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

Practical Autonomous Cyberhealth for resilient SMEs & Microenterprises

Grant Agreement No. 883335
Innovation Action (IA)

D2.4 Use Cases and Risk Reduction measures

Document Identification			
Status	Final	**Due Date**	30-04-2022
Version	1.0	**Submission Date**	29-04-2022

Related WP	WP2	**Dissemination Level (*)**	PU
Related Deliverable(s)	D2.1, D2.2, D2.3		
Lead Participant	INFILI	**Lead Author**	INFILI
Contributors	PALANTIR consortium	**Reviewers**	SPH
			SSE

Keywords:
Use cases, actors, scenarios, threat analysis, risk reduction measures,

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, Katerina Mitropoulou, Dimitris Giagkos	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, Primož Jeran	SFERA

Document History			
Version	Date	Change editors	Changes
V0.1	25/3/2022	WP2 partners	First round of contributions
V0.2	18/4/2022	WP2 partners	Second round of contributions
V0.3	19/4/2022	INF	Version ready for internal review
V1.0	27/4/2022	INF	Final version

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	INFILI	27/04/2022
Quality manager	INFILI	27/04/2022
Project Coordinator	DBC	28/04/2022

Table of Contents

Document Information 3
Table of Contents 4
List of Tables 5
List of Figures 6
List of Acronyms 7
Executive Summary 10
1. Introduction 11
1.1. Objectives and goals of the deliverable 11
1.2. Relation with D2.1 and other WPs 11
2. Use Case Analysis 13
2.1 Use Case #1: Securing private medical practices with lightweight SecaaS 13
2.1.1 Motivation and Overall Description 13
2.1.2 Actors Definition and Mode of Interaction 13
2.1.3 Use Case Detailed Description 14
2.1.4 Hosting Infrastructure 19
2.1.5 Updates since D2.2 20
2.2 Use Case #2: Uninterrupted Electronic Commerce with Cloud SecaaS 20
2.2.1 Motivation and Overall Description 20
2.2.2 Actors Definition and Mode of Interaction 21
2.2.3 Use Case Detailed Description 22
2.2.4 Hosting Infrastructure 30
2.2.5 Updates since D2.2 31
2.3 Use Case #3: Live Threat Intelligence Sharing in a large-scale Edge scenario 31
2.3.1 Motivation and Overall Description 31
2.3.2 Actors Definition and Mode of Interaction 32
2.3.3 Use Case Detailed Description 33
2.3.4 Hosting Infrastructure 37
2.3.5 Updates since D2.2 40
3. Risk Reduction Measures 41
3.1. Overview of the risk assessment methodology 41
3.1.1 Attack Surface Analysis 43
3.1.2 Asset Identification 56
3.2. Application of risk reduction measures to reduce security risks in the PALANTIR UCs 57
3.2.1 UC1 analysis 57
3.2.2 UC2 analysis 60
3.2.3 UC3 analysis 67
4. Conclusions 70
5. References 71

List of Tables

Table 1: UC1 Actors interactions with PALANTIR *14*
Table 2: Step-by-step view of UC1: Securing private medical practices with lightweight SecaaS *15*
Table 3: UC2 Actors interactions with PALANTIR *21*
Table 4: Step-by-step view of UC2: Uninterrupted Electronic Commerce with Cloud SecaaS *22*
Table 5: UC3 Actors interactions with PALANTIR *32*
Table 6: Step-by-step view of UC3: Live Threat Intelligence Sharing in a large-scale Edge scenario *33*
Table 7: Risk reduction measures for UC1: Securing private medical practices with lightweight SecaaS *57*
Table 8: Risk Assessment for UC2: Uninterrupted Electronic Commerce with Cloud SecaaS *60*
Table 9: Risk reduction measures for UC3: Live Threat Intelligence Sharing in a large-scale Edge scenario ... *67*

List of Figures

Figure 1: Conceptual view of the PALANTIR solution *12*
Figure 2: Actor diagram for UC1: Securing private medical practices with lightweight SecaaS *15*
Figure 3: Sequence diagram for UC1: Securing private medical practices with lightweight SecaaS *19*
Figure 4: ORION Athens NFVI-PoP and related infrastructure *20*
Figure 5: Actor diagram for UC2: Uninterrupted Electronic Commerce with Cloud SecaaS *22*
Figure 6: Sequence diagram for UC2: Uninterrupted Electronic Commerce with Cloud SecaaS *29*
Figure 7: Slovenian testbed and related infrastructure *30*
Figure 8: Actor diagram for UC3: Live Threat Intelligence Sharing in a large-scale Edge scenario *33*
Figure 9: Sequence diagram for UC3: Live Threat Intelligence Sharing in a large-scale Edge scenario *37*
Figure 11: 5TONIC infrastructure *39*
Figure 12: Base risk assessment model *42*
Figure 13: Attack graph-based risk assessment model *42*
Figure 14 Example attack graph model *43*
Figure 15 OSI layer presentation for 5G networks *44*

List of Acronyms

Abbreviation / acronym	Description
5G PPP	5G Infrastructure Public Private Partnership
5G-AKA	5G Authentication and Key Agreement
ACL	Access Control List
AI	Artificial Intelligence
BYOD	Bring Your Own Device
CAPEC	Common Attack Pattern Enumeration and Classification
CAPEX	Capital Expenditure
CHAP	Challenge Handshake Authentication Protocol
CIA	Confidentiality, Integrity and Availability
CMS	Content Management System
CP	Control Plane
CRM	Customer Relationship Management
CSP	Cloud Solution Provider
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DDoS	Distributed Denial of Service
DLT	Distributed Ledger Technology
DNS	Domain Name System
DPI	Deep Packet Inspection
EAP	Extensible Authentication Protocol
ENISA	European Union Agency for Cybersecurity
EPC	Evolved Packet Core
FDIC	Federal Deposit Insurance Corporation
FTP	File Transfer Protocol
GSS	Generic Security Service
GUI	Graphical User Interface
ICN	Information Centric Networking
ICT	Information and Communication Technology
IDS	Intrusion Detection System
IoT	Internet of Things
IP	Internet Protocol
iSCSI	Internet Small Computer Systems Interface
ISP	Internet Service Provider
KVM	Kernel Virtual Machine
LAN	Local Area Network
LEAP	Lightweight Extensible Authentication Protocol
LNSC	Lightning Network and Smart Contract
LTE	Long Term Evolution
MAC	Message Authentication Code
ME	MicroEnterprise

Abbreviation / acronym	Description
MEC	Multi-Access Edge Computing
MIMO	Multi Input Multi Output
MISP	Malware Information Sharing Platform
MITM	Man In The Middle
MMML	Multi Modal Machine Learning
mmWave	Millimeter Wave
NAT	Network Address Translation
NetBIOS	Network Basic Input/Output System
NFC	Near Field Communication
NFV	Network Functions Virtualization
NFVO	Network Function Virtualization Orchestration
NIST	National Institute of Standards and Technology
NLP	Natural Language Processing
NSA	Non-Standalone
NVD	National Vulnerability Database
OFDM	Orthogonal Frequency Division Multiplexing
OSI	Open Systems Interconnection
OSM	Open-Source MANO
OTP	Open Transport Protocol
OVS	Open vSwitch
PAN	Personal Area Network
PAP	Password Authentication Protocol
PLS	Physical Layer Security
PoP	Point of Presence
RAN	Radio Access Network
RMF	Risk Management Framework
RPC	Remote Procedure Call
SA	Stand Alone
SAS	Serial Attached SCSI
SC	Security Capability
SDN	Software-Defined Networking
SFTP	Secure File Transfer Protocol
SIEM	Security Information and Event Management
SLA	Service-Level Agreement
SME	Small and Mid-sized Enterprise
SQL	Structured Query Language
SRPC	Secure Remote Procedure Call
SSID	Service Set Identifier
SSL	Secure Sockets Layer
TEID	Tunnel Endpoint Identifier
TLS	Transport Layer Security
UC	Use Case

Abbreviation / acronym	Description
UE	User Equipment
UML	Unified Modeling Language
UMTS	Universal Mobile Telecommunications System
UP	User Plane
VIM	Virtualized Infrastructure Manager
VM	Virtual Machine
VNF	Virtualized Network Function
VPN	Virtual Private Network
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WTA	Web-based Traffic Analysis
XML	Extensible Markup Language
XSS	Cross-Site Scripting

Executive Summary

The present document incorporates the final version of the PALANTIR use cases (UCs) as well as the main findings and high-level identification of measures to reduce security risks in service-oriented infrastructures.

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 share with other SecaaS users.

The three use cases that were identified in D2.2 and finetuned in Section 2 of this deliverable as the 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 accomplished through the proposed architecture, initially documented in D2.1 and finetuned in D2.3. Finally, a subsection is dedicated to the hosting infrastructure of each use case.

In Section 3, an overview of the risk assessment methodology (initially described in D2.2) is complemented with an attack surface analysis and asset identification for software networks and cloud-native deployments. An overview of the attack surfaces related to all PALANTIR delivery modes is provided, discussing vulnerabilities, threats and security solutions, while focusing on the concrete PALANTIR contributions to ensure the security of end-user applications. The categorization of the aforementioned items is detailed using Open Systems Interconnection (OSI) layers, in order to highlight the latent synergies that take place to ensure holistic protection within the context of PALANTIR. Finally, this section presents the risk reduction measurements that each use case will adopt, mapping them to specifc threats and identifying the PALANTIR tools that will be applied, thus paving the way for the pilots of WP6.

1. Introduction

1.1. Objectives and goals of the deliverable

The current document is the deliverable "D2.4 Use Cases and Risk Reduction Measures" which comprises the major outcomes of **"Task 2.3 - Use case analysis"** and **"Task 2.4 Threat and Attack Surface Analysis**", building upon the initial findings of "D2.2 Use Cases, Threat analysis & AS-based risk assessment".

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 were validated along with their detailed specifications to federate the partners on the final version of the PALANTIR architecture, an interim version of which was documented in D2.1 "Requirements & high-level design -Interim" and fine-tuned in D2.3 "Requirements & high-level design - Final". 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. D2.4 provides the final version of the attack surface analysis, complementing the content of D2.2 with a comprehensive analysis of the challenges, vulnerabilities and gaps that are met in service-oriented infrastructures (categorized per OSI-layer), while also mapping specific reduction measures to the corresponding threats that were identified in the attack surface analysis phase of each PALANTIR use case.

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 use 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 the updated D2.3 "Requirements & high-level design - Final" comprises the primary reference point for designing the individual PALANTIR components.

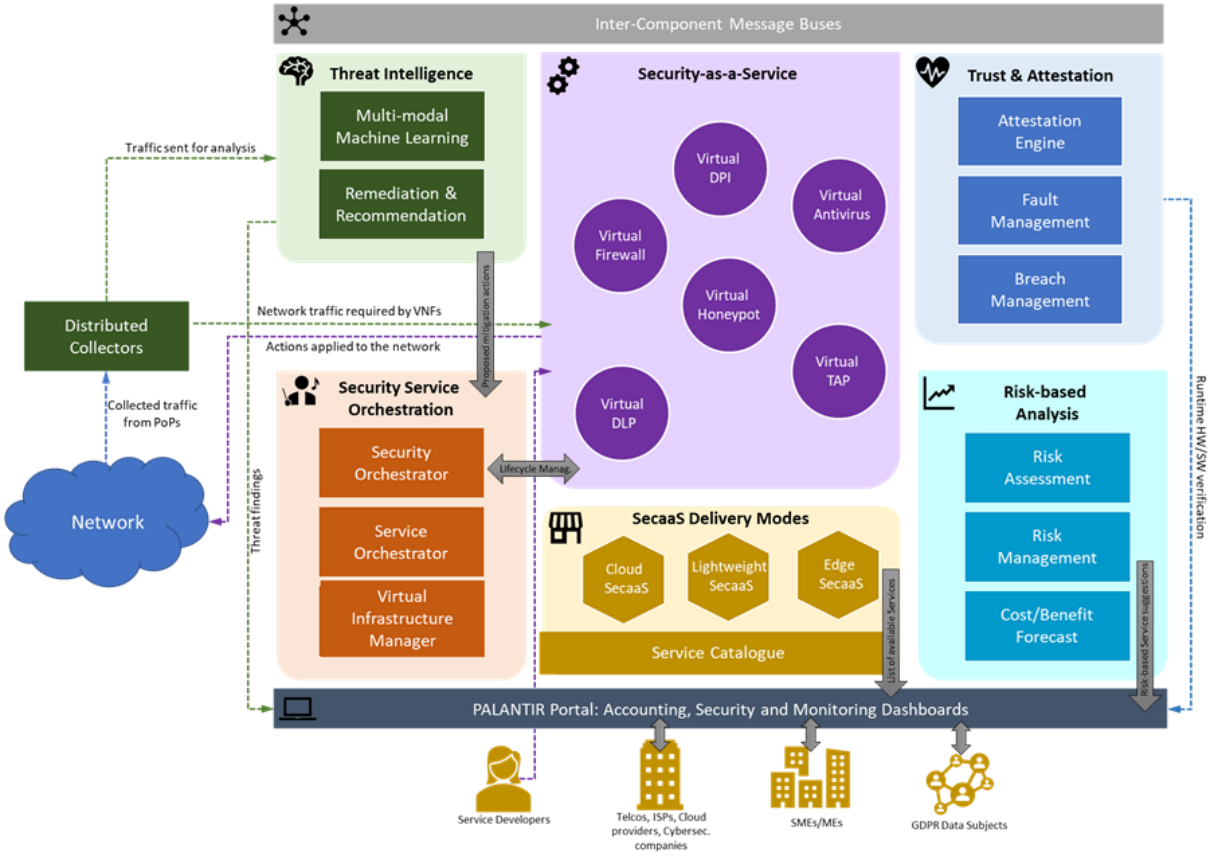

Figure 1: Conceptual view of the PALANTIR solution

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 provides an updated version of the 3 PALANTIR Use Cases that were initially defined in "D2.2 Use Cases, Threat analysis & AS-based risk assessment", based on the feedback of the 1st PALANTIR review. 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 protect patient data and prevent medical identity theft will be supported (referenced as remediation measures in the following subsections). In order to support such use case and showcase the added value of PALANTIR components, a data leakage scenario combined with a Ransomware attack 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 tunnelling)
- 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 and encryption of files that contain sensitive data by performing a ransomware attack. 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. • Encrypts files making them inaccessible to the rightful owner

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).

