Co-funded by the Horizon 2020
Framework Programme of the European Union

Practical Autonomous Cyberhealth for resilient SMEs & Microenterprises

Grant Agreement No. 883335
Research Innovation Action (RIA)

D2.2 Use Cases, Threat analysis & AS-based risk assessment

Document Identification			
Status	Final	**Due Date**	28-02-2021 (M6)
Version	1.0	**Submission Date**	26-02-2021 (M6)

Related WP	WP2	**Dissemination Level (*)**	PU
Related Deliverable(s)	D2.1, D2.3, D2.4		
Lead Participant	INFILI	**Lead Author**	Dimitris Papadopoulos (INF)
Contributors	PALANTIR consortium	**Reviewers**	Angeliki Kapodistria (SPH)
			Dimitris Paraschos (SSE)

Keywords:
Use cases, threat analysis, attack surface, risk-based assessment, actors, scenarios

This document is issued within the frame and for the purpose of the *PALANTIR* project. This project has received funding from the European Union's Horizon2020 Framework Programme under Grant Agreement No. 883335. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the European Commission.

Document Information

List of Contributors	
Name	Partner
Dimitris Papadopoulos, Antonis Litke, Evangelos Mantas	INFILI
George Athanasiou	DBC
Carolina Fernández, Shuaib Siddiqui, Jordi Guijarro, Nil Ortiz, Albert Calvo, Josep Escrig	I2CAT
Gregorio Martinez Perez, Antonio Lopez Martinez, Manuel Gil Perez, Felix Gomez Marmol	UMU
Georgios Gardikis	SPH
Ludovic Jacquin	HPLEB
Davide Sanvito, Roberto Bifulco	NEC
Diego López, Antonio Pastor Perales, Jerónimo Núñez Mendoza	TID
Vangelis Logothetis, Ioannis Neokosmidis	INCITES
Anastasios Kourtis, Andreas Oikonomakis, Dimitris Santorinaios	NCSRD
Akis Kourtis, George Xilouris	ORION
Dimitrios Klonidis, Dimitrios Alexandrou	UBITECH
Izidor Mlakar	SFERA

Document History			
Version	Date	Change editors	Changes
0.1	11/12/20	INF	First draft with proposed structure
0.2	27/01/21	INF	Merged partners' contributions
0.3	28/01/21	INF	Added Section 3 inputs
0.4	05/02/21	INF	Edited contributions and formatting, added linking/introductory texts on sections
0.5	11/02/21	INF	Added exec. summary, intro, conclusions and Section 2 figures
0.6	15/02/21	INF	Added step-by-step description of UCs, acronyms, improved formatting.
0.7	18/02/21	INF	Prefinal, ready for internal review
0.8	23/02/21	INF	Integrated comments from peer review
1.0	25/02/21	INF	Final version

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	INFILI	23/02/21
Quality manager	INFILI	24/02/21
Project Coordinator	DBC	26/02/21

Table of Contents

Document Information 3
Table of Contents 4
List of Tables 5
List of Figures 6
List of Acronyms 7
Executive Summary 9
1. Introduction 10
1.1. Objectives and goals of the deliverable 10
1.2. Relation with D2.1 and other WPs 10
2. Use Case Analysis 12
2.1 Use Case #1: Securing private medical practices with lightweight SecaaS 12
2.1.1 Motivation and Overall Description 12
2.1.2 Actors Definition and Mode of Interaction 12
2.1.3 Use Case Detailed Description 13
2.1.4 Hosting Infrastructure 18
2.2 Use Case #2: Uninterrupted Electronic Commerce with Cloud SecaaS 19
2.2.1 Motivation and Overall Description 19
2.2.2 Actors Definition and Mode of Interaction 20
2.2.3 Use Case Detailed Description 21
2.2.4 Hosting Infrastructure 27
2.3 Use Case #3: Live Threat Intelligence Sharing in a large-scale Edge scenario 28
2.3.1 Motivation and Overall Description 28
2.3.2 Actors Definition and Mode of Interaction 29
2.3.3 Use Case Detailed Description 30
2.3.4 Hosting Infrastructure 34
3. Threat Analysis 37
3.1. Attack Surface Analysis 37
3.1.1 Possible Types of Attacks 38
3.1.2 Overview of Attack Vectors 40
3.1.3 Attack surface analysis of related projects 42
3.2. Risk-Based assessment 45
3.2.1 Risk assessment frameworks survey 45
3.2.2 PALANTIR Risk Assessment approach 50
3.2.3 Preliminary Use Case Risk Assessment 51
4. Conclusions 61
5. References 62
6. Annex A: Consolidated Stakeholders table 64

List of Tables

Table 1: UC1 Actors interactions with PALANTIR *13*
Table 2: Step-by-step view of UC1: Securing private medical practices with lightweight SecaaS *14*
Table 3: UC2 Actors interactions with PALANTIR *20*
Table 4: Step-by-step view of UC2: Uninterrupted Electronic Commerce with Cloud SecaaS *21*
Table 5: UC3 Actors interactions with PALANTIR *29*
Table 6: Step-by-step view of UC3: Live Threat Intelligence Sharing in a large-scale Edge scenario *30*
Table 7: Attack surface analysis of relevant projects *43*
Table 8: ENISA and NIST framework comparison *49*
Table 9: ENISA and NIST resources comparison *50*
Table 10: Risk Assessment for UC1: Securing private medical practices with lightweight SecaaS *52*
Table 11: Risk Assessment for UC2: Uninterrupted Electronic Commerce with Cloud SecaaS *54*
Table 12: Risk Assessment for UC3: Live Threat Intelligence Sharing in a large-scale Edge scenario *59*
Table 13: Consolidated Stakeholders list *64*

List of Figures

Figure 1: Conceptual view of the PALANTIR solution *11*
Figure 2: Actor diagram for UC1: Securing private medical practices with lightweight SecaaS *14*
Figure 3: Sequence diagram for UC1: Securing private medical practices with lightweight SecaaS *18*
Figure 4: ORION Athens NFVI-PoP and related infrastructure *19*
Figure 5: Actor diagram for UC2: Uninterrupted Electronic Commerce with Cloud SecaaS *21*
Figure 6: Sequence diagram for UC2: Uninterrupted Electronic Commerce with Cloud SecaaS *26*
Figure 7: Slovenian testbed and related infrastructure *27*
Figure 8: Actor diagram for UC3: Live Threat Intelligence Sharing in a large-scale Edge scenario *30*
Figure 9: Sequence diagram for UC3: Live Threat Intelligence Sharing in a large-scale Edge scenario *33*
Figure 10: 5GENESIS Athens platform infrastructure *34*
Figure 11: 5TONIC infrastructure *35*
Figure 12: Attack surface analysis asset classification *38*
Figure 13 Threat taxonomy *40*
Figure 14: NIST Core component and functions *46*
Figure 15: NIST risk management framework (RMF) workflow steps *47*
Figure 16: ENISA overall cycle of a Risk Management process *48*
Figure 17: ENISA SME Framework *51*

List of Acronyms

Abbreviation / acronym	Description
BYOD	Bring Your Own Device
CAPEC	Common Attack Pattern Enumeration and Classification
CAPEX	Capital Expenditure
CRM	Customer Relationship Management
CSP	Cloud Solution Provider
CVE	Common Vulnerabilities and Exposures
DNS	Domain Name System
ENISA	European Union Agency for Cybersecurity
EPC	Evolved Packet Core
FTP	File Transfer Protocol
GUI	Graphical User Interface
iSCSI	Internet Small Computer Systems Interface
ISP	Internet Service Provider
KVM	Kernel Virtual Machine
LAN	Local Area Network
LTE	Long Term Evolution
ME	MicroEnterprise
MEC	Multi-Access Edge Computing
MISP	Malware Information Sharing Platform
NAT	Network Address Translation
NFC	Near Field Communication
NFV	Network Functions Virtualization
NFVO	Network Function Virtualisation Orchestration
NIST	National Institute of Standards and Technology
NSA	Non-Standalone
OFDM	Orthogonal Frequency Division Multiplexing
OSM	Open-Source MANO
PAN	Personal Area Network
RAN	Radio Access Network
PoP	Point of Presence
SA	Stand Alone
SAS	Serial Attached SCSI
SDN	Software-Defined Networking
SFTP	Secure File Transfer Protocol
SLA	Service-Level Agreement
SQL	Structured Query Language
UC	Use Case
VIM	Virtualized Infrastructure Manager
VNF	Virtualized Network Function
WAN	Wide Area Network

Abbreviation / acronym	Description
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
5G PPP	5G Infrastructure Public Private Partnership

Executive Summary

The present document summarises the main findings and conclusions of the project activities related to the identification of the PALANTIR use cases (UC) and the consolidation of the Threat analysis & AS-based risk assessment methodology.

PALANTIR provides a multi-layered, infrastructure-wide approach for threat monitoring, cyber-resiliency and knowledge sharing in heterogeneous ecosystems, building upon the features of Software-Defined Networking (SDN), scalable machine learning towards hybrid Threat Intelligence, attestation techniques for secure infrastructure and trusted services, as well as standardization and threat-sharing methods to risk analysis, network operation, monitoring and management.

In order to address the diverse landscape of security requirements, PALANTIR offers a variety of SecaaS delivery modes (cloud/light/edge), showcased through an equal number of use cases, allowing clients to select the level of protection that best fits their needs but also the level of information they would like to communicate to/receive from other SecaaS users.

The three use cases that were identified as most relevant for the PALANTIR framework are the following:

- Use Case #1 *"Securing private medical practices with lightweight SecaaS"*, where PALANTIR will leverage a Lightweight SecaaS gateway to ensure the uninterrupted access of healthcare professionals to sensitive patient data, while hardening their infrastructure against different attack modalities,
- Use Case #2 *"Uninterrupted Electronic Commerce with Cloud SecaaS"*, in which the PALANTIR solution will provide a holistic cybersecurity protection to a Microenterprise, protecting the link between the company's internal and external network, also offering a risk assessment framework to facilitate the early detection of data breach attempts, and
- Use Case #3 *"Live Threat Intelligence Sharing in a large-scale Edge scenario"*, where PALANTIR will showcase the added value of its knowledge sharing framework under realistic scenarios of propagating attacks, which will be experimentally demonstrated in two 5G testbeds.

The aforementioned use cases were refined and analyzed in the context of T2.3 and are thoroughly presented in **Section 2** of this deliverable. Each of them is described based on a common template, complemented by a motivation and overall description subsection, definitions of the involved actors and their in-between interactions. The workflows between actors and the PALANTIR platform are presented as actor-relationship and sequence UML diagrams, followed by a step-by-step overview per use case. This is an exercise to validate that all defined use cases can be realised via the proposed architecture documented in D2.1. Finally, a subsection is dedicated to the hosting infrastructure of each use case.

In **Section 3,** we assess the most prominent security threats and risks in the domain of software networks and cloud-native deployments and propose a risk-based methodology to enable the measurement of the attack surfaces exposed by the different deployments involved in each use case. To this end, Subsection 3.1 provides a comprehensive account of the related network assets and security threats, challenges and risks arising in SME/ME networks, based not only on the latest literature, but also on the condensed experience in attack surface analysis performed in similar research projects by partners of the PALANTIR consortium. The PALANTIR Risk-based assessment framework is described in Subsection 3.2, preceded by a comparison between the ENISA and NIST risk-based approaches. We also provide a preliminary version of the risk assessment for each use case, including a comprehensive definition of the relevant attack classes, entry/exit points, channels and data stores in each PALANTIR deployment. The final version of the Use Case risk assessment, including measures to reduce security risks in the involved service-oriented infrastructures will be documented in D2.4.

1. Introduction

1.1. Objectives and goals of the deliverable

The current document is the deliverable "D2.2 Use Cases, Threat analysis & AS-based risk assessment" which comprises the major outcomes of **"Task 2.3 - Use case analysis"** and **"Task 2.4 Threat and Attack Surface Analysis"**.

Task 2.3 defines the specific use cases for the three offered delivery modes: *Cloud SecaaS* for hosted Managed Security Services, *Lightweight SecaaS* for standalone devices at the premises of the client following the model of Customer Premises Equipment (CPE), and *Edge SecaaS* for infrastructure hosted at the network edge following the paradigm of Multi-Access Edge Computing. The work on the defined use cases yields a description of the involved actors, scenarios, flows of action, pre- and post-conditions as well as information regarding the hosting infrastructure. The defined use cases will be validated along with their detailed specifications to federate the partners on the final version of the PALANTIR architecture, an interim version of which is documented in D2.1 "Requirements & high-level design". The overall work is foreseen to prepare the ground for the refinement of pilots in WP6.

Task 2.4 aims at assessing the threat landscape and historical attack data in order to define an attack surface analysis methodology coherent to the service-oriented infrastructure protected by PALANTIR. It provides a comprehensive definition of the relevant attack classes, entry/exit points, channels and data stores in SDN/NFV and cloud-native deployments and enables the elicitation of a risk-based assessment approach for the quantification of risk factors (damage potential, cost-benefit ratio of the attacker, etc.) in a standardized format. D2.2 provides an interim version of the attack surface analysis and risk assessment to be applied in the context of PALANTIR, while the final version will be included in D2.4 "Risk Reduction measures". This extensive analysis will also form the basis of the monitoring mechanisms developed under WP3.

The primary audience of this document consists of people who will participate in the design and development of the PALANTIR pilots as well as in the implementation of the threat and vulnerabilities mechanisms associated with the assets of the programmable infrastructure. This audience consists primarily of members of the consortium who will design and implement the components and modules of the system. Additionally, this document is of wider interest to extended communities of cyber security stakeholders in order to drive and foster adoption of standardization for the SME/ME sector.

1.2. Relation with D2.1 and other WPs

The presented cases were designed in conjunction with the elicitation of the interim version of the PALANTIR requirements and overall system architecture documented in D2.1. A conceptual view of the PALANTIR architecture is shown in Figure 1 to facilitate readability and tracking of the UC workflows. It is noted that D2.1 comprises the primary reference point for designing the individual PALANTIR components.

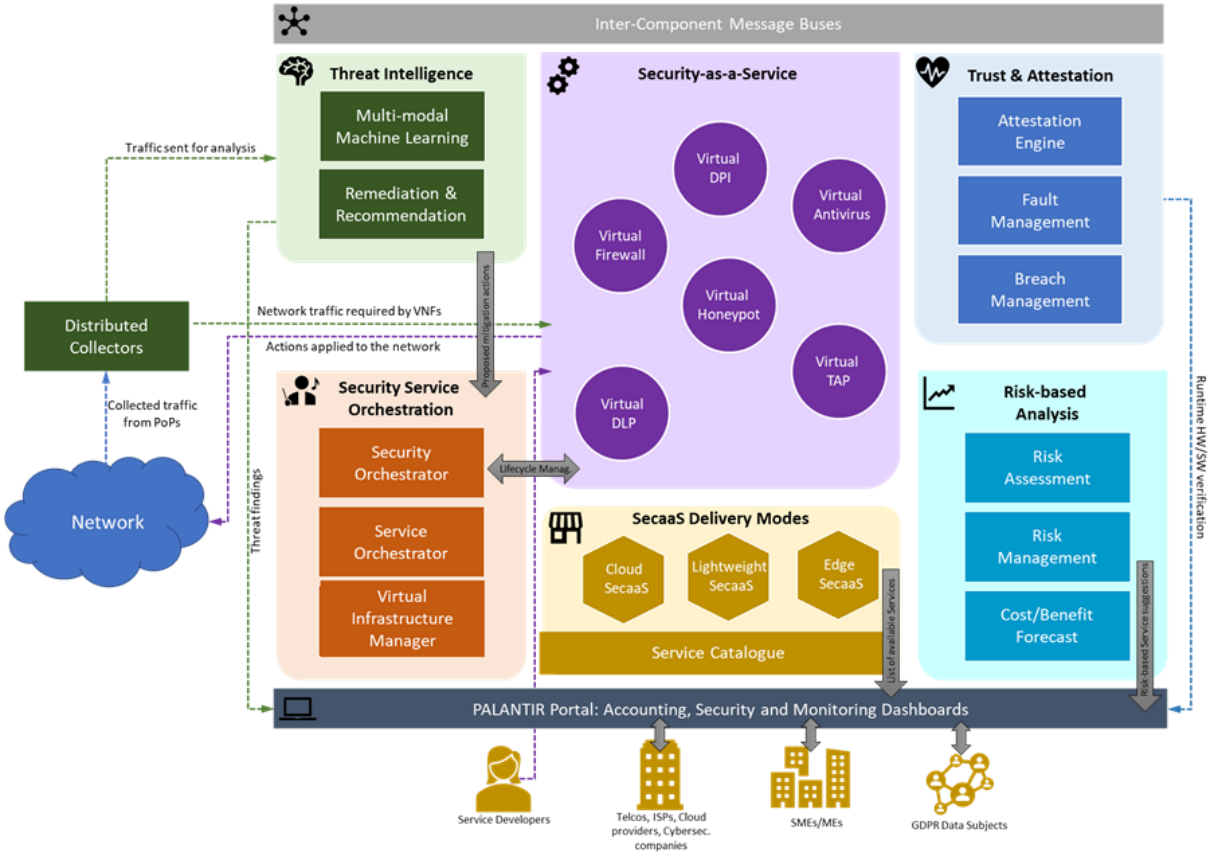

Figure 1: Conceptual view of the PALANTIR solution

A brief description of the workflow between the PALANTIR components is also provided below:

- The *Risk-based analysis* component allows the quantification of security/privacy threats based on security/privacy impact assessment and its correlation with attack surface analysis.
- *Threat Intelligence* traces traffic from the network and VNFs through *Distributed Collectors*, analyses it for signs of malicious activity and outputs the detected anomalies to the *Remediation Engine*.
- The *Remediation Engine* proposes reactive measures against cyberattacks (security rules, new topologies etc) to the *Security Service Orchestrator*.
- The *Security Service Orchestrator* pushes back selected actions and lifecycle management messages to the running *SecaaS*.
- The *Trust & Attestation* component periodically attests the infrastructure's physical and virtual components for signs of compromise.

