PALANTIR

Practical Autonomous Cyberhealth for resilient SMEs & Microenterprises

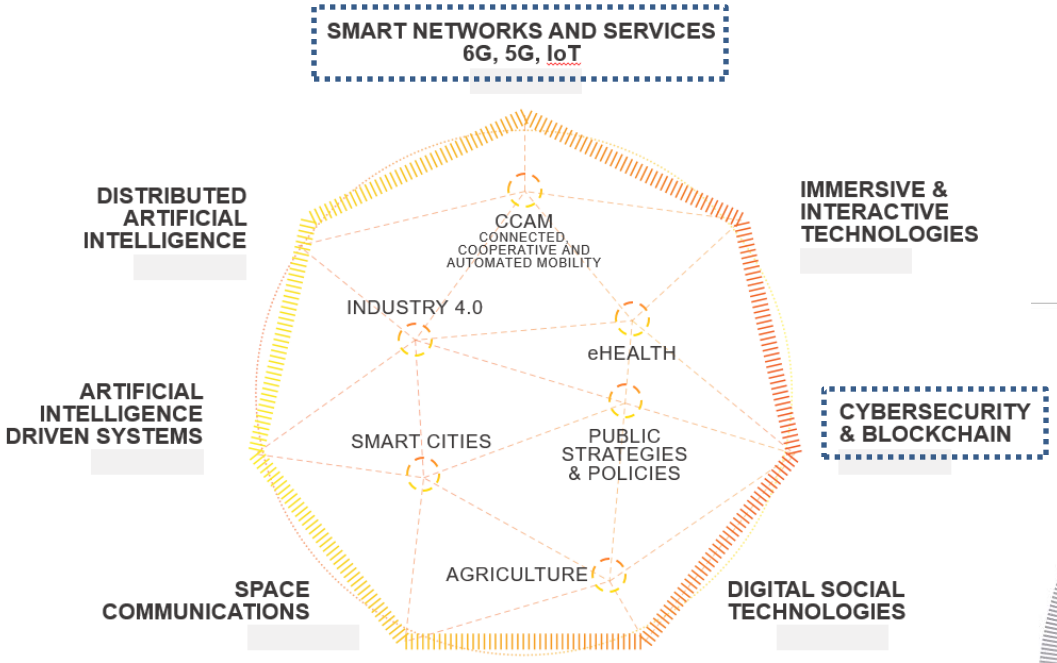
[H2020 – Grant Agreement No. 883335]

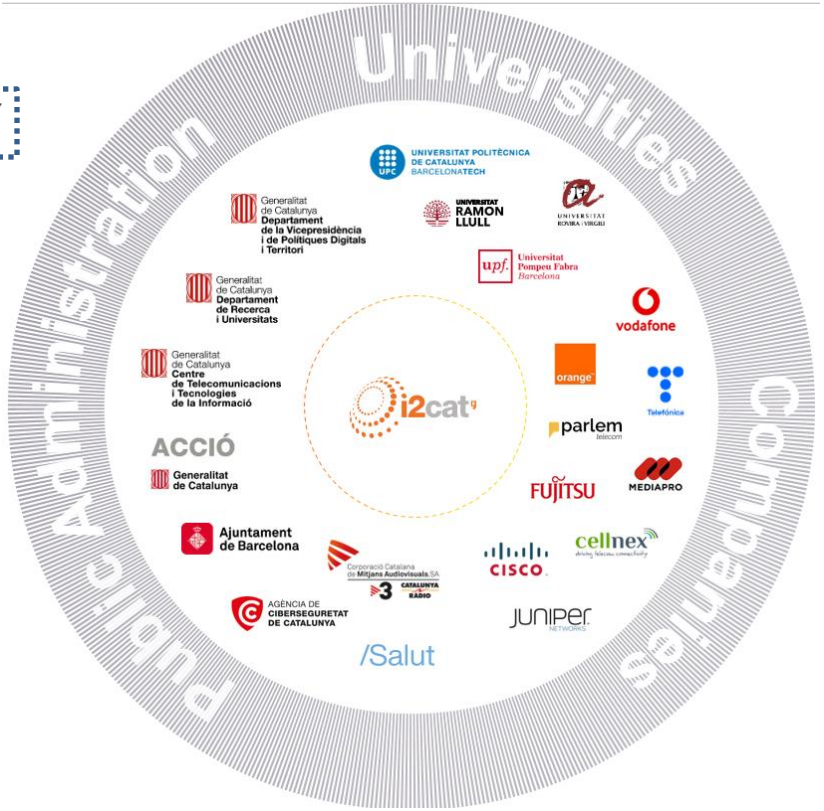
Usecase: SecaaS in Kubernetes

Carolina Fernández
Senior R&D Engineer @ i2CAT

GitOps TechDay Barcelona
November 30th, 2022
(UserZoom @ Barcelona)

About us


SMART NETWORKS AND SERVICES
6G, 5G, IoT
DISTRIBUTED ARTIFICIAL INTELLIGENCE
IMMERSIVE & INTERACTIVE TECHNOLOGIES
CCAM
CONNECTED, COOPERATIVE AND AUTOMATED MOBILITY
INDUSTRY 4.0
eHEALTH
ARTIFICIAL INTELLIGENCE DRIVEN SYSTEMS
CYBERSECURITY & BLOCKCHAIN
SMART CITIES
PUBLIC STRATEGIES & POLICIES
AGRICULTURE
SPACE COMMUNICATIONS
DIGITAL SOCIAL TECHNOLOGIES


