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

Practical Autonomous Cyberhealth for resilient SMEs & Microenterprises

Grant Agreement No. 883335
Research Innovation Action (RIA)

Deliverable 2.1. Requirements & High-Level Design – Interim

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

Related WP	WP2	**Document Reference**	1.0
Related Deliverable(s)	D2.2	**Dissemination Level (*)**	PU
Lead Participant	HPELB	**Lead Author**	Ludovic Jacquin (HPELB)
Contributors	PALANTIR consortium	**Reviewers**	Akis Kourtis (ORION) Arton Lipaj (SFERA)

Document Information

List of Contributors	
Name	Partner
George Athanasiou, Maria Samara	DBC
Ludovic Jacquin	HPELB
Carolina Fernández, Maxime Compastié	i2CAT
Vangelis Logothetis, Ioannis Neokosmidis, Theodoros Rokkas	INCITES
Dimitris Papadopoulos, Evangelos Mantas, Antonis Litke	INFILI
Andreas Oikonomakis, Dimitris Santorinaios	NCSRD
Davide Sanvito	NEC
Akis Kourtis, Georgios Xylouris	ORION
Izidor Mlakar, Arton Lipaj	SFERA
Angeliki Kapodistria, Athanasios Priovolos, Georgios Gardikis	SPH
Antonio Pastor, Diego López	TID
Stelios Tsarsitalidis, Dimitris Klonidis	UBITECH
Gregorio Martínez Pérez, Antonio López Martínez, Manuel Gil Pérez, Félix Gómez Mármol	UMU

Document History			
Version	Date	Change editors	Changes
0.8	19/02/21	HPELB	Draft for internal review.
0.9	24/02/21	HPELB	Draft for internal quality review.
1.0	25/02/21	HPELB	Initial version of the document

Quality Control		
Role	Who (Partner short name)	Approval Date
Deliverable leader	HPELB	25/02/21
Quality manager	INF	25/02/21
Project Coordinator	DBC	26/02/21

Executive Summary

This document presents the requirements for the PALANTIR solution and the high-level architecture designed by the consortium to meet those requirements. This is the initial version of the document and an updated version is scheduled for month 20 (April 2022), which takes into account the feedback from the first cycle of development and evolution of the PALANTIR market.

PALANTIR offers a cybersecurity solution tailored for Small and Medium Enterprises and Micro Enterprises, based on the Security-as-a-Service business model. PALANTIR builds on three sets of innovative technologies:

- **Network Function Virtualisation, Security Capabilities Orchestration and Remote Attestation** to create a flexible, low cost and trustworthy Security-as-a-Service offering.
- **Distributed collection, Machine Learning and Policy-based remediation** to create advanced threat intelligence with a live threat sharing capability.
- **Multi-attribute risk assessment, cost/benefit forecasts and Security Capabilities** to link risk assessment with the cybersecurity offering.

The requirements are elicited from the PALANTIR target market using four methods:

- An **online End-user Questionnaire**, which is partially using the Analytic Hierarchy Process and focuses mainly on business prioritization. The End-user Questionnaire was answered by 31 external end users who may be interested in using PALANTIR.
- An **online Technical Questionnaire**, which targets Subject Matter Experts and focuses mostly on technologies. The Technical Questionnaire was answered by 27 Subject Matter Experts, from within and outside the consortium.
- An **internal requirement analysis** that leverages the broad scope of technical expertise inside the consortium to define the requirements required to successfully demonstrate the PALANTIR use case demonstrations.
- An **analysis of the different laws and regulations** that are currently in place and applies to PALANTIR.

From those methods, 61 functional and 28 non-functional requirements are defined. It should be noted that the analysis of the PALANTIR Use Cases is included in D2.2 instead of this document. Nevertheless, the requirements stemming from this analysis are included in this document.

Considering the requirements defined for the initial phase of PALANTIR, the architecture designed by the consortium is described. This architecture defines more precisely the main components of the PALANTIR technical solution:

- The **Security Capabilities Hosting Infrastructure** is the infrastructure (both the physical platform and the required operating environment) that processes the PALANTIR user' (i.e. the SMEs) network traffic and enforces the Security-as-a-Service solution purchased by the users.
- The **Security Capability Orchestration** is responsible for managing the Security Capabilities used by the Security-as-a-Service offering, by deploying and orchestrating capabilities on the hosting infrastructure as required.
- The **Trust, Attestation and Recovery** monitors the hosting infrastructure to ensure that the physical platform and Security Capabilities are trusted (i.e. operating as it is meant to), to detect faults and breaches and to recover from any anomalous event.
- The **Threat Intelligence** complements the Security Capabilities by providing PALANTIR with advanced analytics based on Machine Learning and Deep Learning. The Threat Intelligence leverages data collected within the hosting infrastructure and from the other components. A Remediation and Recommendation engine is provided to facilitate an automated remediation of the detected threats.
- The **Risk Analysis Framework** equips PALANTIR with the ability to customers, the security risk associated with their information communication and technology systems.

- The **PALANTIR Portal** is the single pane of glass for PALANTIR operators and users, presenting the different dashboards and enabling threat sharing between PALANTIR users.

The interactions between components are described, while the interfaces are specified in subsequent deliverables from the other work packages.

Table of Contents

List of Tables

List of Figures

List of Acronyms

Abbreviation / acronym	Description
AHP	Analytic Hierarchy Process
APT	Advanced Persistent Threat
AI	Artificial Intelligence
CAPEX	Capital expenditures
CERT	Computer Emergency Response Team
CI	Consistency Index
CPE	Customer Premises Equipment
CR	Consistency Ratio
CSIRT	Computer Incident Response Team
DL	Deep Learning
DSS	Decision Support Systems
D*x*.*y*	Deliverable number *y*, belonging to WP number *x*
EC	European Commission
EMS	Element Management System
GDPR	General Data Protection Regulation
HSPL	High-level Security Policy Language
ICT	Information and Communication Technologies
IDPS	Intrusion Detection and Prevention System
IoC	Indicator of Compromise
IR	Incidence Response
ISF	NFVI-based Security Functions
IT	Information Technology
KPI	Key Performance Indicator
MANO	Management and orchestration (NFV)
ME	Micro Enterprise
MISP	Malware Information Sharing Platform
MitM	Man-in-the-middle
ML	Machine Learning
MSPL	Medium-level Security Policy Language
NFV	Network Function Virtualisation
NFVI	Network Function Virtualised Infrastructure
NIST	National Institute of Standards and Technology
OPEX	Operating expenditures
PSF	Physical Security Function
PNF	Physical Network Function
RAF	Risk Analysis Framework (component)
RoT	Root of Trust
SCC	Security Capabilities Catalogue (subcomponent)
SCHI	Security Capabilities Hosting Infrastructure (component)
SCO	Security Capabilities Orchestration (component)

Abbreviation / acronym	Description
SDN	Software-Defined Networking
SecaaS	Security-as-a-Service
SEM	Security Element Manager
SME	Small and Medium Enterprise
SO	Security Orchestrator
SOC	Security Operations Center
SIEM	Security Information and Event Management
STIX	Structured Threat Information Expression
TAR	Trust, Attestation and Recovery (component)
TAXII	Trusted Automated Exchange of Intelligence Information
TCG	Trusted Computing Group
TPM	Trusted Platform Module
TI	Threat Intelligence (component)
T*x*.*y*	Task number *y*, belonging to WP number *x*
UI	User Interface
VIM	Virtual Infrastructure Manager
VM	Virtual Machine
VNF	Virtual Network Function
WAN	Wide Area Network
WAN-Edge SIEM	WAN-Edge based Security Information and Event Management
WLAN	Wireless Local Area Network
WP	Work Package

Introduction

Objectives and goal of the deliverable

PALANTIR creates a technical framework enabling the provision of next-generation, cost-effective Security-as-a-Service (SecaaS) services for Small and Medium Enterprises (SMEs) and Micro-Enterprises (MEs), by leveraging and improving novel technologies such as:

- **Network Function Virtualisation, Security Capability Orchestration and Remote Attestation**, to create a low-cost SecaaS offering: three delivery modes are foreseen for PALANTIR. Cloud SecaaS follows in the model of hosted Managed Security Services, Lightweight SecaaS is deployed in a standalone device at the premises of the client, following the model of Customer Premises Equipment (CPE), and Edge SecaaS is hosted at the network edge following the paradigm of Multi-Access Edge Computing. The variety of delivery modes provides a variety of options to the SecaaS clients.
- **Distributed collection, Machine Learning and Policy-based remediation** to create improved threat intelligence with live threat sharing: anonymised threat data and high-level remediation policies can propagate through SecaaS clients. High-level policies can be translated locally to actionable security rules for each client, providing near-instantaneous protection from a newly discovered threat.
- **Multi-attribute risk assessment, cost/benefit forecasts and a novel Security Capability Catalogue** to link risk assessment with the service market and ensure that clients are matched with appropriate solutions within their budget and tailor-made to their needs. The Service Catalogue democratizes access to multiple service developers.

The current document is the deliverable 'D2.1. Requirements & high-level design – Interim version' which comprises the first major outcome of the task 'T2.1 Requirements elicitation and architecture design'. Task T2.1 is in charge of collecting, identifying and analysing the requirements of the different stakeholders of PALANTIR (end users, infrastructure providers, security capability developers, cyber-security agencies, etc.). As such, this deliverable contains an extensive elicitation of user and technical requirements. This task is also in charge of designing the high-level architecture of PALANTIR and defining the interactions between the main components at a macro level. The outputs of this task are a list of requirements for both, the PALANTIR platform functionalities and operation. The architecture is presented through block diagrams to drive the more detailed specification of each component.

The primary audience of this document consists of the members of the consortium that participate in the design and development of the components and modules of the PALANTIR system. Additionally, the document is of wider interest to stakeholders that are active in the domains of cybersecurity, Big Data analysis, Artificial Intelligence deployed for security purposes and Risk Assessment, including researchers participating and contributing to H2020 projects under the aforementioned topics.

This deliverable is a live document following an iterative approach and thus it is going to have a final version on month 20, which includes the updated requirements, captured by the different user groups engaged during the pilots and the updated and final architecture.

Relation to other Work Packages and Tasks

Within Work Package (WP2), this specific deliverable and task (T2.1) is strongly related with the other tasks, namely T2.2 Legal and Business compliance, T2.3 Use case analysis and T2.4 Threat and Attack surface analysis in the sense that together they fulfil the dominant role of defining the PALANTIR project, its scope analysis and overall specification. Moreover, the requirements elicited and analysed in this deliverable, along with the PALANTIR architecture, drive the development work that takes place under the following Work Packages:

- **WP3 Secure Service Ecosystem for SMEs and MEs**, which aims at delivering the virtualised security services, as well as the framework for their management and orchestration and automated response.
- **WP4 Threat Management and Sharing**, which aims at implementing the catalogue of the security services, accompanied by the appropriate hardware and software integrity attestation and performance verification tools, as well as the Dashboard for the overall management of the PALANTIR framework.
- **WP5 Hybrid Threat Intelligence**, which aims at delivering the analytics framework for distributed network traffic collection, anomaly detection, threat classification and recommendation.

The outcomes of this deliverable are mainly used as input to the technical deliverables of WP3-4-5, as well as the overall integration plans of WP6.

1. PALANTIR Requirements

This document contains the initial set of requirements for PALANTIR. The consortium elected to focus on high-level requirements during the initial phase of the project. These high-level requirements are then refined within the implementation work packages (WP3, WP4, WP5 and WP6) into more detailed requirements that are relevant to the implementation of each WP. The detailed requirements may be included in the updated version of this document: "D2.3 Requirements & high-level design – Final", if they impact the overall PALANTIR design. WP2 is overseeing the other WPs, particularly throughout the refinement phase, to ensure that the detailed requirements are aligned.

1.1. Requirement elicitation methodology

PALANTIR offers Security-as-a-Service in a variety of delivery modes (cloud/light/edge) allowing clients not only to select the level of protection that best fits their needs but also the level of information they would like to communicate to and receive from other PALANTIR users. To this end, it leverages (i) a Risk analysis framework that allows the quantification of security/privacy threats based on security/privacy impact assessment and its correlation with attack surface analysis; (ii) Network Function Virtualisation (NFV) and Software-Defined Networking (SDN) for virtualization and dynamic placement of security appliances in the network; (iii) a hybrid Threat Intelligence framework for real-time incident detection and mitigation, and (iv) a Trust and Attestation framework for securing both infrastructure and services. Three high-level use cases are identified as the most relevant for PALANTIR and are described in detail in D2.2:

- *Use case #1*: Securing private medical practices with lightweight SecaaS for the protection of medical data, illustrating relevant cases of incident detection and mitigation activities to safeguard patient data and prevent medical identity theft.
- *Use Case #2*: Uninterrupted Electronic Commerce with Cloud SecaaS assessing the effectiveness of the PALANTIR framework around secure electronic commerce, with the example of a typical retail and service-oriented microenterprise that uses PALANTIR to combat the attacks, attest the integrity of the infrastructure and exploit the threat sharing capabilities of the platform.
- *Use Case #3*: Live Threat Intelligence Sharing in a large-scale Edge scenario that demonstrates the PALANTIR SecaaS-protected network on a realistic, large-scale scenario, in which it is tasked with jointly analysing data from multiple vendors (i.e. SMEs & MEs) and with leveraging cyber threat intelligence information to and from national and international knowledge sharing infrastructures (e.g. Malware Information Sharing Platform – MISP - instances) to deploy tailored cybersecurity measures.

In the context of D2.1, the high-level requirements that drives the design task were identified. For the elicitation of the requirements, two sources were used:

- **External Requirements:** they are gathered through two online surveys, aimed at prioritizing the use cases and collecting additional requirements from technical experts and end users.
- **Internal Requirements:** they are implied by the technology elements, use cases and user stories, as selected by the PALANTIR consortium and expressing the desired functionalities and interactions with users.

The overall requirements analysis and consolidation is based on the well-established process of dividing the requirements into two categories: functional and non-functional. The functional aspect of the requirements analysis focuses on what a system must do to produce the required operational behaviour. This includes inputs, outputs, states, functions and transformation rules. Functional requirements are the primary source of the requirements that is eventually reflected in the system specification. These have been further grouped accordingly into various groups, based on their origin. A non-functional requirements analysis focuses on what other technical features a system must have in place in order to facilitate the service provision, therefore the listed non-functional requirements have been also organized in a number of thematic categories.

1.1.1. End-user Questionnaire

For the End-user Questionnaire, a subset of questions leverages the Analytic Hierarchy Process (AHP).

1.1.1.1. Decision making using the AHP framework

AHP was proposed and developed by Thomas Saaty [1] in the early 1970s mainly for military purposes. The AHP is actually a multi-criteria decision-making approach. In the past, AHP was extensively used covering several application areas such as education [2], engineering [3], industry [4], manufacturing [5] and resource allocation [6] . Recently, AHP was widely used for selecting and ranking alternatives in the field of Information and Communication Technologies (ICT) [7]–[10].

Analytic Hierarchy Process is a structured technique for dealing with complex decisions. It describes a rational and comprehensive framework for decomposing an unstructured complex problem into a multi-level hierarchy of interrelated criteria, sub-criteria and decision alternatives. By incorporating judgments on qualitative and quantitative criteria, AHP manages to quantify decision makers' preferences. The priorities of criteria, sub-criteria and alternatives are finally reached by combining these judgments.