Furthermore, the present deliverable is linked to the following WPs:

- **WP3** (T3.3), for the implementation of the PALANTIR risk assessment and analysis framework that will enable the application of specific actions towards risk reduction,
- the rest of the technical WPs (**WP4, WP5**) indirectly, to ensure that technical developments will be generally aligned with the presented scenarios,
- **WP6** (T6.2, T6.3, T6.4), providing the guidelines for the realization of three discrete pilots based on the described use cases.

2. Use Case Analysis

This section offers a thorough presentation of the 3 PALANTIR Use Cases that were initially defined in the Document of Action. For each UC, we provide the overall motivation and high-level description, the list of involved actors and their interactions with the platform using actor diagrams, as well as a detailed step-by-step view accompanied by sequence diagrams.

It should be noted that the selection of the following UCs was made with complementarity in mind, as each scenario focuses on a different delivery mode (Lightweight/Cloud/Edge SecaaS). By deploying different SecaaS configurations in different geographically and organizationally dispersed testbed locations with a significant involvement of enterprises, we showcase the ability of PALANTIR to address the specific needs of SMEs/MEs with tailor-made products.

2.1 Use Case #1: Securing private medical practices with lightweight SecaaS

2.1.1 Motivation and Overall Description

Use case 1 implements a Lightweight SecaaS for the protection of small businesses from data breaches and ransomware attacks. To this end, the PALANTIR platform will be leveraged in the scope of medical data protection, where relevant activities to safeguard patient data and prevent medical identity theft will be supported. In order to support such use case and showcase the added value of PALANTIR components, a data leakage scenario will be developed and implemented in a medical practice office to replicate a real-world cybersecurity scenario. Various attack types will be investigated, as to their efficiency and applicability to real world conditions. An indicative set of attacks that will be considered:

- Malware
- Man in the Middle
- Brute force
- Data breach (DNS tunelling)
- Ransomware
- Eavesdropping
- Spoofing

The described scenario will be integrated in an edge pilot deployed in the Athens testbed, where the PALANTIR components will be integrated and will monitor the network. The next step will be to initiate an attack scenario to gain access to the medical data node and start the malicious data transfer. The PALANTIR platform will be able to detect the attack and begin to apply remediation measures, such as application blocking, firewall rule enforcement, etc. The primary goal of this use case is to demonstrate a lightweight cybersecurity solution that can leverage both PALANTIR cloud platform modules that will run remotely, and the local edge modules that will perform the on-site operations, i.e., detection and remediation. Edge operations will receive periodically updated metadata in various forms (weights, models, etc.) that will maintain the platform's readiness in new attacks, and also provide an efficient lightweight SecaaS solution.

2.1.2 Actors Definition and Mode of Interaction

This subsection provides information regarding the actors of UC1 and their interactions with the PALANTIR platform.

- Who are the actors?

We foresee the following principal classes of users (a full list of actors for every use case can be found in the Consolidated Stakeholders table in Annex A):

1. **Healthcare Practitioner**: end-users of PALANTIR, protecting their organization from threats that the healthcare sector faces due to digitalisation and the proliferation of medical data.
2. **PALANTIR Admin**: responsible for the operation of the PALANTIR platform.
3. **Attacker**: malicious cyber actor targeting the healthcare sector by performing ransomware attacks, data theft, and/or disrupting of healthcare services.

- How is every actor interacting with the application/service?

Table 1: UC1 Actors interactions with PALANTIR

Actor	***Role***	***Interacting functionalities***
Doctor / Healtcare Practicioner	End-user	• Installs an end-point device on premises • GUI provides capability to monitor in real-time activity, events and alerts • GUI provides capability to cancel alerts, remove restrictions • GUI provides capability to communicate 24/7 with live support • Interconnects all in-premises equipment with WAN.
PALANTIR Admin	Administrator	• Provides end-point device • Remote monitoring and alert • Updates new functionalities and new algorithms • Communicates in real-time with the end user • Retrieves attack information used for threat sharing purposes • Reconfigures remote endpoint
Attacker	Attacker	• Performs malicious network attacks on medical practice premises, disrupting normal operation. • Leaks sensitive medical records for extortion/blackmail purposes.

2.1.3 Use Case Detailed Description

In this section, we provide the Use Case (Actor-Relationship) UML diagram (Figure 2) followed by a step-by-step view of the use case (Table 2), as well as a Sequence diagram for UC1 (Figure 3).

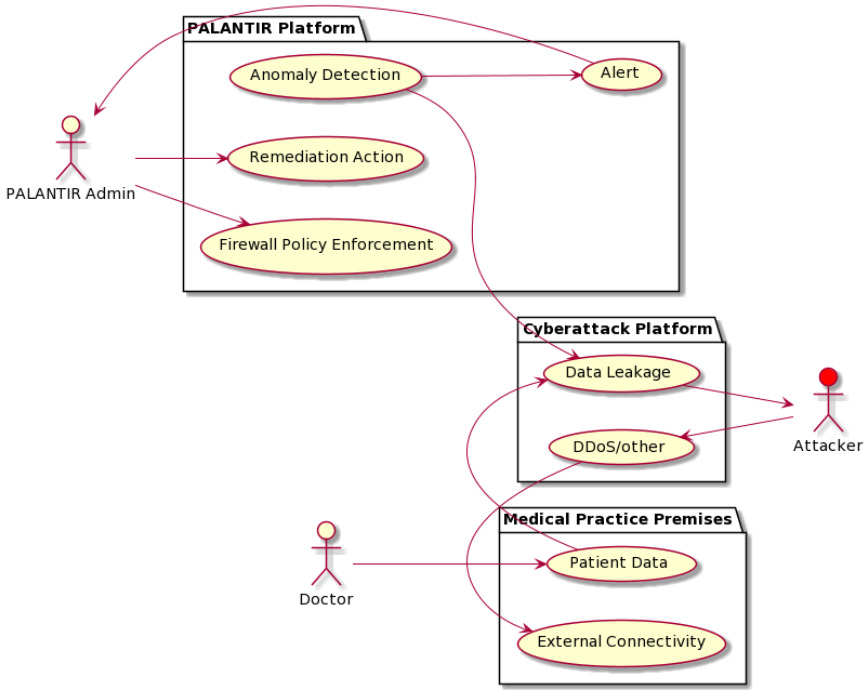

Figure 2: Actor diagram for UC1: Securing private medical practices with lightweight SecaaS

Table 2: Step-by-step view of UC1: Securing private medical practices with lightweight SecaaS

Name	**Patient Data**
Identifier	UC1.1
Description	The Doctor (Heathcare Professional) stores/accesses patient data on-premises (medical practice private data server).
Goal	To access or update sensitive medical records (including referrals and prescriptions, medical examination reports, laboratory tests, radiographs, etc.), or administrative and financial information (e.g., scheduling of medical appointments, invoices for healthcare services and medical certificates for sick leave management).
Preconditions	-
Post conditions	The Doctor is able to access/process patient's data (business as usual).
Actors / Users	Doctor
Dependencies from other functionalities/steps	-
Exceptions	-
Name	**DDoS / Other**
Identifier	UC1.2

Description	A vulnerable medical practice data server is attacked via a malicious actor and access to the server is lost.
Goal	To disrupt the connectivity of the healthcare professional to the private data server and/or steal its credentials.
Preconditions	-
Post conditions	The Attacker manages to disrupt the Doctor's access to the private server.
Actors / Users	Attacker
Dependencies from other functionalities/steps	-
Exceptions	PALANTIR discovers the network attack and blocks the Attacker's access to the network.
Name	**External Connectivity**
Identifier	UC1.3
Description	The Attacker manages to get access of the private medical server.
Goal	To initiate data leakage.
Preconditions	The attacker has managed to disrupt the trusted connection between the healthcare professional and the private server.
Post conditions	The Attacker is able to access/process sensitive medical data.
Actors / Users	Attacker
Dependencies from other functionalities/steps	UC1.2
Exceptions	PALANTIR detects the unathorized access as suspsicious activity and blocks the Attacker's access to the network.
Name	**Data leakage**
Identifier	UC1.4
Description	A vulnerable data server is attacked by the Attacker and sensitive medical data are leaked to a malicious server.
Goal	To leverage stolen medical records for extortion/coercion/blackmail purposes.
Preconditions	Sensitive medical records exist on the private data server and the Attacker has managed to infiltrate.

Post conditions	The Attacker successfully extracts sensitive medical records.
Actors / Users	Attacker
Dependencies from other functionalities/steps	UC1.3
Exceptions	PALANTIR detects the data breach and blocks the network access of the Attacker.
Name	**Anomaly Detection**
Identifier	UC1.5
Description	The PALANTIR Admin leverages the platform's Lightweight SecaaS delivery mode to protect the client's sensitive data.
Goal	To detect potential data leakage and secure the infrastructure.
Preconditions	PALANTIR is deployed on-premises as a Lightweight SecaaS solution.
Post conditions	PALANTIR monitors the network traffic.
Actors / Users	PALANTIR Admin
Dependencies from other functionalities/steps	-
Exceptions	-
Name	**Alert**
Identifier	UC1.6
Description	PALANTIR has detected a threat and issues an alert.
Goal	To notify the end-user (Doctor) of an ongoing attack.
Preconditions	A malicious attack (e.g., data leakage) has occurred and PALANTIR is deployed as a Lightweight SecaaS solution.
Post conditions	The doctor is notified by the PALANTIR portal.
Actors / Users	PALANTIR Admin, Doctor
Dependencies from other functionalities/steps	UC1.4, UC1.5
Exceptions	PALANTIR fails to detect and report the threat.
Name	**Remediation Action**

Identifier	UC1.7
Description	PALANTIR suggests a remediation policy to mitigate the ongoing threat.
Goal	To secure the end-user's infrastructure
Preconditions	A data leakage attempt has occurred and has been successfully detected by PALANTIR.
Post conditions	The remediation policy is sent to the firewall for enforcement.
Actors / Users	PALANTIR Admin
Dependencies from other functionalities/steps	UC1.4, UC1.5
Exceptions	Failure to suggest a relevant remediation policy for the specific threat.
Name	**Firewall Policy Enforcement**
Identifier	UC1.8
Description	PALANTIR applies the suggested remediation policy.
Goal	Disrupt the data leakage attempt.
Preconditions	A relevant remediation policy is suggested for the specific threat.
Post conditions	Remediation policy is applied by the firewall and data leakage is disrupted.
Actors / Users	PALANTIR Admin
Dependencies from other functionalities/steps	UC1.4, UC1.5, UC1.7
Exceptions	Failure to configure the firewall using the suggested remediation guidelines.

The above step-by-step analysis is also depicted in Figure 3. As shown in the sequence diagram for UC1, the Attacker initiates an attack on the Medical Server which -if successful- leads to the leakage of medical data. The Doctor has leveraged a PALANTIR Security Endpoint (after succesful authentication) as Lightweight SecaaS to monitor local traffic. PALANTIR is able to detect the Attacker's malicious activity as an anomaly and issues an alert to the Doctor, while also registering the event for the PALANTIR Admin. A remediation action to block the malicious connection is suggested and enforced by the SecaaS components, leading to the disruption of the data leakage attempt.

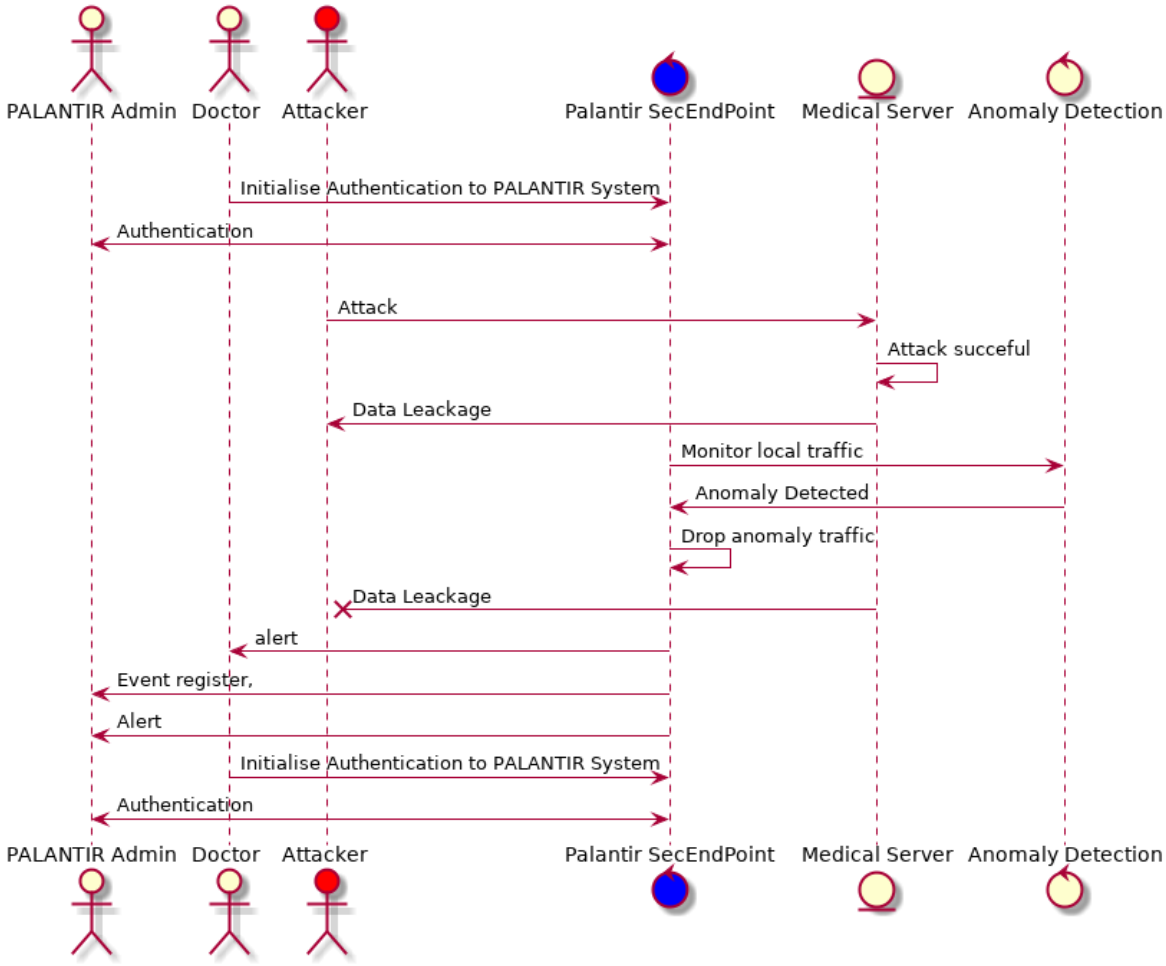

Figure 3: Sequence diagram for UC1: Securing private medical practices with lightweight SecaaS

2.1.4 Hosting Infrastructure

The NFVI Point-of-Presence (PoP) in ORION's Athens site runs the OpenStack Ussuri distribution based on Centos 7.4.1708. The OpenStack controller and a compute node are situated on a single server, thus denoting this an "all-in-one" deployment (Figure 4). The PoP provides networking to the VNFs through OpenStack's Neutron service. All the networking is therefore handled automatically by OpenStack, provided that the required physical networks are present. Available storage includes SAS/iSCSI and EqualLogic high-capacity 3.5" drives. The PoP utilises the OpenStack default back-end drivers and is utilised to deploy VNFs based on the KVM hypervisor, although support for Docker containers via vim-emu is also provided (requiring OSM release 5).

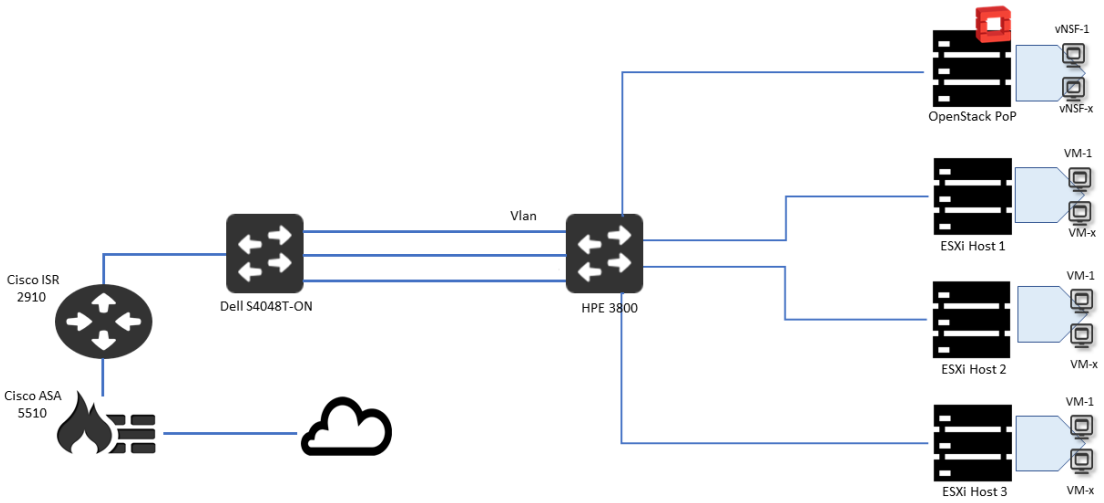

Figure 4: ORION Athens NFVI-PoP and related infrastructure

In addition to the PoP, three bare metal servers running ESXi virtualisation software are provided. The ESXi servers are able to provide VMs for other additional core functionalities such as a Prometheus server, various NFVO releases etc. Additional networking infrastructure includes a Cisco 5500 Series Adaptive Security Appliance (integrating firewall, NAT and Intrusion Detection capabilities), a Cisco 2900 Series Integrated Services Router, and two switches, namely an SDN-enabled HPE Aruba 3800 with the OpenDaylight controller (version Carbon) and a Dell Switch. The NAT is configured either to be dynamic in order to allow all the hosts to reach internet or public addresses, or static NAT to allow also access to specific services from the inside networks to be reachable outside the firewall.