Universities
Companies
Public Administration
UNIVERSITAT POLITÈCNICA DE CATALUNYA BARCELONATECH
Generalitat de Catalunya Departament de la Vicepresidència i de Polítiques Digitals i Territori
UNIVERSITAT RAMON LLULL
UNIVERSITAT ROVIRA I VIRGILI
Universitat Pompeu Fabra Barcelona
Generalitat de Catalunya Departament de Recerca i Universitats
vodafone
Generalitat de Catalunya Centre de Telecomunicacions i Tecnologies de la Informació
orange
Telefónica
i2cat
parlem
ACCIÓ
Generalitat de Catalunya
FUJITSU
MEDIAPRO
Ajuntament de Barcelona
cellnex
CISCO
AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA
juniper
/Salut

About me

Networking

- Automation
- Testbeds
- 5G / B5G / 6G

Virtualisation

- SDN / NFV
- Orchestration
- Private cloud

Security

- SECaaS
- DevSecOps

Problem and motivation

Cost of data breaches

$105k for SMBs

$101k ▲ $105k
2020 2021

IT security budget

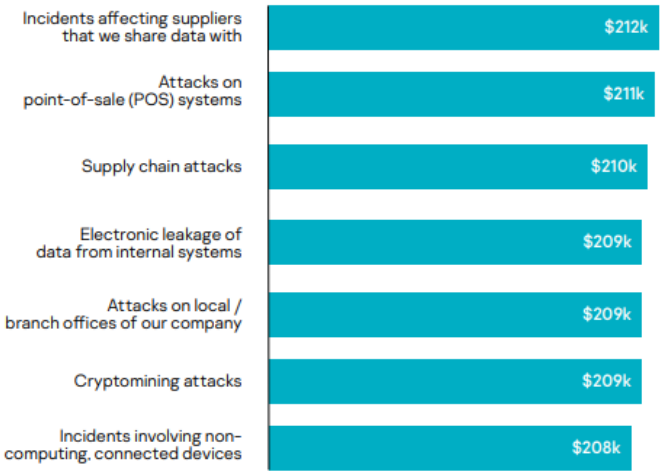
$267k for SMBs

$275k ▼ $267k
2020 2021

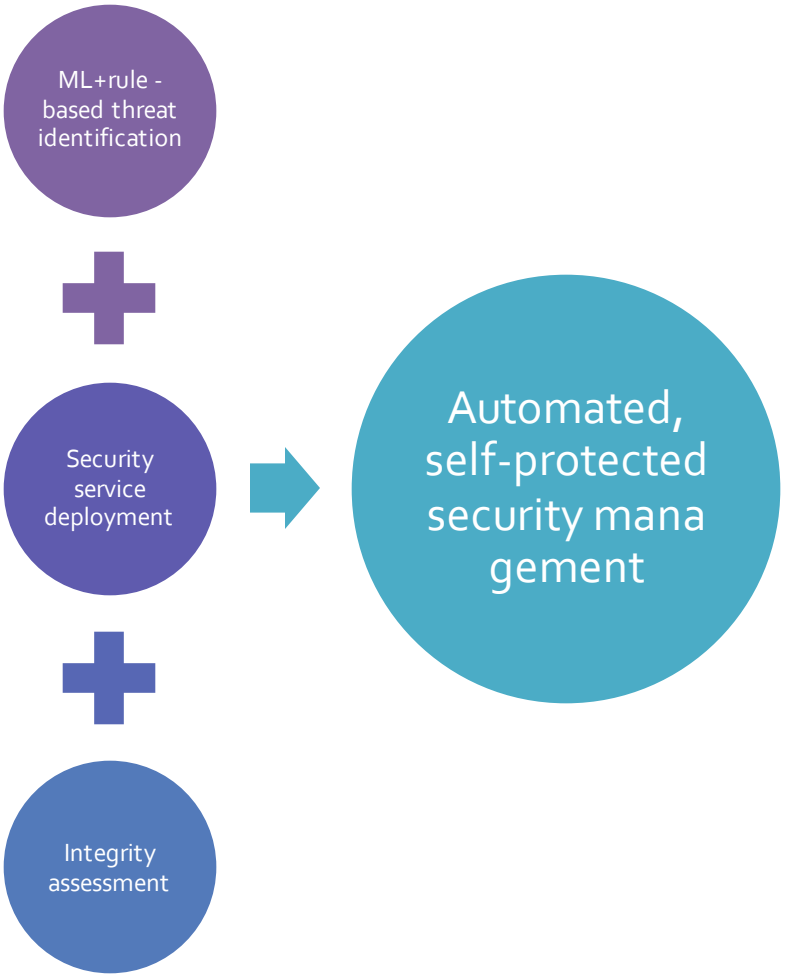
SMBs

	2018	2019	2020	2021
Average IT budget	$1.1m	$1.2m	$1.1m	$1.0m
Average IT security budget	$256k	$267k	$275k	$267k
Expected growth of IT security budget (over three years)	+14%	+11%	+12%	+12%

SMB



Source: https://go.kaspersky.com/rs/802-IJN-240/images/Kaspersky_IT%20Security%20Economics_report_2021.pdf