Cannot delete for some reason

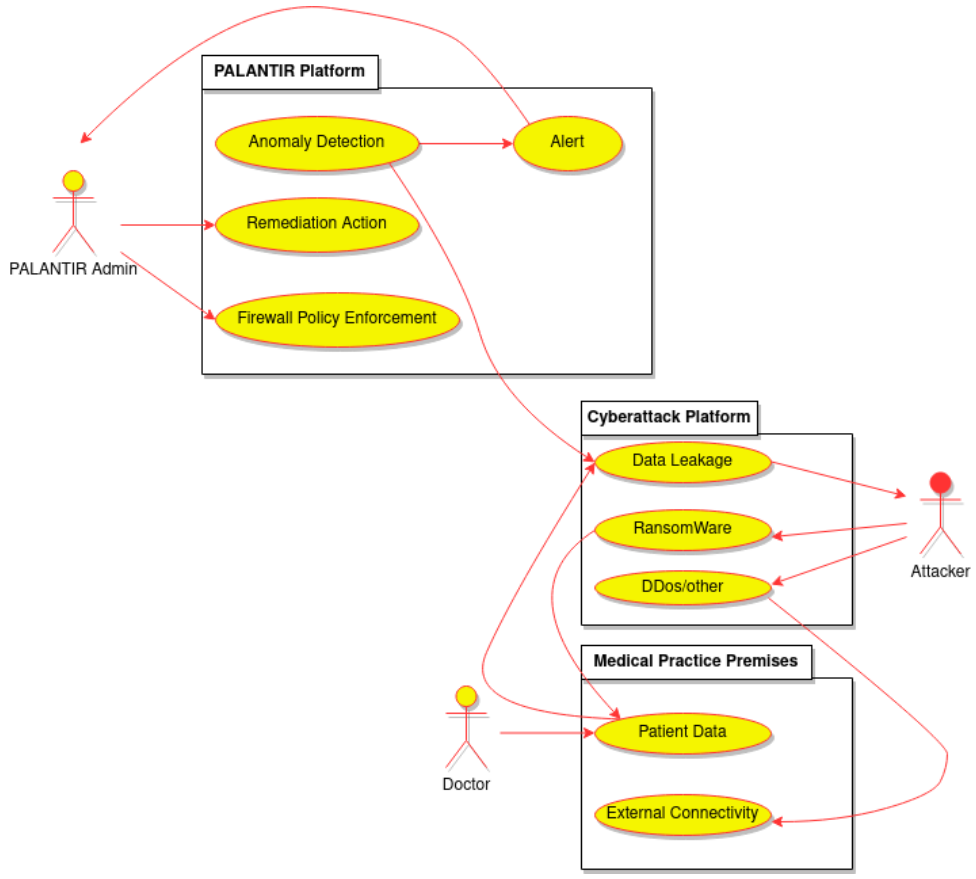

Figure 2: Actor diagram for UC1: Securing private medical practices with lightweight SecaaS

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 unauthorized access as suspicious activity and blocks the Attacker's access to the network.
Name	**Data leakage and encryption**
Identifier	UC1.4
Description	A vulnerable data server is attacked by the Attacker and sensitive medical data are encrypted and leaked to a malicious server.

Goal	To leverage stolen medical records for extortion/coercion/blackmail purposes and gain cryptocurrency profit from ransoms.
Preconditions	Sensitive medical records exist on the private data server and the Attacker has managed to infiltrate.
Post conditions	The Attacker successfully extracts and encrypts 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, file encryption 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 and encrypted data.
Preconditions	A malicious attack (e.g., data leakage,ransomware) 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 and further encryption of data.
Preconditions	A relevant remediation policy is suggested for the specific threat.
Post conditions	Remediation policy is applied by the firewall so data leakage and ransomware attack 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 and encryption of medical data. The Doctor has leveraged a PALANTIR Security Endpoint (after successful 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.

Cannot delete

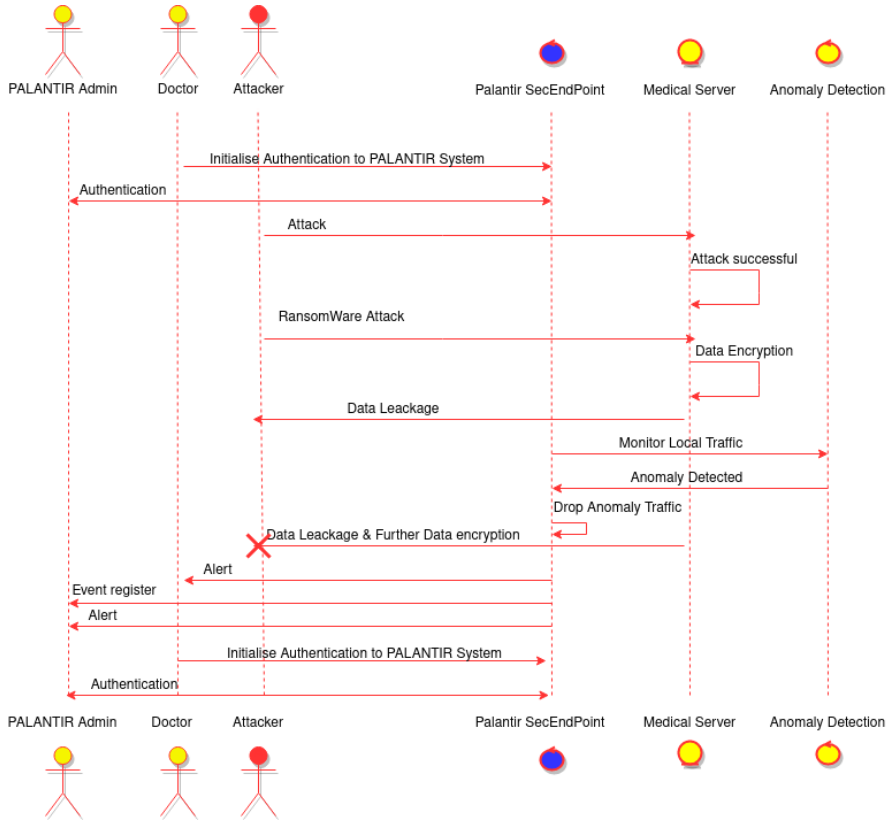

Figure 3: Sequence diagram for UC1: Securing private medical practices with lightweight SecaaS

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).

In addition to the PoP, three bare metal servers running ESXi virtualisation software are provided. The ESXi servers are able to provide host 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.

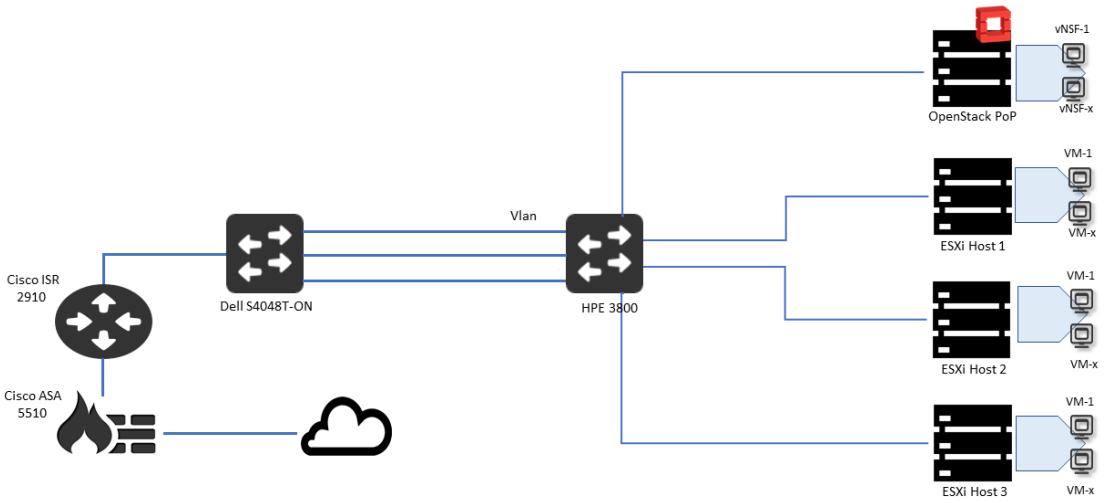

Figure 4: ORION Athens NFVI-PoP and related infrastructure

2.1.5 Updates since D2.2

The updated version of UC1 description contains specific mentions to ransomware attacks, which were identified as the most critical cybersecurity threats in healthcare environments. The actor and sequence diagrams were updated accordingly

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 multiple 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. **Microenterprise 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 (**Error! Reference source not found.**) followed by a step-by-step view of the use case (**Error! Reference source not found.**) as well as the Sequence diagram for UC2 (**Error! Reference source not found.**).

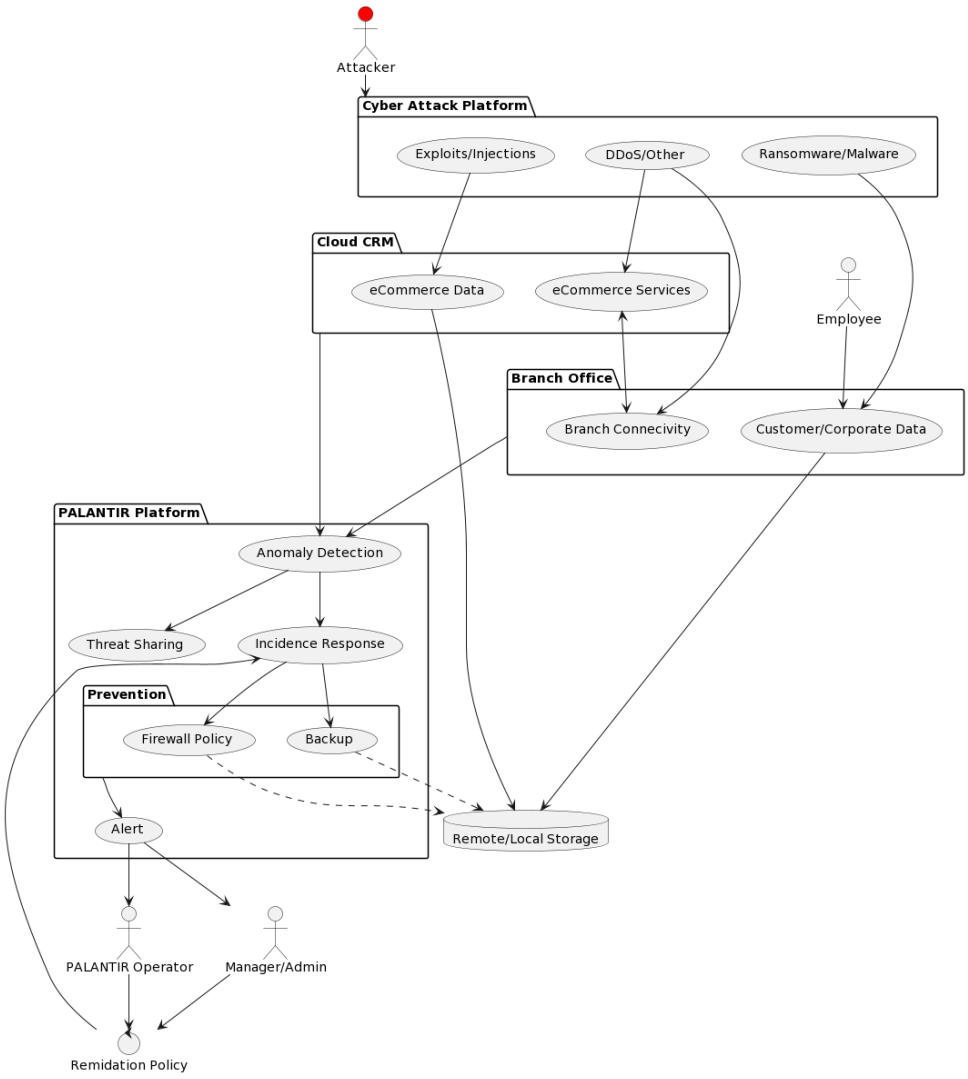

Figure 5: Actor diagram for UC2: Uninterrupted Electronic Commerce with Cloud SecaaS

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

Name	**Branch Connecivity**
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 Services**
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 Data**
Identifier	UC2.4
Description	The employee gets access to the data of the eCommerce database or FTP.
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, UC2.7
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 (e.g. cross-site scripting, SQL injections, Input Validation Vulnerabilities).
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. PALANTIR performs a backup of data (files and database) and stores is in an isolated local or cloud instance for later inspection and post attack restore.
Name	**Ransomware/Malware**
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, UC2.7
Exceptions	PALANTIR detects the propagating attack and blocks the attacker's access to the network. PALANTIR performs a backup of data (files and database) and stores is in an isolated local or cloud instance for later inspection and post attack restore.
Name	**DDoS/Other**
Identifier	UC2.7
Description	A vulnerable cloud CRM is attacked via a malicious actor and access to the server is lost or distributed.
Goal	To slow down or disrupt the connectivity of the SME to its cloud environment and customers to cloud services (i.e. web site) and/or to steal its credentials.
Preconditions	-
Post conditions	The Attacker manages to disrupt the cloud server and block front end services such as website as well as back end services, e.g. backup and caching
Actors / Users	**Atacker**
Dependencies from other functionalities/steps	UC2.6
Exceptions	PALANTIR discovers the network attack and blocks the Attacker's access to the network. PALANTIR performs a backup of data (files and database) and stores is in an isolated local or cloud instance for later inspection and post attack restore.
Name	**Anomaly Detection**
Identifier	UC2.8
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	UC2.9
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	**Incidence Response**
Identifier	UC2.10
Description	PALANTIR proposes remediation actions based on the threat findings. The Incident Response (IR) component utilizes finite state machines (FSM) that allow the deployment of personalized remediation policies.
Goal	To disrupt the attacker's access to the company infrastructure.
Preconditions	PALANTIR has discoved a network threat. PALANTIR Operator and SME/ME Manager/Admin design a new remediation policy
Post conditions	The proposed remediation action is forwarded to the PALANTIR Operator
Actors / Users	PALANTIR Operator
Dependencies from other functionalities/steps	UC2.8, UC2.11

Exceptions	PALANTIR fails to propose a remediation action for the specific threat.
Name	**Remediation policy**
Identifier	UC2.11
Description	The PALANTIR Operator and Manager design a Remediation Policy as FSM.
Goal	To ensure protection of the vital infrastructure and information, aligned with preferences of the customer (SME/ME)
Preconditions	-
Post conditions	A sequence of remediation 'actions' to handle an attack
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	UC2.12
Description	The PALANTIR Operator applies the suggested remediation action. Within the UC2 network security (e.g Firewwall) and data Backup are proposed as minimal SecaaS services. Backup can be defined to be stored in a secure cloud or on an offline machine.
Goal	To prevent the propagation of network threats to the company infrastructure, to prevent data leakage and to conserve data.
Preconditions	-
Post conditions	The remediation actions are applied by the PALANTIR Incidence Response Engine.
Actors / Users	-
Dependencies from other functionalities/steps	UC2.11
Exceptions	Failure to apply suggested remediation due to mismatch in service/network configuration.
Name	**Threat Sharing**
Identifier	UC2.13

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	UC2.8
Exceptions	The Manager refuses to disclose the discovered threat.