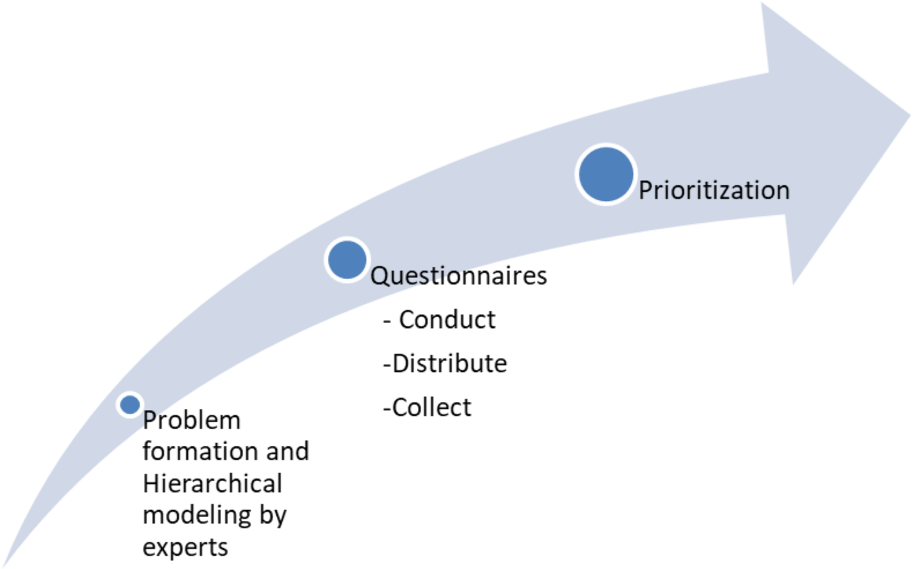


Figure 1: Analytic Hierarchy Process steps

Figure 1 illustrates the required steps of AHP. In the first step, the problem that is investigated is formed while criteria and sub-criteria contributing to objective’s satisfaction are determined through interviews and/or group discussions with experts. The multi-level hierarchy is then constructed (Figure 2) consisting of three levels. In the first level, the objective under investigation is shown. In this work, the factors affecting the adoption and evolution of PALANTIR and its proposed solution in general is examined. In the next level, the criteria, Cr_k with k=1,2,…,N and N the total number of criteria, participating in the decision-making process are determined. Criteria should be general enough, incorporating several features resulting in a rough description of the objective. In the lower level, criteria are further analysed into their sub-criteria SCr_{jk}, where j=1,2,…,M_k and M_k is the number of sub-criteria under criterion k. Sub-criteria represent a specific feature characterizing a criterion. Identification of criteria and sub-criteria is accomplished based on the focus of their preferential independence.

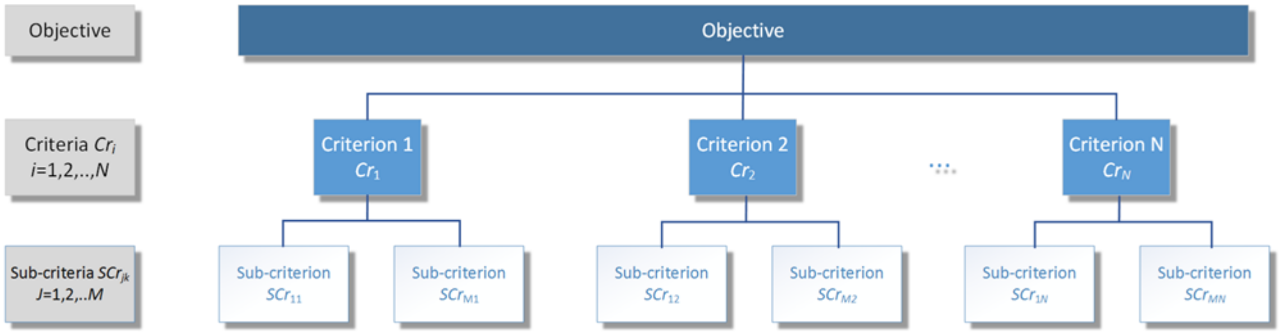


Figure 2: Multi-level hierarchy of interrelated criteria and sub-criteria

Once the hierarchical structure is constructed and criteria and sub-criteria are determined, appropriate questionnaires are conducted and distributed to experts (step 2). This procedure is based on pairwise judgments of experts from the second to the lowest level of the hierarchy. In each level, the criteria (sub-criteria) are compared pair wise according to their degree of influence and based on the specified criteria in the higher level. The described comparisons are performed using the standardized nine levels scale shown in Table 1.

Table 1: The Saaty Rating Scale

Intensity of importance	Definition	Explanation
1	Equal importance	The two criteria contribute equally
3	Moderate importance	Experience and judgment favour one criteria
5	Strong importance	A criterion is strongly favoured
7	Very strong importance	A criterion is very strong dominant
9	Extreme importance	A criterion is favoured by at least an order of magnitude
2, 4, 6, 8	Intermediate values	Used to compromise between two of the above numbers

The set of pairwise comparisons on the N criteria results in an N x N evaluation matrix $A=[A_{ij}]$ in which the elements A_{ij} (>0) represent the relative importance of criterion Cr_i compared to Cr_j. It should be noted that $A_{ii}=1$ for every i while matrix A is symmetrical across the main diagonal that is $A_{ji}=1/A_{ij}$. The same steps are followed regarding sub-criteria of each criterion k and the results are summarized in a similar to A matrix called A_k.

The last step (step 3) towards the evaluation of the objectives is the estimation of criteria and sub-criteria weights, w_k and s_{jk} respectively. This requires the calculation of the principal eigenvector $\mathbf{v}=[v_k]$ (or $\boldsymbol{u_k}=[u_{ik}]$) that is the eigenvector corresponding to the maximum eigenvalue $\lambda_{\max}$ (principal eigenvalue) of matrix $\mathbf{A}$ (or $\boldsymbol{A_k}$). The weights of criterion k and of its sub-criterion j are given by:

$$w_k = \frac{v_k}{\sum_{i=1}^{N} v_i} \tag{1}$$

$$s_{jk} = \frac{u_{jk}}{\sum_{i=1}^{M_k} u_{ik}} \tag{2}$$

where N and M_k is the number of criteria and sub-criteria of criterion k respectively.

Consistency of pairwise comparison matrices

In order to maintain a certain quality level of a decision, the consistency of the data should also be investigated during the analysis. It should be noted that the rank of matrix A (or A_k) equals to 1 and $\lambda_{\max}=N$ (or M_k) if the pairwise comparisons are completely consistent. In this case, weights can be estimated by normalizing any of the columns or rows of A (A_k). A consistency index (CI) was introduced by Saaty in 1977:

$$CI = \frac{\lambda_{\max} - N}{N - 1} \tag{3}$$

where $\lambda_{\max}$ is the largest (maximum) eigenvalue and N is the number of criteria. The final consistency ratio (CR), showing how consistent the judgments have been relative to large samples of purely random judgments, is given by:

$$CR = \frac{CI}{RI} \tag{4}$$

where RI is the random index calculated as the average CI across a large number of randomly filled matrices using the scale described earlier in this section. The random indices for several values of N were calculated by Saaty (2003) and are given in Table 2. The consistency ratio should be less than 0.1. A CR larger than the tolerable level of 0.1 demonstrates the need to exclude the pairwise comparison matrix of this respondent for further analysis so as not affecting the overall accuracy of the results.

Table 2: RI values for different values of *n*

n	1	2	3	4	5	6	7	8	9
RI	0	0	0.58	0.90	1.12	1.24	1.32	1.41	1.45

1.1.1.2. Determining the set of criteria and factors to be used in the surveys

In order to identify the factors that influence the adoption of PALANTIR, a survey was designed in WP2 in line with the AHP methodology.

For this purpose, the following set of criteria covering a wide range of factors were initially defined:

- Business aspects: Factors related to product adoption and economic aspects
- Delivery models, services: Covering ways that services are delivered to end-users
- Cybersecurity services: Related to services offered to end-users
- Novel features: Novel features part of PALANTIR's proposal
- GDPR compliance: GDPR related topics

Each of these criteria was further broken down into sub-criteria that are usually indicative attributes that can be quantified and are closely related to the criteria.

For the **Business aspects** criterion, five sub-criteria have been identified:

- **Cost for training and cybersecurity solutions:** cost associated to training and the use of cybersecurity solutions
- **Clearly defined acceptable use of networks & systems:** knowledge of how resources are utilised to maintain cyber hygiene
- **Skills and regular training of personnel:** the ability to enhance workforce skill and regularly train personnel
- **Regular review of guidelines and measures:** being well informed on best practises related to cybersecurity
- **Incident response plan:** having the ability to counteract cyber attacks

For the **Delivery models, services** criterion, three sub-criteria have been identified:

- **Cloud-hosted cybersecurity services:** services offered through the cloud

- **Customer Premises Equipment Security-as-a-Service (CPE SaaS):** services provided through the use of customer premises equipment
- **WAN-Edge based Security Information and Event Management (WAN-Edge SIEM):** services offered using WAN-edge architecture

For the **Cybersecurity services** criterion, five sub-criteria have been identified:

- **Malware/APT protection:** protection against malware and advanced persistent threats
- **Traffic filtering/Firewall:** filtering and monitoring of incoming and outgoing traffic
- **WLAN encryption:** securing a wireless network from unauthorized access
- **Data breach monitoring:** traffic monitoring for suspicious activity
- **Deep packet inspection:** inspection of IP packets to prevent attacks

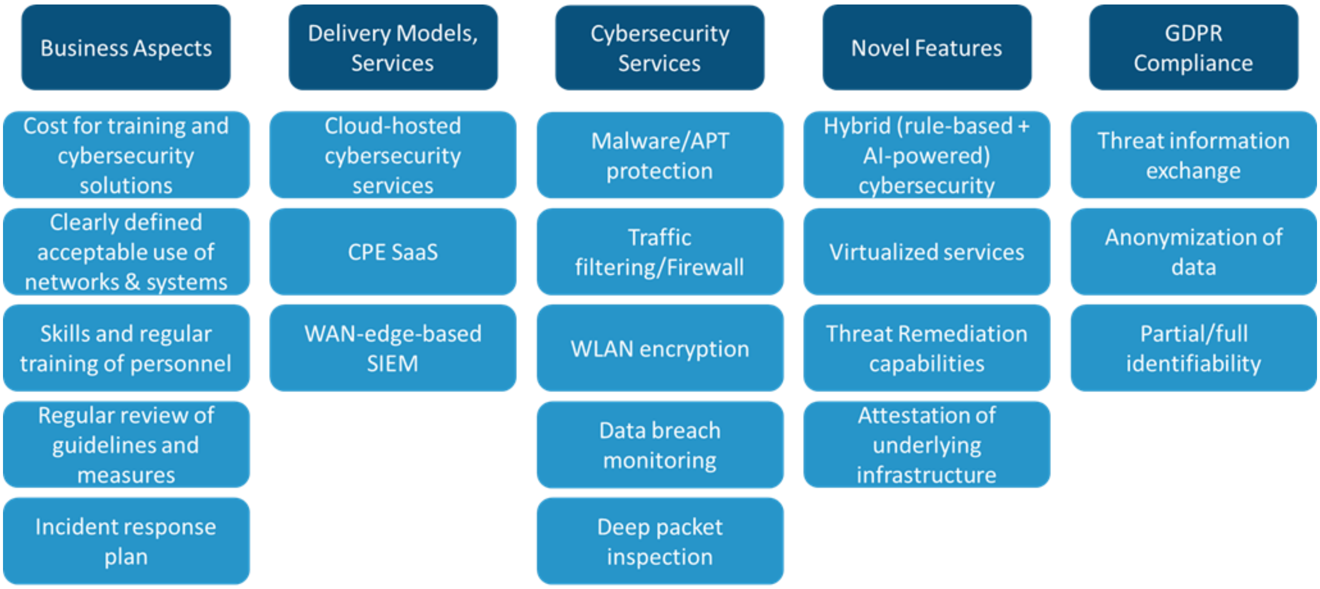
For the **Novel features** criterion, four sub-criteria haves been identified:

- **Hybrid (rule-based + AI-powered) cybersecurity:** hybrid utilisation of rule-based and machine learning
- **Virtualized services:** software enabled cybersecurity services
- **Threat Remediation capabilities:** identification and resolution of threats
- **Attestation of underlying infrastructure:** authentication of hardware and software configuration

For the **GDPR compliance** criterion, three sub-criteria have been identified:

- **Threat information exchange:** sharing of information to establish a more resilient cyber protection ecosystem
- **Anonymization of data:** the de-identification of personally identifiable information
- **Partial/full identifiability:** compliance to partial or full identifiability

The full list of the criteria and the corresponding sub-criteria is illustrated at the following figure.



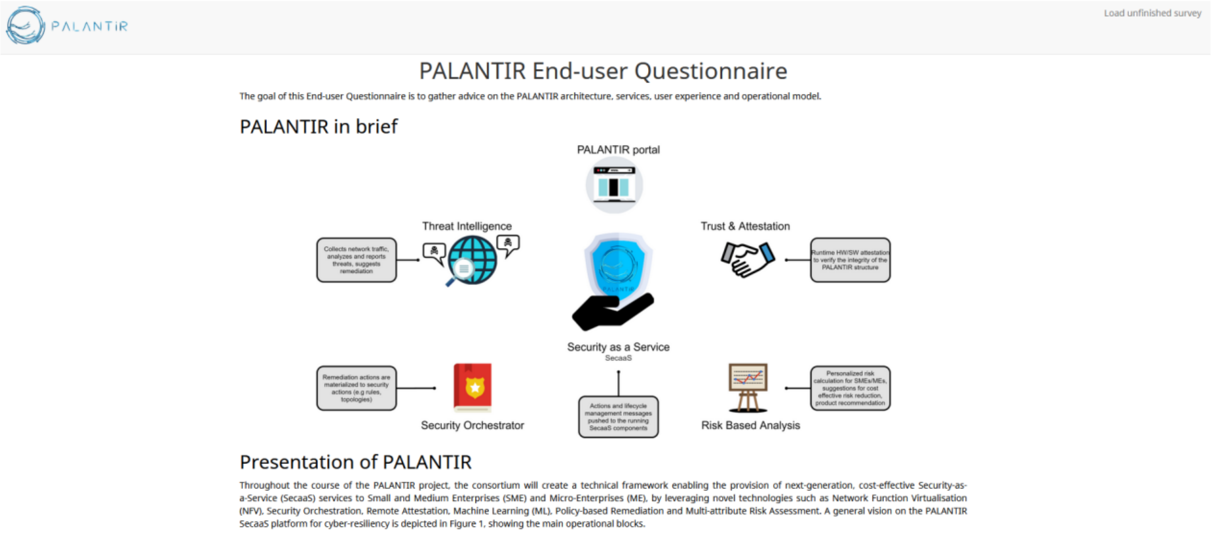
Business Aspects	Delivery Models, Services	Cybersecurity Services	Novel Features	GDPR Compliance
Cost for training and cybersecurity solutions	Cloud-hosted cybersecurity services	Malware/APT protection	Hybrid (rule-based + AI-powered) cybersecurity	Threat information exchange
Clearly defined acceptable use of networks & systems	CPE SaaS	Traffic filtering/Firewall	Virtualized services	Anonymization of data
Skills and regular training of personnel	WAN-edge-based SIEM	WLAN encryption	Threat Remediation capabilities	Partial/full identifiability
Regular review of guidelines and measures		Data breach monitoring	Attestation of underlying infrastructure	
Incident response plan		Deep packet inspection		

Figure 3: Factors affecting PALANTIR adoption and evolution

1.1.1.3. Survey Description

The survey was implemented in the form of an online set of questions created using LimeSurvey (https://www.limesurvey.org/), an open-source tool for web surveys, and hosted at: https://www.incites.eu/pollsurvey/index.php/647187

An introductory page provides information on the project and the AHP methodology as portrayed indicatively in the following figures.



PALANTIR End-user Questionnaire

The goal of this End-user Questionnaire is to gather advice on the PALANTIR architecture, services, user experience and operational model.

