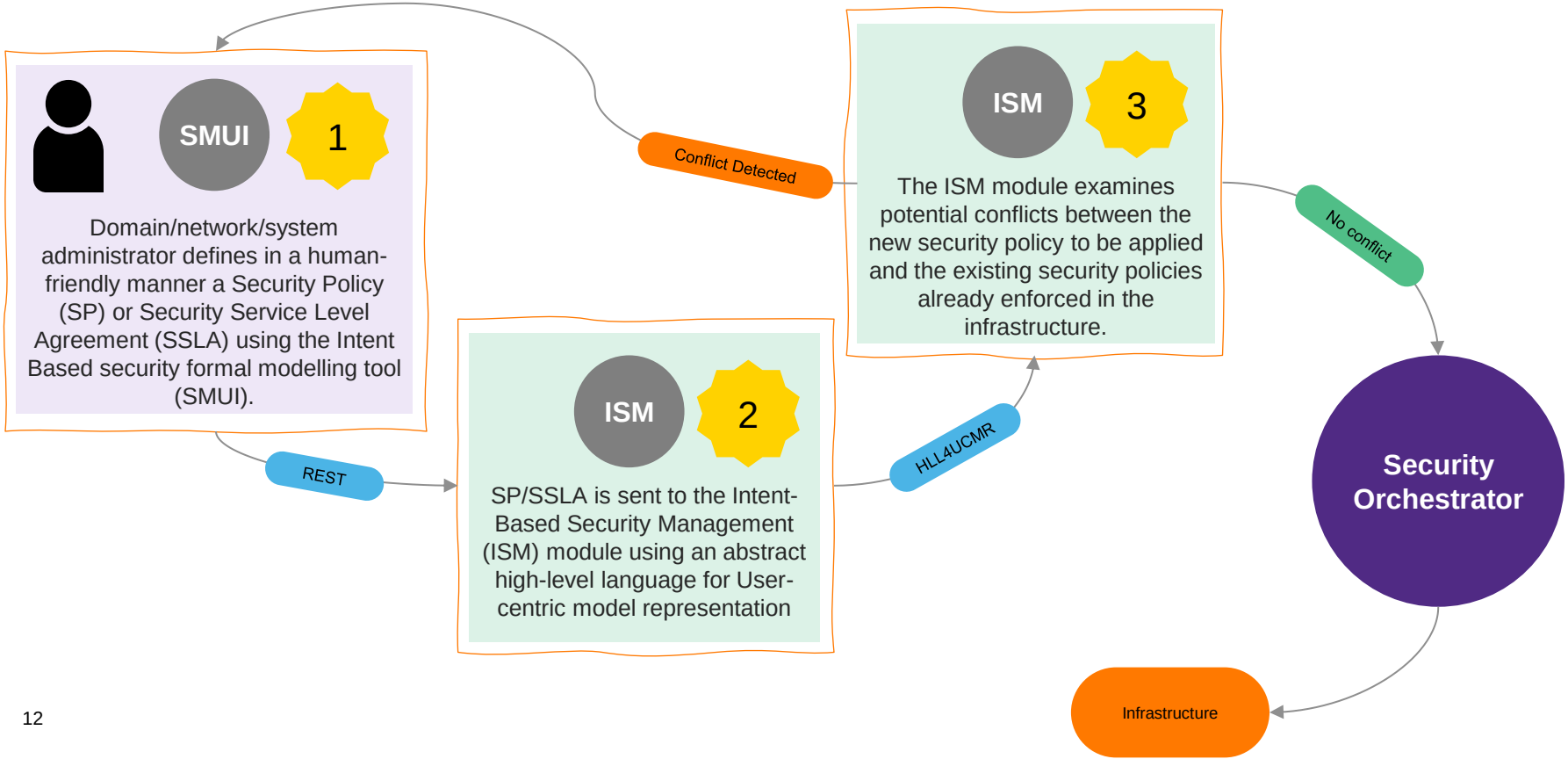
App Onboarding Specifications

Management

Configuration of the Policy Control Function (PCF) with operator-managed trusted apps; enables PCF to provision app configs to various UEs and IoT Devices