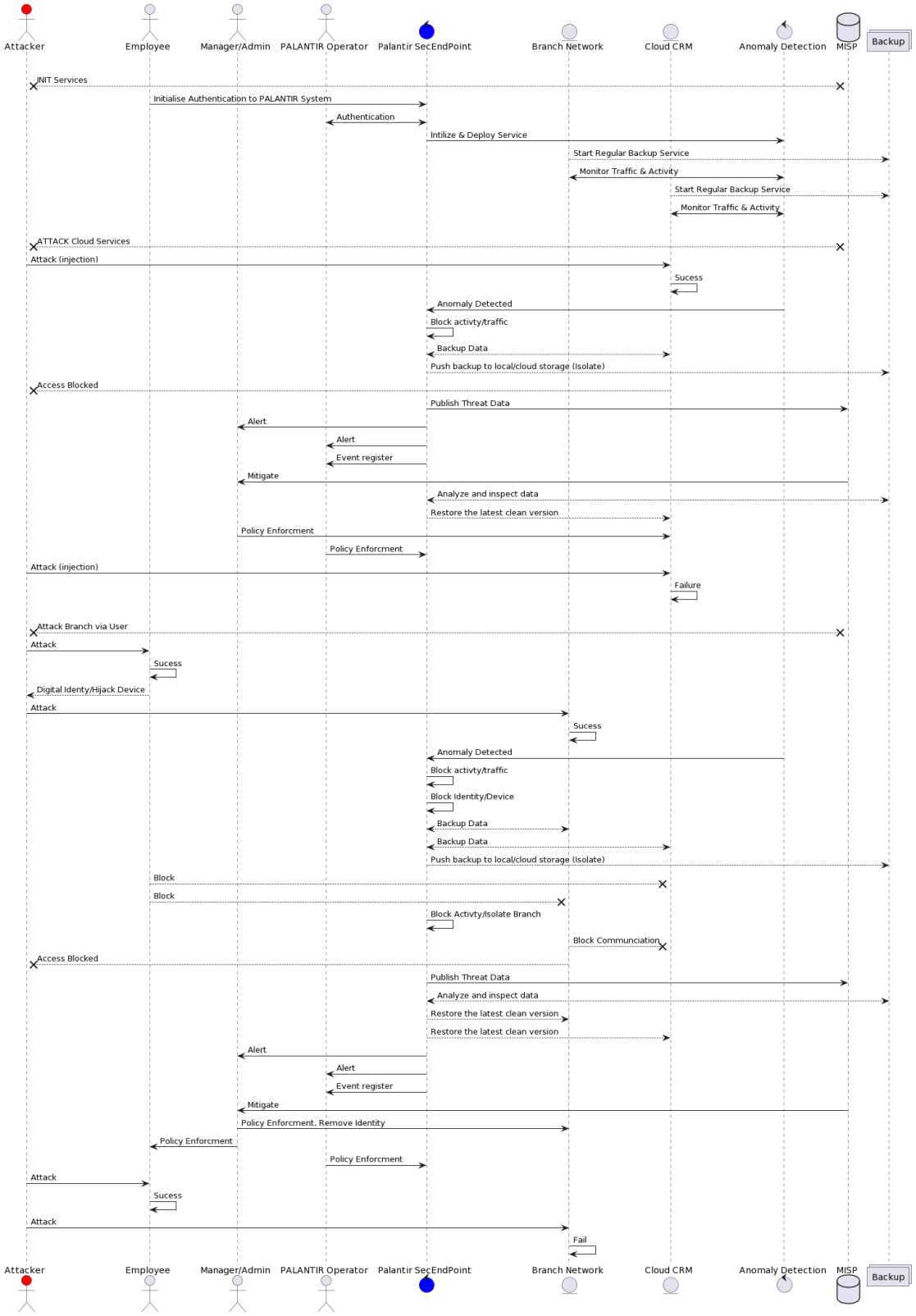

Figure 6: Sequence diagram for UC2: Uninterrupted Electronic Commerce with Cloud SecaaS

The aforementioned step-by-step analysis is also depicted in the sequence diagram of **Error! Reference source not found.**. 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 (**Error! Reference source not found.**). 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.

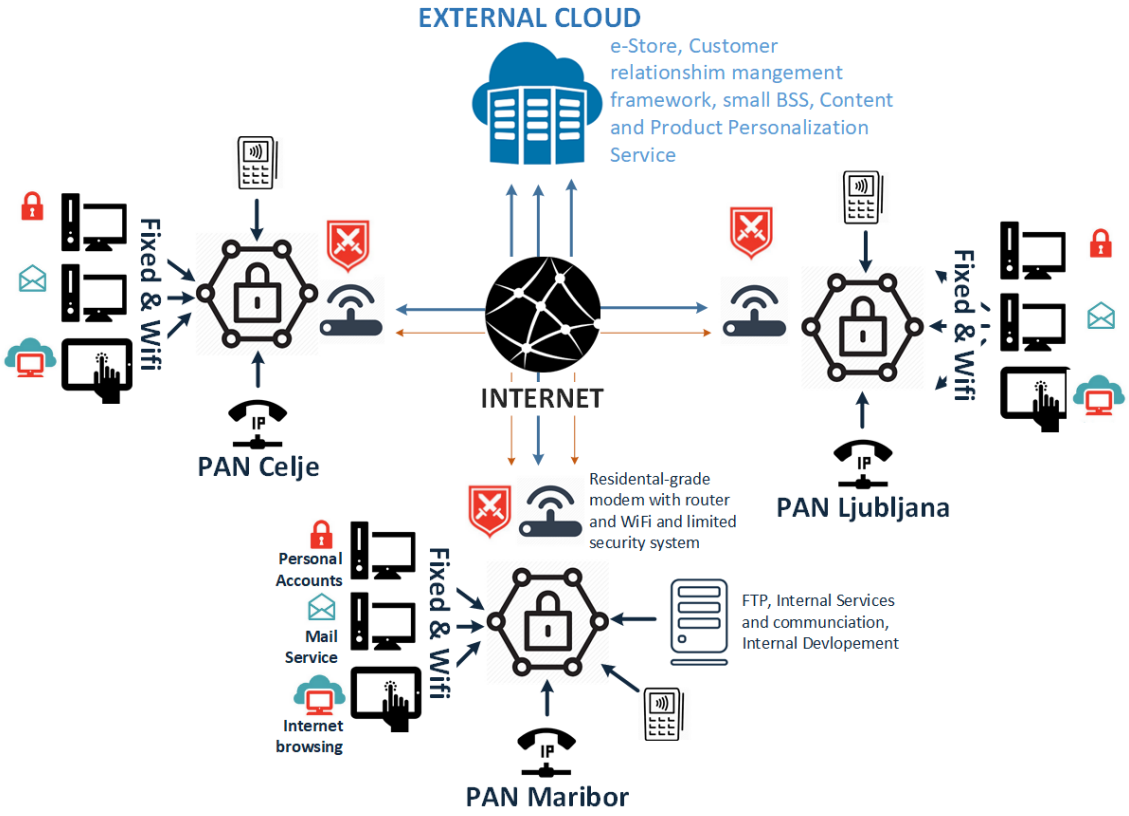

Figure 7: Slovenian testbed and related infrastructure

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).

2.2.5 Updates since D2.2

Added DDos as a relevant threat and the backup service as a possible remediation measure in addition to network security. Updated diagrams according to the more realistic PALANTIR deployment and attack scenarios in UC2, as a direct result of the engagement with demonstrator in UC2 (Akus MicroEnterprise). The updated version also includes the integration of the Incidence Response component, incorporating finite state machines, as an enabler of proactive and personalized remediation policies.

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).

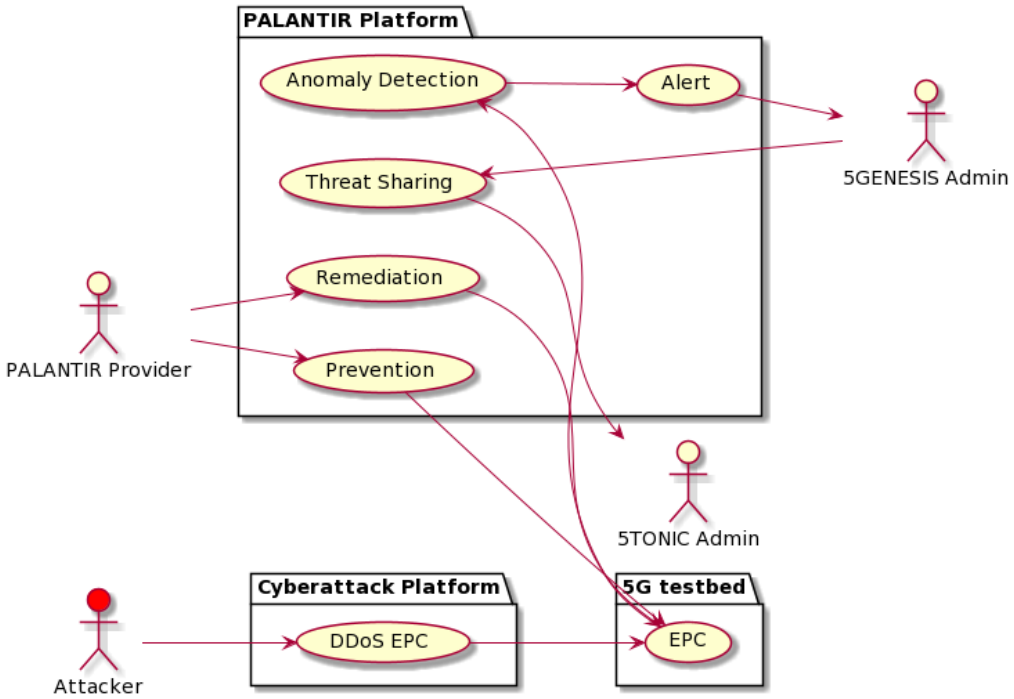

Figure 8: Actor diagram for UC3: Live Threat Intelligence Sharing in a large-scale Edge scenario

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.

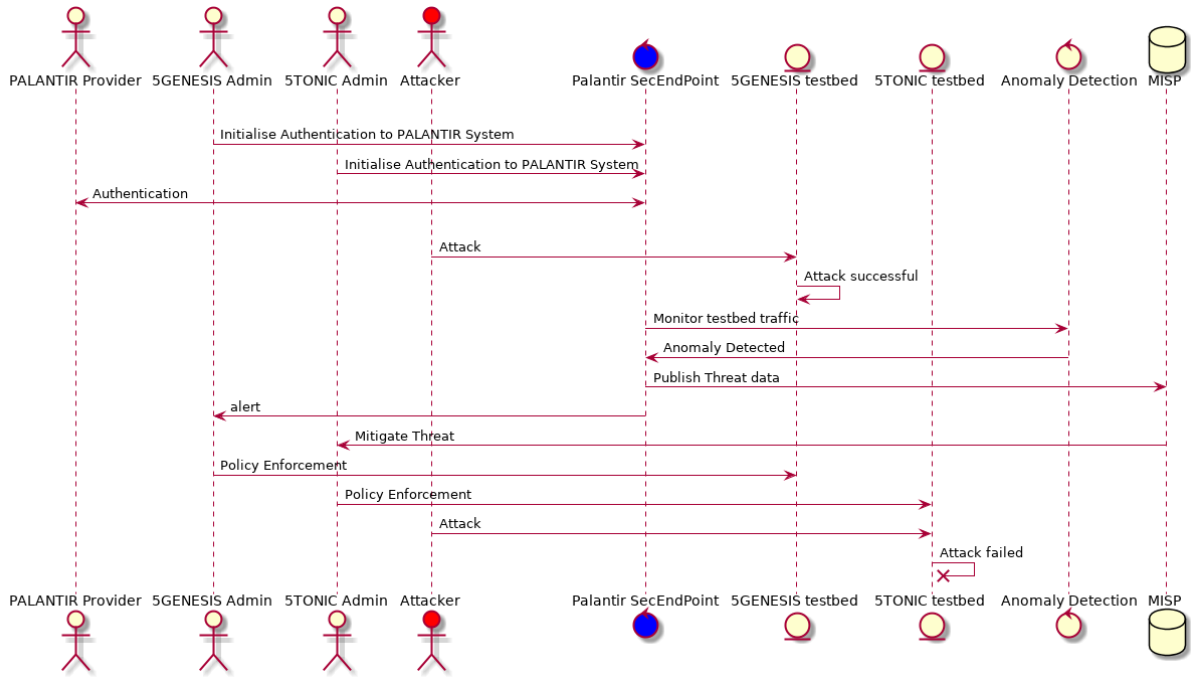

Figure 9: Sequence diagram for UC3: Live Threat Intelligence Sharing in a large-scale Edge scenario

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).

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.

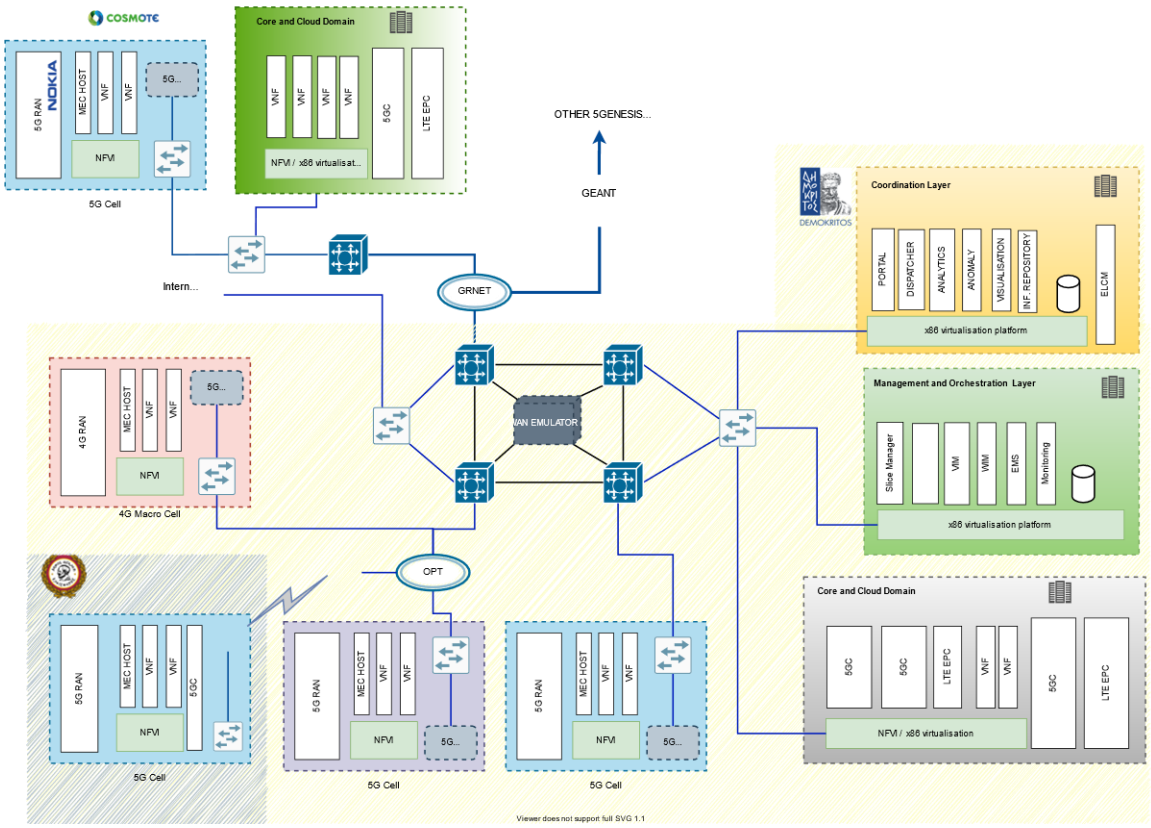

Figure: 5GENESIS Athens platform infrastructure

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

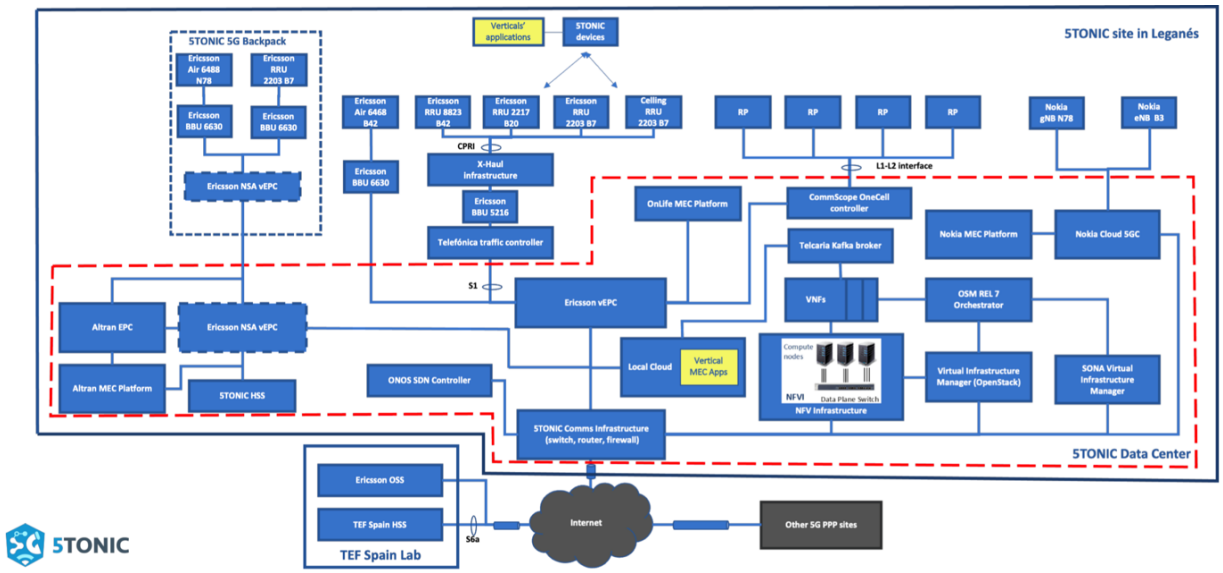

Figure 10: 5TONIC infrastructure

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.