PALANTIR in brief

PALANTIR portal

Threat Intelligence

Collects network traffic, analyzes and reports threats, suggests remediation

Trust & Attestation

Runtime HW/SW attestation to verify the integrity of the PALANTIR structure

Security as a Service
SecaaS

Actions and lifecycle management messages pushed to the running SecaaS components

Remediation actions are materialized to security actions (e.g rules, topologies)

Security Orchestrator

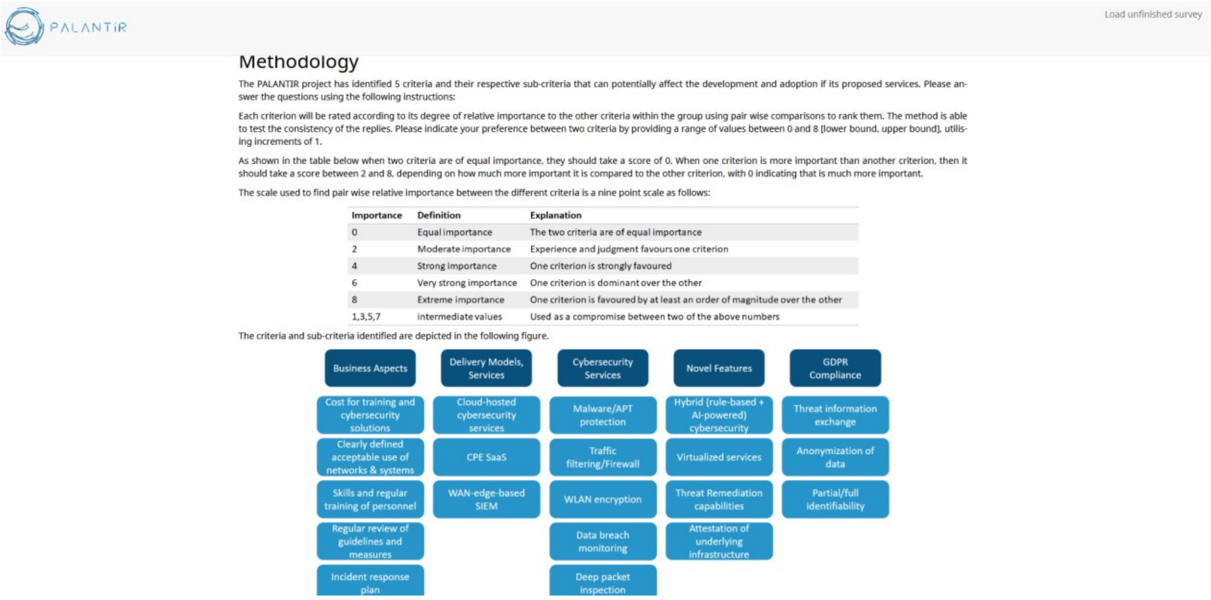
Personalized risk calculation for SMEs/MEs, suggestions for cost effective risk reduction, product recommendation

Risk Based Analysis

Presentation of PALANTIR

Throughout the course of the PALANTIR project, the consortium will create a technical framework enabling the provision of next-generation, cost-effective Security-as-a-Service (SecaaS) services to Small and Medium Enterprises (SME) and Micro-Enterprises (ME), by leveraging novel technologies such as Network Function Virtualisation (NFV), Security Orchestration, Remote Attestation, Machine Learning (ML), Policy-based Remediation and Multi-attribute Risk Assessment. A general vision on the PALANTIR SecaaS platform for cyber-resiliency is depicted in Figure 1, showing the main operational blocks.

Figure 4: End-user survey introductory page



Methodology

The PALANTIR project has identified 5 criteria and their respective sub-criteria that can potentially affect the development and adoption if its proposed services. Please answer the questions using the following instructions:

Each criterion will be rated according to its degree of relative importance to the other criteria within the group using pair wise comparisons to rank them. The method is able to test the consistency of the replies. Please indicate your preference between two criteria by providing a range of values between 0 and 8 [lower bound, upper bound], utilising increments of 1.

As shown in the table below when two criteria are of equal importance, they should take a score of 0. When one criterion is more important than another criterion, then it should take a score between 2 and 8, depending on how much more important it is compared to the other criterion, with 0 indicating that is much more important.

The scale used to find pair wise relative importance between the different criteria is a nine point scale as follows:

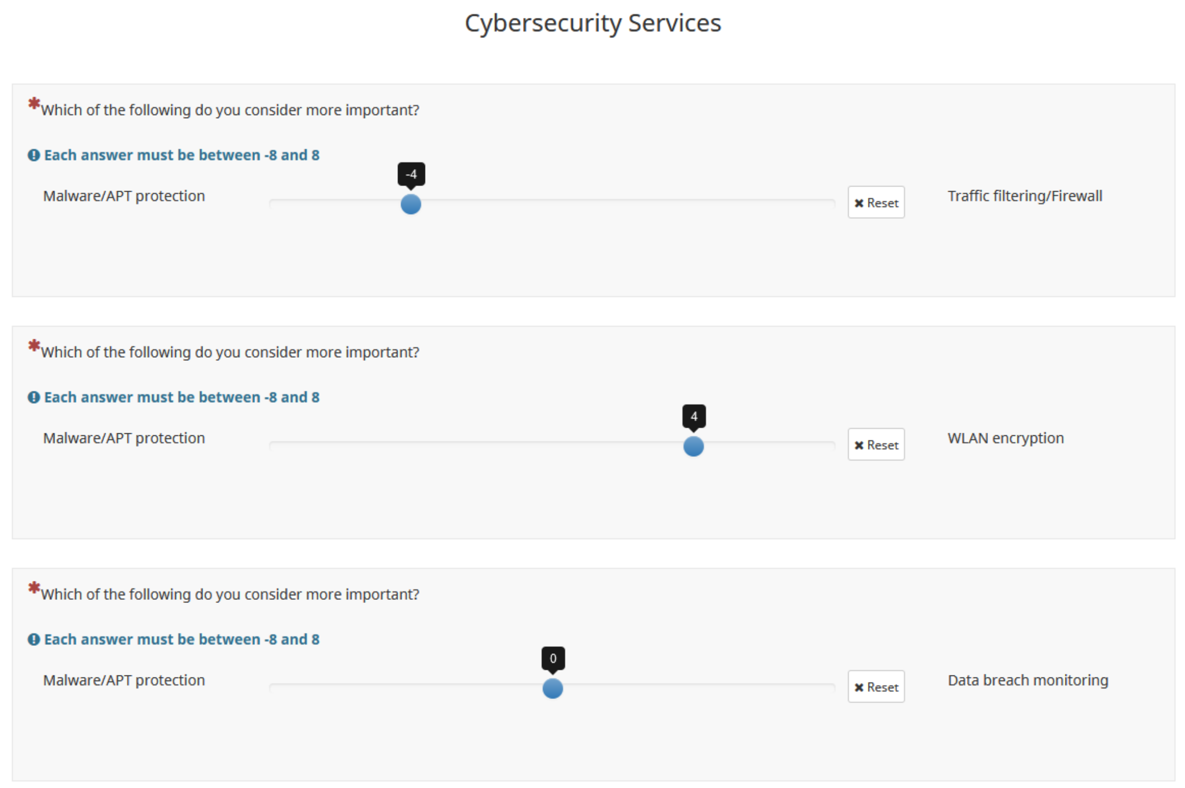
Importance	Definition	Explanation
0	Equal importance	The two criteria are of equal importance
2	Moderate importance	Experience and judgment favours one criterion
4	Strong importance	One criterion is strongly favoured
6	Very strong importance	One criterion is dominant over the other
8	Extreme importance	One criterion is favoured by at least an order of magnitude over the other
1,3,5,7	intermediate values	Used as a compromise between two of the above numbers

The criteria and sub-criteria identified are depicted in the following figure.

Business Aspects	Delivery Models, Services	Cybersecurity Services	Novel Features	GDPR Compliance
Cost for training and cybersecurity solutions	Cloud-hosted cybersecurity services	Malware/APT protection	Hybrid (rule-based + AI-powered) cybersecurity	Threat information exchange
Clearly defined acceptable use of networks & systems	CPE SaaS	Traffic filtering/Firewall	Virtualized services	Anonymization of data
Skills and regular training of personnel	WAN-edge-based SIEM	WLAN encryption	Threat Remediation capabilities	Partial/full identifiability
Regular review of guidelines and measures		Data breach monitoring	Attestation of underlying infrastructure	
Incident response plan		Deep packet inspection		

Figure 5: End-user survey AHP methodology

Figure 6 depicts an example of the AHP question implementation in the survey. Due to technical limitations of the survey tool used, the [1,9] range described in the methodology has been adapted into a [0,8] range while left hand side selection utilises the [-8,0] range. These adaptations come without loss in methodological effectiveness as the numerical representation of the responders' assessments remains unaffected.



Cybersecurity Services

*Which of the following do you consider more important?

Each answer must be between -8 and 8

Malware/APT protection -4 Traffic filtering/Firewall

*Which of the following do you consider more important?

Each answer must be between -8 and 8

Malware/APT protection 4 WLAN encryption

*Which of the following do you consider more important?

Each answer must be between -8 and 8

Malware/APT protection 0 Data breach monitoring

Figure 6: Example of AHP questions

Including a total of 73 questions, some of them not AHP-based, the questionnaire is able to provide a complete picture of the end-users with regards to cybersecurity matters and how they evaluate the importance of the criteria and sub-criteria described in section 1.1.1.2. The full content of the End-user Questionnaire is available in Annex A.: End-user questionnaire.

1.1.2. Technical questionnaire

To elicit the technical requirements for the PALANTIR architecture, a panel of Subject Matter Experts was surveyed through an online questionnaire. Given the broad technical coverage of the consortium, the Subject Matter Experts were selected within the partner's employees that are not part of the project.

While the full questionnaire is available in Annex B.: Technical questionnaire, an overview of the survey is presented in this section. After a presentation of PALANTIR (including the demonstration use cases), the participants were asked questions about their Company and job position, their recommendation about the PALANTIR Infrastructure, the Cybersecurity Services, the Threat Intelligence engine, the Threat Remediation features, the Risk-based Analysis, the User Interface and Experience, and the legal and regulation compliance. The insights, inferred from the participants' answers, are then transformed into requirements. More specifically, PALANTIR prioritises the most requested features – and discarded the unambiguously irrelevant features, considering the features with a similar number of positive and negative votes as optional. The wording used to specify the importance of each requirement is explained in detail in section 1.2.

The survey was implemented in the form of an online set of questions created using LimeSurvey (https://www.limesurvey.org/), an open-source tool for web surveys, and hosted at: https://www.incites.eu/pollsurvey/index.php/379233

1.1.3. Internal requirements

The internal requirements analysis process relies heavily on the involvement of the stakeholders in the whole value chain that the project brings. The PALANTIR consortium includes all necessary stakeholders of the respective value chain and the whole methodology followed has been aligned with this feature of the project. The consortium includes technology developers as well as service providers, integrators, and SecaaS clients who are involved in the project through the pilot activities. This approach allows for a credible validation of the PALANTIR concept, along with different deployment configurations and service operations plans.

It should be noted that the analysis of the PALANTIR Use Cases is included in D2.2 instead of this document. Given that D2.2 also describes the Threat analysis framework and Risk-based assessment methodology to be adopted by the PALANTIR Use Cases, the partners considered that a detailed description of the PALANTIR scenarios preceding the aforementioned methodology would provide a more natural flow to the reader. Nevertheless, the requirements stemming from this analysis are included in this document.

1.1.4. Law regulations compliance

The PALANTIR law regulation compliance is derived from the analysis of the relevant legislations:

- **ENISA's Regulation** is the Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). By making the relevant information available to the public, ENISA, as established by Regulation (EU) No 526/2013 of the European Parliament and of the Council, contributes to the development of the cybersecurity industry in the Union, in particular SMEs and start-ups. ENISA strives for closer cooperation with universities and research entities in order to contribute to reducing dependence on cybersecurity products and services from outside the Union and to reinforce supply chains inside the Union.
- **General Data Protection Regulation (GDPR)**: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance): The GDPR is in place to safeguard citizens' rights in terms of privacy and data protection. It applies to all components that store or process personal data. It also includes data portability to ensure compliance with EU competition laws and avoid customer lock-in conditions.
- **Open Internet Regulation**: Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union (Text with EEA relevance): The Open Internet Regulation establishes rules for net neutrality. It lists traffic classification and rate limiting for the purpose of security as a fair practice. PALANTIR should include a level of transparency on why limiting rules might be applied.
- **Directive 2002/58/EC of the European Parliament and of the Council** of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications): This Directive is expected to be replaced by an ePrivacy Regulation that is being proposed. It applies to communication providers that need to ensure the security and confidentiality of personal communications, and it is extended to safeguard cookies and other online identifiers.
- **European Charter of Fundamental Human Rights**, especially Article 8(1) on the protection of personal data, establishes privacy as a fundamental human right.
- **Treaty of Amsterdam** (1997/1999 establishing the protected grounds against discrimination) & **Treaty of Lisbon** (2007/2009 making the ECHR Bill of Rights legally binding): The definition of discrimination can be considered free-standing and useful to protect citizen rights in data processing activities that can profile their behaviour.

A detailed analysis of the ethical and regulatory framework that applies to PALANTIR is included in deliverables D1.2 and D1.3, which provides ethical and regulatory compliance specifications for the PALANTIR ecosystem. The basis for the derived requirements is that:

- PALANTIR's end-to-end decision making needs to be transparent: This applies to processing (based on the GDPR) and to traffic management (based on the Open Internet Regulation).
- The data subject should be able to control their data.
- No unnecessary processing or profiling should take place.
- There should be accountability and access to a Data Protection Officer and to all related Data Protection Information.
- In case of a data breach, there should be fast response and a timely notification should be sent by the Service Provider.

1.2. Requirements and Key Performance Indicators

PALANTIR adopts a compact tabular format to document system requirements. The purpose is, on one hand, to include all necessary information needed to accompany each requirement, while, on the other hand, to follow a format as compact as possible, saving space and facilitating the browsing of the requirements list. Table 3 below shows the structure of the requirements table.

Table 3: Structure of requirements table

Group X.Y: *[Group description]*		
Req. ID	Requirement description	Origin of requirement
[RX.Y.Z]	*[Description]*	*[Origin]*

The attributes of the requirements are as follows:

Group description: To facilitate management, requirements are organised in groups. Each group is labelled by two digits (X.Y)

- The first digit (X) denotes whether the group includes functional (1) or non-functional (2) requirements. Functional requirements are related to a specific capability of the system (what the system does), whereas non-functional ones are related to a specific quality of the system (how the system does it).
- The second digit (Y) denotes the specific subgroup, as follows:
  - Functional requirements are mostly grouped by the functional aspect of the system to which they are related (e.g. threat sharing, secure services etc.). Currently, functional requirement groups in PALANTIR are:
    - 1.1. Generic functional requirements
    - 1.2. Use Case-Specific functional requirements
    - 1.3. Secure Service Ecosystem requirements (mostly related to WP3 scope)
    - 1.4. Threat Management and Sharing requirements (mostly related to WP4 scope)
    - 1.5. Hybrid Threat Intelligence requirements (mostly related to WP5 scope)
  - Non-functional requirements are mostly grouped by the specific quality attribute of the system which they address. Currently, non-functional requirement groups in PALANTIR are:
    - 2.1. Scalability
    - 2.2. Performance

- 2.3. Security and privacy
- 2.4. Reliability and availability
- 2.5. Manageability and flexibility
- 2.6. Modularity
- 2.7. Openness and Extensibility

Requirement ID: This is a unique identifier for each requirement, facilitating reference to it for traceability purposes. It has the structure RX.Y.Z where X.Y is the ID of the group (see above) to which the requirement belongs, and Z is the sequence number of each requirement within the group, starting with 1.

Requirement description: This includes a brief, yet complete, description of the requirement. It must be stressed out that, at this stage, the requirements are system-wide: they refer to a feature of the system as a whole, without going into individual components. The wording within each requirement shows the requirement level, i.e. whether the requirement is mandatory, recommended or optional. This follows the widely adopted meanings defined in RFC 2119 [11]. More specifically:

- "MUST" / "SHALL" / "MUST NOT" / "SHALL NOT" denotes a mandatory requirement which needs to be fulfilled.
- "SHOULD" / "RECOMMENDED" / "SHOULD NOT" / "NOT RECOMMENDED" denotes a recommended requirement, which can be ignored following appropriate justification – and after the implications have been understood and fully weighed.
- "MAY" denotes a truly optional requirement.

The words above are always in capital to stand out from the rest of the description.

Some non-functional requirements may also include a Key Performance Indicator (KPI) to be fulfilled (e.g. related to accuracy, scalability, response time etc.)

Origin of requirement: This is a brief, yet clear, pointer to where the requirement originates from. This might be the scope baseline of the project, as laid out in the Description of Action, a specific use case, an expressed need or a consultation from an external stakeholder, a suggestion from an expert within the project team or an input from the anonymous questionnaires. The reference must be complete enough so that one can trace back to the originator of the requirement to ask for specific clarifications or further inputs – respecting always the anonymity of external experts, if so required.

