π-Edge Platform and OSM for Security Analytics Automation in Network Slicing

Alexandros Valantasis, Research Engineer
Nikos Psaromanolakis, Staff Research Engineer
Vasileios Theodorou, Senior Research Engineer
Intracom Telecom
Overview

• Motivation

• π-Edge Platform for Edge Computing Automation
  • High Level Architecture
  • Edge Catalogue
  • Security Services

• OSM for automated Security enrichment of slices at the Edge
  • Use case architecture/ workflow

• Demo
Motivation

• **π-Edge**: Edge Management Platform for **Edge Automation**:
  • Platform-as-a-Service (PaaS) delivery model*
  • Automation, maintainability & interoperability with centralized orchestrators (e.g., OSM)
  • Minimization of management overhead

• **Declarative Security Services** for Netw. Slices at the Edge
  • Edge Ecosystems & multi-tenant, multi-party environments → Trust, reliability & robustness to security threats
  • High level declaration of security services → **Zero-Touch** Slice LCM

*presented at OSM#12 Ecosystem Day
π-edge Platform: HL Architecture

**System Manager**

**Centralized NFV MANO**

**Cloud/Core**
- Backend Services
- Inter-domain Networking

**π-Edge Platform**
- Security Services
  - QoS Monitoring Service
  - AutoML (MLOps)
  - SDN Controller
  - Declarative API Gateway
  - Intelligent Edge Agent
  - Cluster Manager
  - IoT Platform
  - Edge Catalogue
  - MEC Services
  - 5G Core Integrator

**Edge Node**
- Virtual Netw. Infra
- Service Function1
- PaaS N
- gNodeB
- IoT GW
- RAN
- UPF
- Device 1
- Device N

© ETSI

OSM#13 Ecosystem Day, 15 June 2022
π-edge Platform: Edge Catalogue

- Edge Catalogue contains:
  - **Service Functions**
    - Smallest units of a deployment (container/pod, VM etc...)
  - **PaaS Services**
    - Each consists of a chain of Service Functions (one or more container/VMs towards an application logic)
  - **Edge Nodes**
    - Represent the supported edge nodes of the edge cluster
Security Services

- Declarative Security API GW
  - Receives request for activating/deactivating a “secured” slice
- Security Actuator & Observer
  - Configures slice VNFs (routes rules, enables security analysis)
  - Informed about the “security” status of each slice
- Search and Analytics Engine for DB persistence
- Monitoring and Interactive Visualization Application
  - Usable GUI for exploring security analytics
Security Services per Slice

- Security Analysis Service (SAS)
  - Supervises the “secured” slice
  - Continuously analyzes user-plane traffic and checks for weird logs per slice
  - Connected to search and analytics engine
  - Decides when the slice should be characterized as “non-trusted”
  - Acts to slice when needed

- Virtual Router
  - Connects the slice (user) VNFs and forwards the traffic to SAS for analysis

```
nst.yaml
...
  automation-service:
  - id: demo-sas
    type: security
    name: demo-sas-automation
    security-policy:
    - threat-type: DDOS
      on-detection: monitor_zoom-in
```

Extended Slice

Virtual Router

Security Services per slice
OSM towards an automated enrichment of slices at the Edge:

Use case

1. NST + NSD + VNFD with SAS field "TRUE"
2. NST + NSD + VNFD extended (with SAS and VyOS)
3. order v-resources (VMs, v-nets etc) for slice
4. instantiate VMs, v-nets etc for Slice
5. configure VNFs

Extended slice

VYOS

VNF1

VNF2

Slice 1

Security Support Services

ElasticSearch

Kibana

Edge Host

© ETSI

OSM#13 Ecosystem Day, 15 June 2022
OSM towards an automated enrichment of slices at the Edge: Use case

7. Identify Suspicious traffic pattern

7.a. inform about suspicious traffic in the slice

7.b. perform action

π-Edge Platform

Security Services
- Security API Gateway
- Security Actuator & Observer

Shared PaaS Services

Security Support Services
- ElasticSearch
- Kibana
Time for the Demo!
THANK YOU!

https://osm.etsi.org/

{savalant, nikpsarom, theovas}@intracom-telecom.com