2.2 Use Case #2: Uninterrupted Electronic Commerce with Cloud SecaaS

2.2.1 Motivation and Overall Description

In this use case, we aim at showcasing a personalized enterprise-grade solution offered to the end-user in an affordable way, by minimizing cost to licenses and software as well as hardware costs. Exploiting edge computing will minimize the impact of computational power (i.e., at most a simple actuator/sensor device on-premises). By exploiting the power of analytics models trained and finetuned on mutliple data sources, we aim at increasing the accuracy and contextual awareness of threat detection and alignment of responses with requirements and expectations of the end-user (i.e., protect assets, data and services based on their value by prioritizing those that are the most valuable to the business). The main goals of this use case are to identify exposed and vulnerable points of entries, to distinguish between regular and irregular traffic and to isolate only the targeted end-point(s) so that the complete business of the company is not blocked.

To this end, UC2 will exploit a Cloud SecaaS variant of PALANTIR, facilitating the training of anomaly detection and threat classification models on a centralized manner, while deploying them on the edge (i.e., in the location near the the end-user) and only place probes to collect data and mechanisms to isolate and protect certain segments of the LAN and mitigate the attacks at the end-user's location.

The main types of attacks/threats we expect are:

- Malware as an attack tool (spam, phishing, downloads, SMiShing)
- Attacks through smart devices (especially Android-based), e.g., spyware on mobile phones
- Broken cryptography and improper session handling while communicating with cloud services
- Ransomware
- Internal attacks due intentionally or accidentally compromised user accounts

- Uneven Cybersecurity Protections (i.e., Security Gaps)
- Distributed Denial of Service (DDoS) attacks

The testbed consists of several residential grade IT equipment, such as residential modems and routers, low-cost switches and small data-servers and various devices connecting to the internet via a private local area network (PAN), allowing for fixed as well as wireless connectivity. In the PAN, there are various devices (from PCs, and mobile devices to more specialized equipment such as VoIP terminals and POS terminals) connecting to the internet. LAN and WLAN networks are bridged and printers, mobile cashiers and mobile POS Terminals allow even NFC and Bluetooth connectivity. Finally, the same router also hosts the public WiFi for customers.

2.2.2 Actors Definition and Mode of Interaction

This subsection provides information regarding the actors of UC2 and their interactions with the PALANTIR platform.

- Who are the actors? Brief description of each.

We foresee the following principal classes of users (a full list of actors for every use case can be found in the Consolidated Stakeholders table in Annex A):

1. **Security Service Provider** (e.g., SFERA): provides outsourced monitoring and management of the PALANTIR security devices and systems.
2. **Microentreprise personnel (employees, managers)**: a microenterprise as an end-user with limited CAPEX, employees, trusted IoT devices (printers, mobile cashiers and mobile POS terminals) employees connecting trusted (company issued PCs and terminals) and untrusted devices (personal devices).
3. **Customer**: visitor connecting to the Internet with their smart devices, protected by PALANTIR.
4. **Attacker**: aiming to perform malicious operations on company infrastructure.

- How is every actor interacting with the application/service?

Table 3: UC2 Actors interactions with PALANTIR

Actor	*Role*	*Interacting functionalities*
PALANTIR Operator	Administrator, PALANTIR Operator	• Provides Cloud SecaaS solution • Remote monitoring and alert • Updates new functionalities and new algorithms • Communicates in real-time with the end user • Retrieves attack information used for threat sharing purposes • Reconfigures remote endpoint
Employee	End-user (Sales, CRM, Accounting)	• Uses network-connected infrastructure (POS terminals, cashier, trusted desktop, personal smart phone, access to cloud services and local services, web browsing, email)
Manager/Admin	End-user (Management)	• Has high-level access from personal mobile devices, smartphones and tablets

Attacker	Attacker	• Performs malicious injections/exploits to the eCommerce Database. • Installs ransomware/malware or similar software to the company infrastructure.

2.2.3 Use Case Detailed Description

In this section, we provide the Use Case (Actor-Relationship) UML diagram (Figure 5) followed by a step-by-step view of the use case (Table 4) as well as the Sequence diagram for UC2 (Figure 6).

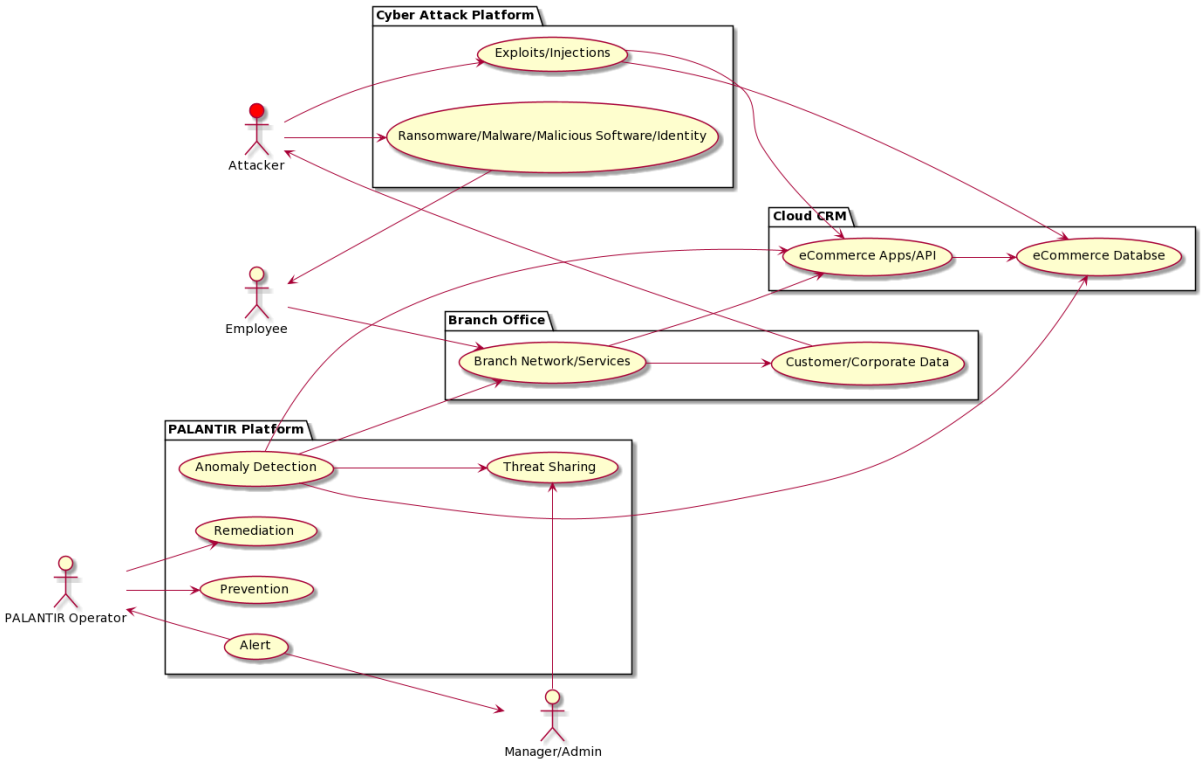

Figure 5: Actor diagram for UC2: Uninterrupted Electronic Commerce with Cloud SecaaS

Table 4: Step-by-step view of UC2: Uninterrupted Electronic Commerce with Cloud SecaaS

Name	**Branch Network/Services**
Identifier	UC2.1
Description	The employee uses the company's branch network and services.
Goal	Everyday business operations (business as usual)
Preconditions	-
Post conditions	The employee interfaces with Cloud services/APIs and/or customer/corporate data.
Actors / Users	Employee

Dependencies from other functionalities/steps	-
Exceptions	-
Name	**Customer/Corporate Data**
Identifier	UC2.2
Description	The employee accesses the company's private servers through the branch network.
Goal	Everyday business operations (business as usual).
Preconditions	Use of the local network.
Post conditions	The employee gets access to confidential customer/corporate data.
Actors / Users	Employee
Dependencies from other functionalities/steps	UC2.1
Exceptions	The company network is unavailable.
Name	**eCommerce Apps/API**
Identifier	UC2.3
Description	The employee remotely accesses the Cloud CRM system applications and APIs.
Goal	To get access to centralized eCommerce database (business as usual).
Preconditions	Use of the local network, availability of cloud services.
Post conditions	The employee gets access to the data of the eCommerce database.
Actors / Users	Employee
Dependencies from other functionalities/steps	UC2.1
Exceptions	The company network or the cloud services are unavailable.
Name	**eCommerce Database**
Identifier	UC2.4
Description	The employee gets access to the data of the eCommerce database.
Goal	Everyday business operations (business as usual).

Preconditions	Use of the local network, availability of cloud services.
Post conditions	The employee processes/downloads the available data for business operations.
Actors / Users	Employee
Dependencies from other functionalities/steps	UC2.3
Exceptions	The company network or the cloud services are unavailable.
Name	**Exploits/Injections**
Identifier	UC2.5
Description	The attacker attempts to exploit the vulnerabilities of the Cloud CRM services.
Goal	To extract sensitive corporate data from the online database.
Preconditions	-
Post conditions	The attacker gets access to the company's Cloud CRM services and databases.
Actors / Users	Attacker
Dependencies from other functionalities/steps	-
Exceptions	The attack is blocked by the PALANTIR Cloud SecaaS solution.
Name	**Ransomware/Malware/Malicious Software/Identity Theft**
Identifier	UC2.6
Description	The attacker attempts to propagate malicious software to the employees.
Goal	To steal employee credentials for data leakage, to install ransomware for extortion schemes.
Preconditions	Employees are connected and using the branch network and the Attacker has exploited a network vulnerability to gain access.
Post conditions	The attacker manages to steal employee's credentials and/or encrypt their files.
Actors / Users	Attacker

Dependencies from other functionalities/steps	UC2.1, UC2.5
Exceptions	PALANTIR detects the propagating attack and blocks the attacker's access to the network.
Name	**Anomaly Detection**
Identifier	UC2.7
Description	The PALANTIR Operator leverages the platform's Cloud SecaaS delivery mode to analyse the network traffic generated by the company's multiple PoPs.
Goal	To secure and protect a network environment with limited security and multiple managed and unmanaged points of entry from data breaches and disruption of critical services.
Preconditions	PALANTIR is deployed as a Cloud SecaaS solution.
Post conditions	PALANTIR is able to protect the company's assets from cyberattacks.
Actors / Users	PALANTIR Operator
Dependencies from other functionalities/steps	-
Exceptions	PALANTIR is unable to analyze the network traffic of one or more company PoPs.
Name	**Alert**
Identifier	UC2.8
Description	PALANTIR detects a threat and issues an alarm.
Goal	To notify interested parties of potentially malicious attempts.
Preconditions	PALANTIR is scanning the network traffic of the company's multiple PoPs and a malicious activity is detected.
Post conditions	The PALANTIR Operator and the Manager are notified for potential threats.
Actors / Users	PALANTIR Operator, Manager
Dependencies from other functionalities/steps	UC2.5, UC2.7
Exceptions	PALANTIR is unable to discover one or more network threats.

Name	Remediation
Identifier	UC2.9
Description	PALANTIR proposes remediation actions based on the threat findings.
Goal	To disrupt the attacker's access to the company infrastructure.
Preconditions	PALANTIR has discoved a network threat.
Post conditions	The proposed remediation action is forwarded to the PALANTIR Operator
Actors / Users	PALANTIR Operator
Dependencies from other functionalities/steps	UC2.8
Exceptions	PALANTIR fails to propose a remediation action for the specific threat.
Name	**Prevention**
Identifier	UC2.10
Description	The PALANTIR Operator applies the suggested remediation action.
Goal	To prevent the propagation of network threats to the company infrastructure, to prevent data leakage.
Preconditions	A remediation action is proposed by PALANTIR.
Post conditions	The remediation action is applied by the PALANTIR security services.
Actors / Users	PALANTIR Operator
Dependencies from other functionalities/steps	UC2.9
Exceptions	Failure to apply suggested remediation due to mismatch in service/network configuration.
Name	**Threat Sharing**
Identifier	UC2.11
Description	The discovered threats are shared between the PALANTIR stakeholders (based on company policy).
Goal	To inform potential targets of propagating network threats.
Preconditions	A threat is discovered by the PALANTIR framework.
Post conditions	Threat information is shared to external stakeholders in a standardized format.

Actors / Users	Manager
Dependencies from other functionalities/steps	UC2.7
Exceptions	The Manager refuses to disclose the discovered threat.

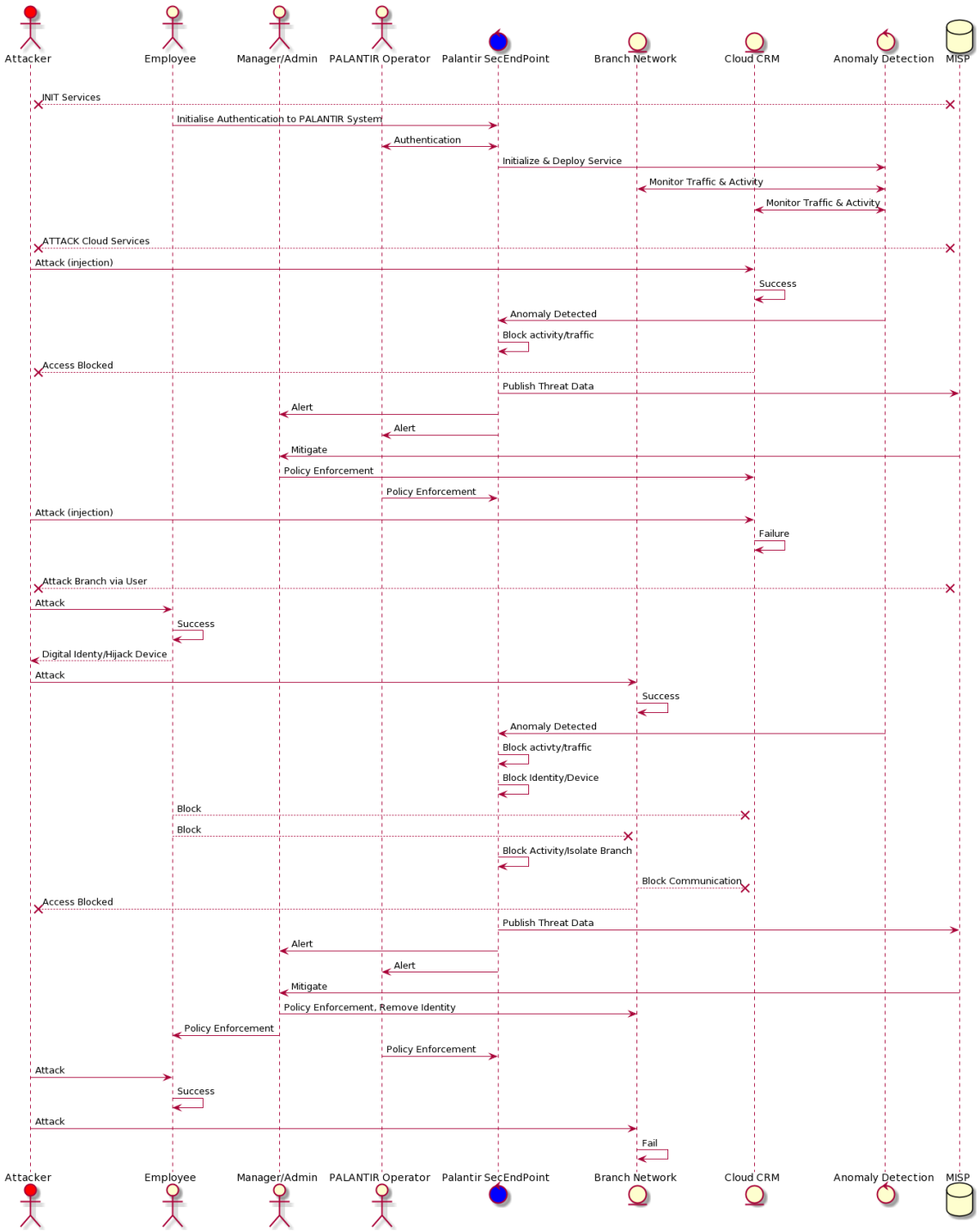

Figure 6: Sequence diagram for UC2: Uninterrupted Electronic Commerce with Cloud SecaaS

The aforementioned step-by-step analysis is also depicted in the sequence diagram of Figure 6. In this scenario, the Attacker attempts to exploit the vulnerabilities of the branch network entry points to extract sensitive corporate data from online infrastructure for extortion purposes. To this end, he propagates malicious software to the Employees and/or interferes with their connection to the branch network and services, in an effort to steal their credentials or other valuable metadata that could provide access to the company's infrastructure (Cloud CRM, eCommerce database). PALANTIR has been deployed as a Cloud SecaaS solution, able to monitor traffic from different PoPs in a centralized manner. It detects the attacker's malicious activity as an anomaly and issues an alert to the PALANTIR Operator and the Manager/Admin of the company. PALANTIR also proposes a remediation action that targets the attacker's activity without disrupting the daily business operations and forwards it for enforcement. The attack is blocked and the relevant threat data can be shared with international knowledge sharing infrastructures (e.g., MISP instance) to deploy tailored cybersecurity measures for similar cases.

2.2.4 Hosting Infrastructure

The Slovenian testbed represents a real-life replica of a network of a typical IT network an ME operates in. Each location has a separate LAN and all can connect to the Cloud (Figure 7). Common Digital Identity Policy is used and OAuth2 is used for authentication and authorization. Account Restriction policy via User Roles is enforced to partially protect the web services.