RIGOUROUS: Intent-based Security Management

An E2E Workflow

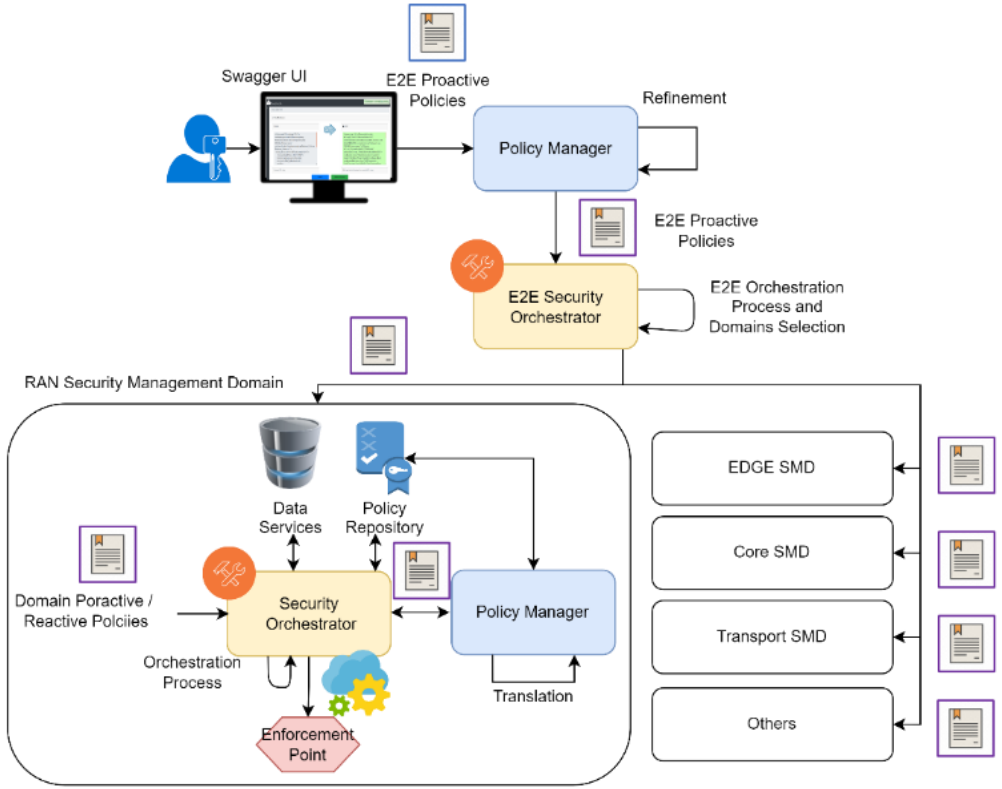


RIGOUROUS: E2E Multi-Domain Orchestration

Pushing past policy-based security management

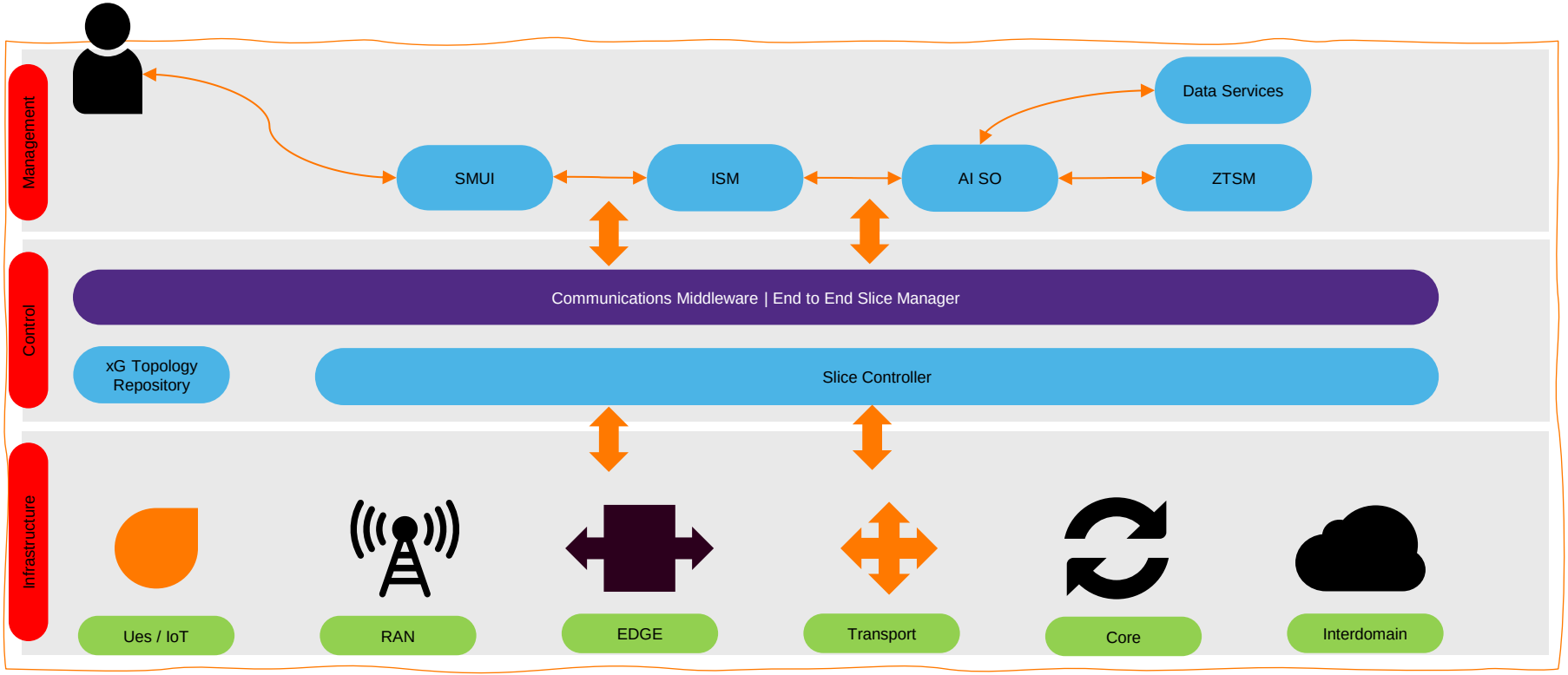
E2E Orchestrator

- The orchestrator will be driven by an A.I. model to make actuation and orchestration decisions
- This relies on modules to translate the intents, policies and behavioral profiles coming from the decision into concrete actions
- Federated Learning (FL) approach to make orchestration decisions