2.3.5 Updates since D2.2

There are not major advancements and changes on UC3 compared to the initial description included in D2.2.

3. Risk Reduction Measures

3.1. Overview of the risk assessment methodology

PALANTIR defines its risk assessment methodology in the following four steps:

- An assessment (quantitative, qualitative)
- An analysis approach (threat-oriented, as set/impact-oriented, or vulnerability oriented)
- An explicit risk model
- A risk assessment process

These four steps are the basis for the Risk Assessment Framework (RAF) developed in the frame of WP3, where the PALANTIR platform users perform the corresponding assessment of their assets and infrastructure and the platform performs an evaluation and recommendation for their protection.

However, the background of these steps is founded on the detailed analysis of the aforementioned components.

A. Risk Assessment Approach

Risk assessments can be held quantitatively or qualitatively. Quantitative risk assessments require monetary or numerical values for risk factors whereas qualitative methods employ non-numeric priority or criticality values. We employ a quantitative approach in our model due to three reasons. First, the underlying metrics of the CVSS has numerical values assigned to them since the CVSS is a quantitative approach. Second, in quantitative approach, the evaluation and the results are based on objective criteria and thus more suitable for an IT system risk assessment. Lastly, quantitative approach is more suited for measuring the security level of an IT system in terms of the three common security pillars (confidentiality, integrity and availability).

B. Analysis Approach

Regarding the analysis approach, assessments can be held in a threat/attacker oriented, asset/impact oriented or vulnerability/architecture-oriented way. Each analysis approach takes into consideration the same risk factors. What differs in each approach is the order of the factors taken into account, thus the importance given to the different factors in each approach changes, which results in a bias introduced to the assessment results.

Vulnerability/architecture centric models focus on system design or vulnerabilities and attacks against each component/vulnerability. Asset/impact centric models identify asset values and impacts on the assets by taking the motivation and capability of the threat sources into account. Threat/attacker centric models put more emphasis on the properties of the attack sources through identifying an attacker and focusing on the attackers' goals and techniques to assess the risk.

Among the three types of risk analysis models, our work fits to the asset and vulnerability centric models, for two reasons. First, threat centric model requires threat intelligence in order to identify attackers specifically, which is beyond the scope of our work. Second, by defining a number of high level metrics, we quantify the risks of both individual assets and the vulnerabilities at the assets, hence satisfying the considerations of the asset and vulnerability centric models.

C. Risk Assessment Model

In this section, the semantics of the risk assessment model is defined in general terms. A detailed explanation together with calculation formulas for each of the components are given in the following sections. We define two different risk assessment models; one for base risk assessment and another for attack graph-based risk assessment, as depicted in Fig. 12 and 13.

Figure 11: Base risk assessment model

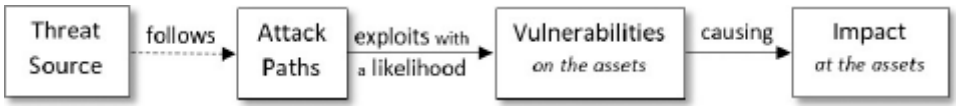

Figure 12: Attack graph-based risk assessment model

Base risk assessment model comprises of four components; assets, vulnerabilities, likelihoods and impacts (attackers are unknown sources with no known parameters. For this reason, threat source in the Fig. 12 is depicted with dashed box).

Attach-graph-based risk assessment model comprises of six components, adding two additional components to the first model, which are the threat sources and attack paths. The attack graph-based model differs from the base model mainly because the probability is not calculated using only the CVSS metrics of the CVEs, but also taking both the capabilities of the threat sources and the attack paths of the exploitations. Thus, attack graph-based risk assessment enables us to quantify risks for single or multiple attack paths and/or attack sources.

The basic tangible elements of risk in an IT system can be enumerated as assets, vulnerabilities, and threats. In our model, an asset is any computer or network equipment, physical or virtual, on which software related vulnerabilities might exist. We also define the term product as software which might have any vulnerabilities on them. Assets might have one or more products on them.

Asset valuations are made on a scale of low, medium, or high according to CIA requirements due to two reasons. First, information security risks arise from the loss of confidentiality, integrity, or availability of information or information systems [1]. Second, FIPS 199 provides information classification as low, medium, or high security based upon the CIA criteria of the assets [2].

Vulnerabilities in a system are those defined in the NVD vulnerability database with their specific CVE IDs. The list of relevant vulnerabilities in a given system could be generated by scanning the system with vulnerability detection tools such as OPENVAS, Nessus etc. Furthermore, for the attack graph-based model, vulnerabilities in a system can be filtered out to identify which of them are not applicable and cannot be exploited, taking into account the protection of tools such as IDS/IPS residing on the attack paths. Thus, vulnerabilities labelled as protected are disregarded for risk calculations.

Vulnerabilities are exploited with a probability that is determined by the low-level metrics derived from the underlying metrics of the vulnerabilities, threat sources and attack paths. In the base model, probabilities corresponding to exploiting CVEs are assumed to be independent thus probability calculation of a single CVE is not affected when there are multiple CVE exploits on an asset. Attack graph-based model, however, considers the probabilities of previous CVEs on the attack path for calculating the probability of CVE exploitation.

Impacts are defined as confidentiality, integrity and availability (CIA) losses at the assets if CVEs are exploited successfully on them. Impacts are computed according to the CIA requirements of the assets and the CIA impacts of the vulnerabilities residing on them.

Threat sources in the model are defined as attackers which could be either hackers attacking from the Internet or malicious users attacking from a specific location inside the network that is under assessment. In the attack graph-based model, threat sources are denoted by two parameters, capability and motivation. Capability of a threat source is the measure of how capable it is in exploiting known

vulnerabilities. Motivation, on the other hand, shows the degree of which an attacker is willing and resolute to capture a target by exploiting vulnerabilities.

Attack paths or attack graphs show how multiple vulnerabilities may be combined for an attack. In our approach, attack graphs represent vulnerabilities on the assets with directed connections between each of them, depicting the cycle free exploitation orders. Vulnerability exploitations on attack graphs are showed as transitions between states. Generating the attack graphs is out of scope in our work (attack graphs can be generated as described by earlier studies e.g., [3]) Fig. 14 illustrates an example attack graph model.

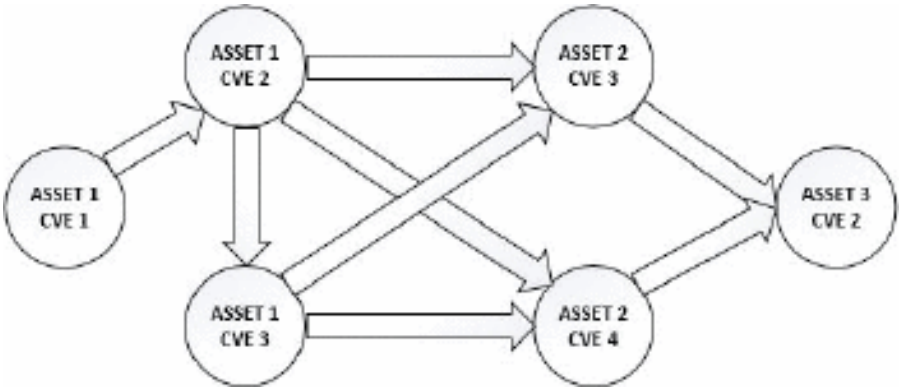

Figure 13 Example attack graph model

3.1.1 Attack Surface Analysis

PALANTIR platform envisions a broader range of services compared to previous generations, supporting an increased number of use cases and applications. The broader application domain leads to increased consumer use and, in turn, increased hacker activity. Due to this chain of events, strong and efficient security measures are required to create a secure and trusted environment for users. In this section, an objective overview of the attack surfaces related to PALANTIR (Edge, cloud, 5G) and their security issues is presented. A categorization of the security technologies using Open Systems Interconnection (OSI) layers is detailed and, for each layer, its vulnerabilities, threats, security solutions, challenges, gaps and open research issues are discussed. While all seven OSI layers are discussed, the most interesting findings are in layer one, the physical layer. In fact, compared to other layers, the physical layer between the base stations and users' device presents increased opportunities for attacks such as eavesdropping and data fabrication. However, no single OSI layer can stand on its own to provide proper security. All layers in the PALANTIR platform must work together, providing their own unique technology in an effort to ensure security and integrity for user sensitive data.

To fully understand the security issues and solutions for 5G networks we use the OSI protocol stack instead of 4-layer TCP/IP format or other layered models. OSI provides three additional layers compared to TCP/IP, namely presentation, session, data link, and physical layers. In TCP/IP instead, application, presentation and session layers are comprised in the application layer, while the network interface layer takes on the functionalities of the data link and physical layers of the seven-layered OSI approach. Therefore, considering the OSI layers allows us to provide a more detailed assessment of the security aspects. Application-driven services, such as the services automated vehicles, AR/VR, and others, are considered to be some of the major innovations in 5G system and beyond. As such, it is very important to secure the application layer. Though in practice, the presentation and session layers may be incorporated into the application and transport layers, respectively, we want to look at the security issues in the session layer and presentation layer functionalities in depth.

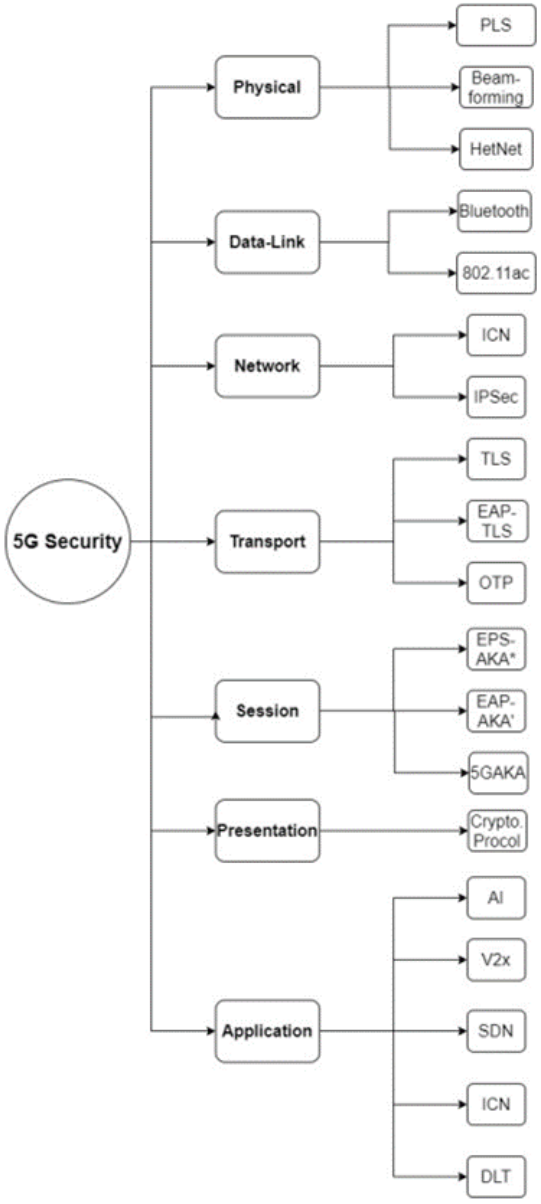

Figure 14 OSI layer presentation for 5G networks

3.1.1.1 5G Security

5G is creating an even more interconnected network, where devices with different capabilities and quality of service constraints need to interoperate. 5G is hence also facing the ever-increasing demand of users for connection and ubiquitous access to the network. Compared to previous generations, 5G is expected to solve six challenges, namely higher capacity, higher data rate, lower end-to-end latency, massive device connectivity, reduced cost, and consistent Quality of Service. At the same time, attackers' capabilities also increased compared to the previous generations. In fact, the computational power of current mobile devices allows for launching complicated attacks from inside the mobile network. Furthermore, the type of attacks and generated malwares are more efficient and effective than those faced by previous generations. This leads to attacks being driven by stronger aims compared to previous generations, including big cyber-crime rings with clear financial, political, and personal

motives. This is further motivated by the fact that the mobile network is not limited to voice and video calls, but also supports a large number of other services and devices, creating a wide attack surface that may lead to severe disruption in the functioning of one of the interconnected networks. Due to the larger number of services and connected devices, and despite the introduced security measure, 5G may still be vulnerable to different types of attacks. In the next sections we will discuss the identified vulnerabilities, organizing the technologies and the associated threat vectors according to the OSI model.

3.1.1.2 Application Layer

The application layer (layer 7) is the layer that processes and formats data so that it can be passed to layer 6, the presentation layer [4]. Layer 7 is the closest layer to the application itself. Application based encryption is considered to be an effective security mechanism for those applications placed onto layer 7. However, the application layer does not include the applications but only the application protocols. As previously discussed, 5G envisions a broader application domain compared to previous generations. In this section, we review some of the application layer services in different use cases, such as ICN, blockchain/DLT, SDN, and Artificial Intelligence (AI).

Blockchain and DLT have recently drawn significant attention from the scientific community, with applications not only in the exchange of cryptocurrencies, but also for networking purposes. Bitcoin is the first introduced blockchain, providing an application layer protocol with an open-source design. Bitcoin was presented in 2008, introducing the concept of a peerto-peer electronic cash exchange. The peer-to-peer exchange concept removes the traditional middle entity, such as an FDIC ensured bank. This means that the transaction can be anonymous, free from government eyes and government taxes. Despite its controversy, Bitcoin is accepted at numerous companies, including newegg.com, a few Subway franchises and small local companies like Grass Hill Alpacas [5] [6] [7] Anyone with access to a computer can use bitcoin. In fact, Bitcon.org walks individuals and businesses through creating a bitcoin wallet and buying bitcoin. Starting from the launch of Bitcoin, other applications, such as Hyperledger, have made use of the blockchain technology [8] [9]. While anonymity is synonymous with Bitcoin, it is not synonymous with blockchain. Among the others, blockchains find applications in networking for vehicular communications, IoT, as well as in the design of radio access networks.