Background: *Ops

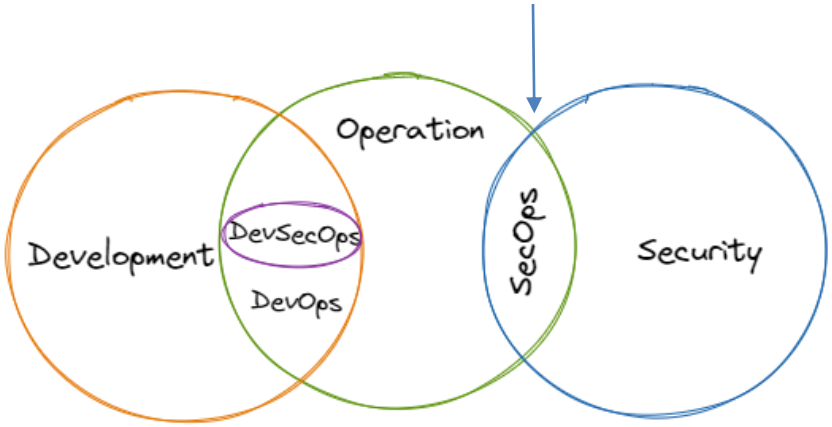
Idea: bring together best practices from multiple domains to accommodate them smoothly, at different levels and as early as possible ("shift-left") in the workflow.

DevSecOps

introduces security earlier in the life cycle of the application development to (i) reduce vulnerabilities and to (ii) align security to IT and business objectives from their conception.

SecOps

integrates security and operation teams and, differently to *DevSecOps*, focuses on securing the application (and systems) along with their maintenance.

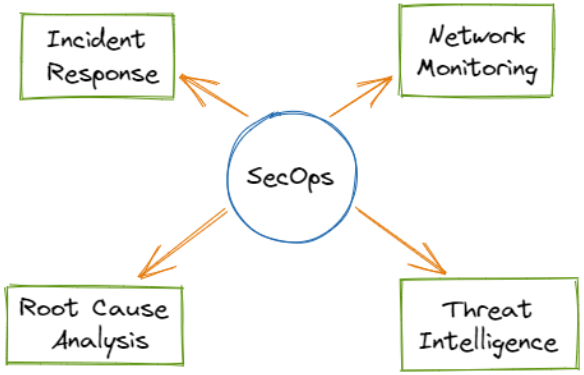


Source: https://www.atatus.com/glossary/secops/

Background: SecOps

Some functions from the security teams will be shared across security and operations:

- Network monitoring: find anomalous events related to security.
- Threat intelligence: gather data on the security events to identify their behaviour and how to react to them.
- Root cause analysis: pinpoint the underlying cause of a security event.
- Incident response: react to such security events.



Source: https://www.atatus.com/glossary/secops/

However, some businesses may lack one or even all departments.
E.g. a small business that employs, if at all, a moderate network-savvy operator.

Background: SECaaS

- Business model in which a Managed Security Service Provider (MSSP) integrates their security services into the infrastructure of a business.
- Based in the SaaS model, working with subscriptions.
- More cost-efficient than if self-managed.

Source: https://outpost24.com/services/managed-services

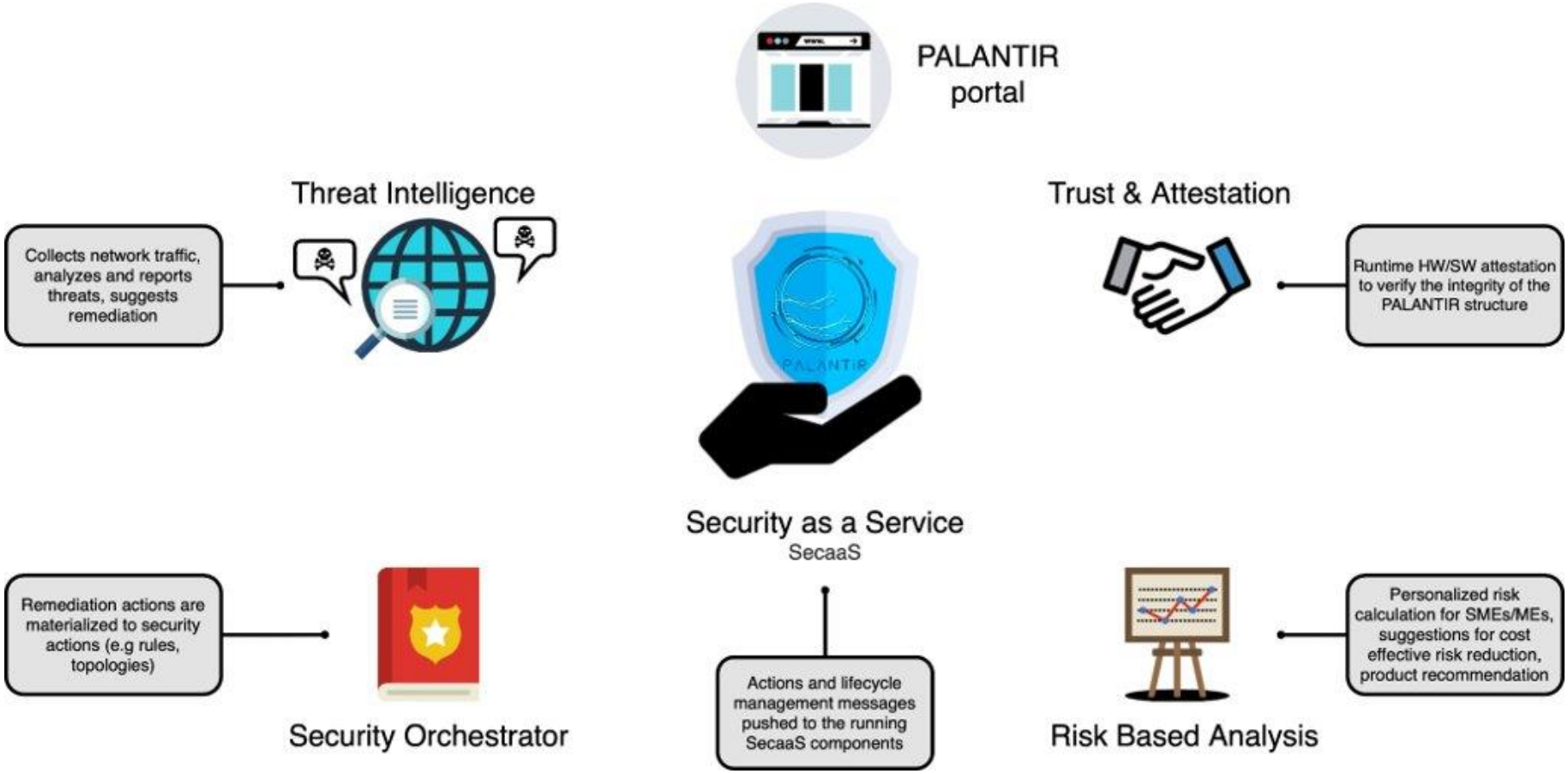
Examples of Security Services:

- Data loss prevention.
- Network security.
- Vulnerability scanning.

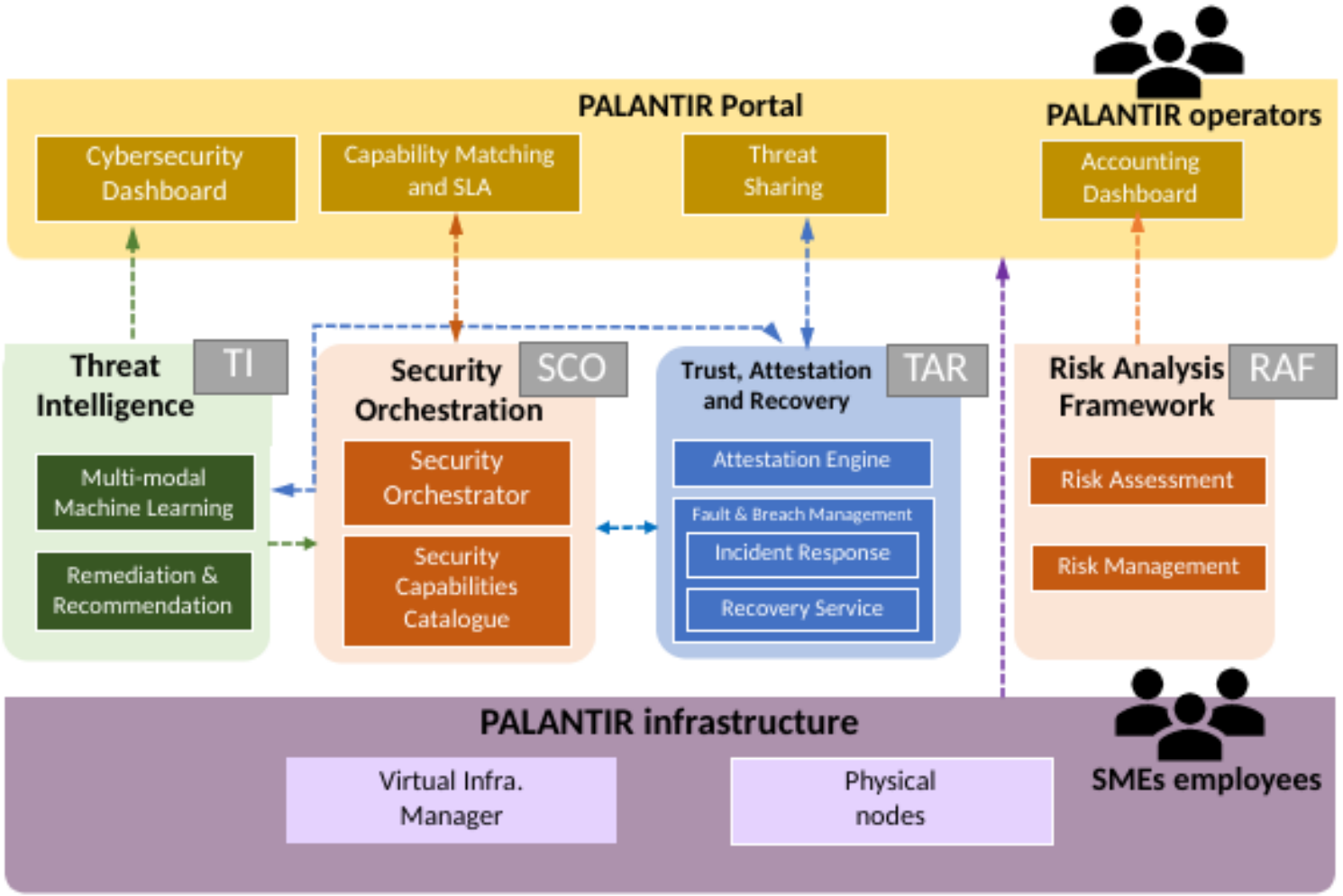
Source: https://teamascend.com/managed-security/

Automating security and explaining security options contributes to alleviate the shortage of knowledge.