Table 4: The requirements table

Group 1.1.: Generic functional requirements		
Req. ID	Requirement description	Origin of requirement
R1.1.1	The platform MUST provide registration and sign-in functionalities for the following roles: users, administrators.	*Description of Action.*
R1.1.2	The platform MUST provide a dashboard in order to present results of analysis.	*Description of Action.*
R1.1.3	The platform MUST provide near-real-time (NRT) data processing functionalities.	*Technical Questionnaire: question 16.* *Description of Action.*
R1.1.4	The platform SHOULD implement communication between PALANTIR components with a lightweight message queue	*Description of Action.*
Group 1.2.: Use Case-Specific functional requirements		

R1.2.1	PALANTIR providers host SHALL provide telemetry and other auditing information relevant to the security mechanisms of the system.	*All use cases.*
R1.2.2	PALANTIR providers host SHALL only allow authenticated users to consume the services provided by the 5G system.	*Use case 3.*
R1.2.3	PALANTIR providers SHALL ensure the necessary network capacity and network resources necessary for the critical operations of the 5G services.	*Use case 3.*
R1.2.4	PALANTIR providers SHALL enable a secure platform for vertical services to be deployed.	*Use case 2.*
R1.2.5	The PALANTIR-introduced security mechanisms should be transparent to the operation of vertical applications.	*All use cases.*
R1.2.6	Security mechanisms used in a complex cybersecurity eco-system SHALL be able to identify, distribute and allocate responsibilities between 5G ecosystem stakeholders.	*Use case 3.*
R1.2.7	The PALANTIR eco-system SHALL be able to publish security KPI measuring the compliance of stakeholder with their Security Level Commitments.	*All use cases.*
R1.2.8	Technologies used by PALANTIR SHOULD be trustable.	*Technical Questionnaire: question 6.* *All use cases.*
R1.2.9	The PALANTIR system MUST provide security mechanisms to ensure that user (and endpoints) data are securely processed and stored wherever it is processed or stored.	*Technical Questionnaire: question 32.* *All use cases.*
R1.2.10	The PALANTIR platform SHOULD provide risk profiling and assessment for a set of input attack surfaces provided from the corresponding stakeholder.	*All use cases.*
R1.2.11	The PALANTIR platform SHOULD support management capabilities for the vulnerabilities of the system under test.	*All use cases.*
R1.2.12	The PALANTIR platform SHOULD provide coherent mitigation plans for corresponding threat and attack vectors.	*All use cases.*
Group 1.3.: Secure Service Ecosystem requirements		
R1.3.1	The platform SHALL be able to instantiate security capabilities.	*Description of Action.*

R1.3.2	The platform SHALL be able to configure security capabilities, whether already deployed or newly instantiated.	*All use cases.*
R1.3.3	The platform SHALL provide a variety of SecaaS packages on the Catalogue.	*Technical Questionnaire: question 9 and 11.* *All use cases.*
R1.3.4	The security capabilities SHALL provide the maximum feasible set of the expected (open) connectors so as to be handled similarly in the catalogue and interact in a similar manner with the orchestration tools.	*Description of Action.*
R1.3.5	The security capabilities SHALL provide the privacy specifications that are shown to infrastructure administrators that ultimately deploy such services.	*Description of Action.*
R1.3.6	The security capabilities SHALL implement the expected (open) Element Management System (EMS) hooks so to be configured by the platform.	*Description of Action.*
R1.3.7	The security capabilities SHALL be uploaded to the catalogue as a pre-packaged bundle containing its basic dependencies. Any external dependency SHALL be provided before its uploading to the Catalogue.	*Description of Action.*
R1.3.8	The security capabilities SHOULD be available in source form and publicly shared so as to allow reusing by others as well as logic auditing.	*Description of Action.*
R1.3.9	The platform SHOULD be able to monitor the deployed security capabilities and expose such data through programming interfaces for other internal components.	*Technical Questionnaire: question 5.*
R1.3.10	The platform SHALL be able to deploy security capabilities from the Catalogue to operate with a copy of network data (off-the-path traffic).	*Technical Questionnaire: question 14.*
R1.3.11	The platform MAY be able to deploy security capabilities from the Catalogue to operate with online network data (on-the-path traffic).	*Technical Questionnaire: question 14.*
R1.3.12	The platform SHALL deploy in cloud/hosted and edge SecaaS delivery modes.	*Technical Questionnaire: question 7.*
R1.3.13	The platform SHOULD deploy in lightweight SecaaS delivery mode with minimal computational resources.	*Technical Questionnaire: question 7.* *Description of Action.*
R1.3.14	The platform SHALL be able to retrieve the basic status for the security capabilities instantiated or available (in the Catalogue).	*Description of Action.*

R1.3.15	The platform SHOULD be able to decide whether to reuse existing security capabilities or if new ones have to be instantiated, according to the received policy specifications.	*Description of Action.*
R1.3.16	The platform SHOULD implement SDN technology in conjunction with NFV technology to facilitate the provision of SecaaS solutions	*Technical Questionnaire: question 7.* *All use cases.*
R1.3.17	The platform SHOULD have additional storage to include security rules, metrics, logs or configurations	*Technical Questionnaire: question 30.* *All use cases.*
R1.3.18	The platform SHOULD provide streaming of resource utilization data for billing in the Dashboard	*All use cases.*
R1.3.19	The platform SHOULD deliver adaptive filtering and traffic control capabilities.	*End-user Questionnaire: question 28 and 34.* *Technical Questionnaire: question 9.* *All use cases.*
R1.3.20	The platform SHOULD deliver port and service scanning capabilities.	*End-user Questionnaire: question 28.* *Technical Questionnaire: question 9.* *All use cases.*
R1.3.21	The platform SHOULD deliver remote attack detection capabilities.	*Technical Questionnaire: question 9.* *All use cases.*
R1.3.22	The platform MUST provide protection from data exfiltration attempts.	*End-user Questionnaire: question 28 and 34.* *Technical Questionnaire: question 9.* *All use cases.*
R1.3.23	The platform SHOULD offer packet inspection capabilities.	*End-user Questionnaire: question 28 and 34.* *Technical Questionnaire: question 9.* *All use cases.*
R1.3.24	The platform SHOULD deliver intrusion detection and prevention capabilities.	*Technical Questionnaire: question 9.* *All use cases.*
R1.3.25	The security capabilities MAY implement techniques such as exact data matching, structured data fingerprinting, statistical methods.	*All use cases.*

R1.3.26	The platform SHOULD deliver additional security capabilities in function of specific use cases tasks	*All use cases.*
R1.3.27	The platform SHOULD provide SecaaS deployment with 5G compatibility	*Use case 3.*
R1.3.28	The platform SHOULD provide an interactive workflow to review risks, statistics and security status of a SMEs.	*All use cases.*
R1.3.29	The platform SHOULD prevent and react against Ransomware attacks	*Technical Questionnaire: question 5.* *All use cases.*
R1.3.30	The platform SHOULD provide network isolation for compromised systems.	*End-user Questionnaire: question 28.* *All use cases.*
R1.3.31	The platform SHOULD provide a service supporting risk assessment framework	*End-user Questionnaire: question 21.* *Technical Questionnaire: question 7.* *All use cases.*
Group 1.4.: Threat Management and Sharing requirements		
R1.4.1	PALANTIR SHOULD deploy mechanisms for the periodic attestation of the platform and the running applications', services' and configurations' integrity.	*End-user Questionnaire: question 27 and 35.* *Technical Questionnaire: questions 5 and 6.*
R1.4.2	PALANTIR SHOULD recover from threats on the Security Capability Hosting Infrastructure.	*End-user Questionnaire: question 35.*
R1.4.3	The platform SHOULD be able to identify and isolate network segments, data or equipment at risk and enable automatic redundancy and (offline) data backup service to prevent corruption or loss of data. The risks are recognised complex reflected primarily in unexpected/unusual behaviour.	*End-user Questionnaire: question 3, 17, 21, 22 and 28.* *Use case 1 and 2.*
R1.4.4	The platform SHOULD be able to collect and analyse the status and health of the underlying infrastructure, including components at risk due to improper communication security (i.e. no or weak encryption), weak passwords, or irregular updates.	*End-user Questionnaire: question 18, 19 and 26.* *All use cases.*
R1.4.5	The platform SHOULD provide a solution to deliver an incidence response plan tailored to specific end-user.	*End-user Questionnaire: question 32, 33 and 34.* *All use cases.*
R1.4.6	The platform SHOULD provide an AI based solution to deliver services, and be shared across the plain field; however, the data-sharing must ensure anonymity.	*End-user Questionnaire: question 36 and 37.* *All use cases.*

Group 1.5.: Hybrid Threat Intelligence requirements		
R1.5.1	The platform SHALL be able to collect and analyse events from heterogeneous sources in near real time in order to detect security incidents	*Technical Questionnaire: question 12 and 14.* *All use cases.*
R1.5.2	The platform SHALL be able to analyse and combine different modalities of data to detect anomalies in nearly real time	*Technical Questionnaire: question 13, 14 and 16.* *All use cases.*
R1.5.3	The platform SHALL be able to automatically classify the type of anomaly/threat and to share the intelligence information in a standard format	*End-user Questionnaire: question 29.* *Technical Questionnaire: question 31.* *All use cases.*
R1.5.4	The platform SHALL be able to analyse an attack report to produce an ordered set of suggested actions (e.g. VNFs configuration) to mitigate the attack	*Technical Questionnaire: question 19 and 20.* *All use cases.*
R1.5.5	The platform SHOULD provide analytics able to detect the most common threat types (malware, MitM, volumetric attacks).	*End-user Questionnaire: question 3.* *Technical Questionnaire: question 17.*
R1.5.6	The platform SHOULD provide analytics able to detect phishing attacks.	*End-user Questionnaire: question 3.*
R1.5.7	The data involved in the analytics processes MUST be anonymized.	*End-user Questionnaire: question 36.* *Description of Action.*
R1.5.8	The platform SHALL provide periodic retrain functionalities for its analytics components (e.g. on a monthly basis).	*Technical Questionnaire: question 15.*
Group 2.1.: Scalability		
R2.1.1	The analytics of the platform SHOULD be able to scale with respect to the number of data sources, the volume and the velocity of data streams.	*Technical Questionnaire: question 13.* *Description of Action.*
R2.1.2	The analytics components of the platform SHOULD be able to deal with the computational and memory limitations posed by large datasets.	*Technical Questionnaire: question 13.*
R2.1.3	The platform SHOULD be capable of accessing Terrabytes of data.	*Technical Questionnaire: question 13 and 34.* *Description of Action.*
Group 2.2: Performance		
R2.2.1	PALANTIR deploys various big data analytics frameworks that have demands in computational power. They MUST be regularly evaluated during development, such	*Description of Action.*

	that they are shown to be accurate with real-time data.	
R2.2.2	PALANTIR SHOULD outperform existing conventional methods from potential competitors.	*Description of Action.*
R2.2.3	The time to discover critical info & alerts in the security dashboard MUST NOT exceed 1 minute.	*Technical Questionnaire: question 16.* *Description of Action.*
R2.2.4	The time to deploy and configure a new security capability MUST NOT exceed 30 seconds.	*Description of Action.*
R2.2.5	The platform MUST propose remediation actions that leads to the successful mitigation of propagating threats for at least 50% of the cases.	*Description of Action.*
R2.2.6	The platform MUST provide at least 5 different proactive mitigation measures transferred via the PALANTIR threat sharing mechanism for the automated mitigation of threats in other PoPs.	*Description of Action.*
R2.2.7	The platform MUST showcase a reduction of false positives and negatives of at least 15% compared to commercial solutions.	*Description of Action.*
Group 2.3.: Security and Privacy		
R2.3.1	PALANTIR platform SHOULD respect data access policies.	*Technical Questionnaire: question 21.* *All use cases.*
R2.3.2	PALANTIR SHOULD be capable of managing different user profiles distinguishing between user roles.	*All use cases.*
R2.3.3	PALANTIR, in accordance with privacy policies, SHOULD store privacy covered data in a protected way.	*Technical Questionnaire: question 32.* *All use cases.*
R2.3.4	Access to protected data SHOULD be possible only to authorized operators.	*All use cases.*
R2.3.5	The applications and technologies used in PALANTIR SHOULD respect all regulations concerning the ethical aspects, especially those related with data protection and privacy.	*End-user Questionnaire: question 29.* *Technical Questionnaire: question 35.* *All use cases.*
R2.3.6	PALANTIR SHOULD cover with state-of-the-art technologies all the aforementioned security aspects.	*All use cases.*
Group 2.4.: Reliability and Availability		
R2.4.1	PALANTIR MUST have a high availability and reliability design, aligned with the	*Technical Questionnaire: question 8.*

	industry standard of 99% that can be monitored, measured and audited.	
R2.4.2	In case of failures, measures SHOULD be taken in order to overcome these in short notice and additional measures for preventing their occurrence.	*All use cases.*
Group 2.5.: Manageability and Flexibility		
R2.5.1	PALANTIR SHOULD be highly usable as well as flexible, even for users that are not considered experts.	*All use cases.*
R2.5.2	The platform MUST offer at least 5 SecaaS capabilities on the Catalogue	*Description of Action.*
Group 2.6.: Modularity		
R2.6.1	The PALANTIR architecture SHOULD follow a layered and modular approach.	*All use cases.*
R2.6.2	The PALANTIR modularity level SHOULD allow enough independence of all modules so as if any module needs to be replaced, this has no consequences to the other modules.	*All use cases.*
Group 2.7.: Openness and Extensibility		
R2.7.1	End users SHOULD be able to use PALANTIR from major operating systems (either to access PALANTIR or on the Information Technology system protected by PALANTIR).	*All use cases.*
R2.7.2	The various components of PALANTIR SHOULD be interoperable with other services implementing common and open standards	*End-user Questionnaire: question 29.*
R2.7.3	PALANTIR SHOULD follow industry best practices and be easy to use and extend by external parties for open-source components.	*All use cases.*
R2.7.4	PALANTIR SHOULD provide programming interfaces for application developers to gather real-time and historic data.	*All use cases.*
R2.7.5	PALANTIR SHOULD reuse existing open-source software and tools, where it is appropriate and possible according the license.	*All use cases.*
R2.7.6	The architecture of PALANTIR MUST be open, extensible, providing ability to add new functional components.	*End-user Questionnaire: question 29.* *Description of Action.*

2. PALANTIR Architecture

The architecture design of PALANTIR follows a scenario-based approach. The use case scenarios are the starting point for defining the system's components and their interfaces. Scenario identification and description takes place at the first phase of the methodology (the user requirements phase) and its conclusion drives a clear definition of the system's goals, actors and requirements, which in turn drives the development of the project and the final demonstrations. In such approaches, it is of high importance that a use case scenario should be well-defined and complete in order to cope with all the necessary information to allow the extraction of concrete end users' goals and requirements that affects the whole lifecycle of the project. The aim of this section is to provide a mapping between the requirements defined and the components of the PALANTIR framework.

The logical and functional views of the PALANTIR architecture are based on the mapping between the requirements (internal and external) and the desired functionalities that the conceptual-based building blocks of PALANTIR should have in order to provide the necessary functionality. This approach enables the logical connection between the various architectural models and the requirements elicited through the conceptual foundation of the project. When a requirement is associated to a key component or sub-system of PALANTIR architecture, it is also linked to all the structures where the key component coexists (component, module, and/or interface). Furthermore, it can be connected in a transparent way increasing thus the effectiveness of the architecture and the development steps that follow. The most important relationships are captured in the beginning of a design project, but as the architecture is realised, new requirements or updates on the existing ones can be transformed into new or enhanced versions of the PALANTIR components, increasing thus the manageability of the PALANTIR architecture.