ICN has been proposed as a novel approach in 5G networks to shift from a user-centric paradigm to a data-centric one. The idea is to enable in-network caching and replication by having data independent from location, application, storage, and means of transportation. Therefore, each data/content is assigned a specific name, and is retrieved without knowing the physical location of the content provider. This provides a significant shift compared to IP based networks, allowing for a significant reduction in network traffic and communications delay. Among the others, ICN has been proposed as an implementation at the application layer [10]. Also, ICN plays an important role in the IoT context. In fact, since devices such as smart sensors and meters are becoming increasingly powerful, they start to act like users, and therefore have specific requirements at the application layer [11]. ICN is used in this context to provide higher network throughput and smaller transmission delays.

• SDN enables a more flexible network management compared to the traditional architectures. A global view of the network is maintained at the SDN software-based controllers, which receive requests from the different applications and provide them with resources to guarantee the required quality of service. At the application layer, SDN involves network components to provide abstraction and supervision for a proper network configuration at any time, as well as orchestration and resource allocation [12].

• AI is now largely adopted as a solution in different domains and all those applications in which classical methods for function parametrization or estimation are not viable. In its supervised implementation, AI exploits previously collected data to train a proper model, and successively takes decisions on newly generated data. AI is widely diffused in the wireless domain, finding applications

such as channel estimation, fault recovery, and resource allocation [13] . We here focus on the challenges and security issues posed by the application of AI at the application layer.

A. Vulnerabilities and Threats

As new kinds of services and paradigms are implemented at the application layer, the associated security and privacy threats pose a significant challenge for their successful deployment:

1) Blockchain: Among blockchain-based currencies, Bitcoin is the most widely used cryptocurrency thus far. Distributed Denial of Service (DDoS) represents a threat toward the Bitcoin protocol. DDoS attacks are capable of causing security breaches to Bitcoin currency exchanges, mining pools, and eWallets. Therefore, the same issues can be reflected into the network application of the blockchain technology. For instance, in vehicular applications, a DDoS attack may cause the vehicle to be disconnected from the infrastructure, causing major damages to both the vehicle and the people in it. Transaction malleability has been pointed out as a cause for security issues. Cryptography can be vulnerable if the wrong type of algorithm is used. For example, there is SHA-256 and double SHA-256. Among these two algorithms, double SHA-256 is the less vulnerable because it is not susceptible to length extension attacks [14]. Additional vulnerabilities to blockchain are replay attacks, sybil attacks, impersonation attacks, and man-in-the-middle attacks. Another major threat is given by the consensus protocol. In particular, 51% attack represents one of the major attacks, in which the majority of the mining power in the network is controlled by a single entity. In this case, this entity may control transactions preventing some of them to be concluded. This also allows the attacker to undermine the possibility of other users getting reward for mining a transaction, therefore monopolizing the reward associated with mining. Furthermore, this would allow the attacker to perform a double spend, in which the same asset is spent twice in the network due to the fact that the attacker gets to mine a transaction at the required time creating a fork in the network. In an initial deployment state, where the network is populated by a small number of devices, the 51% attack represents a concrete threat for the consensus. Therefore, any blockchain application designs shall consider all the significant threats highlighted in literature before obtaining a successful deployment.

2) Information-centric networking: Privacy represents one of the major problems in ICN. In fact, data is associated with names that reveal significant information to a passive eavesdropper. Names in ICN serve both as identifier and locator of data, allowing attackers to infer the identity of the provider based on the content. In a watchlist attack, a malicious user is able to build a predefined list of content names to monitor. The attacker then performs a real-time filtering to delete the request or the content itself based on the users' requests. Therefore, the attacker is able to censor a content, or to perform a Denial of Service (DoS) attack toward a user accessing the content in the watchlist. Furthermore, the attacker is able to monitor a large number of requests for a certain content, hence jeopardizing the privacy of the users searching for that content [15]. ICN names are user-generated content that is recorded into the routing table. This implies that it is possible for a malicious user to act on the application layer to run a resource exhaustion attack. The very same freedom given by name spaces can also be used by producer applications to advertise any desired namespace [16]. A further threat is given by the possibility of an attacker being able to breach the signer's key. In fact, an attacker retrieving a certain content also has access to the singer's public key and signature. This can be used with the content itself to determine the signer's key.

3) Software-defined networks: The application layer of SDN architectures is vulnerable to multiple attacks, given by surfaces such as malicious or bugged applications and weak authorization or authentication [17]. For instance, third-party and control applications may be compromised if not equipped with proper authority restrictions. This may imply the execution of shut down or disconnect commands with the attacker gaining privileges over those applications. A further threat at the application layer is given by the installation of malicious applications on top of the controller. Such malicious applications can be exploited to manipulate and control packet handlers, by means of packet discard,

reordering and disrupting proper packet forwarding. Furthermore, the same applications can be used to infer information about users' activities by means of packet sniffing. Another threat surface is given by the northbound interface, which connects the application plane with the control plane. In case of vulnerable protocols, Application Program Interfaces (APIs), or those without a proper encryption, sensitive information may be exposed to attackers, showing the information exchanged between the controller and the target application. The SDN application layer is also vulnerable toward DoS attacks and their distributed version [18].

4) Artificial Intelligence: One of the most critical threats toward AI is given by adversarial learning. The attacker aims at injecting malicious data inside the learning model, such that training is performed based on malformed/corrupted data. Considering, for instance, classification problem, the goal of adversarial learning is to inject malicious data such that classification no longer return the correct output. The assumption here is that the attacker is able to infer information from the legitimately trained classifier, such that an adversarial dataset can be built [19]. Therefore, an application leaking this kind of information or that can be queried from an external actor is sensitive to adversarial learning attacks. These two scenarios also arise a threat toward the privacy of users. In fact, if the training set is based on costumers' behavior or sensitive information, by querying the learning model, it is possible for an attacker to gather statistical information regarding users or to perform model inversion [20].

B. Security Solutions, Challenges and Gaps

In vehicular networks, OBEs should carefully manage communication between different layers in order to notify changes in identities at the different layers. From an application layer perspective, OBE identity shall be protected from eavesdropping. A new protocol [21], is specific to 5G enabled vehicular networks and addresses reliable, secure and privacy-aware real-time video. In order to solve for impersonation attack and forged video upload, public key cryptography is proposed as possible solution. Transaction malleability has been resolved with ''segwit'', which is implemented as a soft fork change in bitcoin's transaction format for Bitcoin's continued success, it is important that the Bitcoin network scale easily as it grows in popularity and use. Currently, Bitcoin protocol can complete approximately seven transactions per second compared to Visa, which can complete approximately 2000 transactions per second [22]. The outstanding question is whether new security risks will arise while proposing a modified Bitcoin protocol to support greater transactions per second. Bitcoin protocol uses a hash function such as SHA-256, so it will be important for the Bitcoin protocol to be modified to work with stronger hashing algorithms as they are developed. Several blockchain vulnerabilities can be addressed via Lightning Network and Smart Contract (LNSC) [23]. The LNSC is expected to resolve replay attack, impersonation attack and man-inthe-middle attack due to the lightning network's trading management system and the smart contract's general-purpose computations [24]. The sybil attack, which makes use of several fake identities controlled by a single lead fake identity, can be avoided by using TrustChain. In SDN environments, DoS and its distributed version at the application layer pose a significant threat. Therefore, detection and mitigation of such attacks represents one of the core features for security. Machine learning can be exploited for this purpose [25]. However, has previously discussed, machine learning is vulnerable to adversarial attacks. In ICN, data aggregation represents a significant threat towards users' privacy. Therefore, solutions such as the one proposed by authors in [26] need to be included to guarantee arbitrary data aggregation while preserving users' privacy. In AI-based applications, adversarial learning poses one of the major threats. Therefore, a secure system needs to prevent malicious data to be injected in the learning phase. Different solutions for robust classification and anomaly detection have been proposed [27].

3.1.1.3 Presentation Layer

The presentation layer formats the file so that the destination computer understands how to open and present it, including decompression and decryption of files [28] . While encryption will continue to play

an important role in 5G networks, research points to encryption via applications rather than at the presentation layer. Vulnerabilities in layer six can be due to weaknesses in the implementation of the presentation layer functions. Security and privacy threats at the presentation layer.

A. Vulnerabilities and Threats

The insertion of malicious data into files, web pages and applications is a common practice today. More than twenty years ago, Handel et al.[29] reported the possibility of hiding data in the presentation layer by using multimedia components. In recent years, social media applications such as YouTube, Facebook and TikTok have become very popular and are hence widely used. According to Pew Research Center, social media usage for adults has increased from five percent in 2005 to 72% in 2021 [30]. The increase in social media usage is caused, in turn, by the opportunity to insert malicious data into all forms of files used by these platforms, including audio and video. Attackers can insert illegal input into presentation-layer facilities in order to cause issues such as buffer overflows. Inserting illegal input into multimedia files is an easy task for an attacker, as these files tend to be large in size. Format string vulnerabilities can cause a program to crash, provide attackers access control to the program, and cause bad information to be displayed on the output stream. Lastly, since instructions for encryption and decryption are provided at the presentation layer, this opens up vulnerabilities related to cryptography that can be exploited by the attackers to compromise the confidentiality requirements.

B. Security Solutions, Challenges and Gaps

To proactively address the vulnerabilities at the presentation layer, [31] advises thoroughly checking input resulting from the interaction of layers seven and five. This points to the need to provide security at all OSI layers, with each layer working together to guarantee the most secure network possible. Short-cuts in implementation plans that skip over a multi-layer security assessment may end up being disastrous. In addition, it is important to carefully review cryptography protocols periodically, considering the past issues arising with previously released crypto-solutions. This is needed to ensure that not only the existing vulnerabilities and security issues are taken care of, but also to make sure that the emerging threats are proactively addressed before they result in an issue. In addition, the security solutions should diligently validate the input to create a clear delineation from the user input data to the data generated by the program, such that the user input is safe to be used. Any redesign to the presentation layer to resolve security concerns is expected to create additional opportunities for exploitation. Hackers will hence maintain the ability to insert illegal input and take advantage of the format string vulnerabilities in 5G networks as well, if this is not properly mitigated.

C. PALANTIR Contributions

PALANTIR with the development of UC1 regarding medical practices, directly addresses the presentation layer, as a potential attack surface is the medical practitioner's front-end application. Regarding the protection and risk management of the presentation layer vulnerability, PALANTIR platform offers a fully-fledged toolset for threat/attack network detection, thus preventing potential vulnerabilities on upper layers. More specifically, for the edge use case it is of utmost importance to fortify access services, as they are usually heavily involved with user interaction, which renders sensitive user data at risk. The RAF implementation efforts also aim at quantifying the value of data under risk.

3.1.1.4 Session Layer

The session layer is used for application-to-application communications. This layer opens the communication connection, keeps it open while during data transfer and then closes it once the transfer is complete [32]. Session layer provides three security services: authentication, authorization and session restoration [33] Examples of layer 5 protocols are Password Authentication Protocol (PAP), Remote Procedure Call (RPC) and NetBIOS. Furthermore, an authentication framework that is widely used in wireless networks is Extensible Authentication Protocol (EAP). EAP framework provides the flexibility for authentication protocols to fit the specific need of an individual environment. For 5G networks,

authentication is supported by 5G AKA and EAP-AKA', which is the 5G version of EPS-AKA [34]. 5G-AKA and EAP-AKA' are important for secure 5G networking, as they address several vulnerabilities in 4G authentication while being used to authenticate the nodes. Furthermore, they also support the Universal Mobile Telecommunications System (UMTS).

A. Vulnerabilities and Threats

PAP is not very secure, as its credentials are sent in plaintext. This allows an attacker to run sniffing and man-in-the-middle attacks [35]. Systems sometimes are built to use PAP as the last attempt to attain authentication if other, more robust, authentication protocols do not work. RPC fails to provide secure authentication, opening up the possibility of malicious activity. NetBIOS can be set up to permit shared resources in Windows environments. Accordingly, this vulnerability can be used to discover information about various machines on a Windows NT network [36] . EAP as a stand-alone framework does not have security vulnerabilities. However, its variants may be non-secure [37]. An implementation vulnerability for the variant EAP-GSS and LEAP is a dictionary attack, which uses common words in a brute-force attempt to break the code. EAP can use PAP and therefore may be vulnerable to threats associated with PAP. EPS-AKA vulnerabilities include disclosure of the user identity, man-in-the-middle attacks and DoS attacks [38] .

B. Security Solutions, Challenges and Gaps

To aid with the PAP plaintext vulnerability, administrators can build the system to support the Challenge Handshake Authentication Protocol (CHAP). To circumvent the NetBIOS vulnerability, the administrator can disable the system's null session ability using a very strong local admin passwords, and negate shared access to the root of the hard drive. Secure RPC (SRPC) resolves the weak authentication associated with RPC. Security challenges continue to exist with the EAP framework and its associated variants, such as EPS. Examples of such vulnerabilities include: disclosure of the user identity, man-in-the-middle attacks, and DoS attacks. 5G-AKA and EAP-AKA' provide solutions to some of the existing authentication issues in 4G and earlier generations. Some of the key differences between 5G-AKA and EAP-AKA' are given by the operational flow and the exploited key derivation functions. Per analysis of Basin et al. [39], 5G-AKA is affected by several weaknesses, including session key agreement, unlinkability against active attacker and implicit authentication.

C. PALANTIR Contributions

PALANTIR with the development of UC1 and UC3, aims at addressing various session-related vulnerabilities that also have to deal with TEID session, high-jacking and malicious RAN impersonation. PALANTIR platform using advanced AI mechanisms and by monitoring the netflow traffic, can build information graphs related to session information and detect relevant anomalies and risks. The automated detection and mitigation functionalities of the platform can efficiently manage session layer related attacks, by deep inspecting the network and creating various dynamic profiles.

3.1.1.5 Transport Layer

The transport layer has been referred to as the heart of the OSI model, as it is used for computer-to-computer communications. Just like the session layer, it opens communications, keeps them open and closes them once complete. SDN is one of the enabling technologies for the transport layer in 5G networks [40], [41] . It is believed that as 5G is adopted on a mainstream basis, the SDN will to play an important role to get the most out of 5G. As similar to software and hardware, SDN and 5G will dovetail each other. This section reviews transport layer information as it relates.

A. Vulnerabilities and Threats

Transport Layer Security (TLS) from the SDN perspective is seen as vulnerable to DoS attacks, rule modification, and malicious rule insertion. While SDN can improve the functionality of the 5G network, it does pose security challenges. Some of the vulnerabilities associated with SDN are: • Weak

authentication for the applications and users can lead to spoofing attacks; Weak authorization can also lead to man-in-the-middle and unauthorized access related attacks. Security vulnerabilities and challenges for SDN are possible in different planes such as Application (for example, applications that abuse SDN control messages), Control (for example, manipulation of system variables), Interface (Man in the Middle attacks) and Data (Side channel attacks). In case of the application or user requesting a service from the 5G network, before routing information is created for packet traversal, a proper authorization is required for the accountability purposes. Lack of encryption standards can lead to eavesdropping or spoofing related attacks [42] As SDN supports centralized control, it is an easy target for DoS attacks, and exposure of important APIs to the intruder. To implement DDoS attacks, the TCP or UDP SYN messages will be used to flood the host. As a result of the DDoS attacks, the controller is made unavailable to serve other nodes in order to make routing decisions, thereby reducing the performance of the SDN networks. Due to its centralized nature, the controller represents a potential bottleneck and enables the adversaries to sniff the controller traffic. The transport layer protocol proposed for 5G is open transport protocol (OTP). In OTP, TCP modifications and adaptations to retransmit the lost or damaged TCP segments over the wireless link are proposed as solution for 5G networks. As per our review, the vulnerabilities, threats and security challenges are not studied in detail. With respect to EAP-TLS, Zhang et al. [43] point out several design flaws. For instance, 5G networks and subscribers cannot agree on the mutual identification and master key after the successful termination of the session, due to the ambiguities in the specified standards.