The PALANTIR SecaaS platform



PALANTIR architecture



PALANTIR env: service orchestration in the cloud

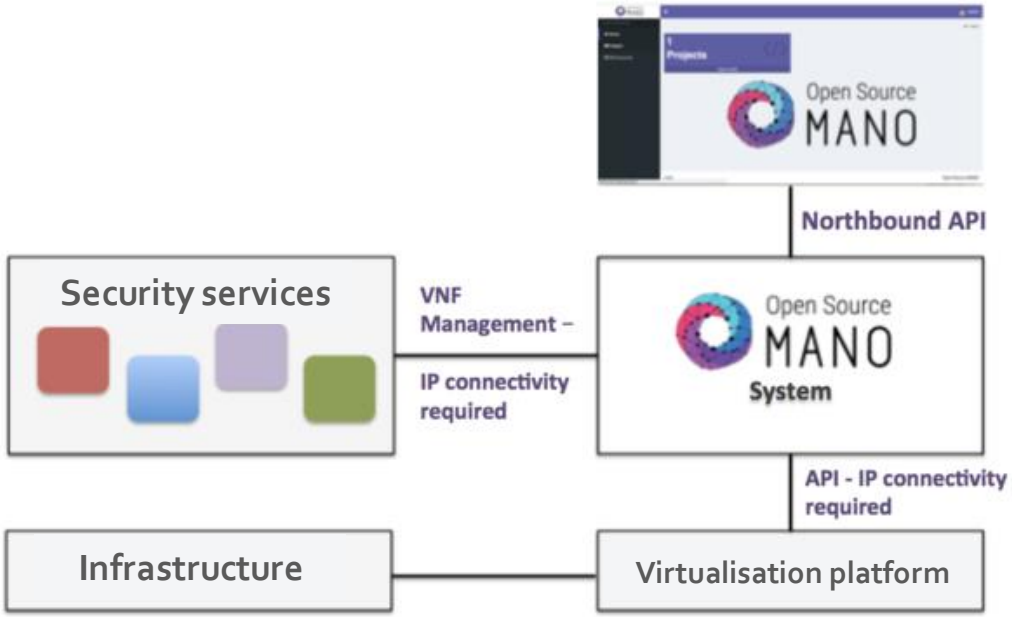
OSM is a service orchestrator that

supports VMs and containers in private (OpenStack, VMware, K8s) and public (AWS, Azure) clouds and

configures services dynamically at multiple points (through Juju)

Services are packaged and described for OSM to handle their lifecycle:

- Instantiation.
- Custom configuration and scaling.
- Deletion.



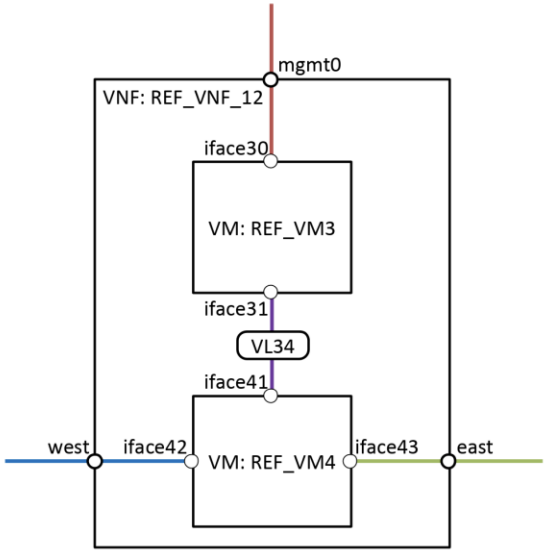
(Modified)
Source: https://osm.etsi.org/docs/user-guide/latest/03-installing-osm.html