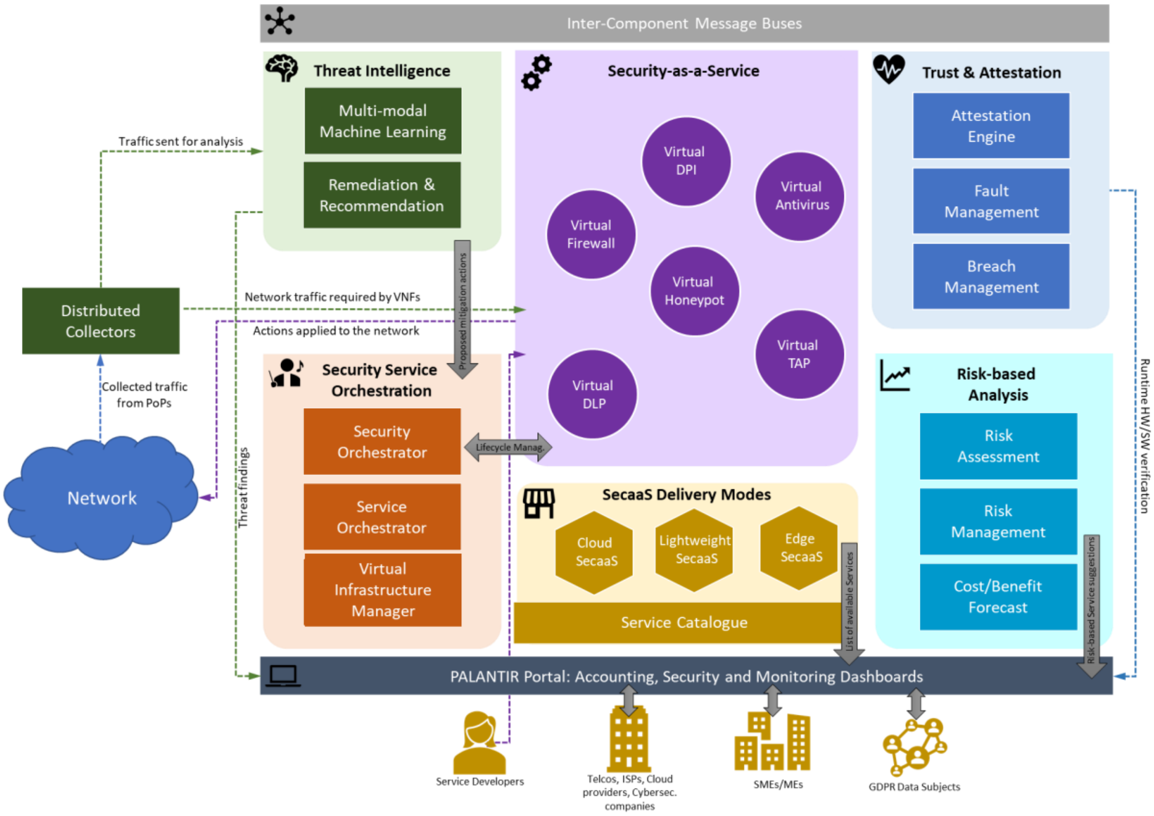
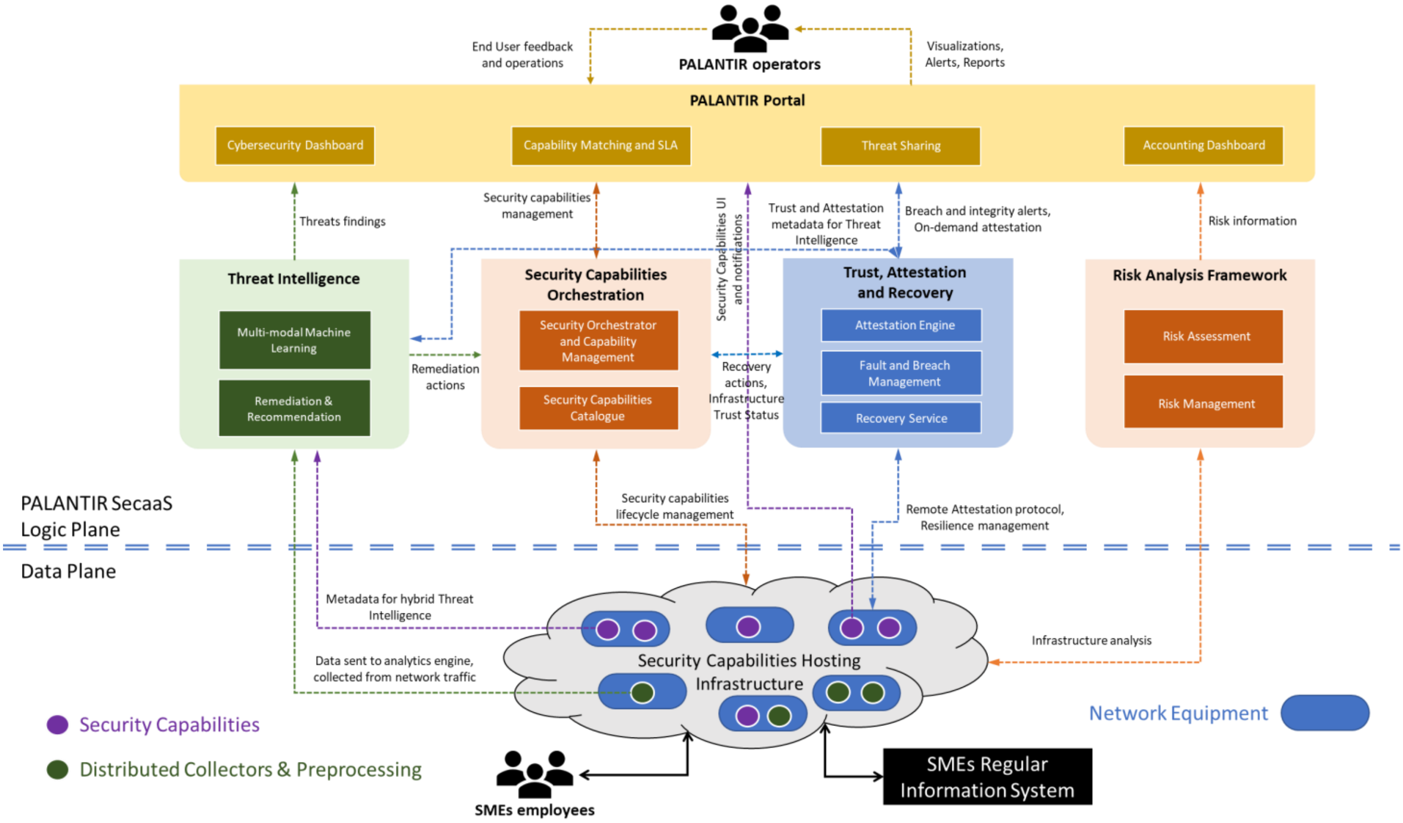


Figure 7: Conceptual PALANTIR solution

The conceptual architectural view of PALANTIR is presented in Figure 7, which is an evolution from the architecture diagram from the Description of Action. Figure 7 illustrates the different concepts used and how they logically fit together in the PALANTIR solution. However, a complete overview of the component inter-communication is presented in Figure 8, where all the logical connections between the main components are defined.



PALANTIR operators
End User feedback and operations
Visualizations, Alerts, Reports
PALANTIR Portal
Cybersecurity Dashboard
Capability Matching and SLA
Threat Sharing
Accounting Dashboard
Threats findings
Security capabilities management
Security Capabilities UI and notifications
Trust and Attestation metadata for Threat Intelligence
Breach and integrity alerts, On-demand attestation
Risk information
Threat Intelligence
Multi-modal Machine Learning
Remediation & Recommendation
Remediation actions
Security Capabilities Orchestration
Security Orchestrator and Capability Management
Security Capabilities Catalogue
Recovery actions, Infrastructure Trust Status
Trust, Attestation and Recovery
Attestation Engine
Fault and Breach Management
Recovery Service
Risk Analysis Framework
Risk Assessment
Risk Management
Security capabilities lifecycle management
Remote Attestation protocol, Resilience management
PALANTIR SecaaS Logic Plane
Data Plane
Metadata for hybrid Threat Intelligence
Data sent to analytics engine, collected from network traffic
Security Capabilities Hosting Infrastructure
Infrastructure analysis
Network Equipment
● Security Capabilities
● Distributed Collectors & Preprocessing
SMEs employees
SMEs Regular Information System

Figure 8: High level PALANTIR architecture

Each component is detailed below and the requirements, which are of critical importance to the component, are listed in their subsection. In addition to those specific requirements, each component is highly likely to have to fulfil the non-functional requirements (groups 2.1.: Scalability, 2.2.: Performance, 2.3.: Security and Privacy, 2.4.: Reliability and Availability, 2.5.: Manageability and Flexibility, 2.6.: Modularity and 2.7.: Openness and Extensibility) as well as the generic functional requirements listed in Table 5.

Table 5: Generic requirements related to most components

Req. ID	Requirement description	Origin of requirement
R1.1.4	The platform SHOULD implement communication between PALANTIR components with a lightweight message queue	*Description of Action.*
R1.2.5	The PALANTIR-introduced security mechanisms should be transparent to the operation of vertical applications.	*All use cases.*
R1.2.8	Technologies used by PALANTIR SHOULD be trustable.	*Technical Questionnaire: question 6.* *All use cases.*
R1.2.9	The PALANTIR system MUST provide security mechanisms to ensure that user (and	*Technical Questionnaire: question 32.*

	endpoints) data are securely processed and stored wherever it is processed or stored.	*All use cases.*

2.1. PALANTIR Components

2.1.1. Security Capabilities Hosting Infrastructure (SCHI)

This section presents an abstract overview of the available infrastructure that is used in order to host the PALANTIR components and their services. Figure 9 illustrates the process of collecting data (metrics, alerts, and traffic data) for PALANTIR clients. Clients may use cloud-hosted PALANTIR services or host some of the components in their premises.

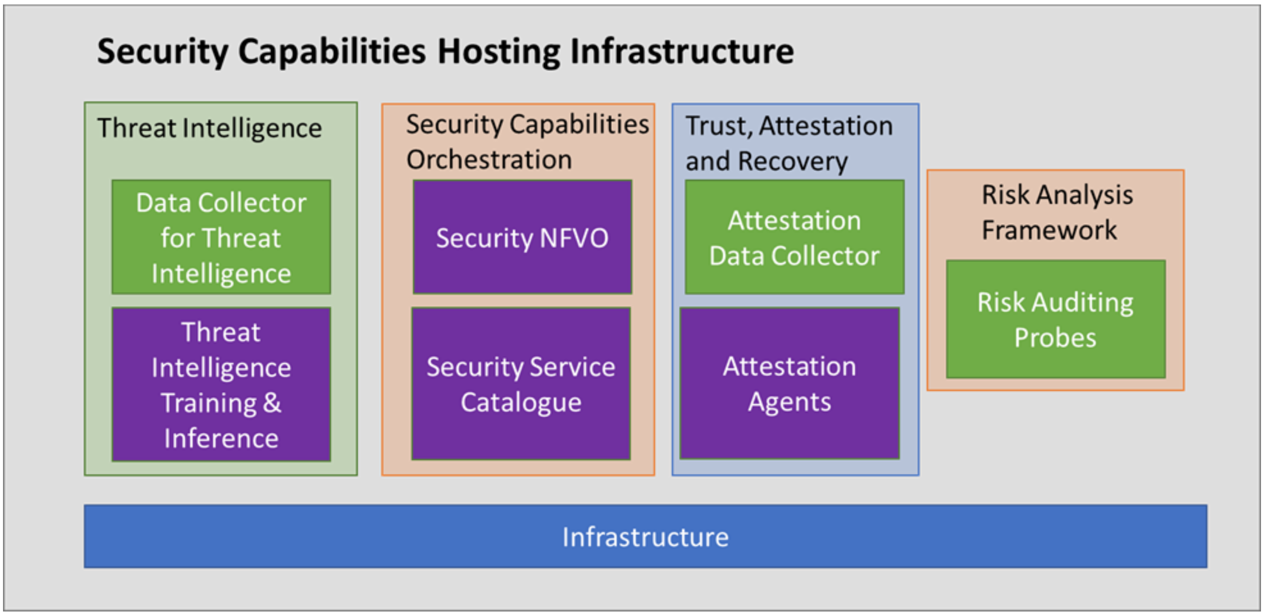

Security Capabilities Hosting Infrastructure
Threat Intelligence
Data Collector for Threat Intelligence
Threat Intelligence Training & Inference
Security Capabilities Orchestration
Security NFVO
Security Service Catalogue
Trust, Attestation and Recovery
Attestation Data Collector
Attestation Agents
Risk Analysis Framework
Risk Auditing Probes
Infrastructure

Figure 9: Logical view of the PALANTIR infrastructure

Each component of the Security Capabilities Hosting Infrastructure serves as the virtual/physical agent entity that collects or processes data for the upper layer PALANTIR components.

Table 6: Requirements related to the Security Capabilities Hosting Infrastructure component

Req. ID	Requirement description	Origin of requirement
R1.2.1	PALANTIR providers host SHALL provide telemetry and other auditing information relevant to the security mechanisms of the system.	*All use cases.*
R1.2.2	PALANTIR providers host SHALL only allow authenticated users to consume the services provided by the 5G system.	*Use case 3.*
R1.2.3	PALANTIR providers SHALL ensure the necessary network capacity and network resources necessary for the critical operations of the 5G services.	*Use case 3.*
R1.2.4	PALANTIR providers SHALL enable a secure platform for vertical services to be deployed.	*Use case 2.*

R1.3.10	The platform SHALL be able to deploy security capabilities from the Catalogue to operate with a copy of network data (off-the-path traffic).	*Technical Questionnaire: question 14.*
R1.3.11	The platform MAY be able to deploy security capabilities from the Catalogue to operate with online network data (on-the-path traffic).	*Technical Questionnaire: question 14.*
R1.3.12	The platform SHALL deploy in cloud/hosted and edge SecaaS delivery modes.	*Technical Questionnaire: question 7.*
R1.3.13	The platform SHOULD deploy in lightweight SecaaS delivery mode with minimal computational resources.	*Technical Questionnaire: question 7.* *Description of Action.*
R1.3.16	The platform SHOULD implement SDN technology in conjunction with NFV technology to facilitate the provision of SecaaS solutions	*Technical Questionnaire: question 7.* *All use cases.*

2.1.2. Security Capabilities

The PALANTIR platform offers the provision of Security-as-a-Service solutions for SME/MEs with minimum resources and critical requirements. SecaaS is a new paradigm created by the Cloud Security Alliance in 2011 [12], which proposes that the security can be offered as a service. This paradigm was born from the need that appeared due to the recent tendency of cyberattacks, which compromise and impact in the cybersecurity of people, companies, institutions and countries.

The Security-as-a-Service component consists of the deployment of security services on-demand, with personalised characteristics associated with the client. The **SecaaS Capabilities** can be deployed into **Virtualized Network Functions (VNFs)**, which consists of one or more virtual machines / containers running different software and processes. The **Security Capabilities** can also be implemented as a set of SDN flows or security configurations depending on the capability being implemented and the hosting platform's features.

Finally, different deployment paradigms, such as **Dew** [13], **Edge and Cloud computing**, can be used to bring the SecaaS solutions into the client. Characteristics and needs of each client can serve as a decision factor for using a given deployment paradigm.

Subcomponents

The SecaaS component is composed of some subcomponents, which belong to the aforementioned technology. In this sense, this component is based on the ETSI GS NFV-SEC 013 specification [14], where different subcomponents are added to the initial architecture proposed for the NFV technology. The subcomponent architecture – and their interaction with other PALANTIR components - is presented in Figure 10, in an abstract manner as they are specifically defined during the development, testing and integration process.