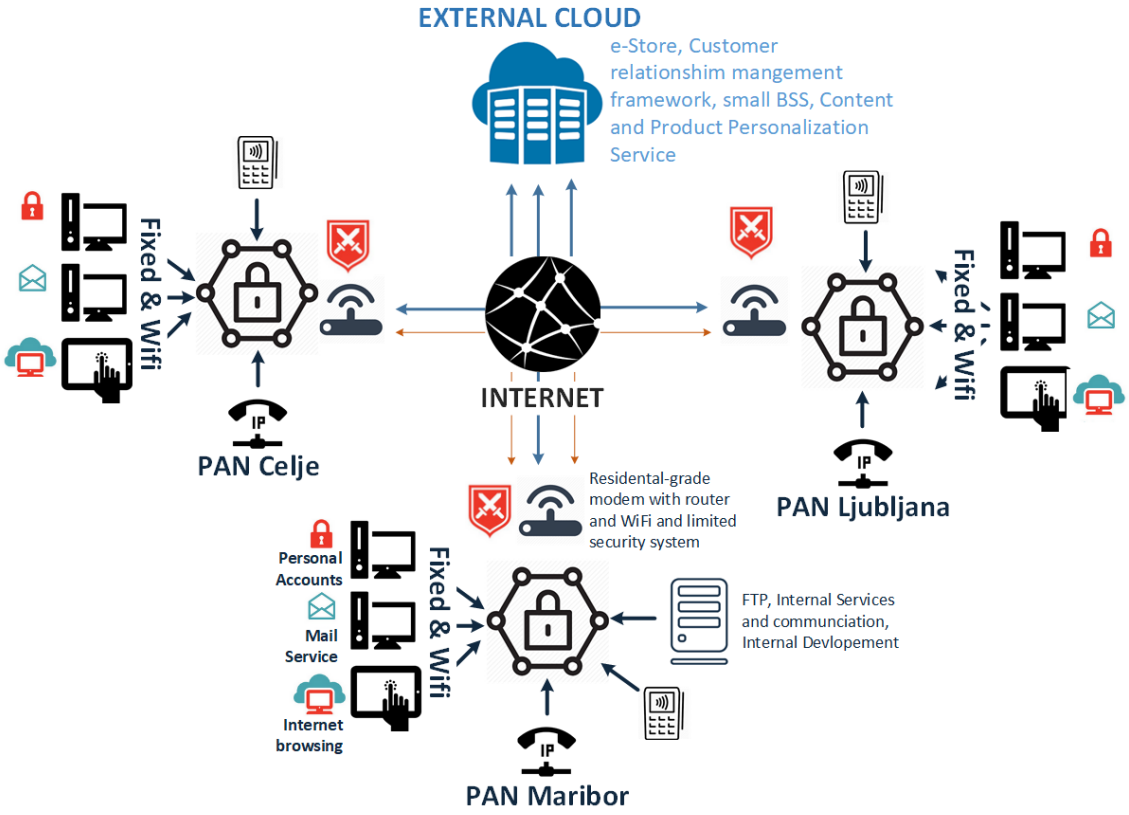

Figure 7: Slovenian testbed and related infrastructure

LAN: The network consists of several residential grade IT equipment, such as residential modems and routers, low-cost switches and small data-servers and various devices connecting to the internet via a private local area network (PAN) allowing for fixed as well as wireless connectivity. In general, fixed connections ''plug and play'' (i.e., DHCP server on the router) are protected by a firewall. As outlined in the high-level overview such a LAN consists of residential grade IT equipment, and various devices

(from PCs, and mobile devices to more specialized equipment such as VoIP terminals and POS terminals) connecting to the internet.

Wireless network: A typical network hosts bridged LAN and WLAN networks and, in some cases, (i.e., for printers and cashiers) with NFC connectivity. The Wifi connections are protected by common WLAN mechanism (i.e., WEP, WPA, WPA2, etc.). In some cases, even NFC is enabled.

Cloud: Deployed commercially available cloud solutions to host the enterprise related services. In UC2, the cloud hosting is a rented virtual sever operating on the PLESK platform. In addition to web applications, SQL and non-SQL databases it also hosts an FTP server to which all of the locations have credentials-based access. (via SFTP). The server can be updated and allows for limited vulnerability assessment and reporting.

Services: Within the virtual space the ME implements and runs its CRM, e-retail store, mail servers, product and content personalization and a small BSS framework to improve efficiency and flexibility. The majority of personal customer data is stored and handled in the cloud. Access to various services is user/password protected and some services also support SSL. In case of SI testbed, the ME also owns a small private data-server which is hosted in one of the PANs (Maribor). This server is used for internal process and for running apps which are not supported by the cloud instance. In this server, limited personal information of both employees and customers is also stored and processed. The server is secured via openly available software solutions.

Local server: A small private server is deployed in the main offices in Maribor., used for document storage, corporate-sensitive data storage and for running customized services which are not supported by the cloud instance. The server is secured via openly available software solutions. The server may be accessed Remotely via remote desktop solutions (i.e., TeamViewer and TigerVNC) or via SSH. Users have access to specific applications running on the server (FTP, HTTP and HTTPs)

2.3 Use Case #3: Live Threat Intelligence Sharing in a large-scale Edge scenario

2.3.1 Motivation and Overall Description

This use case will be experimentally demonstrated in the 5TONIC and 5GENESIS testbeds. These 5G-enabled testbeds can emulate traffic from multiple SecaaS clients on their edge network as well as parallel complex attacks, in large scale MEC scenarios. UC3 will incorporate the virtual network infrastructure as well as SDN/NFV infrastructure comprised of high-performance servers for the execution of NFV management software and deployment of SDN controllers. The different elements of the testbed can be flexibly interconnected using OpenFlow switches. 5TONIC provides multi-site capability by incorporating infrastructure and equipment located at TID premises. A part of these labs is the Mouseworld, a configurable generator of labelled network traffic datasets, supporting dynamic network topologies (by means of an NFV infrastructure), experiment scheduling to configure and run predefined scenarios, and dataset labelling from the knowledge derived from the scheduled experiments.

The PALANTIR coordination efforts will be focused on deploying the PALANTIR components on various levels of the utilized virtual networks, while SSE will deploy realistic cyberattack scenarios of propagating attacks (e.g., DDoS, WannaCry) that will be simultaneously directed to multiple the clients of the PALANTIR solution. In this context, we plan to leverage PALANTIR by:

- Detecting the common threat addressed to multiple clients
- Publishing the incident to a knowledge sharing platform (e.g., MISP)
- Retrieving relevant threat intel information in order to produce an appropriate mitigation plan
- Relaying high-level mitigation policies through the PALANTIR provider to the other SecaaS clients.

2.3.2 Actors Definition and Mode of Interaction

This subsection provides information regarding the actors of UC3 and their interactions with the PALANTIR platform.

- Who are the actors?

We foresee the following principal classes of users (a full list of actors for every use case can be found in the Consolidated Stakeholders table in Annex A):

1. **PALANTIR administrator**: responsible for the operation of the PALANTIR platform.
2. **PALANTIR provider**: vendor of the PALANTIR secure WAN endpoint.
3. **5GENESIS Admin**: administrator of the 5GENESIS testbed.
4. **5TONIC Admin**: administrator of the 5TONIC testbed.
5. **Service Developer**: develops secure services for the PALANTIR platform.
6. **SecaaS end user**: leverages PALANTIR as an end-point cybersecurity solution in their premises.
7. **SecaaS client**: client accessing the network, protected through PALANTIR SecaaS.
8. **Attacker**: who uses the testbed as a channel for propagating cyberattacks, inadvertently distributing malware to other clients.

- How is every actor interacting with the application/service?

Table 5: UC3 Actors interactions with PALANTIR

Actor	*Role*	*Interacting functionalities*
PALANTIR Provider	Service provider	• Provides PALANTIR SecEndPoint • Remote monitoring and alert • Updates new functionalities and new ML/DL algorithms • Communicates in real-time with 5G admins • Retrieves attack information used for threat sharing purposes • Threat Mitigation plan • Threat Sharing
5G Testbed Admin (5TONIC/5GENESIS)	Infrastructure Provider	• Administration/provision of 5GENESIS testbed • Realtime monitoring • Threat Detection • Policy Enforcement
Attacker	Attacker	• Performs propagating cyberattacks targeting many network clients simultaneously.

2.3.3 Use Case Detailed Description

In this section, we provide the Use Case (Actor-Relationship) UML diagram (Figure 8) followed by a step-by-step view of the use case (Table 6), as well as the Sequence diagram for UC3 (Figure 9).

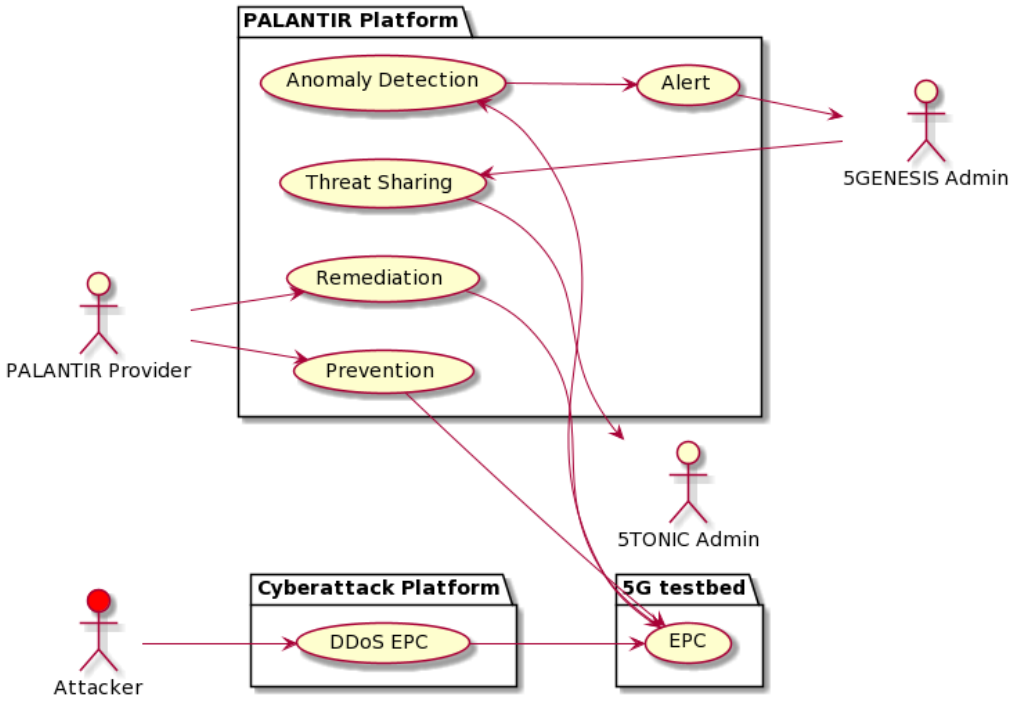

Figure 8: Actor diagram for UC3: Live Threat Intelligence Sharing in a large-scale Edge scenario

Table 6: Step-by-step view of UC3: Live Threat Intelligence Sharing in a large-scale Edge scenario

Name	**DDoS EPC**
Identifier	UC3.1
Description	The Attacker performs a DDoS attack to the 5GENESIS virtual EPC that simulates an ISP network.
Goal	To disrupt the network services of the simulated ISP (5GENESIS testbed).
Preconditions	-
Post conditions	The resources of the 5G testbed are saturated.
Actors / Users	Attacker
Dependencies from other functionalities/steps	-
Exceptions	The attack is detected by the PALANTIR SecaaS solution.
Name	**EPC**

Identifier	UC3.2
Description	The 5TONIC EPC is the target of a scalable network threat (e.g., DDoS).
Goal	To disrupt the network services of the ISP.
Preconditions	A network attack is targeted towards the 5GENESIS testbed.
Post conditions	The connectivity to the 5GENESIS testbed is lost.
Actors / Users	Attacker
Dependencies from other functionalities/steps	UC3.1
Exceptions	The attack is detected by the PALANTIR SecaaS solution before saturating the network resources of the testbed.
Name	**Anomaly Detection**
Identifier	UC3.3
Description	The PALANTIR Provider leverages the platform Edge SecaaS delivery mode to analyse the testbed's network traffic.
Goal	To detect propagating network threats that will set the operation of the simulated ISP at risk.
Preconditions	PALANTIR is deployed as an Edge SecaaS solution.
Post conditions	PALANTIR analyses the traffic of the 5GENESIS testbed.
Actors / Users	PALANTIR Provider
Dependencies from other functionalities/steps	-
Exceptions	-
Name	**Alert**
Identifier	UC3.4
Description	PALANTIR detects the propagating threat and issues an alert.
Goal	To protect the ISP network services.
Preconditions	The PALANTIR platform is monitoring the 5GENESIS network traffic.
Post conditions	PALANTIR notifies interested parties of the threat findings.
Actors / Users	PALANTIR Provider, 5G Testbed Admin

Dependencies from other functionalities/steps	UC3.3
Exceptions	PALANTIR is unable to detect the network threat.
Name	**Remediation**
Identifier	UC3.5
Description	PALANTIR proposes remediation actions based on the threat findings.
Goal	To disrupt the attacker's access to additional testbed nodes.
Preconditions	PALANTIR has discoved a network threat.
Post conditions	The proposed remediation action is forwarded to the PALANTIR Provider.
Actors / Users	PALANTIR Provider
Dependencies from other functionalities/steps	UC3.4
Exceptions	PALANTIR fails to propose a remediation action for the specific threat.
Name	**Prevention**
Identifier	UC3.6
Description	The PALANTIR Provider applies the suggested remediation action.
Goal	To prevent the propagation of network threats to additional simulated ISP nodes.
Preconditions	A remediation action is proposed by PALANTIR.
Post conditions	The remediation action is applied by the PALANTIR security services.
Actors / Users	PALANTIR Operator
Dependencies from other functionalities/steps	UC3.5
Exceptions	Failure to apply suggested remediation due to mismatch in service/network configuration.
Name	**Threat Sharing**
Identifier	UC3.7
Description	The discovered threats are shared between the PALANTIR ISP nodes (to the 5TONIC testbed)

Goal	To inform potential targets (5TONIC) of propagating network threats.
Preconditions	A threat is discovered by the PALANTIR framework.
Post conditions	Threat information is shared to external stakeholders in a standardized format.
Actors / Users	5G Testbed Admin
Dependencies from other functionalities/steps	UC3.6
Exceptions	-

The above step-by-step analysis is also depicted in the sequence diagram of Figure 9. The Attacker deploys propagating attacks to the 5GENESIS testbed which is protected by the PALANTIR Edge SecaaS solution. In this case, the PALANTIR provider is a CSP that deploys the SecaaS on the network edge following the MEC paradigm, offering an umbrella of protection to multiple tenants in large-scale edge scenarios. The attack on the 5GENESIS tenant is detected by PALANTIR as an anomaly and an alert is issued to the testbed administrator along with a suggested remediation policy, which is enforced to the current tenant. The threat data is also published to another tenant (5TONIC testbed) via the knowledge sharing infrastructure (e.g., MISP), resulting in a proactive policy enforcement that prevents the further propagation of the attack.

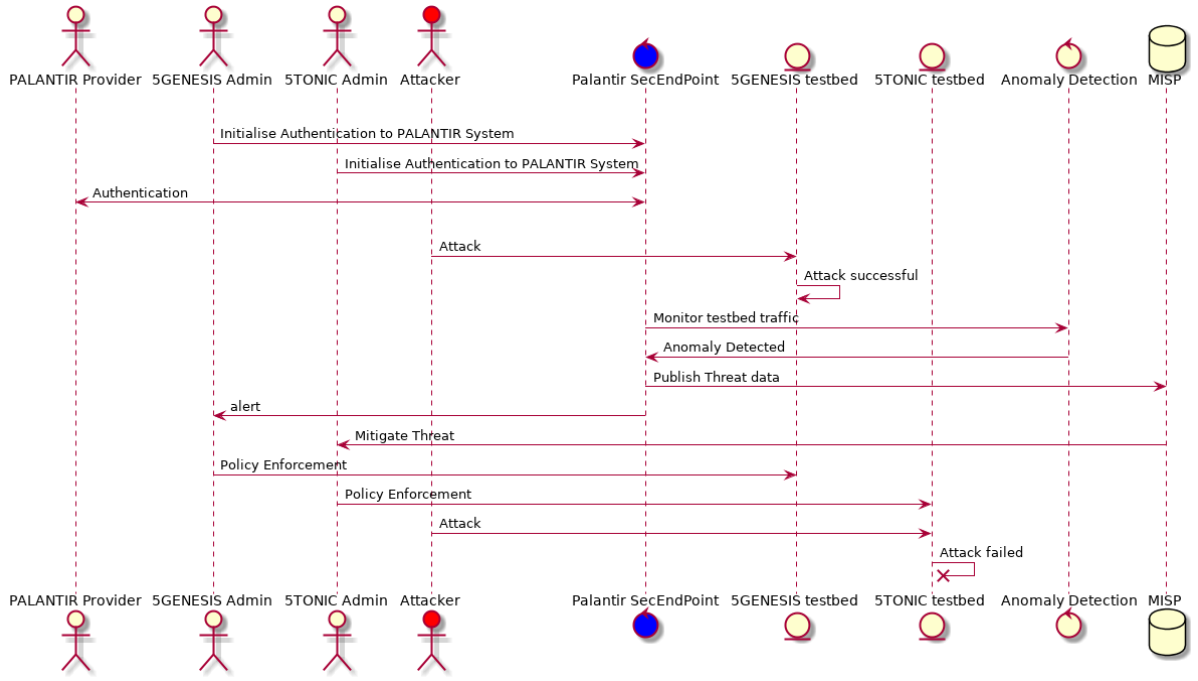

Figure 9: Sequence diagram for UC3: Live Threat Intelligence Sharing in a large-scale Edge scenario

2.3.4 Hosting Infrastructure

2.3.4.1. 5GENESIS Athens Platform

The Athens 5G platform features 5G and 4G radio access technologies (RATs) deployed in both indoor and outdoor environments combining software network technologies (Figure 10).