PALANTIR env: automated ops for security services

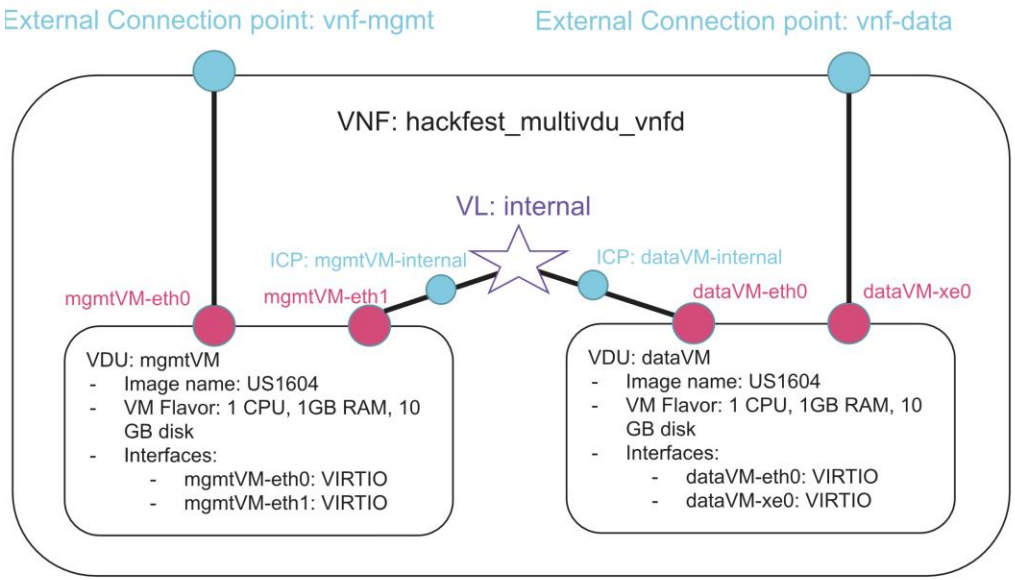
The security services are abstracted through an OSM package, containing:

- OSM descriptor.
- Helm chart (optional, for complex deployments).
- Juju charm (optional, for extra runtime configuration).

And then deployed via K8s.



Source: https://osm.etsi.org/gitlab/vnf-onboarding/vnf-onboarding-guidelines/-/blob/master/o1-requirements.md



Source: https://osm.etsi.org/gitlab/vnf-onboarding/vnf-onboarding-guidelines/-/blob/master/o2-dayo.md

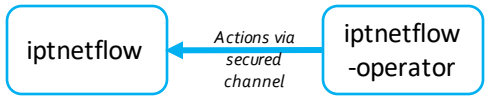
PALANTIR env: automated ops for security services

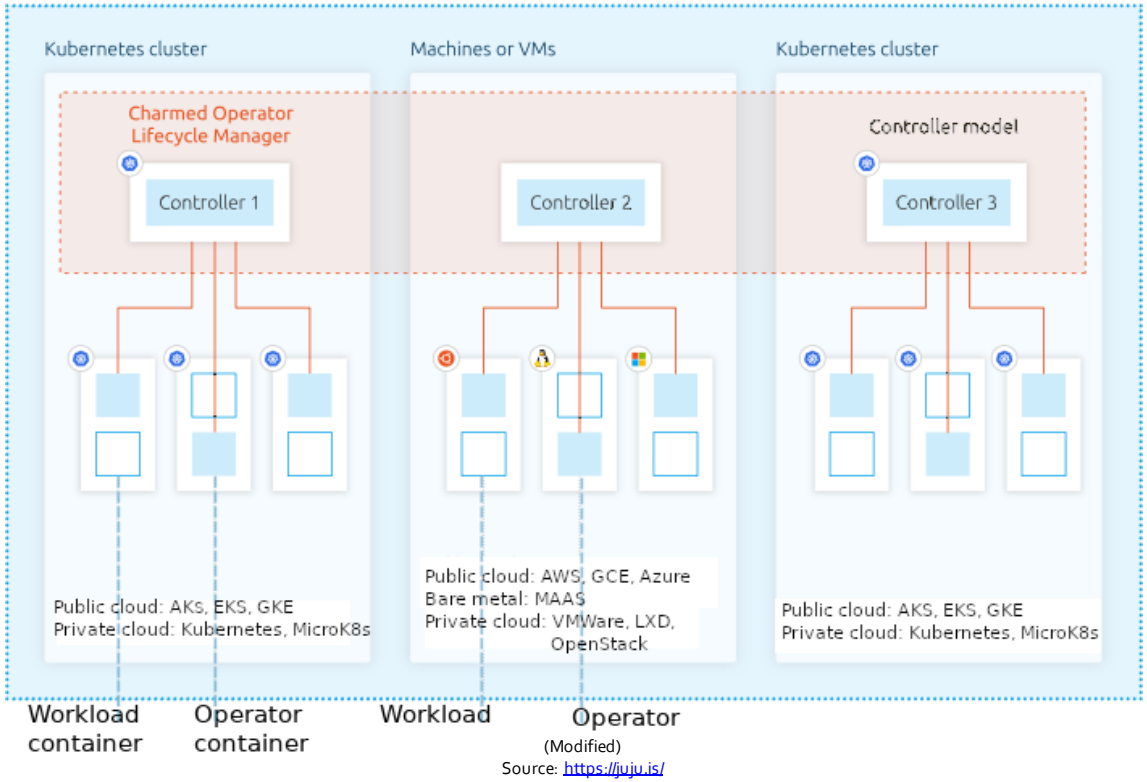
The security services are abstracted through an OSM package, containing:

- OSM descriptor.
- Helm chart (optional, for complex deployments).
- Juju charm (optional, for extra runtime configuration).