- Decide best actions for dynamic provisioning, deployment, and reconfiguration (during operation) of the virtual network security functions and associated intents and policies
- Orchestrator will consider the time and space varying parameters of the network, such QoS capacities, actual resources constraints (CPU, RAM, storage), system status, current deployed policies, and detection instances



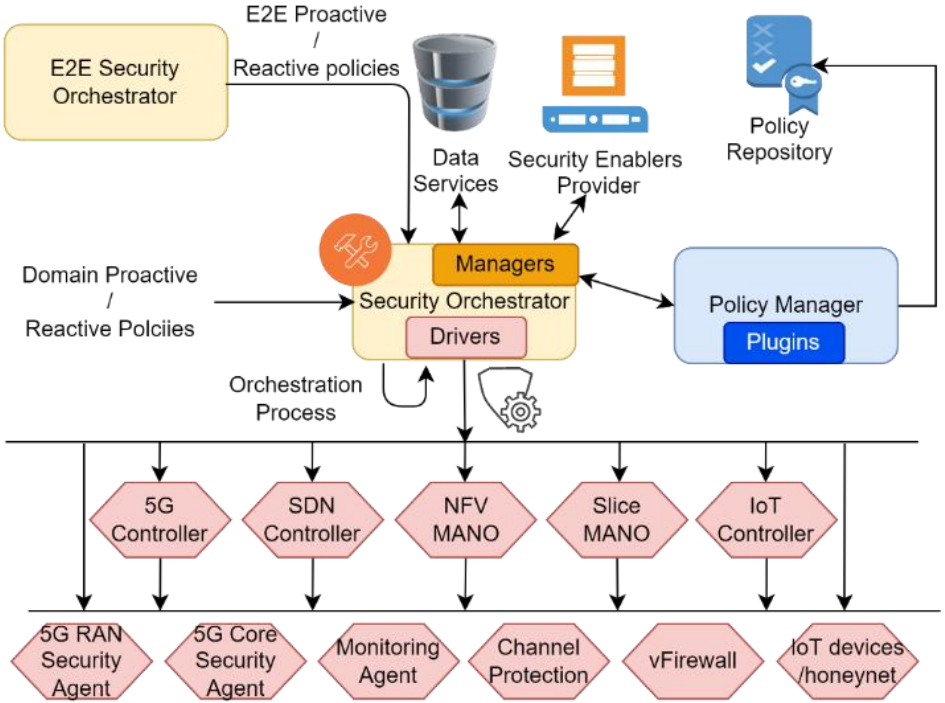
RIGOUROUS: E2E Multi-Domain Orchestration