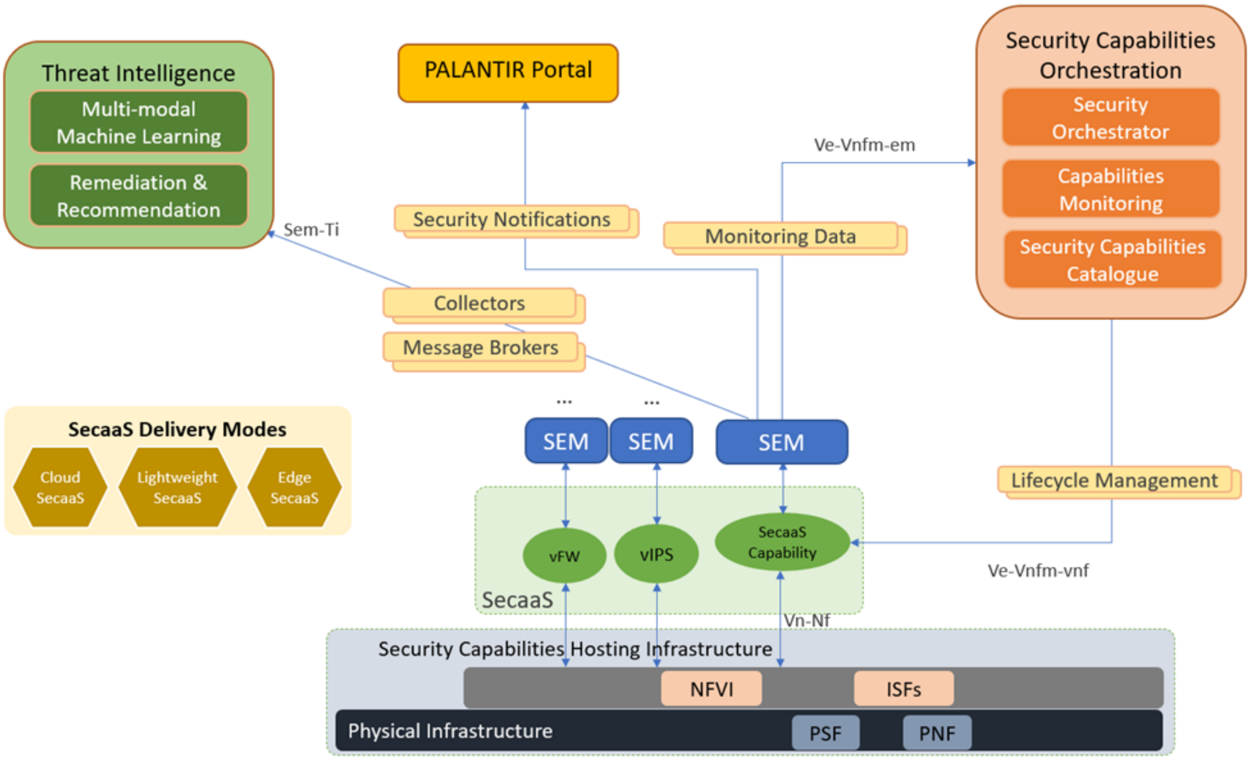


Figure 10: The SecaaS component architecture

- **Security Element Manager (SEM)** acts as an intermediary between the SecaaS capabilities and the rest of the PALANTIR infrastructure. Mainly, the SEM exposes the data collected and events created by the SecaaS capabilities for the Threat Intelligence and PALANTIR Portal components. Besides, it is responsible for managing the SecaaS capabilities lifecycle and security configurations through communication with the Security Capabilities Orchestration component. At last, each SecaaS capability is associated with a SEM.
- **SecaaS Capabilities** are responsible for the SME/ME protection and they can be implemented under different deployment strategies called SecaaS delivery modes, which are use-case specific. The platform deploys capabilities, such as traffic filtering (e.g. firewall), traffic analysis (e.g. an Intrusion Detection and Prevention System - IDPS), and additional features, such as Security Configurations and Machine Learning abilities. These run on top of the NFVI.
- **Network Function Virtualised Infrastructure (NFVI)** contains the underlying components of the infrastructure, which are used to host the SecaaS capabilities. It exposes the available resources as virtualized resources to SecaaS capabilities.
- **NFVI-based Security Functions (ISFs)** are concrete services provided by the NFV infrastructure, designated to implement security hardware/software capabilities to the NFV infrastructure itself, such as hypervisor-based firewall and hardware security modules.
- **Physical Security/Network Functions (PSF/PNFs)** are part of the non-virtualised traditional network and are in charge of protect the physical part of the infrastructure and network.

Table 7: Requirements related to the Security Capabilities component

Req. ID	Requirement description	Origin of requirement
R1.3.1	The platform SHALL be able to instantiate security capabilities.	*Description of Action.*
R1.3.2	The platform SHALL be able to configure security capabilities, whether already deployed or newly instantiated.	*All use cases.*

R1.3.3	The platform SHALL provide a variety of SecaaS packages on the Catalogue.	*Technical Questionnaire: question 9 and 11.* *All use cases.*
R1.3.4	The security capabilities SHALL provide the maximum feasible set of the expected (open) connectors so as to be handled similarly in the catalogue and interact in a similar manner with the orchestration tools.	*Description of Action.*
R1.3.5	The security capabilities SHALL provide the privacy specifications that are shown to infrastructure administrators that ultimately deploy such services.	*Description of Action.*
R1.3.6	The security capabilities SHALL implement the expected (open) Element Management System (EMS) hooks so to be configured by the platform.	*Description of Action.*
R1.3.7	The security capabilities SHALL be uploaded to the catalogue as a pre-packaged bundle containing its basic dependencies. Any external dependency SHALL be provided before its uploading to the Catalogue.	*Description of Action.*
R1.3.8	The security capabilities SHOULD be available in source form and publicly shared so as to allow reusing by others as well as logic auditing.	*Description of Action.*
R1.3.14	The platform SHALL be able to retrieve the basic status for the security capabilities instantiated or available (in the Catalogue).	*Description of Action.*
R1.3.19	The platform SHOULD deliver adaptive filtering and traffic control capabilities.	*End-user Questionnaire: question 28 and 34.* *Technical Questionnaire: question 9.* *All use cases.*
R1.3.20	The platform SHOULD deliver port and service scanning capabilities.	*End-user Questionnaire: question 28.* *Technical Questionnaire: question 9.* *All use cases.*
R1.3.21	The platform SHOULD deliver remote attack detection capabilities.	*Technical Questionnaire: question 9.* *All use cases.*
R1.3.22	The platform MUST provide protection from data exfiltration attempts.	*End-user Questionnaire: question 28 and 34.* *Technical Questionnaire: question 9.* *All use cases.*

R1.3.23	The platform SHOULD offer packet inspection capabilities.	*End-user Questionnaire: question 28 and 34.* *Technical Questionnaire: question 9.* *All use cases.*
R1.3.24	The platform SHOULD deliver intrusion detection and prevention capabilities.	*Technical Questionnaire: question 9.* *All use cases.*
R1.3.25	The security capabilities MAY implement techniques such as exact data matching, structured data fingerprinting, statistical methods.	*All use cases.*
R1.3.26	The platform SHOULD deliver additional security capabilities in function of specific use cases tasks	*All use cases.*

2.1.3. Security Capabilities Orchestration (SCO)

In the PALANTIR platform, the **Security Capabilities Orchestration** component is in charge of the overall management of the security capabilities (i.e., security network services, policies, configurations and similar features), considering its deployment and reconfiguration, as well as part of its monitoring. Specifically, it oversees:

- The interaction of the Security Orchestrator (SO) with the NFV Management and orchestration (MANO) related to the SecaaS services registered in the Security Capabilities Catalogue (SCC): the onboarding of such packages, their instantiation/deployment and configuration in a given infrastructure (VIM), depending on the deployment mode (cloud, edge, lightweight).
- The enforcement of the security policies and configuration provided as an output of threat mitigation recommendations or as result of attestation reports. This can be done on services or different types of software or hardware nodes or devices, were these considered adequate. Some examples can be the SDN reconfiguration (via a control plane) to provision required networking setup for a given service or action, or some measure taken on unsuccessfully attested nodes.
- The monitoring of part of the security capabilities and the NFVI environment, as well as potentially generating alerts based on specific conditions that can be used for reporting, displaying and logic enforcement in upper layers.

The SCO leverages 3rd party tools for the management of the NFVI infrastructure (VIM), on the orchestration of VNFs (NFV MANO) and on the management of the programmable network (SDN controller). Such tools are integrated with this component yet, since alien to PALANTIR, these cannot be considered part of SCO and are thus not bundled with it.

Figure 11 depicts one possible view of the architecture for SCO and its interactions with both other components within the PALANTIR platform and other elements in the NFV infrastructure (NFVI) environment.

It is worth noting that the architecture is expected to be compliant with ETSI NFV-SEC 013 [14] and ETSI NFV-SEC 024 standards [32], which deal with the security management and monitoring specification in an NFV environment. An early, first draft version mapping the components and interactions to such standards is provided below.

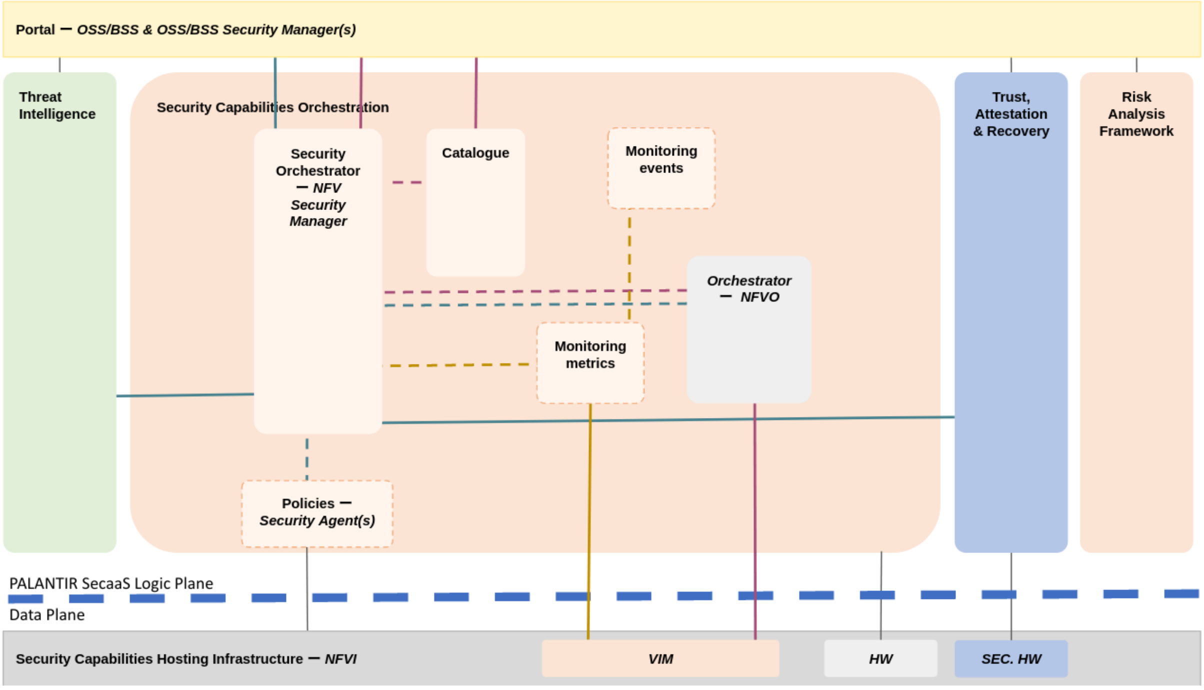

Portal — OSS/BSS & OSS/BSS Security Manager(s)
Threat Intelligence
Security Capabilities Orchestration
Security Orchestrator — NFV Security Manager
Catalogue
Monitoring events
Orchestrator — NFVO
Monitoring metrics
Policies — Security Agent(s)
Trust, Attestation & Recovery
Risk Analysis Framework
PALANTIR SecaaS Logic Plane
Data Plane
Security Capabilities Hosting Infrastructure — NFVI
VIM
HW
SEC. HW

Figure 11: Example of Security Capabilities Orchestration architecture

Subcomponents

In order for the SCO component to perform the coordination of such capabilities, the onboarding, instantiation and configuration (as well as performance) perspectives have to be taken into account, in a different level, by the SO and the SCC. All of this allows this component to act as the entry point from the capabilities' operational side and to provide part of the monitoring on the capabilities.

On the one hand, the SCC hosts the set of security capabilities to be used. The SCC stores the base packages for the Security Capabilities in a trusted way, and keeps their security and privacy specifications, billing information and other required metadata. Packages are essentially functional and include all necessary security metadata about Security Capabilities as well as privacy descriptors (including also deployment details). These capabilities are, in turn, packaged as images, such as images for containers or Virtual Machines (VMs). If a security capability needs not include such an image, the package includes pieces of logic or parameters, such as SDN flows or P4 programs [33], to be sent to active network elements through secure interfaces. The SCC is searchable, and can be accessed by the Risk Analysis Framework component to identify the proper Security Capabilities and by correlating with the outcome of the analysis. The SCC also interfaces with the security and the accounting dashboard to leverage a User Interface that enacts the deployment of security capabilities, so as to deploy capabilities or have a brief inspection of the overall deployment.

On the other hand, the SO obtains the service packages along with user-inserted metadata, to later instantiate and configure the desired capabilities. Basic instructions of which security services or capabilities to deploy are provided to the SO by the SCC, and basic deployment status information is provided by the orchestrator. The foreseen modules for SO are listed below:

- *Packages*: leverages the packaged services from the SSC, as well as processing any information from them as required and onboarding in the NFVO.
- *Metrics*: performance-related information can be retrieved from specific capabilities (such as CPU load, RAM consumption, number of instances of deployed services) or from other

environments, e.g., the VIM. Such collection of usage metrics can be used to make decisions in an upper layer or display information, e.g., related to billing or Service-Level Agreement.

- *Life Cycle Management*: makes it possible to instantiate and configure the security services that are running in the SecaaS environment. Performance considerations are expected to be applied to some extent, e.g., to minimise time for service instantiation ETSI NFV-SEC013 [14].
- *Events*: based on the metrics retrieved by the specific subcomponent, programmable alarms and actions could be triggered based on predefined conditions set by the user.
- *Policies*: through its interaction with the Threat Intelligence and the Trust, Attestation & Remediation components, the SCO obtains the policies that are to be translated before configuring and/or securing the deployed VNFs. The capability model defined in the IETF I2NSF WG [15] may be considered for such translation.

Table 8: Requirements related to the Security Capabilities Orchestration component

Req. ID	Requirement description	Origin of requirement
R1.2.6	Security mechanisms used in a complex cybersecurity eco-system SHALL be able to identify, distribute and allocate responsibilities between 5G ecosystem stakeholders.	*Use case 3.*
R1.3.2	The platform SHALL be able to configure security capabilities, whether already deployed or newly instantiated.	*All use cases.*
R1.3.3	The platform SHALL provide a variety of SecaaS packages on the Catalogue.	*Technical Questionnaire: question 9 and 11.* *All use cases.*
R1.3.7	The security capabilities SHALL be uploaded to the catalogue as a pre-packaged bundle containing its basic dependencies. Any external dependency SHALL be provided before its uploading to the Catalogue.	*Description of Action.*
R1.3.9	The platform SHOULD be able to monitor the deployed security capabilities and expose such data through programming interfaces for other internal components.	*Technical Questionnaire: question 5.*
R1.3.10	The platform SHALL be able to deploy security capabilities from the Catalogue to operate with a copy of network data (off-the-path traffic).	*Technical Questionnaire: question 14.*
R1.3.11	The platform MAY be able to deploy security capabilities from the Catalogue to operate with online network data (on-the-path traffic).	*Technical Questionnaire: question 14.*
R1.3.14	The platform SHALL be able to retrieve the basic status for the security capabilities instantiated or available (in the Catalogue).	*Description of Action.*
R1.3.15	The platform SHOULD be able to decide whether to reuse existing security capabilities or if new ones have to be instantiated, according to the received policy specifications.	*Description of Action.*

R1.3.16	The platform SHOULD implement SDN technology in conjunction with NFV technology to facilitate the provision of SecaaS solutions	*Technical Questionnaire: question 7.* *All use cases.*

2.1.4. Threat Intelligence (TI)

The Threat Intelligence component complements the protection provided by the SecaaS Capabilities with advanced analytics mechanisms based on Machine Learning and Deep Learning to detect cybersecurity threats and provide intelligible suggestion to address them.

This component is divided in three modules:

- Distributed Collectors.
- Multi-Modal Machine Learning.
- Remediation & Recommendation.

The **Distributed Collectors** are in charge of collecting network data from heterogeneous sources ranging from the physical infrastructure (e.g. routers, switches and compute clusters) up to the virtualised security services running on top of it. Input data comes in different formats (e.g. network flow data, events and logs) and needs to be efficiently collected by a set of agents, pre-processed and anonymised in real-time in a format suitable for the ingestion by the Multimodal Machine Learning module. In addition, the data is stored in a distributed file system.