And then deployed via K8s.

```
palantir@osm:~$ kubectl get pod -n iptnetflow-kdu
NAME                                READY   STATUS
iptnetflow-79b77668c9-wt4vh         1/1     Running
iptnetflow-operator-0               1/1     Running
modeloperator-8448c9c8d5-2bblw      1/1     Running
```





(Modified)
Source: https://juju.is/

PALANTIR env: automated ops for security services

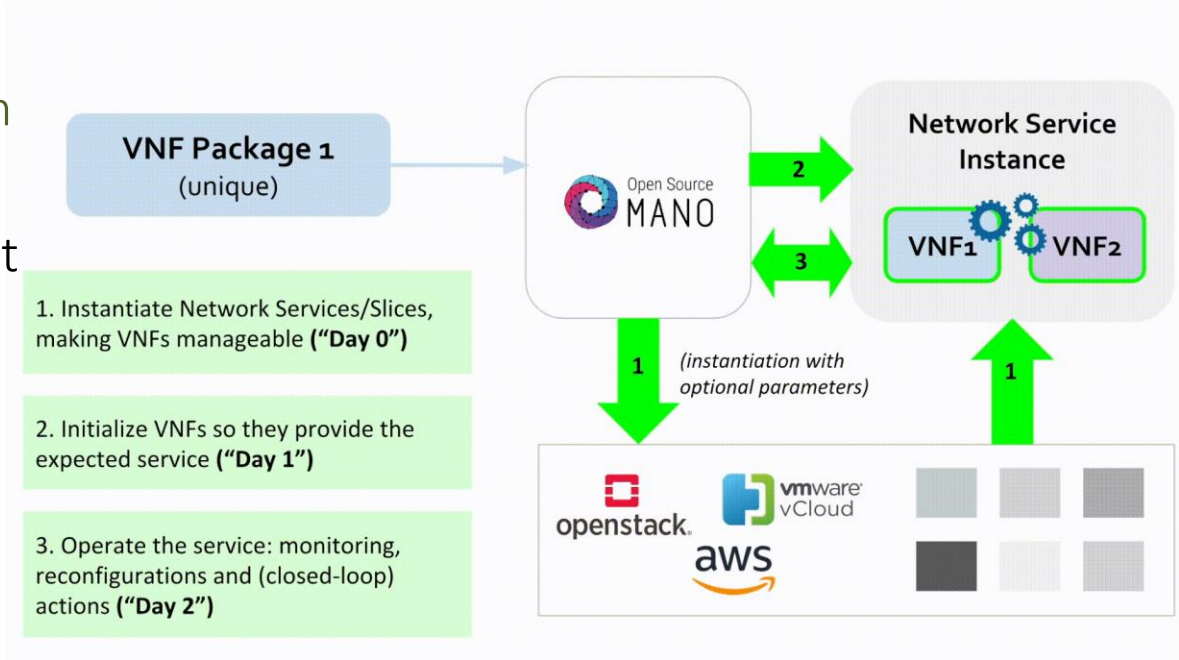
The security services are abstracted through an OSM package, containing:

- OSM descriptor.
- Helm chart (optional, for complex deployments).
- Juju charm (optional, for extra runtime configuration).

And then deployed via K8s.

Why bundling everything in a new package?

It abstracts the deployment & provides extra functionality supported by OSM (day0/1/2 actions to configure at instantiation, boot and runtime).



Source: https://osm.etsi.org/gitlab/vnf-onboarding/vnf-onboarding-guidelines/-/blob/master/oo-introduction.md

PALANTIR env: security services

- Intrusion Detection System (IDS)
- Deep Packet Inspection (DPI)
- Network Netflow Sniffer (NNS)
- Lightweight Shipper for Logs (L-SL)
- Firewall and Router (FW)
- Wazuh (SIEM)
- Web-based Traffic Analysis (WTA)
- Virtual Private Network (VPN)