The DevSecOps – Human in the loop - approach



RIGOUROUS: E2E Multi-Domain Orchestration

Orchestrator Policies Enforcement



Policies Enforcement

Common Policy Repository
Supports playbooks ingestion / translation

Plugin-based
Ease of deployment + 3rd party can write their own plugins

Proactive / Reactive Policies
Enables granularity for multi-domain specs

Drivers Reutilization
Existing drivers with common methods (APIs) can be reused

E2E
Existing drivers with common methods (APIs) can be reused

Orange Romania Use-Case

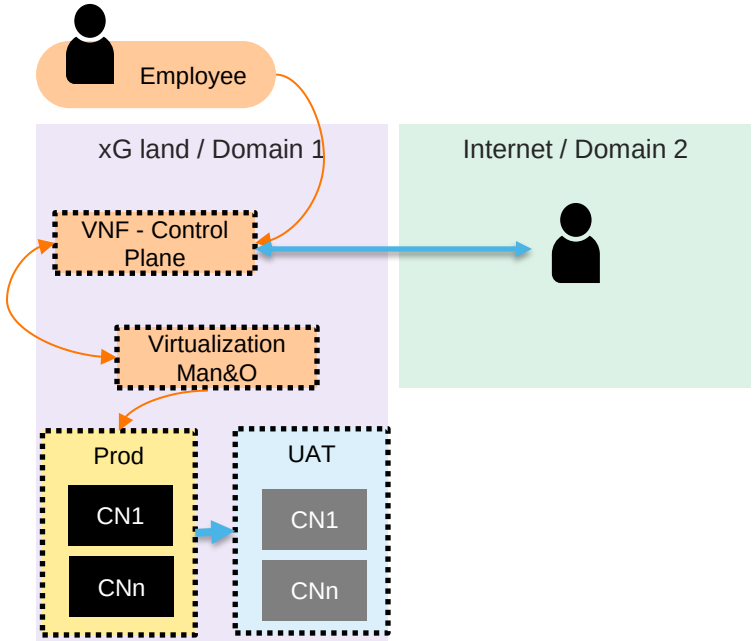
Protection of 6G-enabled Services against Cyber Threats

1

Unauthorized access to the 5G/6G Infrastructure through privilege abuse (insider threat) and by exploiting software vulnerabilities or erroneous configurations (external threat).

By Authentication Abuse:

1. ORO employee with access to administrative credentials to OROs Facility
2. Logs in from an unsanctioned terminal
3. Performs an action that changes the parameters of a VNF in production
4. Disrupts service availability and integrity of a B2B customer's frontend
5. Moves laterally through the 5G Facility
6. Gains access to 5G Virtualization Control Plane subsystems
7. Disrupts service continuity by migrating containers in production to a User Acceptance Test (UAT) environment.