The **Multi-Modal Machine Learning** module is responsible for the implementation of Anomaly Detection methods based on Machine Learning (ML) and Deep Learning (DL) techniques. Different modalities of data coming from different sources (e.g. traffic flows information, network topologies and logs) are combined together into a unified representation scheme, i.e. a Knowledge Graph, which allows to apply feature extraction methods to automatically select the most important features from the data and to adopt advanced ML/DL techniques to detect complex cyber-attacks. Once anomalies are detected, a further step is taken to classify the specific network threat. Finally, by adopting a hybrid approach, these novel analytics-based methods are simultaneously combined together and with more traditional signature-based intrusion detection systems (deployed as SecaaS). The outcomes of the different methods are aggregated and reported to the Remediation & Recommendation module.

The **Remediation & Recommendation** module is in charge of defining mitigation recommendations based on the results of the previous module. The outcome of this module is the generation of a set of high-level policies to address a specific network security threat which are then translated to a set of medium-level policies (i.e. a set of security requirements) to configure the appropriate VNFs together with their suggested order of deployment. The generated medium-level policies undergo a conflict analysis against inconsistencies or non-enforceable policies and a report is provided either to an administrator or to an automatic system to solve them.

Table 9: Requirements related to the Threat Intelligence component

Req. ID	Requirement description	Origin of requirement
R1.1.3	The platform MUST provide near-real-time (NRT) data processing functionalities.	*Technical Questionnaire: question 16.* *Description of Action.*
R1.3.29	The platform SHOULD prevent and react against Ransomware attacks	*Technical Questionnaire: question 5.* *All use cases.*
R1.4.6	The platform SHOULD provide an AI based solution to deliver services, and be shared across the plain field; however, the data-sharing must ensure anonymity.	*End-user Questionnaire: question 36 and 37.* *All use cases.*

R1.5.1	The platform SHALL be able to collect and analyse events from heterogeneous sources in near real time in order to detect security incidents	*Technical Questionnaire: question 12 and 14.* *All use cases.*
R1.5.2	The platform SHALL be able to analyse and combine different modalities of data to detect anomalies in nearly real time	*Technical Questionnaire: question 13, 14 and 16.* *All use cases.*
R1.5.3	The platform SHALL be able to automatically classify the type of anomaly/threat and to share the intelligence information in a standard format	*End-user Questionnaire: question 29.* *Technical Questionnaire: question 31.* *All use cases.*
R1.5.4	The platform SHALL be able to analyse an attack report to produce an ordered set of suggested actions (e.g. VNFs configuration) to mitigate the attack	*Technical Questionnaire: question 19 and 20.* *All use cases.*
R1.5.5	The platform SHOULD provide analytics able to detect the most common threat types (malware, MitM, volumetric attacks).	*End-user Questionnaire: question 3.* *Technical Questionnaire: question 17.*
R1.5.6	The platform SHOULD provide analytics able to detect phishing attacks.	*End-user Questionnaire: question 3.*
R1.5.7	The data involved in the analytics processes MUST be anonymized.	*End-user Questionnaire: question 36.* *Description of Action.*
R1.5.8	The platform SHALL provide periodic retrain functionalities for its analytics components (e.g. on a monthly basis).	*Technical Questionnaire: question 15.*

2.1.5. Trust, Attestation and Recovery (TAR)

The Trust, Attestation and Recovery component is responsible for continuously monitoring the PALANTIR's Security Capability Hosting Infrastructure to detect signs of attacks or erroneous behaviour. The TAR is also leveraged by the Security Capabilities Orchestration to ensure no untrusted node or capability is used to enforce the PALANTIR SecaaS solution. Upon detection of an issue, the TAR orchestrates its recovery, for example by requesting isolation of a node of termination of a capability.

Subcomponents

The TAR achieves its role in the PALANTIR architecture through three subcomponents, each implementing specific functions:

- The **Attestation Engine** monitors SCHI by leveraging the Trusted Computing paradigm and extending it with runtime verification. Trusted Computing as the security paradigm, promoted by the Trusted Computing Group (TCG) [16] that builds on roots of trust (RoT) to protect critical data (e.g. cryptographic keys, secrets) and to detect subversion of the hardware, firmware, software or configurations.
  In Trusted Computing, any firmware or software component is responsible for measuring any code or data that is security critical and to record the measurement in a RoT. This recursive architecture stops at the initial boot vector of a platform and the RoT, which together are called

the Trusted Computing Base: the minimal set for component that are inherently trusted because their misbehaviour cannot be detected (i.e. they are not measured before being used). When the TAR wants to verify the integrity of a platform, the RoT is queried to securely retrieve the list of measurements recorded since boot. Then the TAR compares this list of measurements with the expected software and configuration of the platform: an incorrect, missing or additional measurement evidences an unexpected security posture of the platform: this protocol is called remote attestation. This trust and attestation solution can be implemented using a Trusted Platform Module (TPM) [17] as the RoT, leveraging the Measured Boot feature of UEFI [18] and the Grub2 bootloader [19], and the Linux Integrity Measurement Architecture [20] on the platforms of the SCHI.

While Trusted Computing mainly focuses on boot- and load-time measurement, coupled with periodic remote attestation, PALANTIR also supports runtime verification. The TAR leverages the memory inspection capability of the platform, when present, to detect any unexpected change of code or data already loaded in memory.

Finally, the TAR verifies the hardware of the platforms by ensuring that their components have not been changed since manufacture – unless an authorised hardware modification happened. While such verification can be done through manual inspection of the platforms, the TAR automates such verification by leveraging emerging technologies in that field, such as TCG Platform Certificates [21] or the DMTF (formerly known as the Distributed Management Task Force) Security Protocol and Data Model (SPDM) [22].

- The **Fault and Breach Management** integrates and connects the PALANTIR's security information and event management (SIEM) with an available mitigation services by delivering an Incidence Response (IR) engine. Security incidents often expose critical security vulnerabilities that security operators have to address [23]. While SIEM helps to detect suspicious activity or behaviour of the system (threats/attacks/faults) the aim of IR is to is to identify an attack, contain the damage, and eradicate the root cause of the incident by, triggering mitigation policies (e.g. blocking the source, isolating the exposed part of the infrastructure) and delivering a baseline to implement policy changes to prevent future incidents. Namely, a cyber incident, occurs mainly unannounced, and abrupt thus responding to it quickly reduces losses, restore processes and services, and mitigate exploited vulnerabilities [24]. Thus, IR takes place under considerable time pressure in a dynamic and rapidly changing organizational environment with high levels of information load, information diversity and task uncertainty [25].

  Overall, IR requires command, control and coordination of diverse people, processes, and technologies to develop situation awareness of the threat and incident environment within a rapidly evolving organizational context. However, Information Technology (IT) support is often seen a cost-centre rather than revenue generator. As a result, organizations often focus on operational objective of IT continuity rather to defending the information resources [26]. The organizations most often invest into a metaphorical ''shield'' a SIEM which consists of: formal controls (e.g., risk management, policy, and procedures), informal controls (e.g. training), technological controls (e.g., firewalls, intrusion detection systems, anti-virus software, layers of encryption), physical controls, administrative controls (e.g. ISO/EIC 27001 [45], NIST 800–53 [46]) and regulatory frameworks (e.g. GDPR, PCI-DSS [44], SOX [42], HIPAA [43]). Since, from time to time this shield may fail, the role of IR to restore the integrity of the shield by detecting the occurrence of an incident, containing the impact of the incident as much as possible, and eradicating the threat from the organization [27]. Due primarily to resourcing constraints, incident response teams in micro, small to medium sized organizations tend to be created in an ad hoc and reactive manner, at the time the incident is detected, from non-dedicated employees with some computer skills [28]. Large and well-resourced organization, on the other hand, particularly in the finance, telecommunications and defence sectors are likely to have a Security Operations Center (SOC) for continuous monitoring, analysis and response to security incidents across a large attack surface (networks and systems, servers and databases, network and wireless access points) [29]. However, for these actions to be effective, organizations need significant Situation Awareness of the threat environment as well as the attack surface (organizational assets and operations).

PALANTIR adopts the linear and plan-driven process models to deliver semi-automatic IR model [30], especially designed to mitigate the capital expenditures (CAPEX) as the main constraint of adapting effective IR strategies in highly dynamic and dense socio-technical environments [31]; with situational awareness as the main complexity in both large industry and SME/ME environments. It consists of sequential stages. In the first stage, **Prepare**, the security operators (or SOC teams) prepare the target environment by building the requisite technological toolkits, response processes, and governance structures (e.g. policies, accountability). To mitigate the CAPEX PALANTIR provides Risk Analysis Framework, which exploits similarity of business and already report threats (threat sharing mechanism) to: i) personalize process for the targeted entity and ii) minimize the cost of the process specifically when targeting MEs/SMEs. Once an incident is detected by PALANTIR's Security Orchestration components (second stage, **Identify**), the PALANTIR's IR platform automatically triggers a policy, predefined in stage 1, to contain the incident from causing further impact to the organization. To deliver the platform, PALANTIR adopts the concept of Decision Support Systems (DSS) and existing, open source frameworks such as: TheHive [37], MIG [38], AlienVault [39], Cyphon [40], and SIFT [41]. In the case of high severity incidents, this step may involve taking mission critical systems offline. Since, in the step 3, **Eradication**, the IR team to identify and remove the root cause of the incident (e.g. malware in organizational networks and systems), the DSS must implement messaging system to alter the targeted stakeholders (i.e. admin, operator, owner, etc.) and provide means to analyse and 'visualize' the incident. After the threat or incident was completely handled the IR engine must allow the IR teams to restore IT services to their routine operations in stage 4, **Recovery**. Finally, in stage 5, **Follow up**, the IR teams can reflect on the incident handling experience where 'lessons learned' are incorporated into standard operating procedures. The IR teams can also exploit threat sharing process to improve polices by exploiting successful polices already deployed in production environments and also to contribute with their solutions and strategies.

- The **Recovery Service** ensures the resilience of the SCHI by orchestrating the recovery actions required once a platform, or capability, become untrusted or when a fault or breach is detected. The recovery strategies are manifold and diverse in their nature: a platform can be rebooted or isolated by re-routing the network traffic around it, a Security Capability can be implemented using a different solution or re-configured, etc. Such scope of recovery actions requires a flexible way of selecting the desired recovery strategy for each situation, by using configurable playbooks for example.

Table 10: Requirements related to the Trust, Attestation and Recovery component

Req. ID	Requirement description	Origin of requirement
R1.3.30	The platform SHOULD provide network isolation for compromised systems.	*End-user Questionnaire: question 28.* *All use cases.*
R1.4.1	PALANTIR SHOULD deploy mechanisms for the periodic attestation of the platform and the running applications', services' and configurations' integrity.	*End-user Questionnaire: question 27 and 35.* *Technical Questionnaire: questions 5 and 6.*
R1.4.2	PALANTIR SHOULD recover from threats on the Security Capability Hosting Infrastructure.	*End-user Questionnaire: question 35.*
R1.4.3	The platform SHOULD be able to identify and isolate network segments, data or equipment at risk and enable automatic redundancy and (offline) data backup service to prevent	*End-user Questionnaire: question 3, 17, 21, 22 and 28.* *Use case 1 and 2.*

	corruption or loss of data. The risks are recognised complex reflected primarily in unexpected/unusual behaviour.	
R1.4.4	The platform SHOULD be able to collect and analyse the status and health of the underlying infrastructure, including components at risk due to improper communication security (i.e. no or weak encryption), weak passwords, or irregular updates.	*End-user Questionnaire: question 18, 19 and 26.* *All use cases.*

2.1.6. Risk Analysis Framework (RAF)

PALANTIR provides a risk-based assessment similar to the ENISA SME framework [36], which allows the client to know the risks associated with its information systems, network, components, architecture, etc. In this sense, a risk assessment approach needs to be selected and established in order to find, design, develop and deploy the required mechanisms that allow PALANTIR to perform a correct risk-based analysis. The approach is described in detail in D2.2.

In this document, a set of requirements is defined based for the RAF of PALANTIR. This set of requirements is based upon the use cases and is abstracted to address PALANTIR architecture in a holistic manner. Specific use case requirements per scenario and test bed are defined in detail in D2.2.

Table 11: Requirements related to the Risk Analysis Framework component

Req. ID	Requirement description	Origin of requirement
R1.2.7	The PALANTIR eco-system SHALL be able to publish security KPI measuring the compliance of stakeholder with their Security Level Commitments.	*All use cases.*
R1.2.10	The PALANTIR platform SHOULD provide risk profiling and assessment for a set of input attack surfaces provided from the corresponding stakeholder.	*All use cases.*
R1.2.11	The PALANTIR platform SHOULD support management capabilities for the vulnerabilities of the system under test.	*All use cases.*
R1.2.12	The PALANTIR platform SHOULD provide coherent mitigation plans for corresponding threat and attack vectors.	*All use cases.*
R1.3.31	The platform SHOULD provide a service supporting risk assessment framework	*End-user Questionnaire: question 21.* *Technical Questionnaire: question 7.* *All use cases.*
R1.4.5	The platform SHOULD provide a solution to deliver an incidence response plan tailored to specific end-user.	*End-user Questionnaire: question 32, 33 and 34.* *All use cases.*

2.1.7. PALANTIR Portal

In the PALANTIR platform, the **Portal** allows access to front-end elements of PALANTIR components that regard the entire project. The dashboard's instances provide access to different elements, depending on the type of users. Secondly, the Security Dashboard provides views for actions at "operation time", in real-time, such as a view of alerts that are triggered by the TI, the TAR and event notifications generated by the Security Capabilities. The Security Dashboard also enables the SecaaS clients to review threat data and policies that are shared between different users, in order to build services tailored to their needs via a wizard-like environment. The Security Dashboard environment also provides a unified incident view (fusing information from multiple SMEs/MEs). Generally, the Security Dashboard includes all threat sharing and reporting capabilities, to provide views tailored to each stakeholder.

Subcomponents

The PALANTIR Portal implements the aforementioned functionality through some subcomponents, with the most important functionality being the real-time information stream, which depicts the current status of the infrastructure as well as any identified problems and alerts in real-time. Integration in this case is of utmost importance, as most components have some interaction with the portal and its related subcomponents. A draft of the foreseen subcomponents for the PALANTIR portal and Security Dashboard is shown, as they are subjects to changes as both consensus within the project as well as development, testing and integration progress. These subcomponents are listed below:

- **Central Portal and Security Dashboard User Interface (UI)**: The central Portal is the entry point for the project's UIs. Through it, and depending on the user, views from the various implemented tools and mechanisms become accessible. These views include risks identification, analysis and management aspects, policy definition aspects, infrastructure management and orchestration aspects and billing, account and performance visualisation aspects. These views are combined in the Security Dashboard UI. Some key kinds of views in the dashboard UI are accounting views for tracking of profits, costs and purchases, and the visualisations of security analytics.
- **User management** component: In order to achieve access control as well as the differentiation of views per stakeholder, a user management component is in place. Users, access control lists, and roles are kept in this subcomponent.
- **Indicators of Compromise (IoC) Database**: This subcomponent exposes an IoC database, which allows for storage and communication of technical and non-technical information about malware samples, incidents, attack patterns, defence intelligence and attacker profiles. The IoC database can store all such information in standardized formats, such as Structured Threat Information Expression (STIX) [34] or Trusted Automated Exchange of Intelligence Information (TAXII) [35].
- **Correlation mechanism**: Automatic correlation mechanism that, by discovering relationships between attributes, can help when similar situations occur in different organizations. The attributes that, through correlation, provide recommended solutions, are indicators of malware, incidents, attacker profiles, and security intelligence. This mechanism makes heavy use of the IoC database for both storage and retrieval. This component facilitates knowledge sharing with Computer Emergency Response Teams (CERT) and Computer Incident Response Teams (CSIRT).