snort, suricata

ipt-netflow

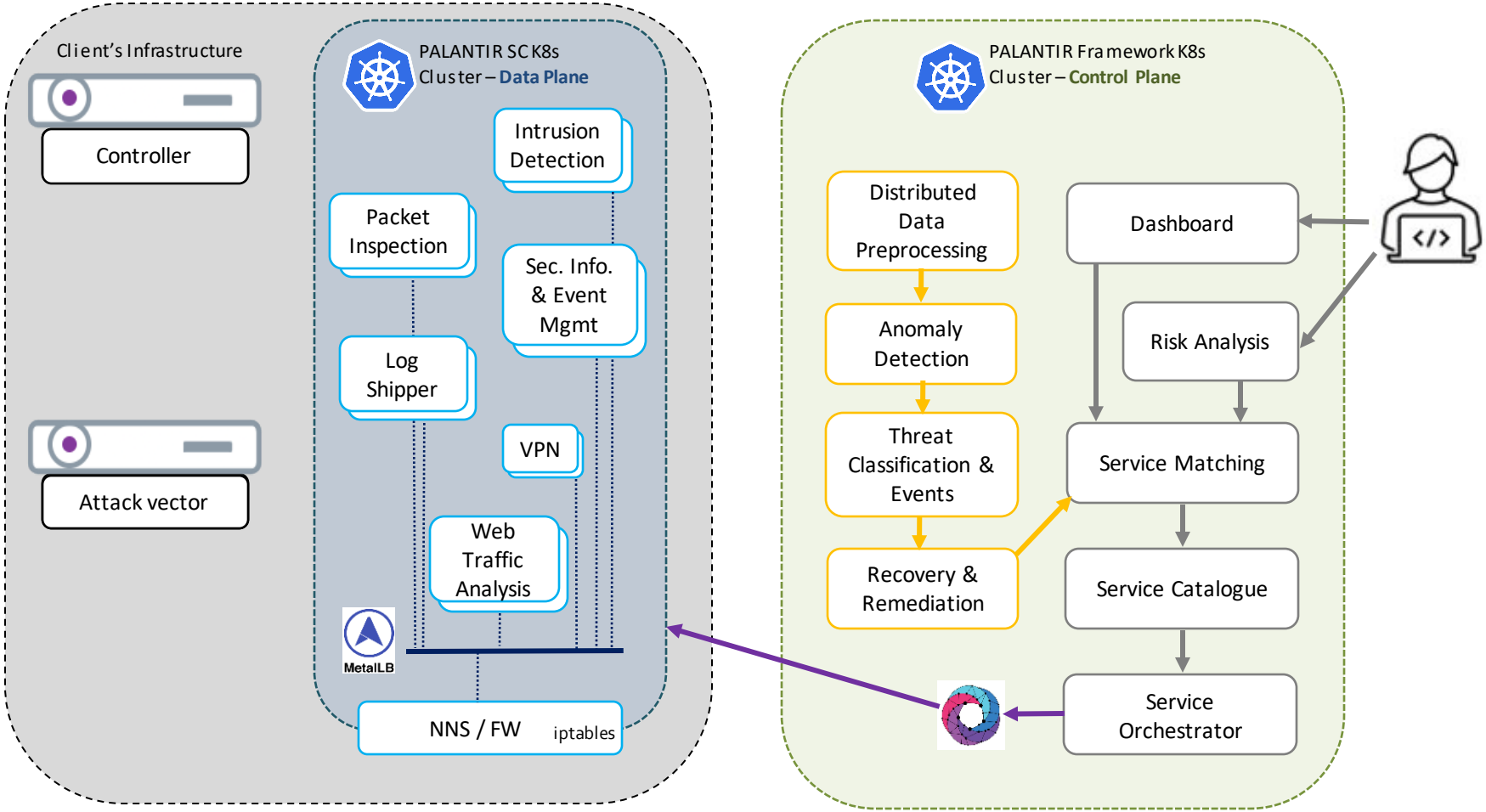
descriptors (packages)

```
descriptor-packages/
├── nsd
│   ├── dpi_ns
│   │   ├── snort_ns
│   │   │   └── snort_cnf_nsd.yaml
│   │   └── suricata_ns
│   │       └── suricata_cnf_nsd.yaml
│   └── iptnetflow_ns
│       └── iptnetflow_cnf_nsd.yaml
└── xnfd
    ├── dpi_cnf
    │   ├── snort_cnf
    │   │   ├── juju-bundles
    │   │   │   ├── bundle.yaml
    │   │   │   └── snort_ubuntu-20.04-amd64.charm
    │   │   └── snort_cnfd.yaml
    │   └── suricata_cnf
    │       ├── juju-bundles
    │       │   ├── bundle.yaml
    │       │   └── suricata_ubuntu-20.04-amd64.charm
    │       └── suricata_cnfd.yaml
    └── iptnetflow_cnf
        ├── iptnetflow_cnfd.yaml
        └── juju-bundles
            ├── bundle.yaml
            └── iptnetflow_ubuntu-20.04-amd64.charm
```

charms (cloud actions)

```
juju-charms/
├── dpi
│   ├── snort
│   │   ├── actions.yaml
│   │   ├── charmcraft.yaml
│   │   ├── config.yaml
│   │   ├── metadata.yaml
│   │   ├── requirements-dev.txt
│   │   ├── requirements.in
│   │   ├── requirements.txt
│   │   ├── run_tests
│   │   ├── snort_ubuntu-20.04-amd64.charm
│   │   ├── src
│   │   │   └── charm.py
│   │   └── test_charm.py
│   └── suricata
│       ├── actions.yaml
│       ├── charmcraft.yaml
│       ├── config.yaml
│       ├── metadata.yaml
│       ├── requirements-dev.txt
│       ├── requirements.in
│       ├── requirements.txt
│       ├── run_tests
│       ├── src
│       │   └── charm.py
│       ├── suricata_ubuntu-20.04-amd64.charm
│       └── test_charm.py
└── iptnetflow
    ├── actions.yaml
    ├── charmcraft.yaml
    ├── config.yaml
    ├── iptnetflow_ubuntu-20.04-amd64.charm
    ├── metadata.yaml
    ├── requirements-dev.txt
    ├── requirements.in
    ├── requirements.txt
    ├── run_tests
    ├── src
    │   └── charm.py
    └── test_charm.py
```

PALANTIR env: K8s clusters for control and data



PALANTIR env: considerations & lessons learnt

OSM and services

- Snapshots (K8s status) and services' backups are lifesavers.
- Iterate on services to expose extra logic via day-2 operations (e.g. service internal status for monitoring).

Kubernetes for OSM

- Tailored K8s deployment: OpenEBS for PV and PVC management, MetalLB for L2 service exposure in specific network segment.
- Specific version (1.23.x, *pre-containerd*).

Kubernetes

- Restriction on #instances exposing ports to the port (e.g. FW).
- Frequently review for issues if resources are constrained, e.g. *NodePressure* if limiting deployment to specific workers with TPM.

Further information

https://www.palantir-project.eu

https://twitter.com/ProjectPalantir

https://cutt.ly/dJgx7Pn

info@palantir-project.eu

PALANTIR has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No. 883335