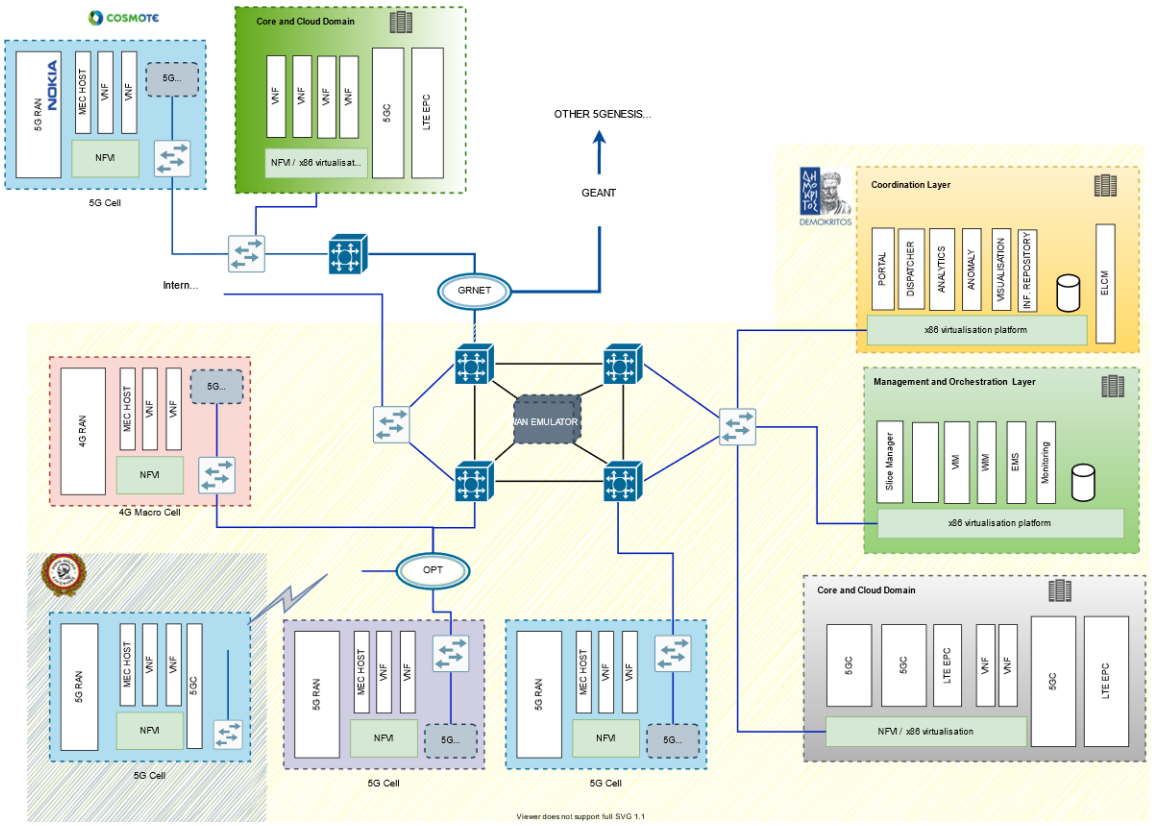

Figure 10: 5GENESIS Athens platform infrastructure

Radio Access: 5G New Radio (NR), is one of the most highlighted features of 5G. 5GNR encompasses a new OFDM-based air interface, designed to support the wide variation of 5G device-types, services, deployments and spectrum. 5GENESIS proposes two alternative implementations of 5GNR, provided by the vendors RunEL and ECM (i.e., OAI). In addition, the Athens platform integrates two commercial solutions Amarisoft 5G CallBox which supports both NSA and SA 5G Core and RAN deployments and Nokia Airscale 5G Macro Cell.

Transport Network

SDN Spine - Leaf Network: The WAN backbone network on the NCSRD site is composed by several physical SDN Switches forming a spine – leaf architecture. All the switches are OpenFlow enabled and support OpenFlow protocol version 1.3. They are controlled by a centralized OpenDayLight (ODL) SDN controller, which is responsible for installing forwarding rules (flows) on each switch.

IP Core Network Gateway: An Integrated Services Router (ISR) by Cisco, alongside a Firewall (i.e., Cisco ASA 5510), are used for the realization of the core network gateway on the NCSRD site. Through these nodes the NCSRD core network is connected to the Internet, via the access provided by Greek Academic network provider (GRNET). Moreover, it is also used as the endpoint for the interconnection between NCSRD and COSMOTE sites using the QinQ Ethernet transport. Finally, a VPN concentrator

server allows remote users to connect to the NCSRD testbed via VPN offering all the standard tunnel types (i.e., OpenVPN, IPSec, Anyconnect).

WAN Emulator: The WAN emulator is implemented by the Mininet (Mininet, n.d.) network emulator, running on a physical server on NCSRD site. It provides an easy way to get correct system behavior experiment with various realistic network topologies, while it runs real code including standard Unix/Linux network applications as well as the real Linux kernel and network stack.

NFV Management and Orchestration: Network Function Virtualisation (NFV) is critical part of the 5G deployments. The purpose of the NFV Management and Orchestration is to allow the provision of Network Services (NS) over the managed NFV infrastructures. In the Athens platform NFVIs are available in all sites of the platform. It is expected that in those locations various NSs will be provisioned and in some cases even the core network functions could be virtualised and orchestrated as a NS.

The NFV Orchestrator in the Athens platform is OSM release 6. OSM is one of the most popular open-source platforms for NFV orchestration, and, being developed under the ETSI umbrella, is also aligned with the ETSI NFV specifications.

The infrastructure virtualisation and management of the physical resources is achieved via the Virtualisation Infrastructure Manager (VIM). This component is based on Opestack Cloud distribution when virtualisation is achieved by VMs and on Kubernetes when the virtualisation is achieved by means of containers.

2.3.4.2. 5G Telefonica Open Network Innovation Centre (5TONIC)

The global 5G Telefonica Open Network Innovation Centre (5TONIC) was created in 2015 by Telefonica I+D and IMDEA Networks Institute as a leading European hub for knowledge sharing and industry collaboration in the area of 5G technologies. Currently, 5TONIC is a key infrastructure part of the Infrastructure projects in the 5G PPP phase 3, 5GVINNI and 5GEVE, and for advance verticals, such as 5GROWTH. The site already has a deployed network infrastructure for supporting pre-5G trials and a number of use-cases detailed in www.5tonic.org.

Figure 11 illustrates the infrastructure that is currently available for experimentation at the 5TONIC laboratory.

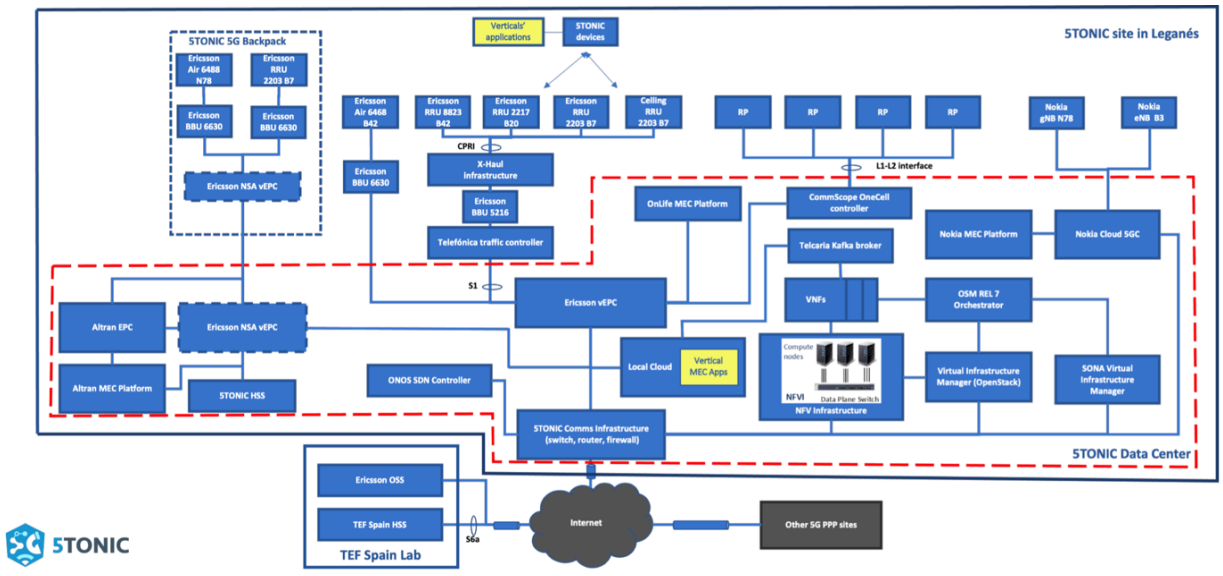

Figure 11: 5TONIC infrastructure

The main components of 5TONIC are the Radio access and Core technology (LTE and 5G), the communication infrastructure, and the NFV management and infrastructure.

Radio Access and Core technology and Infrastructure: The Radio Access Network (RAN) comprises OpenSource OpenAirInterface (OAI) New Radio (NR) with an initial deployment of the radio in a srsLTE solution, that is currently migrating to a OAI LTE/5G ecosystem with 5G NR support. The radio hardware is based on USRP B200 mini. Alternatively, Ericsson NR is available that comprises the Baseband 6630, and new radio unit AIR 6468 B42. The hardware is 5G NR ready, fully compliant to 3GPP R15 and later. 5G Plug-in Massive MIMO over LTE TDD is also available. The support of an SA 5G deployment is currently ongoing. As part of the Core technologies, two alternatives are available OpenSource OAI Next Generation Core (NGC) and Ericsson NGC. The Ericsson core network equipment is a vEPC-in-a-box that fulfills the vEPG, vSGSN-MME, and vPCRF. Both types of core hardware have support for 5GNR NSA and the second one could support SA with software upgrade. The support of an SA 5G deployment is currently ongoing, with the upgrade of the EPC to NGC.

Transport and communication infrastructure: The 5TONIC site is connected through a high-speed network access to the Internet via RediMadrid, RedIRIS and GEANT. Secure external access may be provided via VPN gateways, allowing different solutions to support management, control and data operations from remote network locations, depending on specific requirements. Also, Telefonica transport network is used to interconnect the site to additional Telefónica premises. Finally, all devices are interconnected by 24-port 10Gbps Ethernet switches.

NFV management and infrastructure: The 5TONIC NFV infrastructure (NFVI) is deployed with OpenStack Stein and KVM as VMs manager and Kubernetes cluster. The computing resources available for VNFs and control plane includes several NFVI physical Nodes based in Intel® Xeon® architecture, with multiples cores, multiple Gb of RAM and several interfaces of 1-10 Gbps. Related to management, several MANagement and Orchestration (MANO) platforms, following are available:

- Open-Source Mano (OSM), with NFV-Orchestrator and VNF Manager based on OSM Rel. SEVEN, the VIM based on OpenStack Stein, and SDN based on OVS and Whitebox switches.
- Service orchestration based on OpenSlice (https://openslice.io), supporting a Network Slice as a Service (NSaaS) model
- OpenNESS Intel's MEC solution following the ETSI GR MEC 017 document statements including the OpenNESS controller and the OpenNESS compute node is a dedicated physical server within the NFVI. Edge apps running as VMs or OS containers are both supported.

The 5TONIC environment described can be considered as part of the service hosting infrastructure for the PALANTIR project. It will provide hosting for several PALANTIR components related to network infrastructure, security as a service VNFs and service orchestration.

3. Threat Analysis

In Section 3, we present the attack surface analysis related to SME/ME networks, focusing on the possible types of attacks and attack vectors based on related literature, also offering a comprehensive view of the attack surface analysis applied in similar projects by partners of the PALANTIR consortium. Moreover, we provide a detailed comparison of the existing risk-based assessment frameworks from ENISA and NIST and justify the selection of the framework that is adopted for the purposes of the project. The current section is also linked with Section 2, as it provides a preliminary version of the risk assessment for each use case, including a definition of the relevant attack classes, entry/exit points, channels and data stores in each PALANTIR deployment.

3.1. Attack Surface Analysis

In this subsection, we review threats and potential compromises related to the security of networks in SME/MEs. To provide a comprehensive account of the emerging threat landscape, this section has identified related network assets and the security threats, challenges and risks arising for these assets.

As commonly defined, an asset is anything that has value and therefore requires protection. Due to their value, assets become the targets of threat agents. Threat agents are human or software agents, which may wish to abuse, compromise and/or damage assets. Threat agents may perform attacks, which create threats that pose risks to assets.

In a typical Information and Communication Technology system (ICT), assets can be: (a) hardware, software and communication components; (b) communication links between them; (c) data that control the function of the system, are produced and/or consumed by it, or flow within it; (d) the physical and organizational infrastructure within which the ICT system is deployed, and (e) the human agents who interact with the system and may affect its operation (e.g., users, system administrators etc.).

Valuable assets of a network infrastructure are presented that are commonly found in the literature in a hierarchical manner[1]. Based on a single first top layer classification these assets are distinguished into (Figure 12):

- **Data Assets**: This asset group includes all assets of the network deployments that include the physical instances of the network such as switching devices (Switches/Routers) and the communication medium (wired or wireless). Data assets include both hardware and software (e.g., Firmware, or a more or less full-fledged operating system and software switch) of the so-called network elements.
- **Application Assets**: This asset group includes software applications that are used to implement any network explicitly, directly. Application assets include also hardware that is used to run these applications (e.g., Servers)
- **Users**: This asset group includes any User that is using equipment interacting with data.
- **Service provider IT Infrastructure Assets**: This asset group includes any component of an IT infrastructure that is used by or belongs to any service provider in the SME/MEs from a billing system to stored data of an end user in a cloud.
- **Network service provider physical infrastructure Assets**: This asset group includes physical assets of the network service providers including every construction (e.g., Buildings, data centres etc.), machinery as well as the power supply networks
- **Human Assets**: This asset group includes any human in the SME/MEs and network administrators to simple end users.

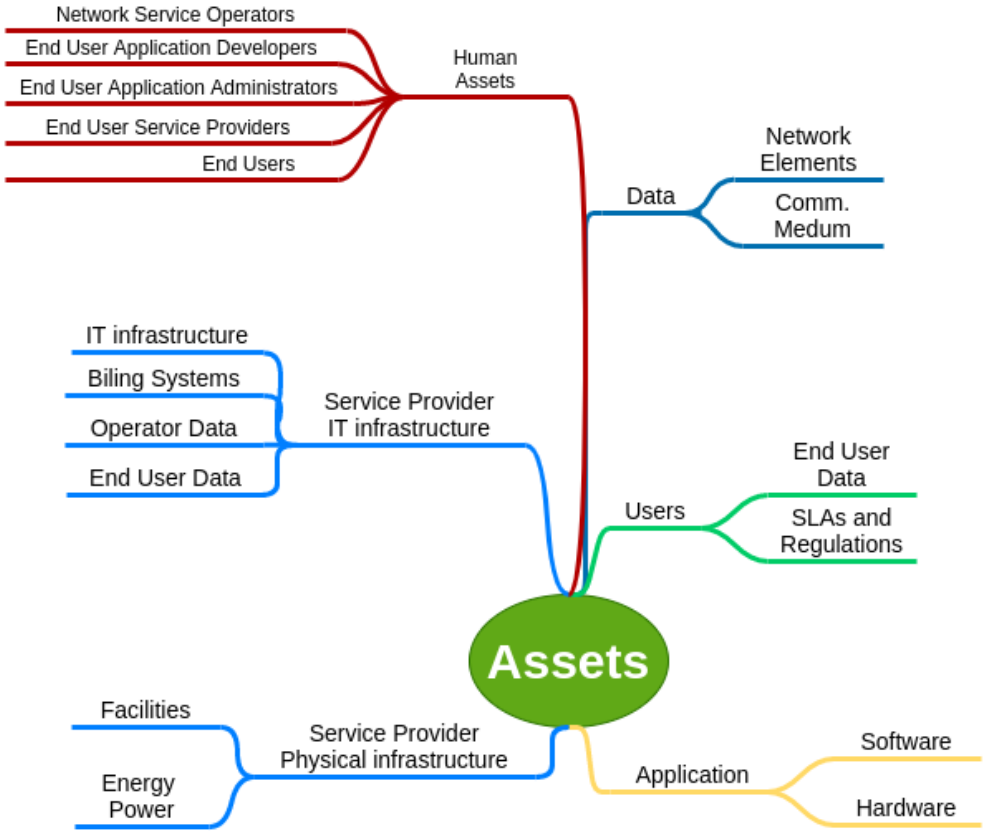

Figure 12: Attack surface analysis asset classification

3.1.1 Possible Types of Attacks

Taxonomy is a classification approach used now in many research fields, including Cybersecurity, in which a threat taxonomy groups threats in hierarchical classes according to certain common characteristics (Figure 13). This classification becomes fundamental for identifying the detection and prevention approaches to be applied, as different cyberattacks require different methods according to their nature[2].

Taxonomy of Threats:

- **Nefarious activity/abuse (NAA)**: This threat category is defined as "intended actions that target ICT systems, infrastructure, and/or networks by means of malicious acts with the aim to either steal, alter, or destroy a specified target"
- **Eavesdropping/Interception/ Hijacking (EIH)**: This threat category is defined as "actions aiming to listen, interrupt, or seize control of a third-party communication without consent"
- **Physical attacks (PA)**: This threat category is defined as "actions which aim to destroy, expose, alter, disable, steal or gain unauthorised access to physical assets such as infrastructure, hardware, or interconnection"
- **Damage (DAM)**: This threat category is defined as intentional actions aimed at causing "destruction, harm, or injury of property or persons and results in a failure or reduction in usefulness"

- **Unintentional Damage (UD)**: This threat category is defined as unintentional actions aimed at causing "destruction, harm, or injury of property or persons and results in a failure or reduction in usefulness"
- **Failures or malfunctions (FM)**: This threat category is defined as "insufficient functioning of an (Internet infrastructure) asset.
- **Outages (OUT)**: This threat category is defined as "unexpected disruptions of service or decrease in quality falling below a required level"
- **Disaster (DIS)**: This threat category is defined as "serious disruption of the functioning of a society
- **Legal (LEG)**: This threat category is defined as "legal actions of third parties (contracting or otherwise), in order to prohibit actions or compensate for loss based on applicable law"

Physical threats: This type of attack refers to actions (attacks) aimed at destroying, disabling, altering or stealing physical ICT infrastructure assets. This type of threat applies to any network and computing infrastructure, including SDN/5G infrastructures. Physical threats are very important due to the virtualisation of networking functions, which may result in deploying such functions in remote servers and data centres. Despite the existence of physical protection mechanisms (e.g., physical surveillance and surveillance cameras, security locks, security guards), physical breaches and insider threat attacks still occur. Examples of such attacks include fraud, sabotage vandalism, theft, information leakage/sharing, unauthorised physical access and terrorist attacks.