B. Security Solutions, Challenges and Gaps

Security should be pre-built into the SDN architecture, and delivered as a service in order to provide privacy and integrity to connected resources [44]. This is made possible by using an architecture with two communication channels, i.e., the control and data channels. The control channel transports only the control data between the control and data planes. On the other hand, the user communication data is transported only through the data channel. As technology morphs and improves to release new solutions in areas such as SDN, security should be considered. Building t security into SDN will aid in defending against attacks at the transport layer, and in turn will defend against attacks towards the overall 5G architecture. This is achieved by designing components to secure the SDN controller, protecting the flow layer of the SDN, and hardening interfaces such as application programming interfaces and communication channels. Since SDN inherently provides the logical centralized control, it supports robust security monitoring and protection. It also enables rapid deployment of security policies, that may not be easily possible in traditional security approaches. The SDN approach by Ahmed et al. has the potential to provide security protection not only from a virtualized environment perspective, but also from a physical environment perspective. There are several open issues that need attention in securing SDN. For example, network virtualization in SDN is vulnerable to multiple issues such as rewrite problems, spoofing attacks, implementation of action isolation, and DoS attacks etc. In the future, these security challenges at the transport layer need to be addressed by the security community to ensure the security of 5G.

C. PALANTIR Contributions

PALANTIR directly contributes to the detection, mitigation and remediation of various attacks in the transport layer as the entire platform is end-to-end Openflow-based, rendering the entire deployment totally software configurable. Regarding detection PALANTIR develops specific detection mechanisms for OVS related attacks and with its Firewall implementation can mitigate malicious traffic and protect various targets. Finally, the software defined network of the platform can dynamically redirect traffic flows, without operation disruption, thus developing an E2E solution for various scenarios. SDN is a key enabler not only in terms of infrastructure but also in terms of programming, as it allows the PALANTIR platform to modify and create alternative traffic data paths real time and based on the security and risk vulnerabilities of the assets under protection. SDN and NFV still offer an ample area

to experiment and patch up risk vulnerabilities, coming from the dynamicity of the network and the shared resources that certain VNF implementations offer.

3.1.1.5 Network Layer

The network layer instructs packet routing. This layer supports adding information as to where, how, and when packet routing happens in order to prevent congestion. With 5G networking, security will need to be implemented in multiple OSI model layers to ensure the protection of data. ICN plays an important role at the network layer as well, as it has been proposed as a new paradigm to tackle the inefficiencies and architectural problem of existing networks. The network layer of ICN assigns a unique name to each content, which is later used for routing over the network. Different from IP-based routing, content requests search for the closest available copy regardless of the destination machine's address. This section investigates the security issues of both traditional IP-based content routing and ICN. In the former architecture, we investigate the use of IPsec to achieve security at the network layer.

A. Vulnerabilities and Threats

Breaking the IPSec is generally considered not feasible. However, IPSec alone cannot provide security for 5G networking. It must work in conjunction with other successful security protocols in other layers of the OSI model to ensure security. Apart from generic threats like DoS, other threats from the network layer perspective include man-in-the-middle attack, IP Spoofing, injection, eavesdropping, packet sniffing, and Gateway attacks represent a significant threat. Due to the new technologies in 5G, specialized threats such as virtualization and multi-edge computing, edge node overload, and abusing of edge open APIs need to be taken into consideration [45]. One of the innovations that is proposed in 5G network standard is network slicing, which has unique security challenges. For example, if an adversary gets access to one slice, they can conduct attacks on other network slices, resulting in security threats toward confidentiality, integrity and availability. Specifically, if an adversary is able to tamper the network slice selection data, unauthorized devices or the adversaries may use such information to connect to a particular network slice and consume resources [46]. Network Function Virtualization Infrastructure, which is part of 5G network, has several potential threats and vulnerabilities, such as the potential infection of Virtual Machine (VM) images by the attacker. These infections, in turn, result in data leakage, DoS attacks, performance degradation of other VMs, and hijacking of the components of the compromised hypervisor. Although ICN may prevent attacks to the IP-based internet architecture such as DoS, it is still vulnerable to different types of attacks [47]. In fact, resource exhaustion, publisher unavailability, and route depletion pose threats toward the availability of the content. For instance, considering stateful routing, routers need to keep record of requested/received packets per interface until the request is consumed. This mechanism is vulnerable to DoS attacks, in which the attacker aims at disrupting forward services or overloading network traffic by issuing an excessive number of requests. Requests flooding can also be exploited to jeopardize the publisher's availability. In fact, by sending an excessive number of requests for the same content publisher, the publisher's availability is undermined and the related content unreachable. In route depletion attacks, saturation is exploited at the routing table, filling it with malicious content belonging to different domains. This jeopardizes the correct forward of content requests to publishers or to available cached data copies. Furthermore, delay in the replies or lack of replies may also be exploited by an attacker to disrupt users' services [48]. Content caching exhibits vulnerabilities undermining content integrity and availability. Examples of attacks toward caching include cache snooping, pollution and poisoning. In cache snooping, the attacker obtains sensitive information regarding a user or a group of users, therefore undermining their privacy. This may be obtained by gaining access to lists of cached content and by monitoring its content, or the time difference between replies from publisher or nearby caches. The gain obtained by caching may be disrupted by means of cache pollution. In fact, if an attacker populates a cache with useless content, the routing algorithm needs to search content in remote points in the network. Cache poisoning also exploits

the injection of malicious data in caches. In this case, however, the attacker's goal is to distribute fake content in the network.

B. Security Solutions, Challenges and Gaps

For the segment between the Broadcast Multicast - Service Center and Evolved Node Base station, IPSec can provide authenticity, integrity, and confidentiality over a unicast link. Implementation of IPSec at the network layer will be fundamental in providing confidentiality, integrity, data-origin authentication, and protection against replay attacks for each individual packet [49]. Unfortunately, IPSec cannot extend all the way to the User Equipment (UE). We will discuss different security measures in the Physical layer section to provide base station to UE security solutions. However, the authors have not implemented and evaluated their approach. While some solutions have been proposed for network slicing, there are several limitations and gaps that need to be addressed. Machine learning-based solutions have been proposed to address the security threats in network layer. However, the experimentation has not been conducted in a realistic scenario, so the proposed solutions cannot be deemed as reliable in real-world scenarios [50] . For a successful deployment of ICN, security solutions should provide content integrity and availability, authenticity, certified content provenance, and ensure users' privacy. In order to prevent the aforementioned DoS attacks to content routing, hash functions on pending request tables have been proposed as a countermeasure. Content caching attacks may instead be prevented by means of signature verification, and by monitoring caches' content. Although different solutions have been proposed for content routing [51] and caching attacks [52], still mobility and scalability represent a significant challenge. Furthermore, centralization shall be avoided, in order to prevent a single point of failure being a target for the attacker.

C. PALANTIR Contributions

All PALANTIR use cases tackle network layer related risks, vulnerabilities and attacks, as the core detection and mitigation tools developed for the platform are mainly focused on network analysis and netflow dissection and deep inspection. The multi-modality of the technologies used for network security and the convergence with the AI backend offer a cybersecurity toolset that can analyse the underlying network infrastructure in great detail and detect various attacks and threats. Additionally, the virtualized orchestration solution of PALANTIR, renders it easily deployable across different environments and setups, and across different endpoint-types of the network. The platform can equally fortify, edge, cloud and 5G network deployments with the same efficiency and low-complexity.

3.1.1.6 Data Link Layer

The data link layer supports the integrity of the point-to-point transmission. It determines what type of technology and protocol is being used, so data can be successfully transferred to the physical layer. The 5G protocols consists of a user plane (UP) and a control plane (CP). The UP layer refers to the Data Link Layer. This layer is made up of four different sublayers: service data adaptation protocol, packet data convergence protocol, radio link control, and medium access control [53]. In 5G, flexibility is one important security requirement that needs to be considered. For example, some applications would require end-to-end security rather than relying on the security functionality provided by the core network. For those applications, that require end to end security, the applications would require security considerations in data link layer. Wireless point-to-point protocol transmission examples are IEEE 802.11 and Bluetooth. The standard 802.11, also known as WiFi, is the original wireless local area network standard protocol which has since been improved to 802.11ac, with a transfer max rate of 1.3 gigabytes per second. Bluetooth, on the other hand, has a max rate of three megabytes per second and a much smaller range of connectivity of 10 meters.

A. Vulnerabilities and Threats

The Access Stratum (AS) that is associated with the UP traffic is vulnerable to multiple threats, and further protection is required. This, in turn, results in customer data and communication flow being intercepted between the user equipment and centralized server by the rogue base stations. Possible solutions include Integrity Protection security algorithms [54] [0]. Sybil attack also represent a threat in this context, where the attacker replicates and manages more than one identity on a single device [55]. For example, CloudCracker is capable of evaluating 300 million WPA passwords in 20 minutes, and therefore potentially cracking a WiFi password in a reasonable time frame. Bluetooth is a high-risk protocol in public areas because of the ease of transferring data to a close range. Bluejacking and Bluesnarfing are two types of attacks that, when a user accepts an unsolicited message, result in personal information leakage. Attacks in the mobile edge computing environment is possible in this layer through DDoS type of attacks. The routing process, i.e., delivery of the packet from the sender to the transmitter in a multi-hop network, may be vulnerable to different types of attack. In particular, blackhole attacks are the most impactive ones. In a blackhole attack the attacker, upon receiving a packet to forward in the routing process, eliminates the packet therefore preventing it from reaching the intended receiver [56]. A different version of this attack is grayhole attack, with the main difference that the attacker does not systematically drop packets. Instead, packets are dropped in a random fashion. Although grayhole attacks may have lower impact in the overall network, they are also more difficult to be identified, as random drops may be due to malfunctioning of devices. Another variant of this attack is given by the sinkhole attack, where a node advertises itself as the best route in the network, such that packets are pass through it and are redirected to the sink node and hence discarded. In a fog environment, IoT devices are vulnerable to multiple treats at the data link layer. In fact, due to their limited power resources and to the huge number of connected devices, they provide multiple attack surfaces. Example of such attacks are DoS, and replay attacks, where a data packet is captured by the attacker and retransmitted in later sessions to impersonate the victim node. Furthermore, these devices are vulnerable to sybil attacks, where malicious node generates a fake virtual node to exploit resources from the network.

B. Security Solutions, Challenges and Gaps

Some of the attacks at the data link layer could be prevented by end-to-end security encryption protocols such as SSL. Threat intelligence solutions using machine learning and artificial intelligence can also be applied to mitigate threats at the user plane level. For example, device type and behavior profile can be detected to identify and mitigate botnets, malware, DDoS attacks etc. Augmented protection approaches using extensible authentication protocol (EAP) may help the core network to authenticate the devices the secondary protection at this layer. Authors in [57] suggest two solutions for WiFi security, 1) updating the firmware on Access Points, and 2) deploying Machine Learning-based Intrusion Detection Systems. With respect to the machine learning-based solution, the slow convergence of the learning algorithms is an issue for their application in Intrusion Detection System, and should be taken into consideration. This is particularly critical when mitigating real-time attacks. Real time solutions for machine learning-based intrusion detection systems represent a fundamental component of 5G network. A possible solution is proposed by authors in [58], where a light gradient boosting machine is used as detection algorithm. A deep learning-based approach is proposed by authors in [59], where an autoencoder network is trained to recognize four different type of attacks. Although most of the intrusion detection systems is based on machine learning techniques, non machine learning-based solutions can be exploited to mitigate the aforementioned shortcomings. For instance, the energy consumption of nodes and a suitable blacklist can be exploited in conjunction with connected dominating sets. A different approach for intrusion detection considers also the location of the devices, where a null space-based homomorphic MAC scheme can be deployed to guarantee efficient detection in terms of computational complexity and communication overhead. Cause effect relationship an also be exploited for intrusion detection. In particular, a code book-based approach can be exploited to associate keys to alerts to facilitate the alert correlation process. However, significant research efforts are still needed to

provide general real-time intrusion detection systems. As a third-party security measure, a Virtual Private Network (VPN), can provide an additional layer of security by acting as a container for the 802.11 network. Bluetooth can be secured by simply making the device undiscoverable when in public areas. In regards to the DDoS types of attacks, a combination of caching, anti-DDoS technologies can mitigate the DDoS attacks. One of the important challenges for security solution at this layer is balancing latency and power requirements as the high-speed encryption and integrity requirements would mean high power consumption, which is again a limitation in the mobile environment. To address the Sybil and replication attacks, techniques such as building trusted certification solution for infrastructure-less domain. In addition, the techniques such as resource (radio, storage and computational) testing and position verification, to counter identity replication and spoofing. Different solutions have been proposed in literature to mitigate blackhole, grayhole, and sinkhole attacks. The joint identification of blackhole and grayhole attacks has been proposed by authors in [60], and a preamble TDMA solution is proposed to mitigate the effect of such attacks. Data is periodically collected from network's nodes to verify both the data authenticity and consequently assign a trust level.

C. PALANTIR Contributions

PALANTIR contributes on the development of tools and services for botnet attack detection, and aims to apply these across all use cases. Regarding the data link layer PALANTIR addresses potential risks with an upper layer approach and by deploying various agents across all layers of the testbed. Since, data layer is of particular interest to UC3, dedicated agents and extensions have been implemented to collect the telemetry from the EPC to the RAN layer and detect attacks that are not directly related to the application layer. This helps PALANTIR to provide a holistic solution for 5G networks and in general wireless communications. PALANTIR telemetry with its modular and scalable approach can fit to different environments and capture a holistic view of the network and underlying infrastructure.

3.1.1.7 Physical Layer

The physical layer, also known as layer one, deals with voltage values, which in turn are converted to digital signals, and transmitted by a physical electrical or optical port. The core of the 5G infrastructure will remain connected with physical fiber cable, but the edge of the 5G infrastructure - the segment closest to the UE - will be predominately wireless [61]. Three progressive 5G technologies are within the wireless segment: HetNet, massive MIMO, and mmWave. The term HetNet refers to a network in which different cell types and access technologies coexist, playing a fundamental role in the expansion of the 5G network. Massive MIMO envisions the deployment of a larger number of antennas compared to previous antennas technology. mmWave instead envisions the shift towards higher transmission frequencies. Therefore, MIMO and mmWave refer to more physical related aspects. Since wireless signals are transmitted through the air, hackers have opportunities to to intercept and interfere with the wireless segment. In this section, we discuss the physical layer security and threats in 5G networks.