Orange Romania Use-Case

Protection of 6G-enabled Services against Cyber Threats

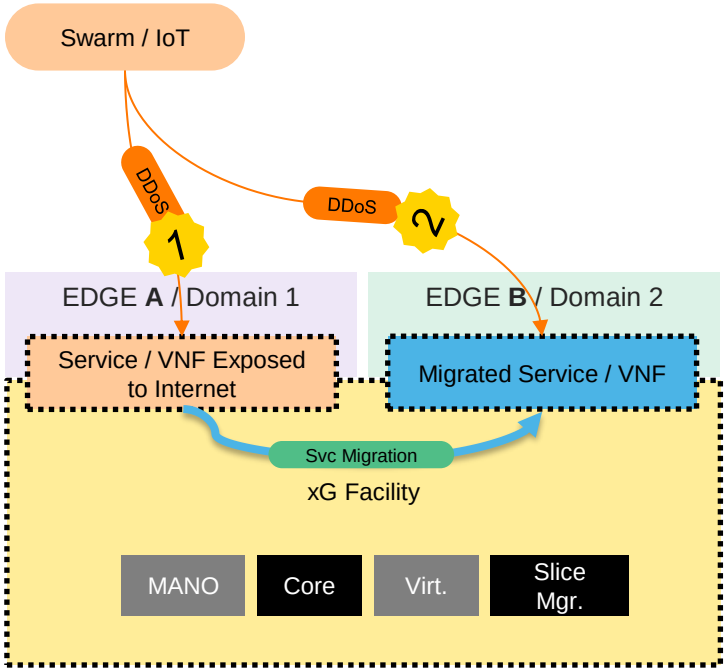
2

Abnormal Traffic / Distributed Denial of Service attack targeting System Components.

In this scenario, a **service** exposed through **an EDGE** component of ORO 5G Facility is **targeted and attacked** with a heavy load of unsolicited traffic, rendering the service unavailable to its intended consumers.

The service is a B2B Customer Web Portal, running atop a web server.

Although the application is decomposed and supported through microservices, with fast replication capabilities and resilience-by-design deployment, the unwanted traffic is generated from a potent **botnet** and the attackers successfully targets **subsequent iterations** of the service, on **different EDGE interfaces.**



Orange Romania Testbed

Orange 5G Lab

DevSecOps
Fully integrated
DevSecOps
environments

Testing Environment
Replicates production
xG Networks at scale

3GPP Release 16
Fully compliant Rel. 16
5G Facility

Collaborative
Built & Operated in
collaboration with
Technical Universities

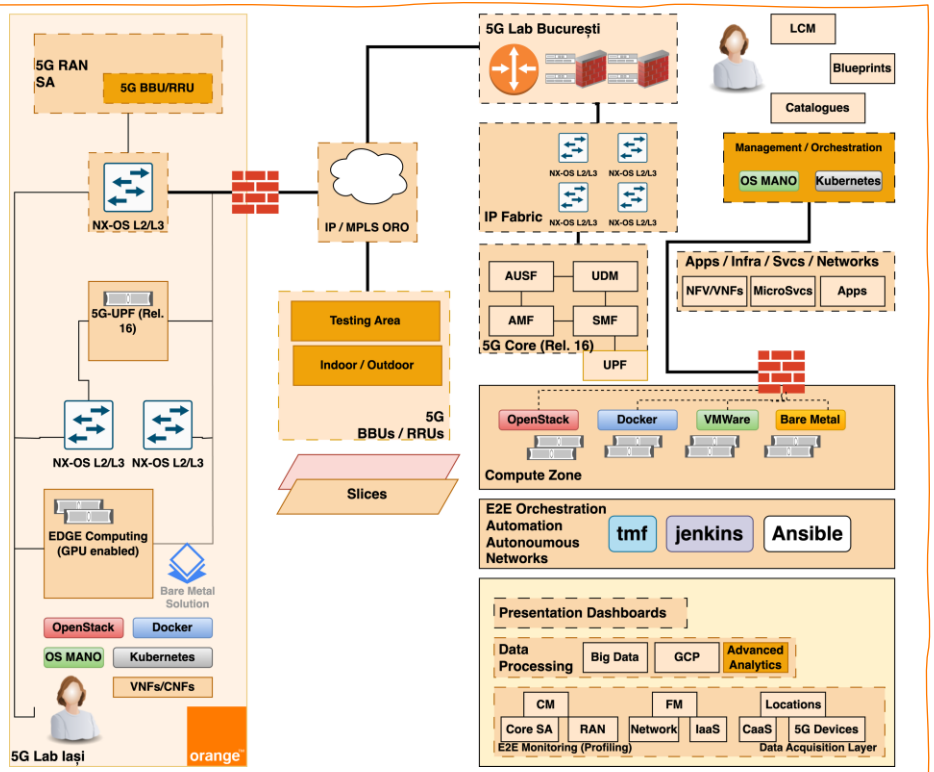
Multi-domain capable
2 (soon 3) 5G Labs,
can be used as multi-
domain environments