Damage/loss: This type of threat refers to intentional or unintentional destruction of ICT infrastructure. It may be physical as for example the destruction of a server or take the form of a cyber damage as, for example, mixing-up information in a data centre due to maintenance errors or erroneous system administration.

Failures/malfunctions: This type of threats refers to failures or insufficient functioning of network and infrastructure subsystems. Examples of this threat type include failure or malfunctioning of devices including network elements, controllers and network management applications, disruption of the communication links, and/or failure of service providers.

Outages: This type of threat refers to the interruption or failure in the supply of a service. More specifically interruption of support services such as Internet and electricity, the loss of network connectivity either due to cable errors or the loss of (part of) a wireless network, or loss of human (e.g., strike of employees of a network operator) or physical resources.

Disaster: A disaster is a sudden incident that interrupts the daily activities of the society. It can be categorised in disasters caused by the intervention of human (environmental) or natural disasters such as floods, earthquakes etc.

Legal: Since the 5G landscape is of multi-operator nature, where all operators will be interconnected to each other, multi-operator related threats are very important. In this landscape, operators of the SDN infrastructure that will not honestly stick to business agreements (SLAs) should be considered. Moreover, measures for non-repudiation of SLAs between different operators should be considered.

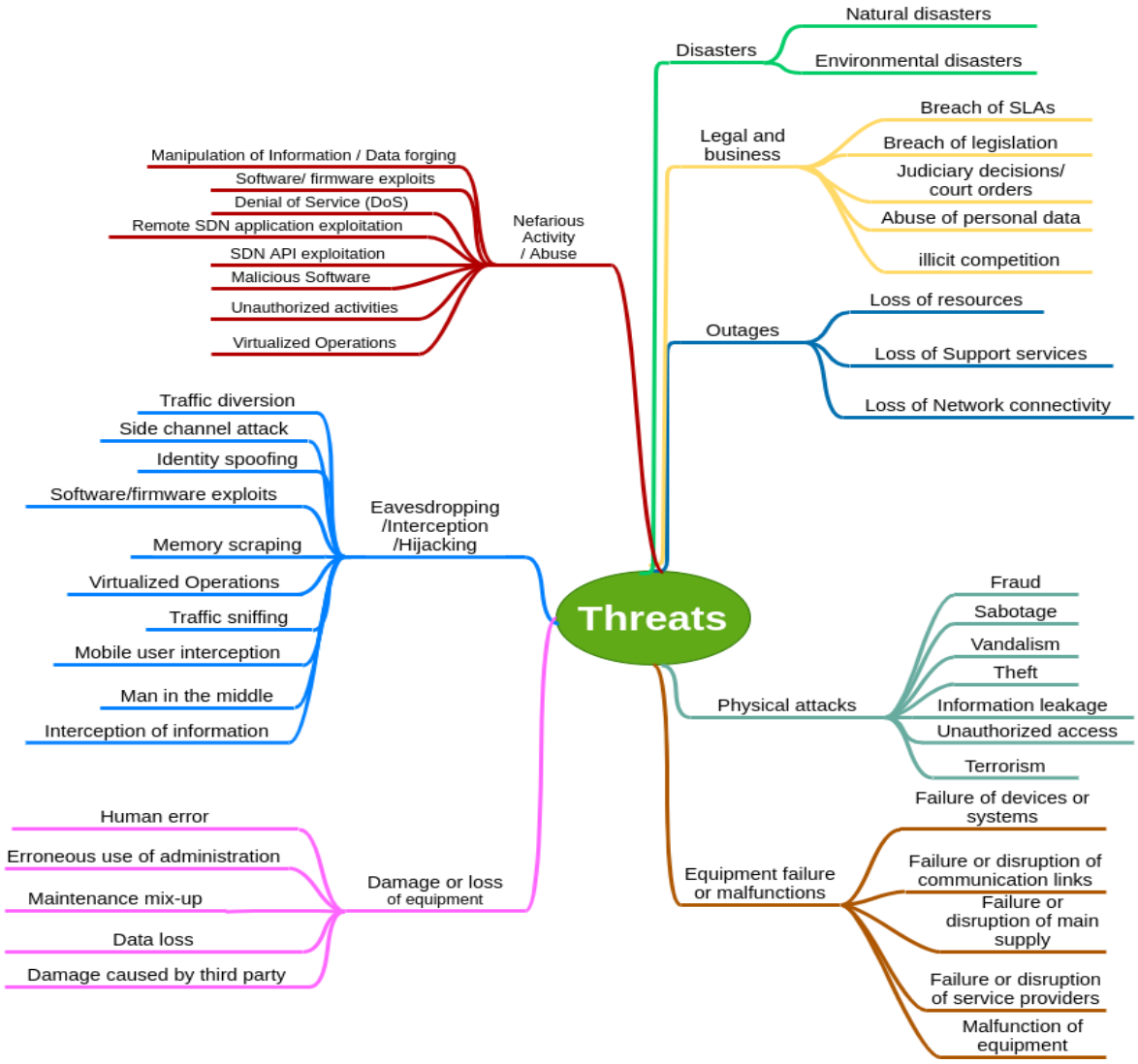

Figure 13 Threat taxonomy

3.1.2 Overview of Attack Vectors

An attack vector is a path or means by which an attacker can gain unauthorized access to a computer or network to deliver a payload or malicious outcome. Attack vectors allow attackers to exploit system vulnerabilities, install different types of malware and launch cyber attacks. Attack vectors can also be exploited to gain access to sensitive data, personally identifiable information (PII) and other sensitive information that would result in a data breach[3].

Specific Attacks on Networks:

- **Traffic diversion:** This threat involves compromising a network element in order to divert traffic flows and to enable eavesdropping. Traffic diversion is a threat relating to network elements of the data plane. A specific kind of traffic diversion that is available in virtualized networks is network slice trespassing. This occurs when the mandatory isolation between slices is compromised in any active node or when the enforcing access to a slice in the edge equipment is either bypassed or misconfigured. This ends with alien traffic circulating on a given slice [4].

- **Side channel attack:** This threat involves extracting information on existing flow rules that are used by network elements. The threat can be realised by exploiting patterns of network operations (e.g., exploiting the time required for establishing a network connection). Side channel attacks are a threat relating to network elements of the data plane[5].
- **Flooding attack:** Flooding attacks involve compromising a network component in order to make it flood other components, which it interacts with. Flooding occurs through the transmission of data that can exhaust component resources and lead to a reduction or complete shutdown of the service provided by the component. Flooding attacks occur primarily for network components of the data plane. In such cases, the threat involves compromising a network component in order to make it flood its controller with network messages, and overload and eventually exhaust the controller's resources[6].
- **Software/firmware exploits:** This threat involves exploiting vulnerabilities of the software/firmware in order to cause some malfunction, reduction or disruption of service, eavesdrop data or destroy/compromise data. Software/firmware exploits of network elements and controllers cause the malfunction or even their termination of operation. In the case of switches, for example, the exploited switches can drop, slow down, clone or deviate network traffic. Exploited switches software/firmware can also create forged traffic in order to exhaust other switches and/or the controllers the switches are connected to[7].
- **Denial of Service (DoS):** This threat relates to attacks aimed at causing reduction or disruption of a network service. At the data plane, DoS can be caused by attackers, which flood the bandwidth or resources of network elements. This arrack type in many occasions originates from multiple compromised systems, such as botnets, which are flooding the targeted network with traffic. At the control plane, a DoS can be caused by congesting controllers through a large number of forged flow arrivals, causing network performance degradation and interruption. DoS attacks may also appear at the application plane affecting, for example, network management applications[8].
- **Identity spoofing:** Identity spoofing is a threat where a threat agent successfully determines the identity of a legitimate entity and then masquerades this entity in order to launch further attacks. Identity spoofing is a threat that can affect any type of software component or human agents[9].
- **API exploitation:** This threat involves exploiting the API of a software component in order to launch different types of further attacks such as the unauthorised disclosure, compromise of integrity and/or destruction of information, or the unauthorised destruction/degradation of service[10].
- **Memory scraping:** This threat arises when an attacker scans the physical memory of a software component in order to extract sensitive information that is it not authorised to have[11].
- **Remote application exploitation:** In this threat, an attacker gains access or obtains higher access privileges to an application by exploiting software vulnerabilities of it. This can then be used to execute operations illegitimately[12].
- **Traffic sniffing:** Traffic sniffing involves tapping data flows within a network. In SDN, traffic sniffing has been identified primarily as an attack upon the communication link between an application and a switch/router in order to gain access to important data or application-level credentials. Traffic sniffing can be enabled by the use of weak or no encryption in the relevant communication link. It should be noted that traffic sniffing might also be used for legitimate reasons (e.g., for network monitoring and administration) and if used in this manner it should not be regarded as an attack[13].

Specific Attacks on wireless Networks:

- **DoS attack**: SDN centralizes the network control platforms and enables programmability in communication networks. These two disruptive features, however, create opportunities for cracking and hacking the network. For example, the centralized control will be a favorable choice for DoS attacks, and exposing the critical Application Programming Interfaces (APIs) to unintended software can render the whole network down. The SDN controller modifies flow rules in the data path, hence the controller traffic can be easily identified. This makes the controller a visible entity in the network rendering it a favorite choice for DoS attacks[14].
- **Hijacking attacks**: The Session Hijacking attack consists of the exploitation of the web session control mechanism, which is normally managed for a session token[15].
- **Signaling storms**: Internet of Things devices, gateways and networks, rely either on mobile networks or on Internet Protocols to support their connectivity. However, it is known that both types of networks are susceptible to different types of attacks that can significantly disrupt their operations. In particular 3rd and 4th generation mobile networks experience signalling related attacks, such as signalling storms, that have been a common problem in the last decade[16].
- **Configuration attacks**: Current Network Function Virtualization (NFV) platforms do not provide proper security and isolation to virtualized telecommunication services. One of the main challenges persistent to the use of NFV in mobile networks is the dynamic nature of Virtual Network Functions (VNFs) that leads to configuration errors and thus security lapses[17].
- **Saturation attacks**: A saturation attack may disturb the normal delivery of packets and even make the SDN system out of service by flooding the data plane, the control plane, or both. (e.g., flooding SDN controllers with SYN (tcp 3-way handshake packets)[18].
- **Man-in-the-middle attacks**: A man-in-the-middle attack using ARP poisoning can intercept the traffic between a client and the SDN controller and be able to capture login credentials of the controller[19].
- **Reset and IP spoofing**: This attack again is based on tcp, where the attacker hides his IP by using another one (probably trusted to the victim) and then sends multiple reset packets causing control channels to fail[20].
- **Scanning attacks**: LTE Cell Scanner and Tracker (open source) software that can be used to sniff an LTE mobile access network and obtain information on the network topology and design[21].
- **Semantic information/Timing/Boundary attacks**: All these attacks compromise the location of a victim[22].
- **IMSI catching attacks**: (International Mobile Subscriber Identification). A telephone eavesdropping device used for intercepting mobile phone traffic and tracking location data of mobile phone users. Essentially a "fake" mobile tower acting between the target mobile phone and the service provider's real towers, it is considered a man-in-the-middle (MITM) attack[23].

3.1.3 Attack surface analysis of related projects

In this section we provide a list of attack surface analysis applied in previous projects by partners of the PALANTIR consortium, listed in Table 7:

Table 7: Attack surface analysis of relevant projects

Project Name	Partner Name	Attack Vectors	Detection Enablers	Mitigation Enablers	Attack Surface (Affected Component/ layer)
5GZORRO	UMU	Collusion and Sybil attacks Code injection, overflow attack, data leak Data forging, memory cripting Spoofing attack, DoS Side-channel attack	Pule-based IDS: predefined rules and signatures for detecting known threats Anomaly detection: ML-based techniques to learn the behaviour by analysing network data and forming a baseline Anomaly-Based Firewalls or Signature-Based firewalls	Configuration of firewall policies Isolation of 5GZORRO platform components using TEEs functionalities (VIM trusted execution) Limit the number of dynamic requests to the server under attack (filter traffic) End-to-end encryption in inter-domain communications	Stakeholders (CSPs or 3rd Party Providers) Core components: SDNs, NFVs, VIM, MANO
SHIELD	(SHIELD team)	DDoS Malware Cryptojacking Data breach (DNS tunelling)	Detection: LDA, Autoencoders, SVN Classification: Random Forests	Traffic redirection, traffic blocking	Endpoints
	(SHIELD team)	SDN rules manipulation Firmware modification	Attestation	Configuration restore	SDN switches
	(SHIELD team)	VNF integrity violation	Attestation	VNF shutdown & restoration of	VNFs

				previous instance	
Inspire5G-plus	TID	DoS, malware caused by potential VNF software vulnerabilities Priviledge escalation, and VM escape exploiting vulnerabilities in virtualization layer (hypervisors)	Machine Learning technique: Anomaly detection, traffic patters identification	hypervisor introspection. The hypervisor introspection acts as a host-based IDS	NFV Infrastructure and MANO
		DoS in switches (flooding, ARP poisoning) Topology poisoning attacks: injecting malicious hosts for MItM new network applications for SDN	ML enhanced network intrusion detection tools Periodic Topology checks	Enhanced authenticatio n Isolation of the applications	SDN Control plane
		MitM, eavesdropping, spoofing	ML enhanced network intrusion detection tools Periodic Topology checks	capacities of filtering in the data plane monitoring service enciphering/ deciphering functions to assure the data confidentialit y	the access network where MEC is present
SPIDER (5G Cyber Range)	TID	cryptomining	ML enhance d network intrusion	Report	VNFs

			detection tools		
		Attack a DNS Infrastructure (UDP/53 and DoH)	ML enhanced network intrusion detection tools	Report	DNS infrastructure
		Encrypted vulnerability scaning over TLS	ML enhanced network intrusion detection tools	Report	Web services
		Components with vulnerable versions	Review components Versions	Software upgrade	Services

3.2. Risk-Based assessment

3.2.1 Risk assessment frameworks survey

The goal of this section is to describe and compare the two most common risk management frameworks, namely the NIST Risk Management Framework (NIST RMF) and the ENISA framework for Risk Management.

3.2.1.1 NIST Framework

In this section, the risk management framework (RMF) developed by the National Institute of Standards and Technology (NIST)[24] is discussed.

The RMF serves as guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk. It is a series of documents which intent to provide a holistic and comprehensive risk management process based on three components.

The Cybersecurity Framework consists of three main components: Core, Implementation Tiers, and Profiles.

The Core is a set of desired cybersecurity activities and outcomes organized into Categories and aligned to Informative References. The Framework Core is designed to be intuitive and to act as a translation layer to enable communication between multi-disciplinary teams by using simplistic and non-technical language. The Core consists of three parts: Functions, Categories, and Subcategories. The Core includes five high level functions: Identify, Protect, Detect, Respond, and Recover. These 5 functions are not only applicable to cybersecurity risk management, but also to risk management at large. The next level down is the 23 Categories that are split across the five Functions. Figure 14 depicts the Framework Core's Functions and Categories.

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Figure 14: NIST Core component and functions

The five Functions included in the Framework Core are: Identify, Protect, Detect, Respond, Recover:

- **Identify**: The Identify Function assists in developing an organizational understanding to managing cybersecurity risk to systems, people, assets, data, and capabilities.
- **Protect**: The Protect Function outlines appropriate safeguards to ensure delivery of critical infrastructure services.
- **Detect**: The Detect Function defines the appropriate activities to identify the occurrence of a cybersecurity event.
- **Respond**: The Respond Function includes appropriate activities to take action regarding a detected cybersecurity incident.
- **Recover**: The Recover Function identifies appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

The NIST RMF framework is comprised of 6 steps which defines the process of conducting the risk analysis of the company's assets, as depicted on Figure 15.

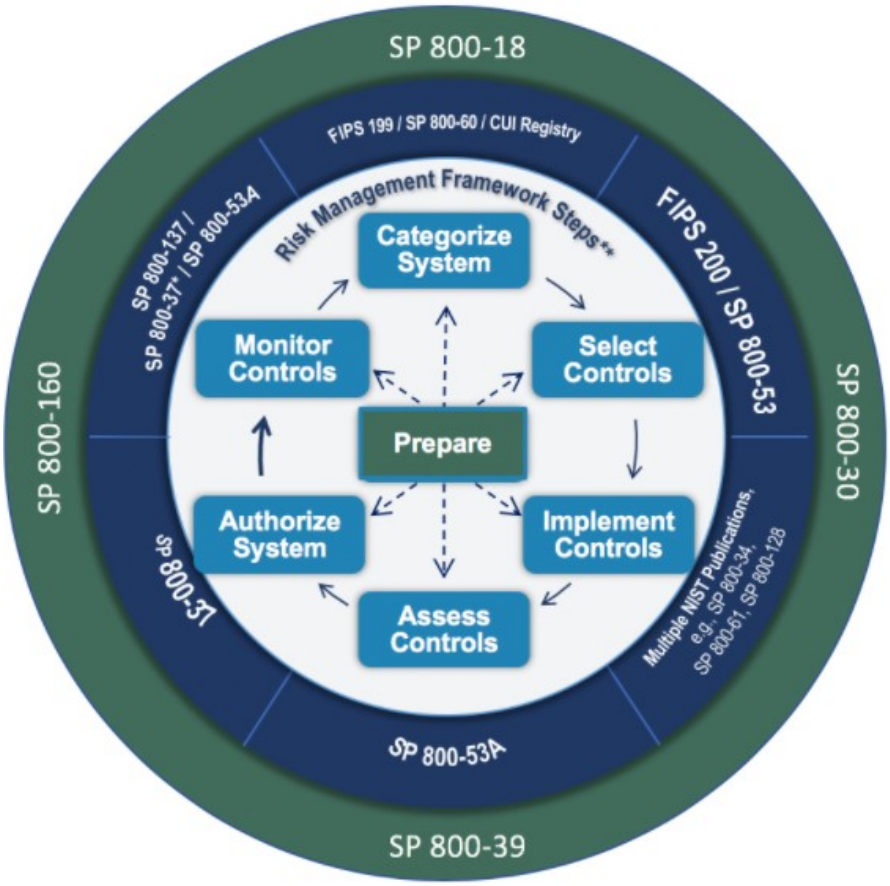

Figure 15: NIST risk management framework (RMF) workflow steps

The six steps defined on the RMF: Prepare, Categorize, Select, Implement, Assess, Authorize, Monitor, are based around the **security controls** for each task of the process, instead of a classic asset-based approach, where the risk assessment is performed individually on each cluster of assets with the same characteristics.