A. Vulnerabilities and Threats

Due to the transmission of wireless signals in free space, attackers can obtain private information from oscillations in the observed power. Eavesdropping enables the attacker to obtain cipher text. Merely obtaining the cipher text does not mean the attacker can read it. However, if a large number of cipher texts is captured, it is easier to infer the security scheme applied at the upper OSI layers, and opening the gate for private information to be stolen. Data fabrication and privacy violation attacks exploit physical layer vulnerabilities during wireless transmissions. Signal amplification attacks currently exist in 4G networks and are expected to increase on 5G. A signal amplification attack can be performed by botnets using various infected devices within a single cell area. The increase in ports on mobile devices opens the possibility of attacks through multiple forms of connectivity. Ports can be physical and logical. Mobile devices are especially vulnerable to logical port attacks, as each mobile app may present the opportunity for an attacker to take advantage of an open port in the individual app. According to the

University of Michigan, open ports can be used to obtain private information [62]. As each user adds a new app to their mobile device, the vulnerabilities increase. One of the security issues concerning heterogeneous network is how to define an access authentication method that can adapt to various network structures [63]. Also, due to the open nature of the wireless channel of 5G heterogeneous networks, the wireless communication system is more vulnerable to imitation, theft, and other external attacks that needs attention and security by design. Due to the complex nature and higher requirements for 5G networks, the resulting wireless communication network system is complex and highly modular. Hence, if one module is under attack, the entire wireless communication network system security is jeopardized.

B. Security Solutions, Challenges and Gaps

Three possible solutions are proposed for eavesdropping attempts: power control, beamforming, and clustering. Power control relies on detecting the wire-tappers and adjusting the transmission power. By making changes to the transmission power, the eavesdropper will not be able to access the private information. Beamforming also involves identifying attackers by using transmission power. Beamforming and power control can be used together, but the algorithm implementing such a solution has not been perfected yet. Clustering involves grouping users together to keep out the hacker. Clustering must work hand in hand with a method to identify the hackers, such that they can be isolated from a non-hacker group. PLS is a new network security solution that entails the use of noise, interference and fading to decrease the ability for intruders to capture readable data [64]. Furthermore, they also show the benefits of a decreased computational complexity with respect to higher layers cryptography. Reduced power consumption and artificial noise insertion in massive MIMO systems are effective in averting eavesdropping attacks. As for devices' ports, a suggested workplace solution is to scan all employees' phones for viruses or scan employees' phones randomly. A further solution for secure routing has been proposed by authors in [65] , where authors propose a jamming mechanism with optimized transmit power to efficiently deliver the content while preserving data security. In the MIMO context, different PLS solutions based on artificial noise have been proposed. Zhou et al. [66] noted that sharing of large-scale spectrum in 5G heterogeneous networks leads to many security and privacy challenges. To address these issues, they developed a privacy-preserving, incentive compatible, and spectrum-efficient framework that is based on blockchain. In this framework, they built a smart contract, which allows the users to sign a contract with the base station for spectrum sharing and receive dedicated payments based on their contributions. In addition, they also built the framework to support the details of secure spectrum sharing and consensus-based incentive mechanism design. The proposed solution is limited due to performance degradation issues, which can be improved further by learning through historical observations such as user behavior, load profiles and traffic distribution. The solution also did not consider multiple service providers or multiple base stations. The hash algorithms that aid the proof of work has vulnerabilities, and they need to be addressed. It can be concluded that PLS is the key framework for 5G security, as it contributes to secure 5G at every layer of the OSI model. However, due to the lack of direction as to which standards will eventually be implemented in the 5G environment, it is difficult to determine which protective measures are worth further investigation. This uncertainty is not uncommon in technology, and multiple standards are likely to be heavily financed and researched. Since it has not been determined if one single 5G technology, such as HetNets, will win out over another, it is difficult to focus on one set of security issues. The scale of the 5G network could impact the ability of security solutions to work, so HetNets, MIMO, mmWave, and D2D, can be used depending on the scale of the solution.

C. PALANTIR Contributions

As PALANTIR mainly focuses on the data layer and above the physical layer attacks, are not directly addressed, but are nonetheless taken into account during the RAN agent implementation and extensions. The physical layer is directly related to UC3, thus the agents and protocols used for data layer are applied with the same performance and efficiency for the physical layer. Observations and meta-information

that is harvested from the attack scenarios during UC3 in the 5GENESIS testbed are also shared and communicated in a MISP-based manner to the 5TONIC testbed. This can help build a more secure 5G ecosystem as-a-whole, given that PALANTIR RAN agents are technology agnostic and can be applied to various verndor-specific and open-source EPC and RAN implementations of 5G infrastructure. The modularity of both the platform and the relevant broker and agent components, can further help to open and externalize the open-source SIEM ecosystem as-a-whole.

3.1.2 Asset Identification

As previously described in D2.2, asset identification is an important process affiliated with a risk assessment that helps to mitigate or reduce security risks. Organizations need to identify the following: the assets critical for their operations; the threats to each asset's confidentiality, integrity, and availability; and asset vulnerabilities. The quantification of each risk in terms of its consequences and likelihood of occurring produces a prioritized list of risks for further action. Managers must then consider how to control the higher priority risks by selecting one of four basic strategies: avoidance, mitigation, transference, or acceptance.

As commonly defined, an asset is anything that has value to an organization and therefore, requires some measure of protection. 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:

- **Network:** These are assets which provide continuous flow of connectivity from one computer to another within the same network or over the internet. They provide the necessary platform for connecting computers and other devices to a network or over the internet. The following ICT assets are Network articles:
- **Hardware:** These are tangible assets which provide the necessary computing capability to run various software and system applications for specific use and purpose. It also includes assets which provide the required output for the software and system application
- **Software:** These are intangible assets which provide the necessary tools in assisting users deliver their daily tasks. Majority of these assets are provided off-the-shelf such as Microsoft's Windows, Office, Internet Explorer, etc. Generally, these assets are computer programs designed with specific use and purpose.
- **Support Facility:** These are assets which provide the desired infrastructure support and protection in maintaining the more critical ICT assets in running condition. In case of power failure and/or spikes in electricity supply, assets under support facility classification will provide the necessary backup and support to keep the essential ICT assets working and protected.
- **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.
- **Human Assets**: This asset group includes any human in the SME/MEs and network administrators to simple end users

3.2. Application of risk reduction measures to reduce security risks in the PALANTIR UCs

In D2.2, we described the risk assessment process that SME/MEs need to follow in order to identify potential hazards they may face and analyze the negative impact that they would have on their organizations, following the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF). The next step for an enterprise is to apply the necessary risk reduction/mitigation measurements based on the results of the risk assessment. This process ensures that SME/MEs will be able to (i) effectively reduce the risk of threats and hazards they might encounter and (ii) minimize the effects of those potential hazards.

PALANTIR is responsible for developing and offering a set of monitoring and remediation Security Capabilities (SCs) that enterprises can install and utilize in order to implement the risk reduction strategy based on their needs. These SCs have been extensively described in the respective technical deliverables of the project. Following the risk assessment introduced in D2.2, this section presents the risk reduction measurements that each use case will adopt, identifying the PALANTIR tools that will be applied to each one. The following tables provide a mapping between the identified threats for each use case and the PALANTIR SC that will be used as the respective risk reduction measurement.

3.2.1 UC1 analysis

Table 7: Risk reduction measures 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)	Applied PALANTIR SC
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.	Intrusion Detection System (IDS) SC using signature-based and anomaly-based detection techniques for detecting the MITM attack. Backup (BUp) SC to ensure that sensitive data will not be modified or deleted.

								Firewall and Router (FW) SC for preventing unauthorized extraction of stored data.
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	Intrusion Detection System (IDS) with the help of the Multi-Modal Machine Learning (MMML) for detecting the flood attack. Firewall and Router (FW) SC to isolate the attacker's generated traffic.
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 specially crafted for	Opportunity to attack internal devices and enact a series of other remote attacks	4	2	Attack Detection Traffic Diversion ACL policying	Deep Packet Inspection (DPI) applies advanced packet filtering techniques for detecting the malicious actor's packets. Firewall and Router (FW) SC to block the attack.

			this purpose.					
A01	CAPE C-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	Web-based Traffic Analysis (WTA) SC for monitoring layer 7 application protocols and the packets to the IP layer, such as layer 7 flows, application protocols, the websites visited, etc. Firewall and Router (FW) SC for preventing data leakage to the attacker.

3.2.2 UC2 analysis

Table 8: Risk Assessment for UC2: Uninterrupted Electronic Commerce with Cloud SecaaS

Threat id3	Threat Cat. Id2	Adversarial Technique1	Threat Description	Consequence of Incident	Impact (business level)	Likehood	Countermeasures (if applicable)	Applied PALANTIR SC
D01	CAPEC-94	Man-in-the-Middle Attack	The attacker positions himself/herselft 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	Intrusion Detection System (IDS) SC using signature-based and anomaly-based detection techniques for detecting the attack. Backup (BUp) SC to ensure that sensitive data will not be modified or deleted. Firewall and Router (FW) SC for preventing unauthorized access to stored data and services
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 informatio	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.	5	2	cryptographic tokens ML driven 'randomized' process of user action conformation or identity confirmation Activity Recognition ML supported verification of authentication	*NOT APLICABLE TO PALANTIR SC*

			n or upload malware.	Session hijacking and exploitation of sessions cookies and session cookie-based authentication				
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	Intrusion Detection System (IDS) with the help of the Multi-Modal Machine Learning (MMML) for detecting the flood attack. Deep Packet Inspection (DPI) for inspecting incoming IP packets and analyzing traffic flows. Firewall and Router (FW) SC to isolate the attacker's generated traffic.
A04	CAPEC-89, CAPEC-98	Phising and Phamring	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	Web-based Traffic Analysis (WTA) SC for monitoring layer 7 application protocols and the packets to the IP layer, such as layer 7 flows, application protocols, the websites visited, etc. Network Netflow Sniffer (NNS) to collect the network traffic and prepare the

								packets to be sent to other PALANTIR components. Backup (BUp) SC to ensure that sensitive data will not be modified or deleted. Firewall and Router (FW) SC for preventing unauthorized access to stored data and services
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 device or user device with access to cloud server	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 Access to corporate and customer accounting data Unauthorized Use of Device Resources and exploit of trusted devices	4	2	Attack Detection Activity Recognition Detection data leakage using ML mechanisms Firewall policies	Deep Packet Inspection (DPI) for inspecting incoming IP packets and analyzing traffic flows. Web-based Traffic Analysis (WTA) SC for monitoring layer 7 application protocols and the packets to the IP layer, such as layer 7 flows, application protocols, the websites visited, etc. Backup (BUp) SC to ensure that sensitive data will not be modified or deleted. Firewall and Router (FW) SC for preventing unauthorized access to stored data and services

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	Web-based Traffic Analysis (WTA) SC for monitoring layer 7 application protocols and the packets to the IP layer, such as layer 7 flows, application protocols, the websites visited, etc. Backup (BUp) SC to ensure that sensitive data will not be modified or deleted. Firewall and Router (FW) SC for preventing unauthorized access to stored data and services
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	Network Netflow Sniffer (NNS) to collect the network traffic and prepare the packets to be sent to other PALANTIR components. Firewall and Router (FW) SC for preventing unauthorized access to stored data and services

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	Deep Packet Inspection (DPI) for inspecting incoming IP packets and analyzing traffic flows. Backup (BUp) SC to ensure that sensitive data will not be modified or deleted. Firewall and Router (FW) SC for preventing unauthorized access to stored data and services
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	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	Intrusion Detection System (IDS) SC using signature-based and anomaly-based detection techniques for detecting the attack usin NLP based incoming data filtering. Web-based Traffic Analysis (WTA) SC for monitoring layer 7 application protocols and the packets to the IP layer, such as layer 7 flows, application protocols, the websites visited, etc. Deep Packet Inspection (DPI) for

			a header of the mail message..					inspecting incoming IP packets and analyzing traffic flows. Firewall and Router (FW) SC for preventing unauthorized access to stored data and services
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	Network Netflow Sniffer (NNS) to collect the network traffic and prepare the packets to be sent to other PALANTIR components. Backup (BUp) SC to ensure that sensitive data will not be modified or deleted. Firewall and Router (FW) SC for preventing unauthorized access to stored data and services
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	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	Web-based Traffic Analysis (WTA) SC for monitoring layer 7 application protocols and the packets to the IP layer, such as layer 7 flows,

			forgotten passwords.				email-based authentication Prevent login/password recovery functionality to be vulnerable to an injection style attack.	application protocols, the websites visited, etc. Network Netflow Sniffer (NNS) to collect the network traffic and prepare the packets to be sent to other PALANTIR components. Firewall and Router (FW) SC for preventing unauthorized access to stored data and services
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 exists 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	Web-based Traffic Analysis (WTA) SC for monitoring layer 7 application protocols and the packets to the IP layer, such as layer 7 flows, application protocols, the websites visited, etc. Network Netflow Sniffer (NNS) to collect the network traffic and prepare the packets to be sent to other PALANTIR components. Backup (BUp) SC to ensure that sensitive data will not be

								modified or deleted. Firewall and Router (FW) SC for preventing unauthorized access to stored data and services

3.2.3 UC3 analysis

Table 9: Risk reduction measures 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)	Likehood	Countermeasures (if applicable)	Applied PALANTIR SC
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.	Intrusion Detection System (IDS) SC using anomaly-based detection techniques and Multi-Modal Machine Learning (MMML) for detecting for detecting the anomalous behaviour of the network. Firewall and Router (FW) SC for blocking the generated

								attack traffic.
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.	Intrusion Detection System (IDS) SC using signature-based and anomaly-based detection techniques for detecting the MITM attack. Firewall and Router (FW) SC to apply new network policies and routing in order avoid the MITM attack.
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.	Deep Packet Inspection (DPI) for inspecting incoming IP packets and analyzing traffic flows. Web-based Traffic Analysis (WTA) SC for monitoring application

								protocols, the visited websites, etc.
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	Web-based Traffic Analysis (WTA) SC to prevent social engineering and phishing attacks by monitoring multiple user-centric applications. Firewall and Router (FW) SC to prevent sensitive data leakage.

4. Conclusions

This document presented the updated definition of the PALANTIR use cases, the involved actors and workflows, based on the feedback acquired during the 1st project review. Moreover, the attack surface analysis (categorized per OSI layer) and asset identification processes related to the protection of service-oriented infrastructures was complemented with the mapping of specific risk reduction measures to the threats identified in the PALANTIR 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 vulnerabilities and threats, security solutions, challenges and gaps in the domain of software networks and cloud-native deployments was conducted based on recent literature and partners' experience, highlighting the extensivity of PALANTIR's holistic protection across many different layers. Finally, the attack surface analysis conducted in the context of D2.2 was enriched with explicit risk reduction measures (developed within the course of the project) that will be considered for the application of tailored countermeasures, during the upcoming pilots.

All PALANTIR partners contributed to this endeavor, achieving a consensus among the consortium members on the next phases of the pilots planning and execution.

5. References

[1] NIST Special Publication 800–30R1: Guide for conducting risk assessments, NIST, pp. 95, September 2012.

[2] Standards for security categorization of federal information and information systems, FIPS, vol. 199, pp. 13, February 2004.

[3] A. Singhal and X. Ou, "Security Risk Analysis of Enterprise Networks Using Probabilistic Attack Graphs", Computer, pp. 24, 2011.

[4] S. Harris and F. Maymi, ‘‘Cissp exam guide,’’ Tech. Rep., 2016, pp. 483–1083.