E2E
Provides xG E2E
Testing, Simulations,
Validation Capabilities

București
UPB

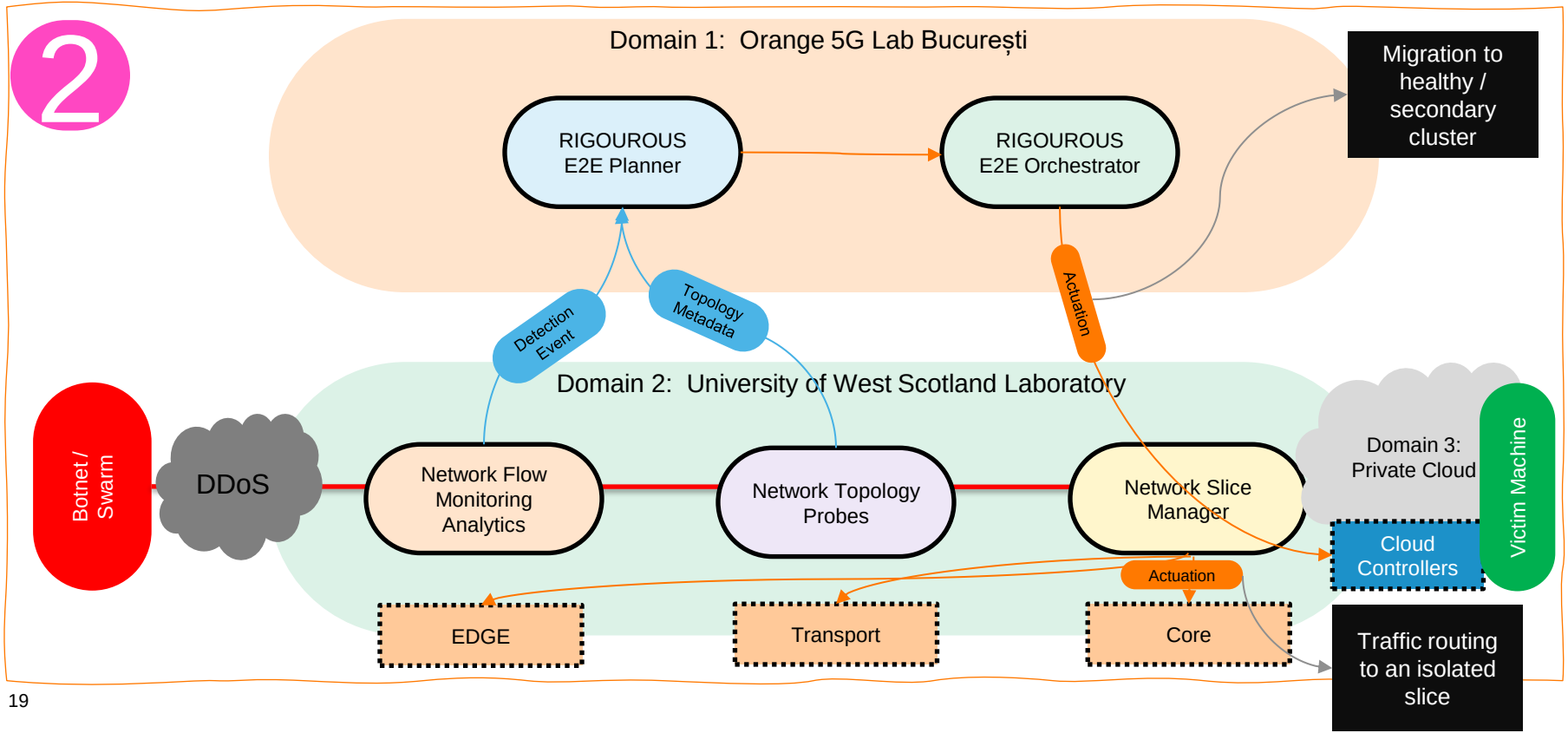
Iași
TUI

Performance
3200+ CPU Cores
20+ TB RAM
Up to 200 Gbps
Networks



Orange Romania Use-Case Piloting

Orange 5G Lab



Key Takeaways

1

Complexity

5G and future xG networks are flexible, efficient and complex. Complexity usually stems larger attack surface.

2

Devices

IoT Security is broken so 5G Networks need to address this at the Edge.

3

Threats

Large volume of new threats makes monitoring and mitigation a difficult endeavor. 5G Security will rely heavily on A.I. for increased visibility, anomaly detection and orchestration

4

Orchestration

Is essentials to ensuring reliable xG multi-domain communications

Thank you!