Overall, the architecture presented enables a RMF to be very **scalable**, **automatable**, and **transversal** to different business **profiles**, since risk management is a never-ending task, having tools and procedures resilient to entropy and adaptable to regulation and policy changes, is a must.

3.2.1.2 ENISA Framework

In this section the ENISA framework for Risk Management[25] is discussed. In the present form, Risk Management for ENISA is considered to be the umbrella under which several processes/activities concerning the identification, mitigation, management and control of risks take place. For the sake of the presentation, an integrated view of Risk Management is presented in terms of a “big picture”, i.e., the five processes and their activities (Figure 16). Furthermore, this figure shows possible interfaces among the processes presented.

In practice, any of the Risk Management processes can be used as an entry point to the Risk Management process or can be performed in isolation. Many organizations, for example, perform Risk Treatment without the performance of Risk Assessment or without the prior establishment of a Corporate Risk Management Strategy. Others might perform Risk Assessment and then proceed directly with other activities of ISMS. The ideal sequence for the performance of the processes of Risk Management is to start with the establishment of a Corporate Risk Management Strategy and proceed according to the

orange cyclic arrow as indicated in the figure, whereas mutual interactions between the processes might also be performed (e.g., performance of Risk Assessment after a Risk Acceptance).

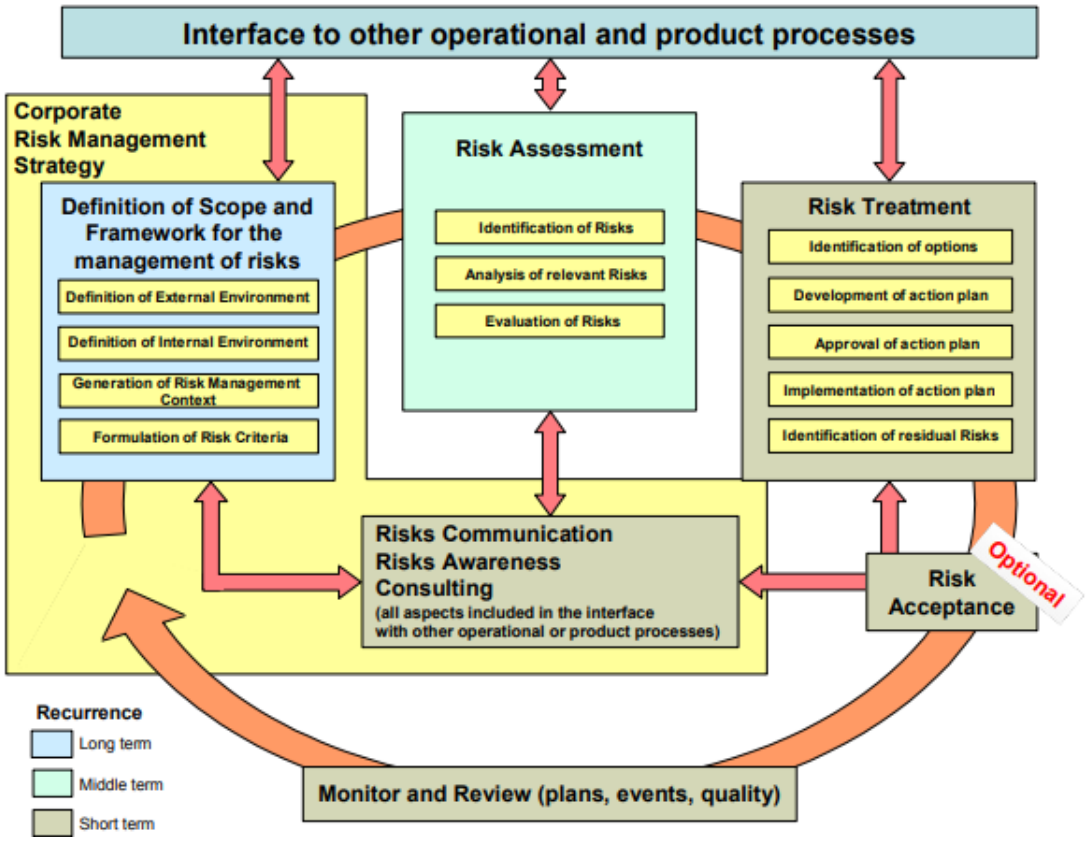

Figure 16: ENISA overall cycle of a Risk Management process

It is worth mentioning, that no effective Risk Management system can be established in an organization, if it lacks such interfaces and especially to other relevant operational or product processes (see box at the top of Figure 16). For the definition of Risk Management itself, the ENISA definition is adopted:

Risk Management is the process, distinct from Risk Assessment, of weighing policy alternatives in consultation with interested parties, considering Risk Assessment and other legitimate factors, and selecting appropriate prevention and control options.

Risk Management is considered as consisting of the five main processes shown in the figure above: Definition of Scope, Risk Assessment, Risk Treatment, Risk Communication and Monitor and Review. It is worth mentioning, that the two processes Definition of Scope and Risk Communication are considered to make up the Risk Management Strategy (represented in Figure 16 by the yellow box).

For the above-mentioned processes of Risk Management, the following definitions are used:

- **Definition of Scope:** Process for the establishment of global parameters for the performance of Risk Management within an organization. Within the definition of scope for Risk Management, both internal and external factors have to be taken into account.
- **Risk Assessment:** A scientific and technologically based process consisting of three steps, risk identification, risk analysis and risk evaluation.
- **Risk Treatment:** Process of selection and implementation of measures to modify risk. It can also include avoiding, optimizing, transferring or retaining risk
- **Risk Communication:** A process to exchange or share information about risk between the decision-maker and other stakeholders inside and outside an organization (e.g., departments and

outsourcers respectively). The information can relate to the existence, nature, form, probability, severity, acceptability, treatment or other aspects of risk.

- **Monitor and Review:** A process for measuring the efficiency and effectiveness of the organization's Risk Management processes is the establishment of an ongoing monitor and review process. This process makes sure that the specified management action plans remain relevant and updated. This process also implements control activities including re-evaluation of the scope and compliance with decisions.

Overall ENISA covers the broader topic of Risk Management and does not focus considerably on Risk Assessment in relation to cybersecurity. It also worth noting that the document is relatively dated (published in 2006).

In addition to the above more generic approach of Risk Management, ENISA has published a deliverable titled "Information Package for SMEs" [26] discussed in the following section, that provides guidelines on the application of Risk Management for SMEs.

3.2.1.3 NIST and ENISA framework comparison

In this section, NIST and ENISA frameworks are presented and compared (Table 8). We provide some differences between them regarding the followed approach, security control-based approach (NIST) and risk-based approach (ENISA).

Table 8: ENISA and NIST framework comparison

<table>
<tr><th colspan="2">ENISA Framework</th><th colspan="2">NIST Framework</th></tr>
<tr><th>Step</th><th>Purpose</th><th>Purpose</th><th>Step</th></tr>
<tr><td>Corporate Risk Management Strategy</td><td colspan="2">Similar purpose</td><td>Prepare Step</td></tr>
<tr><td rowspan="2">Risk Assessment</td><td rowspan="2">Risks identification and evaluation</td><td>Risks identification</td><td>Categorize Step</td></tr>
<tr><td>Select sec. controls</td><td>Select Controls</td></tr>
<tr><td rowspan="2">Risk Treatment</td><td rowspan="2">Action plan creation, implementation and evaluation</td><td>Implement sec. controls</td><td>Implement Controls</td></tr>
<tr><td>Assess sec. controls</td><td>Assess Controls</td></tr>
<tr><td>Risk Acceptance</td><td colspan="2">Similar purpose</td><td>Authorize Controls</td></tr>
<tr><td>Monitor and Review</td><td colspan="2">Similar purpose</td><td>Monitor Controls</td></tr>
</table>

Both frameworks have a first similar step, where the organisation is evaluated and the environment is defined, the risk management context is created and the definition of criteria definition is established. The second step is also similar, as both frameworks propose the assets identification and the risks associated with them.

The following steps are different in both frameworks. On one hand, the ENISA framework follows a **risk-based approach**, and the central steps of its framework focus on addressing the risks and creating an action plan to react to them. When this action plan is implemented, the methodology concludes with the risk acceptance, risks that cannot be avoided due to different reasons, such as costs or danger of risk, and the monitor and review to improve the approach with the experience and its use in the organisation.

On the other hand, the NIST framework follows a **security control-based approach**. This framework uses the risks' identification and evaluation as an intermediate step to select the necessary security controls, which will be implemented and deployed in the organisation. Thanks to the security controls, the NIST framework can be automated. The last steps are aligned with the ENISA framework, where the risk acceptance and monitor/review procedures are performed.

Another important aspect is the availability of resources based on ENISA and NIST methodologies, when considering how to implement and automate the frameworks. In this sense, Table 9 is presented.

Table 9: ENISA and NIST resources comparison

	Year	SME approach	Guides	Tools	Protocols
ENISA Framework	2006	Yes	Webpage	Proprietary and outdated tools	---
NIST Framework	2010 (v1), 2018 (v2)	Yes	SP 800-53, SP 800-34, etc.	OpenSCAP, etc.	SCAP, OSCAL, etc.

As we can see, the ENISA framework was started earlier, and only presents one version from 2006. The NIST framework provides two versions, with its more recent second release from 2018. However, both frameworks have considered the SME/MEs environment and have a specific approach for SME/MEs.

Regarding the available resources, ENISA offers tools collection but some of them are outdated and the rest of tools are proprietary software. By contrast, NIST offers several protocols, such as SCAP[27] and OSCAL[28], which allows us to automate various processes within the risk management.

As a result of this comparison, we can say that the NIST framework is a newer project with a wider catalogue of up-to-date tools, protocols and guides to facilitate the risk analysis and management tasks.

3.2.2 PALANTIR Risk Assessment approach

PALANTIR should provide a risk-based assessment like that provided by the ENISA SME framework[29], which allows the platform client to know the risks associated with its information systems, network, components, architecture and so on. In this sense, a risk assessment approach needs to be selected and established in order to find, design, develop and deploy possible mechanisms that allow PALANTIR to perform a correct risk-based analysis.

As we mentioned above, NIST and ENISA methodologies have been analysed, and one of them should be established as the chosen approach to use in PALANTIR. A main consideration to have in mind when selecting one of them is the demographic origin of the institution that has carried out the approach. Therefore, ENISA framework should be first considered and prioritised in a project performed in the framework of the European research.

However, in the comparison between the ENISA and NIST frameworks performed in Section 3.2.1.3, it has been possible to check that the NIST framework presents a higher maturity level, with more technologies and tools created; as well as the age difference between both projects and related tools. Due to this reason, the need to take advantage of NIST tools is fundamental to PALANTIR's interests.

On the other hand, ENISA proposes the ENISA SME framework divided in four phases presented in Figure 17.

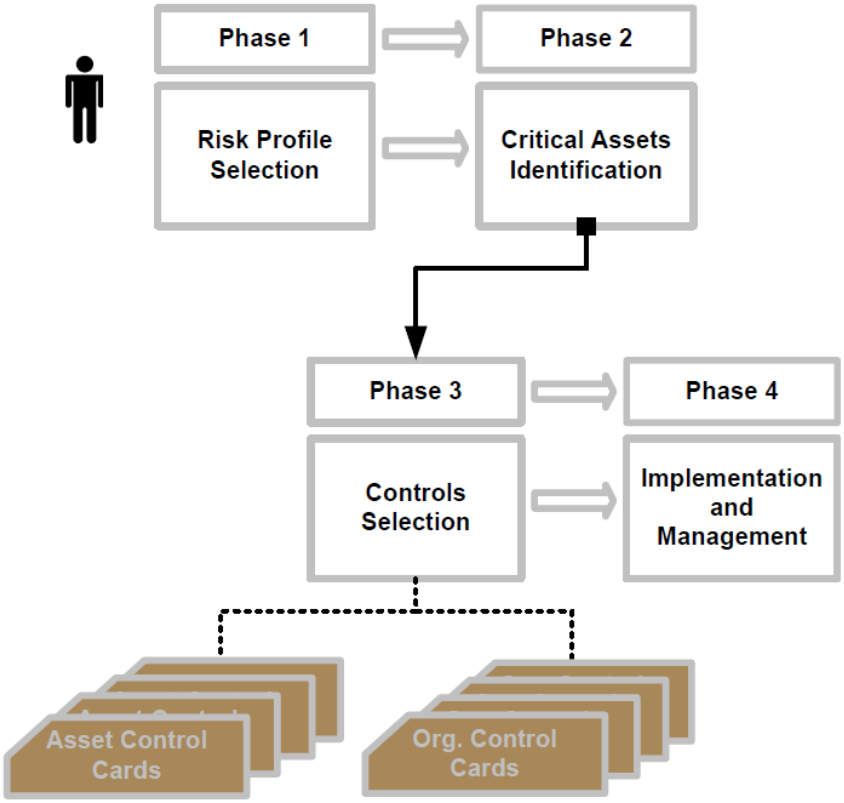

Figure 17: ENISA SME Framework

This framework follows a hybrid risk-based and security controls-based approach, which allows us to position this approach between ENISA and NIST frameworks. The main advantage this framework provides is the possibility to use methods and tools provided by both methodologies, since the first two phases are risk-based, and the last two are the ones based on security controls. This reason highlights that ENISA SME approach is the best option to adopt in the PALANTIR project.

PALANTIR can design and implement different risks profiles, which will adapt to the client needs. The risk profile selection will be joint to the critical assets' identification, the unique step with more human interaction, since the client should enumerate the assets found in its organisation. The last two phases will be designed and deployed with the NIST tools, due to the selection, implementation and management of the security controls applied with the results of the first two phases.

In addition, the last two phases will be performed in an automated way thanks to the NIST tools, which offer interesting functionalities, such as vulnerabilities tests, security services deployments, customised security settings and lifecycle management.

3.2.3 Preliminary Use Case Risk Assessment

This section provides a preliminary version of the risk assessment for each use case, including a comprehensive definition of the relevant attack classes, entry/exit points, channels, data stores etc. in each PALANTIR deployment. The following tables (one for each UC) are organized using the Common Attack Pattern Enumeration and Classification (CAPEC) system[30], a comprehensive dictionary and classification taxonomy of known attacks developed by MITRE[31] that can be used by analysts, developers, testers, and educators to advance community understanding and enhance defenses. In cases where the addressed threat was not included in the CAPEC system, the Common Vulnerabilities and Exposures (CVE) system[32] was used as a reference method for publicly known security vulnerabilities.

This view organizes attack patterns hierarchically based on mechanisms that are frequently employed when exploiting a vulnerability. The categories that are members of this view represent the different techniques used to attack a system.