[5] J.Chokun. (2018). Who Accepts Bitcoins as Payment? List of Companies, Stores, Shops. [Online]. Available: https://99bitcoins.com/who-acceptsbitcoins-payment-companies-stores-take-bitcoins

[6] Newegg. Bitcoin Accepted. [Online]. Available: https://promotions. newegg.com/nepro/16-6277/index.html

[7] Kryptomoney. (2017). Subway Accepts Bitcoin as Payment. [Online]. Available: https://kryptomoney.com/subway-accepts-bitcoins-inpayment

[8] M. Lucas. (2017). The Difference Between Bitcoin and Blockchain for Business. https://www.ibm.com/blogs/blockchain/2017/05/thedifference-between-bitcoin-and-blockchain-for-business/

[9] M. Moniruzzamana, S. Khezra, A. Yassineb, and R. Benlamri, ‘‘Blockchain for smart homes: Review of current trends and research challenges,’’ Comput. Electr. Eng., vol. 83, May 2020, Art. no. 106585.

[10] R. Ullah, M. A. U. Rehman, M. A. Naeem, B.-S. Kim, and S. Mastorakis, ‘‘ICN with edge for 5G: Exploiting in-network caching in ICN-based edge computing for 5G networks,’’ Future Gener. Comput. Syst., vol. 111, pp. 159–174, Oct. 2020.

[11] M. Huang, A. Liu, N. N. Xiong, T. Wang, and A. V. Vasilakos, ‘‘An effective service-oriented networking management architecture for 5Genabled Internet of Things,’’ Comput. Netw., vol. 173, May 2020, Art. no. 107208

[12] N. Psaromanolakis, A. Ropodi, P. Fragkogiannis, K. Tsagkaris, L. A. Neto, A. El Ankouri, M. Wang, G. Simon, and P. Chanclou, ‘‘Software defined networking in a converged 5G fiber-wireless network,’’ in Proc. Eur. Conf. Netw. Commun. (EuCNC), Jun. 2020, pp. 225–230.

[13] R. Shafin, L. Liu, V. Chandrasekhar, H. Chen, J. Reed, and J. Zhang, ‘‘Artificial intelligence-enabled cellular networks: A critical path to beyond-5G and 6G,’’ IEEE Wireless Commun., vol. 27, no. 2, pp. 212–217, Apr. 2020.

[14] D. Dasgupta, J. M. Shrein, and K. D. Gupta, ‘‘A survey of blockchain from security perspective,’’ J. Banking Financial Technol., vol. 3, no. 1, pp. 1–17, Apr. 2019, doi: 10.1007/s42786-018-00002-6

[15] E. G. AbdAllah, H. S. Hassanein, and M. Zulkernine, ‘‘A survey of security attacks in information-centric networking,’’ IEEE Commun. Surveys Tuts., vol. 17, no. 3, pp. 1441–1454, 3rd Quart., 2015.

[16] E. Ngai, B. Ohlman, G. Tsudik, E. Uzun, M. Wählisch, and C. A. Wood, ‘‘Can we make a cake and eat it too? A discussion of ICN security and privacy,’’ ACM SIGCOMM Comput. Commun. Rev., vol. 47, no. 1, pp. 49–54, Jan. 2017.

[17] J. C. C. Chica, J. C. Imbachi, and J. F. B. Vega, ‘‘Security in SDN: A comprehensive survey,’’ J. Netw. Comput. Appl., vol. 159, Jun. 2020, Art. no. 102595.

[18] C. Benzaïd, M. Boukhalfa, and T. Taleb, ‘‘Robust self-protection against application-layer (D)DoS attacks in SDN environment,’’ in Proc. IEEE Wireless Commun. Netw. Conf. (WCNC), May 2020, pp. 1–6.

[19] D. Lowd and C. Meek, ‘‘Adversarial learning,’’ in Proc. 11th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining, 2005, pp. 641–647.

[20] R. Shokri, M. Stronati, C. Song, and V. Shmatikov, ‘‘Membership inference attacks against machine learning models,’’ in Proc. IEEE Symp. Secur. Privacy (SP), May 2017, pp. 3–18

[21] H. Eiza, Q. Ni, and Q. Shi, ‘‘Secure and privacy-aware cloud-assisted video reporting service in 5G-enabled vehicular networks,’’ IEEE Trans. Veh. Technol., vol. 65, no. 10, pp. 7868–7881, Mar. 2016.
[22] G. Vidan and V. Lehdonvirta, ‘‘Mine the gap: Bitcoin and the maintenance of trustlessness,’’ New Media Soc., vol. 21, no. 1, pp. 42–59, Jul. 2018, doi: 10.1177/1461444818786220.
[23] D. Dasgupta, J. M. Shrein, and K. D. Gupta, ‘‘A survey of blockchain from security perspective,’’ J. Banking Financial Technol., vol. 3, no. 1, pp. 1–17, Apr. 2019, doi: 10.1007/s42786-018-00002-6.
[24] K. Wang, Y. Zhang, S. Guo, M. Dong, R. Q. Hu, and L. He, ‘‘IEEE access special section editorial: The Internet of Energy: Architectures, cyber security, and applications,’’ IEEE Access, vol. 6, pp. 79272–79275, 2018.
[25] C. Benzaïd, M. Boukhalfa, and T. Taleb, ‘‘Robust self-protection against application-layer (D)DoS attacks in SDN environment,’’ in Proc. IEEE Wireless Commun. Netw. Conf. (WCNC), May 2020, pp. 1–6.
[26] C. Xu, L. Zhang, L. Zhu, C. Zhang, X. Du, M. Guizani, and K. Sharif, ‘‘Aggregate in my way: Privacy-preserving data aggregation without trusted authority in ICN,’’ Future Gener. Comput. Syst., vol. 111, pp. 107–116, Oct. 2020.
[27] D. J. Miller, Z. Xiang, and G. Kesidis, ‘‘Adversarial learning targeting deep neural network classification: A comprehensive review of defenses against attacks,’’ Proc. IEEE, vol. 108, no. 3, pp. 402–433, Mar. 2020.
[28] F. Behrouz and C. Sophia, ‘‘Data communications and networking,’’ Forouzan With Sophia Chung Fegan, 2007.
[29] T. Handel, G. Theodore, and T. Maxwell, ‘‘Hiding data in the OSI network model,’’ in Proc. Int. Workshop Inf. Hiding, 1996, pp. 23–28.
[30] Pew Research Center. Social Media Fact Sheet. [Online]. Available: https://www.pewresearch.org/internet/fact-sheet/social-media/
[31] S. Harris and F. Maymi, ‘‘Cissp exam guide,’’ Tech. Rep., 2016, pp. 483–1083.
[32] W. F. Emmons and A. S. Chandler, ‘‘OSI session layer: Services and protocols,’’ Proc. IEEE, vol. 71, no. 12, pp. 1397–1400, Dec. 1983.
[33] D. Basin, J. Dreier, L. Hirschi, S. Radomirovic, R. Sasse, and V. Stettler, ‘‘A formal analysis of 5G authentication,’’ in Proc. ACM SIGSAC Conf. Comput. Commun. Secur., Oct. 2018, pp. 1383–1396.
[34] S. Harris and F. Maymi, ‘‘Cissp exam guide,’’ Tech. Rep., 2016, pp. 483–1083.
[35] E. Schultz. (2000). The Windows NT Network Environment. [Online]. Available: http://www.informit.com/articles/article.aspx?p=130690&seqNum=11
[36] H. S. Lallie, L. A. Shepherd, J. R. C. Nurse, A. Erola, G. Epiphaniou, C. Maple, and X. Bellekens, ‘‘Cyber security in the age of COVID19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic,’’ Comput. Secur., vol. 105, Jun. 2021, Art. no. 102248.
[37] M. A. Abdrabou, A. D. E. Elbayoumy, and E. A. El-Wanis, ‘‘LTE authentication protocol (EPS-AKA) weaknesses solution,’’ in Proc. IEEE 7th Int. Conf. Intell. Comput. Inf. Syst. (ICICIS), Dec. 2015, pp. 434–441.
[38] D. Basin, J. Dreier, L. Hirschi, S. Radomirovic, R. Sasse, and V. Stettler, ‘‘A formal analysis of 5G authentication,’’ in Proc. ACM SIGSAC Conf. Comput. Commun. Secur., Oct. 2018, pp. 1383–1396.
[39] M. Knight. (2017). 5G+SDN: When Worlds Collide. [Online]. Available: https://about.att.com/innovationblog/when_worlds_collide
[40] Akhunzada, A. Gani, N. B. Anuar, A. Abdelaziz, M. K. Khan, A. Hayat, and S. Khan, ‘‘Secure and dependable software defined networks,’’ J. Netw. Comput. Appl., vol. 61, pp. 199–221, Feb. 2016.
[41] J. Yao, Z. Han, M. Sohail, and L. Wang, ‘‘A robust security architecture for SDN-based 5G networks,’’ Future Internet, vol. 11, no. 4, p. 85, Mar. 2019
[42] J. Zhang, L. Yang, W. Cao, and Q. Wang, ‘‘Formal analysis of 5G EAP-TLS authentication protocol using proverif,’’ IEEE Access, vol. 8, pp. 23674–23688, 2020

[43] M. Liyanage, I. Ahmed, M. Ylianttila, J. L. Santos, R. Kantola, O. L. Perez, M. U. Itzazelaia, E. M. De Oca, A. Valtierra, and C. Jimenez, ‘‘Security for future software defined mobile networks,’’ in Proc. 9th Int. Conf. Next Gener. Mobile Appl., Services Technol., Sep. 2015, pp. 256–264.
[44] K. Saleem, G. M. Alabduljabbar, N. Alrowais, J. Al-Muhtadi, M. Imran, and J. J. P. C. Rodrigues, ‘‘Bio-inspired network security for 5G-enabled IoT applications,’’ IEEE Access, vol. 8, pp. 229152–229160, 2020.
[45] X. Zhang, A. Kunz, and S. Schröder, ‘‘Overview of 5G security in 3GPP,’’ in Proc. IEEE Conf. Standards Commun. Netw. (CSCN), Sep. 2017, pp. 181–186.
[46] E. Mannes and C. Maziero, ‘‘Naming content on the network layer: A security analysis of the information-centric network model,’’ ACM Comput. Surveys, vol. 52, no. 3, pp. 1–28, Jul. 2019.
[47] M. Wählisch, T. C. Schmidt, and M. Vahlenkamp, ‘‘Lessons from the past: Why data-driven states harm future information-centric networking,’’ in Proc. IFIP Netw. Conf., 2013, pp. 1–9
[48] M. Jinsong and M. Yamin, ‘‘5G network and security,’’ in Proc. 7th Int. Conf. Comput. Sustain. Global Develop. (INDIACom), 2020, pp. 249–254
[49] J. Li, Z. Zhao, and R. Li, ‘‘Machine learning-based IDS for softwaredefined 5G network,’’ IET Netw., vol. 7, no. 2, pp. 53–60, Mar. 2017.
[50] J. Burke, P. Gasti, N. Nathan, and G. Tsudik, ‘‘Secure sensing over named data networking,’’ in Proc. IEEE 13th Int. Symp. Netw. Comput. Appl., Aug. 2014, pp. 175–180.
[51] M. Conti, P. Gasti, and M. Teoli, ‘‘A lightweight mechanism for detection of cache pollution attacks in named data networking,’’ Elsevier Comput. Netw., vol. 57, no. 16, pp. 3178–3191, 2013
[52] C. Kolias, G. Kambourakis, A. Stavrou, and S. Gritzalis, ‘‘Intrusion detection in 802.11 networks: Empirical evaluation of threats and a public dataset,’’ IEEE Commun. Surveys Tuts., vol. 18, no. 1, pp. 184–208, 1st. Quart., 2016.
[53] 5G Americas. (2020). Security Considerations for the 5G Era. A 5G Americas White Paper. https://www.5gamericas.orgwpcontentuploads202007Security-Considerations-for-the-5G-Era-2020-WP-Lossless.pdf
[54] M. Faisal, S. Abbas, and H. U. Rahman, ‘‘Identity attack detection system for 802.11-based ad hoc networks,’’ EURASIP J. Wireless Commun. Netw., vol. 2018, no. 1, p. 128, Dec. 2018.
[55] G. Li, Z. Yan, and Y. Fu, ‘‘A study and simulation research of blackhole attack on mobile AdHoc network,’’ in Proc. IEEE Conf. Commun. Netw. Secur. (CNS), May 2018, pp. 1–6.
[56] L. C. Sejaphala and M. Velempini, ‘‘The design of a defense mechanism to mitigate sinkhole attack in software defined wireless sensor cognitive radio networks,’’ Wireless Pers. Commun., vol. 113, no. 2, pp. 977–993, Jul. 2020.
[57] Z. A. Zardari, J. He, N. Zhu, K. Mohammadani, M. Pathan, M. Hussain, and M. Memon, ‘‘A dual attack detection technique to identify black and gray hole attacks using an intrusion detection system and a connected dominating set in MANETs,’’ Future Internet, vol. 11, no. 3, p. 61, Mar. 2019.
[58] D. Jin, Y. Lu, J. Qin, Z. Cheng, and Z. Mao, ‘‘SwiftIDS: Real-time intrusion detection system based on LightGBM and parallel intrusion detection mechanism,’’ Comput. Secur., vol. 97, Oct. 2020, Art. no. 101984
[59] M. Lin, B. Zhao, and Q. Xin, ‘‘ERID: A deep learning-based approach towards efficient real-time intrusion detection for IoT,’’ in Proc. IEEE 8th Int. Conf. Commun. Netw. (ComNet), Oct. 2020, pp. 1–7.
[60] Z. A. Zardari, J. He, N. Zhu, K. Mohammadani, M. Pathan, M. Hussain, and M. Memon, ‘‘A dual attack detection technique to identify black and gray hole attacks using an intrusion detection system and a connected dominating set in MANETs,’’ Future Internet, vol. 11, no. 3, p. 61, Mar. 2019.
[61] N. Yang, L. Wang, G. Geraci, M. Elkashlan, J. Yuan, and M. D. Renzo, ‘‘Safeguarding 5G wireless communication networks using physical layer security,’’ IEEE Commun. Mag., vol. 53, no. 4, pp. 20–27, Apr. 2015.

[62] M. Riggins. (2017). Mobile Device Security: Defend Your Ports! [Online]. Available: https://inspiredelearning.com/blog/open-ports/
[63] Z. Lv, A. K. Singh, and J. Li, ‘‘Deep learning for security problems in 5G heterogeneous networks,’’ IEEE Netw., vol. 35, no. 2, pp. 67–73, Mar. 2021.
[64] L. Sun, K. Tourki, Y. Hou, and L. Wei, ‘‘Safeguarding 5G networks through physical layer security technologies,’’ Wireless Commun. Mobile Comput., vol. 2018, pp. 1–2, Sep. 2018.
[65] Y. Xu, J. Liu, Y. Shen, X. Jiang, Y. Ji, and N. Shiratori, ‘‘QoS-aware secure routing design for wireless networks with selfish jammers,’’ IEEE Trans. Wireless Commun., vol. 20, no. 8, pp. 4902–4916, Aug. 2021
[66] Z. Zhou, X. Chen, Y. Zhang, and S. Mumtaz, ‘‘Blockchain-empowered secure spectrum sharing for 5G heterogeneous networks,’’ IEEE Netw., vol. 34, no. 1, pp. 24–31, Jan. 2020.