3.2.3.1 Risk Assessment of Use case #1: Securing private medical practices with lightweight SecaaS

Table 10: Risk Assessment for UC1: Securing private medical practices with lightweight SecaaS

Threat id[3]	Threat Cat. Id[2]	Adversarial Technique[1]	Threat Description	Consequence of Incident	Impact (business level)	Likelihood	Countermeasures (if applicable)
D01	CAPEC-94	Man-in-the-Middle Attack	The attacker positions himself/herselft between the Medical practitioner's device and the online medical services, in order to gain access to private medical data.	Retrieval/Modification of Sensitive/Personal private data. Illegal drug prescription. Publication of medical exam vouchers. Patient Identity theft.	4	2	Detection of MITM attack based on monitoring of local infrastructure and leverage of ML mechanisms.
D02	CAPEC-125	Flooding	The attacker performs UDP/TCP flood attack, overwhelming the practitioner's resources. When successful this attack prevents legitimate users from accessing the service and can cause the target to crash.	Medical Practitioner cannot access online services.	3	4	Detection of flooding Firewall policy enforcement to discard malicious flows ACL policies to restrict, local attacking device
D03	CVE-2020-16043 CVE-2021-23961	NAT Slipstreaming	NAT Slipstreaming allows a bad actor to bypass NAT/firewall and remotely access any TCP/UDP service bound to a victim machine as a result of the target visiting a malware-infected website	Opportunity to attack internal devices and enact a series of other remote attacks	4	2	Attack Detection Traffic Diversion ACL policying

Threat id[3]	Threat Cat. Id[2]	Adversarial Technique[1]	Threat Description	Consequence of Incident	Impact (business level)	Likelihood	Countermeasures (if applicable)
			specially crafted for this purpose.				
A01	CAPEC-441	Malicious Logic Insertion	The medical practitioner accidentally installs or adds malicious logic (also known as malware) in the form of a seemingly benign component of a fielded system. This logic is often hidden from the user of the system and works behind the scenes to achieve negative impacts.	Access to the component currently deployed at a victim location. Unlawful logging of information and data leakage to the attacker	4	1	Detection data leakage using ML mechanisms Firewall policies

1. Only applicable on deliberate threat
2. The Threat Cat ID is same to Threat ID for non-adversarial threat
3. The threat id starts with:
    a. "D" → represents Deliberate threat
    b. "A" → represents Accidental threat
    c. "O" → Other types of threat

3.2.3.2 Risk Assessment of Use case #2: Uninterrupted Electronic Commerce with Cloud SecaaS (SFERA)

Table 11: Risk Assessment for UC2: Uninterrupted Electronic Commerce with Cloud SecaaS

Threat id[3]	Threat Cat. Id[2]	Adversarial Technique[1]	Threat Description	Consequence of Incident	Impact (business level)	Likelihood	Countermeasures (if applicable)
D01	CAPEC-94	Man-in-the-Middle Attack	The attacker positions himself/herself between the employee and the cloud-CMS (and business logic)	Retrieval/Modification of Sensitive/Personal private data from customers. Retrieval/Modification of Sensitive Corporate Information. Insert of malicious code in cooperate web pages and commercial front-ends as the baseline for further web-based-attacks (e.g. XSS, Phishing)	3	2	Detection of MITM attack based on monitoring of local infrastructure and leverage of ML mechanisms. Secure communications channel
D02	CAPEC-94 CAPEC-194 CAPEC-62 CAPEC-593	Counterfeit Websites, Fake the Source of Data	The attacker creates duplicates of legitimate websites or even exploits D01 to inject fake links to corporate pages. When users visit a counterfeit site, the site can gather information or upload malware.	Retrieval/Modification of Sensitive/Personal private data from customers. Retrieval/Modification of Sensitive Corporate Information. Malicious 'link' can be processed and accepted by the targeted application with the users' privilege level. Session hijacking and exploitation of sessions cookies and session cookie-based authentication	5	2	cryptographic tokens ML driven 'randomized' process of user action conformation or identity confirmation Activity Recognition ML supported verification of authentication

Threat id[3]	Threat Cat. Id[2]	Adversarial Technique[1]	Threat Description	Consequence of Incident	Impact (business level)	Likelihood	Countermeasures (if applicable)
D03	CAPEC-125	Flooding	The attacker performs UDP/TCP flood attack, overwhelming the companies local and or cloud resources. When successful this attack prevents legitimate users from accessing the service and may cause distribution in business process and also negative impact on brand	Customers and Employees cannot access services	3	2	Detection of flooding Firewall policy enforcement to discard malicious flows ACL policies to restrict, local attacking device
A04	CAPEC-89, CAPEC-98	Phising and Pharming	An attacker masquerades as a legitimate entity and fools the employee into entering sensitive data into supposedly trusted locations	Opportunity to steal the employee's corporate user identity and gain access to private/sensitive information	4	1	Detection data leakage using ML mechanisms Firewall policies
A05	CAPEC-657, CAPEC-186 CAPEC-441, CAPEC-187 CAPEC-629	Malicious Software Update or Logic insertion as a result of spoofing, pharming, phising	An attacker uses deceptive methods to cause the employee to user or an automated process to download and install dangerous code that compromises the on-site	Opportunity to steal the employee's corporate user identity and gain access to private/sensitive information Unlawful logging of information and data leakage to the attacker	4	2	Attack Detection Activity Recognition Detection data leakage using ML mechanisms Firewall policies

Threat id[3]	Threat Cat. Id[2]	Adversarial Technique[1]	Threat Description	Consequence of Incident	Impact (business level)	Likelihood	Countermeasures (if applicable)
			device or user device with access to cloud server	Access to corporate and customer accounting data Unauthorized Use of Device Resources and exploit of trusted devices			
D06	CAPEC-113 CAPEC-160 CAPEC-121 CAPEC-554 CAPEC-272	Abuse or Bypass Existing Functionality	The attacker manipulates the use or processing of an interface (e.g., Application Programming Interface (API), SQL Injection) resulting in an adverse impact upon the security of the system.	Bypass the access control and execute functionality not intended by the interface compromising the system.	3	1	Traffic/application monitoring and Attack detection using ML mechanisms Parameter verification and validation
D07	CAPEC-220 CAPEC-90 CAPEC-594 CAPEC-595	Vulnerabilities of the communication protocol and network traffic	The attacker abuses or manipulates the client-server (authentication) protocol.	Creating a window for multiple types of further attacks such as spoof other clients or servers, read sensitive information or even modify content of the messages and integrate malware or malicious code. The attacker is able to map the target and/or the destination server without having to directly filter the traffic between them.	4	2	Handshake protocol with challenge HMAC to hash the response Introducing randomness, preventing duplication of attack paterns Traffic/application monitoring and Attack detection using ML mechanisms Secure communications channel

Threat id[3]	Threat Cat. Id[2]	Adversarial Technique[1]	Threat Description	Consequence of Incident	Impact (business level)	Likelihood	Countermeasures (if applicable)
D08	CAPEC-240 CAPEC-137 CAPEC-175	Malicious content injection (code, parameter, resource)	The attacker abuses one of the previously mentioned attacks to force ingest arbitrary code, file or database resource.	Disruption of the behaviour of a target either through crafted data submitted via an interface for data input, or the installation and execution of malicious code or malware on the target system.	4	1	Audit log written to a separate host. NLP to detect attack and temporary prevent use of resources or processing of information being ingested NLP to sanitize input content and payload Regular patching and updates of software
D09	CAPEC-134	Email Injection	A web site with a link to "share this site with a friend" where the user provides the recipient's email address and the web application fills out all the other fields, such as the subject and body. In this pattern, an attacker adds header and body information to an email message by injecting additional content in an input field used to construct a header of the mail message.	Can be used as prerequisite or tool for some of previously mentioned attacks Can result in corporate or customers sensitive data leak	3	1	ML-based (NLP) and content verification between the application and the mail server

Threat id[3]	Threat Cat. Id[2]	Adversarial Technique[1]	Threat Description	Consequence of Incident	Impact (business level)	Likelihood	Countermeasures (if applicable)
D10	CAPEC-612 CAPEC-613	Manipulation the Wifi Network (SSID Tracking, MAC Address Tracking)	Attacker passively listens for WiFi messages and WiFi management frame messages containing the Service Set Identifier (SSID) and logs the associated data.	The attacker is able to associate an SSID or MAC with a particular user or set of users (for example, when attending a public event), the attacker can then scan for this SSID to track that user in the future.	2	1	Automatic randomization of WiFi MAC addresses Frequently change the SSID to new and unrelated values
D11	CAPEC-49 CAPEC-50	Password manipulation (brute force, recovery exploit)	Attacker either actively tries to successfully login or exploits the feature to help users recover their forgotten passwords.	The attacker can get access to user credentials	2	1	Traffic monitoring and isolation of devices with repetitive traffic patterns Changes to application logic and email-based authentication Prevent login/password recovery functionality to be vulnerable to an injection style attack.
D12	CAPEC-497 CAPEC-635 CAPEC-580	Probing and exploration, Attacks based on file systems	Attacker implements probing and exploration activities to: i) determine if common key files exist ii) determine security information about a remote target system	A window and knowledge to implement more damaging attacks	2	1	Traffic monitoring and isolation of devices with repetitive traffic patterns Access Control and file protection mechanisms Software restriction policy to identify and block programs that may be used to acquire peripheral information

1. Only applicable on deliberate threat
2. The Threat Cat ID is same to Threat ID for non-adversarial threat
3. The threat id starts with:
    a. "D" → represents Deliberate threat
    b. "A" → represents Accidental threat
    c. "O" → Other types of threat

3.2.3.3 Risk Assessment of Use case #3: Live Threat Intelligence Sharing in a large-scale Edge scenario (NCSRD)

Table 12: Risk Assessment for UC3: Live Threat Intelligence Sharing in a large-scale Edge scenario

Threat id[3]	Threat Cat. Id[2]	Adversarial Technique[1]	Threat Description	Consequence of Incident	Impact (business level)	Likelihood	Countermeasures (if applicable)
D01	CAPEC-231	Oversized Serialized Data Payloads (XML DoS)	Applications often need to transform data in and out of serialized data formats by using a parser. The attacker will supply oversized payloads in input vectors that will be processed by the parser causing high resources consumption.	Resource Consumption Execute Unauthorized Commands Gain Privileges	4	2	ML-based (NLP) and content verification against canonical data.
D02	CAPEC-94	Man-in-the-Middle Attack	The attacker positions himself/herselft between the victim and the providers eNodeB.	Retrieval/Modification of Sensitive/Personal private data from the victim's mobile device.	4	2	Detection by using ML Algorithms ACL policies to restrict the attacker.
D03	CAPEC-141	Cache poisoning	The attacker targets specific applications caches (e.g a web browser cache) that the victim is using in order to cache data that aids the attacker's objectives.	Redirection to malicious web sites that install malware. Retrieval/Modification of Sensitive/Personal private application data such as passwords and usernames.	4	3	Checking and analysing payloads or other statistical flow and session-based features using ML algorithms.

Thread id[3]	Threat Cat. Id[2]	Adversarial Technique[1]	Threat Description	Consequence of Incident	Impact (business level)	Likelihood	Countermeasures (if applicable)
A01	CAPEC-164	Mobile Phishing	Attacker may convince the user to enter sensitive data by using the means of SMS or email.	Retrieval/Modification of Sensitive/Personal private application data such as passwords and usernames	4	1	Detection data leakage using ML mechanisms Firewall policies

1. Only applicable on deliberate threat
2. The Threat Cat ID is same to Threat ID for non-adversarial threat
3. The threat id starts with:
    a. "D" → represents Deliberate threat
    b. "A" → represents Accidental threat
    c. "O" → Other types of threat

4. Conclusions

This document presented a first approach to the definition of the PALANTIR use cases, the involved actors and workflows, the attack surface analysis related to the protection of networks in SME/MEs and the risk-based assessment methodology that will be implemented to reduce cybersecurity risks in the context of the documented UCs.

A thorough technical analysis of the identified use cases covering the different delivery modes, using actor-relationship and sequence UML diagrams, followed by a step-by-step presentation of the scenarios, pre- and post- conditions initially proves that the proposed workflows can effectively accommodate all system use cases, preparing the ground for the PALANTIR pilots.

Furthermore, an assessment of the security threats and risks in the domain of software networks and cloud-native deployments was conducted based on recent literature and partners' experience, leading to the consolidation of a risk-based assessment framework that will be implemented in the context of WP3. The proposed framework was also adapted for the described use cases, in order to measure the attack surface of each envisioned PALANTIR deployment.

All PALANTIR partners contributed to this endeavor, achieving a consensus among the consortium members on the next phases of the system development.

5. References

[1] L. Beaudoin and P. Eng, "Asset valuation technique for network management and security," 2006, doi: 10.1109/icdmw.2006.32.

[2] C. Lévy-Bencheton, L. Marinos, R. Mattioli, T. King, C. Dietzel, and J. Stumpf, *Threat Landscape and Good Practice Guide for Internet Infrastructure*. 2015.

[3] Y. Hori *et al.*, "A comprehensive security analysis checksheet for openflow networks," in *Lecture Notes on Data Engineering and Communications Technologies*, 2017.

[4] A. Munir, Z. Qian, Z. Shafiq, A. Liu, and F. Le, "Multipath TCP traffic diversion attacks and countermeasures," 2017, doi: 10.1109/ICNP.2017.8117547.

[5] R. Spreitzer, V. Moonsamy, T. Korak, and S. Mangard, "Systematic Classification of Side-Channel Attacks: A Case Study for Mobile Devices," *IEEE Commun. Surv. Tutorials*, 2018, doi: 10.1109/COMST.2017.2779824.

[6] M. Jensen, N. Gruschka, and N. Luttenberger, "The impact of flooding attacks on network-based services," 2008, doi: 10.1109/ARES.2008.16.

[7] A. P. Fournaris, L. P. Fraile, and O. Koufopavlou, "Exploiting hardware vulnerabilities to attack embedded system devices: A survey of potent microarchitectural attacks," *Electron.*, 2017, doi: 10.3390/electronics6030052.

[8] S. Dong, K. Abbas, and R. Jain, "A Survey on Distributed Denial of Service (DDoS) Attacks in SDN and Cloud Computing Environments," *IEEE Access*, 2019, doi: 10.1109/ACCESS.2019.2922196.

[9] O. A. Osanaiye, "Short Paper: IP spoofing detection for preventing DDoS attack in Cloud Computing," 2015, doi: 10.1109/ICIN.2015.7073820.

[10] A. Pradhan and R. Mathew, "Solutions to Vulnerabilities and Threats in Software Defined Networking (SDN)," 2020, doi: 10.1016/j.procs.2020.04.280.

[11] B. Hawkins, "InfoSec Reading Room Case Study : The Home Depot Data Breach," *SANS Inst.*, 2015.

[12] J. Hizver, "Taxonomic Modeling of Security Threats in Software Defined Networking," *Blackhat 2015*, 2015.

[13] A. Bhandari, S. Gautam, T. K. Koirala, and M. Ruhul Islam, "Packet sniffing and network traffic analysis using TCP—A new approach," 2018, doi: 10.1007/978-981-10-4765-7_28.

[14] L. Dridi and M. F. Zhani, "A holistic approach to mitigating DoS attacks in SDN networks," 2018, doi: 10.1002/nem.1996.

[15] K. Cheng, M. Gao, and R. Guo, "Analysis and research on HTTPS hijacking attacks," 2010, doi: 10.1109/NSWCTC.2010.187.

[16] M. Q. Khan, "Signaling Storm Problems in 3GPP Mobile Broadband Networks, Causes and Possible Solutions: A Review," 2019, doi: 10.1109/iCCECOME.2018.8658708.

[17] F. Reynaud, F. X. Aguessy, O. Bettan, M. Bouet, and V. Conan, "Attacks against Network Functions Virtualization and Software-Defined Networking: State-of-the-art," 2016, doi: 10.1109/NETSOFT.2016.7502487.

[18] R. Mohammadi, R. Javidan, and M. Conti, "SLICOTS: An SDN-based lightweight countermeasure for TCP SYN flooding attacks," *IEEE Trans. Netw. Serv. Manag.*, 2017, doi: 10.1109/TNSM.2017.2701549.

[19] C. Li, Z. Qin, E. Novak, and Q. Li, "Securing SDN Infrastructure of IoT-Fog Networks from MitM Attacks," *IEEE Internet Things J.*, 2017, doi: 10.1109/JIOT.2017.2685596.

[20] N. Vlajic, M. Chowdhury, and M. Litoiu, "IP spoofing in and out of the public cloud: From

policy to practice," *Computers*, 2019, doi: 10.3390/computers8040081.

[21] M. De Vivo, E. Carrasco, G. Isern, and G. O. De Vivo, "A review of port scanning techniques," *Computer Communication Review*. 1999, doi: 10.1145/505733.505737.

[22] I. Ahmad, T. Kumar, M. Liyanage, J. Okwuibe, M. Ylianttila, and A. Gurtov, "5G security: Analysis of threats and solutions," 2017, doi: 10.1109/CSCN.2017.8088621.

[23] F. Van Den Broek, R. Verdult, and J. De Ruiter, "Defeating IMSI catchers," 2015, doi: 10.1145/2810103.2813615.

[24] Joint Task Force, "Risk management framework for information systems and organizations:," 2018.

[25] ENISA, "Integration of RM/RA with Operation Processes," Berlin, Germany, 2008.

[26] ENISA, "Information Package for SMEs," 2007.

[27] NIST, "Security Content Automation Protocol SCAP." https://csrc.nist.gov/projects/security-content-automation-protocol/.

[28] NIST, "OSCAL: the Open Security Controls Assessment Language." https://pages.nist.gov/OSCAL/.

[29] ENISA, "ENISA Risk Management approach for SME/MEs," 2009.

[30] S. Barnum, "Common attack pattern enumeration and classification (CAPEC) schema description," *Cigital Inc, http//capec. mitre. org/documents/ ...*, 2008.

[31] MITRE, "MITRE ATT&CK, a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations." https://attack.mitre.org/.

[32] MITRE, "CVE - Common Vulnerabilities and Exposures," *Common Vulnerabilities Expo.*, 2016.

6. Annex A: Consolidated Stakeholders table

We provide a full list of the envisioned stakeholders of the PALANTIR ecosystem across all use cases, in Table 13. Given that actors are always stakeholders, but this relation is not bidirectional, it may be the case that some stakeholders do not appear in the use cases and are not present in the UC actor and sequence diagrams (e.g., PALANTIR Developers). They, however, play an important role in the development of the platform and are also affected by the outcomes of the project.

Table 13: Consolidated Stakeholders list

Role	***Interacting functionalities***	***Aliases***
Service provider	• Provides cloud, end-point device, SecEndPoint protection • Remote monitoring and alert • Update new functionalities and new algorithms • Communicates in real-time with the end user • Retrieve attack information used for threat sharing purposes • Reconfigures remote endpoint • Threat Mitigation plan • Threat Sharing	PALANTIR operator PALANTIR administrator System administrator Security service provider Service provider & Integrator
Infrastructure Provider	• Administration/provision of network infrastructure (e.g., 5G testbed) • Realtime monitoring • Threat Detection • Policy Enforcement	5GENESIS Admin 5TONIC Admin 5G Administrator 5G Testbed Provider
PALANTIR Developer	• Builds VNFs for the PALANTIR ecosystem	Service Developer
PALANTIR Platform End user	• Installs an end-point device in premises • Communicates with the PALANTIR admin • GUI provides capability to monitor in real-time activity, events and alerts • GUI provides capability to cancel alerts, remove restrictions • GUI provides capability to communicate 24/7 with live support • Is able to apply mitigation actions for their organisation • Interconnects all in-premises equipment with WAN. • Access to POS terminals, cashier, trusted desktop, personal smart phone, access to cloud services and local services, web browsing, email	SecaaS end user Doctor Healthcare Practitioner SecaaS client CRM employee Accounting employee Sales employee Manager CEO Company visitor Customer

	• Access to trusted desktop, personal smart phone, access to cloud services and local services, web browsing, email • High-level access from personal mobile devices, smartphones and tablets • Smart phone access, unrestricted access to public WiFi	
Attacker	• Performs malicious network attacks on medical practice premises, disrupting normal operation. • Leaks sensitive medical records for extortion/blackmail purposes. • Performs malicious injections/exploits to the eCommerce Database. • Installs ransomware/malware or similar software to the company infrastructure. • Performs propagating cyberattacks targeting many network clients simultaneously.	
GDPR data subject	• Her/his data is protected by the PALANTIR SecaaS	Customer Client Patient
Cybersecurity agency	• Benefiting from the threat sharing functionalities	