Table 12: Requirements related to the PALANTIR Portal component

Req. ID	Requirement description	Origin of requirement
R1.1.1	The platform MUST provide registration and sign-in functionalities for the following roles: users, administrators.	*Description of Action.*
R1.1.2	The platform MUST provide a dashboard in order to present results of analysis.	*Description of Action.*
R1.3.18	The platform SHOULD provide streaming of resource utilization data for billing in the Dashboard	*All use cases.*

R1.3.28	The platform SHOULD provide an interactive workflow to review risks, statistics and security status of a SME	*All use cases.*

2.2.Inter-Component interfaces

Following the PALANTIR architecture and component role's description, this section presents the interaction between the main components of the PALANTIR architecture. It is the starting point of the technical WPs for specifying the interfaces of each component being developed, or used, in PALANTIR.

2.2.1. Security Capabilities Hosting Infrastructure

The SCHI manages the backend intercommunication and hosting capabilities of the PALANTIR component ecosystem. This module interacts with the rest of the PALANTIR platform through the following interfaces/message buses:

- **Data Collector for Threat Intelligence**: This interface provides the endpoint for the PALANTIR Threat Intelligence component to collect underlying monitoring and networking data to use them as input for threat training, and detection. This interface includes the agents running on devices under PALANTIR supervision to monitor their state and risk state.
- **Threat Intelligence Training & Inference**: This interface provides the ML mechanisms running under the Threat Intelligence component to collect the processed data ready to be used either for training, or inference and assess the risk of the infrastructure under test.
- **Security Capabilities Orchestration**: This interface communicates with the SCO component and provides the API binding of a service orchestration solution to the PALANTIR platform.
    - **Security Capability Catalogue**: This interface provides the API for the security service catalogue of the PALANTIR platform in the frame of SCO component.
- **Attestation Data Collector**: This interface collects the attestation monitoring data for the Trust, Attestation and Recovery component.
- **Attestation Agents**: This interface provides the API for attestation agents to connect to the PALANTIR platform and report the attestation state.
- **Risk Auditing Probes**: This interface collects the risk assessment reports for the corresponding use cases running, so as to be processed by the Risk Analysis Framework component.

2.2.2. Security Capabilities

The PALANTIR SecaaS Capabilities needs the interaction and coordination of different PALANTIR components, as well as the collaboration with them to obtain different data sources and improve the SecaaS capabilities functionality. The SecaaS component interacts with the components presented in Figure 10:

- The **Threat Intelligence** component offers advanced analytics capabilities based on Machine Learning and Remediation techniques. The communication between this component and SecaaS component is performed with a *Control Loop* where TI component traces traffic from the SecaaS capabilities through *Distributed Collection* for signs of malicious traffic.
- The SecaaS component needs to be orchestrated and managed by a component with the necessary requirements to perform this task. The **Security Capabilities Orchestrator** manages different necessary SecaaS capabilities characteristics for the correct functioning, such as its *lifecycle management*, the *SecaaS services monitoring* and the *SecaaS services deployment* on-demand considering the real-time context information. The communication is also produced with a *Control Loop* and is performed when malicious traffic is detected, and selected actions must be executed with the SecaaS capabilities.
- The SecaaS capabilities can detect anomaly activities produced in the PALANTIR client, when these actions are identified, security notifications are created and transmitted to the **PALANTIR**

Portal. This interaction is necessary to notify the client of dangerous activities in the environment concerned.

2.2.3. Security Capabilities Orchestration

When obtaining specific information within the PALANTIR platform, the following subcomponents inside SCO are expected to interact with a number of PALANTIR components.

SCO interacts with:

- The **Threat Intelligence** component, which ingests information from the environment and models behaviours based on Machine Learning to identify potential threats. The remediation recommendations are then provided to the SCO in order to be applied or enforced as a way to mitigate such threats.
- The **Trust, Attestation & Remediation** component, in charge of performing periodic attestation of different hardware and software nodes so as to identify possible untrusted states. If such situation occurs, the SCO obtains specific security controls, configurations or policies that are to be translated in order to configure the security capabilities for proper use.
- The dashboards, accessible through the **PALANTIR Portal** and able to show cybersecurity alerts, the status of the running services and other information. The SCC subcomponent also uses the Portal to present its UI to the PALANTIR users, based on their account's role.

SCC interacts with:

- The **Accounting and Security dashboards**, accessible through the **PALANTIR Portal**: the portal can also be used to provide access to the SCC, based on the user account's role, to expose a set of UIs for PALANTIR with, among others, features related to the catalogue. The user account control is basically part of this component, and the SCC uses it as well.
- The **Risk Analysis Framework** component: the security/privacy threats are identified based on impact assessment and its correlation with attack surface analysis. The overall risk is to be tracked and managed in a dynamic scenario where threat intelligence is updated. Such information should be useful for the SCC, so as to obtain the suitability of a service and the way it can minimize risk by being deployed on the network in each case, and thus creating recommendations for service deployment, and sorting the catalogue of services according to each user's needs.

Besides the interactions with other PALANTIR components, the SCC interacts with the SO subcomponent so that the latter can obtain the service packages, potentially their metadata and possibly instructions on security service graphs to be deployed - as well as the SO providing basic deployment status information.

Finally, SCO also interfaces against 3rd-party tools providing extra functionality but alien to the PALANTIR platform, such as the VIM and SDN controller or the MANO NFVO

2.2.4. Threat Intelligence

The Threat Intelligence component communicates mainly with the **Security Capabilities** and the Security Capabilities Orchestration components creating a control loop. Threat Intelligence's Distributed Collectors module traces traffic from the network and the VNFs (i.e. from the Security Capability Hosting Infrastructure), analyses it for signs of malicious activity and outputs the detected anomalies to the Remediation & Recommendation module. The reactive measures to the cyber threats are then sent to the **Security Capabilities Orchestration** component, whose Security Orchestrator and Capability Management module pushes selected actions back to the Security-as-a-Service component.

Another inter-component communication is required for the sharing of threat data and remediation options, via the provider, with the other SecaaS clients. The Threat Intelligence component thus communicates also with the **PALANTIR Portal** component. Threat Intelligence data is shared using

STIX format, while remediation policies adopt the Medium-level Security Policy Language (MSPL) and High-level Security Policy Language (HSPL) formats.

2.2.5. Trust, Attestation and Recovery

The TAR works in collaboration with most of the other components in the PALANTIR architecture, either to attest them, to leverage them for fault management, to retrieve the expected state of the attested components or to orchestrate recovery once an issue has been found for example.

- **Security Capabilities Hosting Infrastructure**: The TAR interacts with the SCHI's devices mostly to run the remote attestation protocols, which retrieve the attestation proof from the RoT. Therefore, the TAR requires a communication channel with each individual attester (the platform being attested), more precisely with the RoT of the attester. From an architecture standpoint, there is no constraint outside of having a communication channel as it can be secured end-to-end between the RoT, which holds a private key and associated certificate, and the TAR. Moreover, the communication can be either a push - from the attester to TAR, or pull - from the TAR out of the attester – model; this is depending on the protocol implementation.
- **Security Capabilities Orchestration**: As the SCO is responsible for managing and deploying Security Capabilities over the SCHI, it is a critical partner component of TAR: the orchestration information is used by TAR to understand the infrastructure topology and how the Security Capabilities are deployed. The interface between the two components is also used by TAR to notify SCO about the recovery actions that need to be put in place. Within SCO, the Security Capability Catalogue is leveraged by TAR to retrieve the expected measurement used to attest the deployed services.
- **Threat Intelligence**: TAR outputs metadata into the TI component, to be consumed there by the different analytic algorithms being used. Examples of metadata are the attestation results for the platform of SCHI, the attestation results for the Security Capabilities, the Fault or Breach detected, the Recovery actions. The TI could use the attestation results with other evidences to detect attacks such as Advanced Persistent Threat.
- **PALANTIR Portal**: TAR uses the Portal to present the security alerts and notifications related to the attestation or fault and breach management capabilities of the TAR. The Portal is also used to present the recovery actions – either recommended or applied – to the PALANTIR administrator. Access to the audit trails of TAR is one of the features that are exposed to the operators through the Portal.

2.2.6. Risk Analysis Framework

PALANTIR can design and implement different risks profiles, which adapts to the client needs. The risk profile selection is joint to the critical assets' identification, the unique step with more human interaction, since the client should enumerate the assets found in its organisation. The last two phases are designed and deployed with the tools like the one provided by NIST (the US' National Institute of Standards and Technology), due to the selection, implementation and management of the security controls applied with the results of the first two phases.

The corresponding interfaces of the Risk Analysis Framework are:

- **PALANTIR Portal**: The Risk Analysis Framework assess the risk of the underlying test case and generates a report. This report is communicated to the portal of the platform so as the PALANTIR provider can access the risk assessment in a visualized manner.
- **Security Capabilities Hosting Infrastructure**: This interface refers to the communication with the RAF endpoint and collects from it the necessary information for the generation of the report.

2.2.7. PALANTIR Portal

The UIs of the PALANTIR portal are essentially the "face" of other important components of the PALANTIR platform. Eventually, most components are in fact somehow connected to the dashboards.

As such, the PALANTIR Portal and Security Dashboard is expected to interact at least with the following components, using message queues or data buses:

- **Security Capabilities Catalogue**: The Accounting Dashboard provides access to the Service Catalogue, when an authorized user is logged in.
- **Risk Analysis Framework**: The security/privacy threats are identified based on impact assessment and its correlation with attack surface analysis. The overall risk is to be tracked and managed in a dynamic scenario where threat intelligence is updated. This information is sent to the security dashboard, as both a risk assessment view, and warnings/notifications.
- **Security Capabilities Orchestration**: Supplementary information by the security orchestrator is used by the dashboards. Moreover, the user account management subcomponent is utilized by the orchestrator. Finally, the orchestrator is responsible for the routing of the information from each security service to the appropriate dashboard view in the PALANTIR Portal. Finally, a basic overview of the running services is provided from the Security Orchestrator to the Portal.
- **Security Capabilities**: Monitoring data, security analytics, inferences from intelligent security services, alerts and notifications, are all sent to the security dashboard. As such, each security service defines the data it provides to the Portal, along with an accompanying view (UI) that is specific to it. As such each package of a security service, should also contain the aforementioned definitions.
- **Threat Intelligence**: The Threat Intelligence is meant to forward all threat findings to the PALANTIR Portal. The portal shows an alert, and the information regarding the detected threat becomes accessible to the portal’s user.

Conclusions

This document defines the initial requirements and overall architecture for the PALANTIR platform; all partners contributed to this work and the content of this document drives the first iteration of the implementation of the different components. A second iteration of WP2, particularly T2.1, produces an updated version of this document, which is "D2.3. Requirements & high-level design – Final". D2.3 takes into account the feedback from the initial implementation work of the different components to address any gap that the partners find during the first half of the project.

The requirements are derived from two online questionnaires and their analysis performed by the consortium. One questionnaire targets the potential end users of PALANTIR to gather both their technology and business expectations; the other questionnaire focused on technical subject matter experts to advise the project on technology choices. Partners from the consortium analysed the use cases presented in the Description of Action and the law and regulations that apply to PALANTIR to define additional requirements for the technical solution. This document specifies around 90 requirements for PALANTIR.

Then, this document refines the conceptual architecture from PALANTIR's Description of Action to create a block diagram architecture that drives the implementation WPs. Each component's role in the overall architecture is described and the interactions between components are detailed. The specific requirements that apply to a given component are also listed.

This deliverable equips the technical partners with the overall PALANTIR architecture and the requirements that each component must meet for PALANTIR to succeed.

References

[1] T. L. Saaty, “A scaling method for priorities in hierarchical structures,” *J. Math. Psychol.*, 1977, doi: 10.1016/0022-2496(77)90033-5.

[2] A. M. A. Bahurmoz, “The Analytic Hierarchy Process at Dar Al-Hekma, Saudi Arabia,” *Interfaces (Providence).*, 2003, doi: 10.1287/inte.33.4.70.16374.

[3] A. Kengpol and C. O’Brien, “Development of a decision support tool for the selection of advanced technology to achieve rapid product development,” *Int. J. Prod. Econ.*, 2001, doi: 10.1016/S0925-5273(00)00016-5.

[4] G. Noci and G. Toletti, “Selecting quality-based programmes in small firms: A comparison between the fuzzy linguistic approach and the analytic hierarchy process,” *Int. J. Prod. Econ.*, 2000, doi: 10.1016/S0925-5273(99)00131-0.

[5] M. M. Albayrakoglu, “Justification of new manufacturing technology: A strategic approach using the analytical hierarchy process,” *Prod. Invent. Manag. J.*, 1996.

[6] R. W. Saaty, “The Analytic Hierarchy Process: Planning, Priority Setting, Resource Allocation (Decision Making Series),” *Math. Model.*, 1980.

[7] G. Dede, T. Kamalakis, and D. Varoutas, “Evaluation of optical wireless technologies in home networking: An analytical hierarchy process approach,” *J. Opt. Commun. Netw.*, 2011, doi: 10.1364/JOCN.3.000850.

[8] G. Dede, T. Kamalakis, and D. Varoutas, “Towards a roadmap for future home networking systems: An analytical hierarchy process approach,” *IEEE Syst. J.*, 2011, doi: 10.1109/JSYST.2011.2158683.

[9] S. Nikou, J. Mezei, and H. Bouwman, “Analytic Hierarchy Process (AHP) approach for selecting mobile service category: (Consumers’ preferences),” 2011, doi: 10.1109/ICMB.2011.29.

[10] Q. Song and A. Jamalipour, “Network selection in an integrated wireless lan and UMTS environment using mathematical modeling and computing techniques,” *IEEE Wirel. Commun.*, 2005, doi: 10.1109/MWC.2005.1452853.

[11] RFC2119: Key words for use in RFCs to Indicate Requirement Levels, Network Working Group IETF.

[12] Cloud Security Alliance – SecaaS definition

[13] Ray, Partha Pratim. An introduction to dew computing: definition, concept and implications. IEEE Access, 2017, vol. 6, pp. 723-737.

[14] ETSI NFV-SEC013: Security Management and Monitoring specification

[15] IETF Interface to Network Security Functions (I2NSF) WG

[16] Trusted Computing Group.

[17] TCG Trusted Platform Module Library Specification, Family “2.0”, Trusted Platform Module Working Group, TCG.

[18] TCG PC Client Specific Platform Firmware Profile Specification, PC Client Working Group, TCG.

[19] GNU GRUB Measured Boot, GNU.

[20] Linux Integrity Measurement Architecture.

[21] TCG Platform Certificate Profile, Infrastructure Working Group, TCG.

[22] Security Protocol and Data Model (SPDM) Architecture, Security Task Force, DMTF.

[23] Vallentin, M., Paxson, V., & Sommer, R. (2016). VAST: A Unified Platform for Interactive Network Forensics. In 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI'16) (pp. 345-362).

[24] Onwubiko, C., & Ouazzane, K. (2020). SOTER: A playbook for cybersecurity incident management. IEEE Transactions on Engineering Management.

[25] J. Steinke, B. Bolunmez, L. Fletcher, V. Wang, A.J. Tomassetti, K.M. Repchick, S.J. Zaccaro, R.S. Dalal, L.E. Tetrick: Improving cybersecurity incident response team effectiveness using teams-based research, IEEE Secur. Priv., 13 (4) (2015), pp. 20-29.

[26] A. Ahmad, J. Webb, K.C. Desouza, J. Boorman Strategically-motivated advanced persistent threat: definition, process, tactics and a disinformation model of counterattack. Comput. Sec., 86 (2019), pp. 402-418.

[27] Ahmad, A., Maynard, S. B., Desouza, K. C., Kotsias, J., Whitty, M. T., & Baskerville, R. L. (2021). How can organizations develop situation awareness for incident response: A case study of management practice. Computers & Security, 101, 102122.

[28] A. Ahmad, J. Hadjkiss, A.B. Ruighaver: Incident Response Teams - Challenges in Supporting the Organizational Security Function, Comput. & Sec., 31 (5) (2012), pp. 643-652.

[29] E. Agyepong, Y. Cherdantseva, P. Reinecke, P. Burnap Challenges and performance metrics for security operations center analysts: a systematic review J. Cyber Sec. Technol. (2019), pp. 1-28.

[30] P. Cichonski, T. Millar, T. Grance, K. Scarfone. Nist Special Publication 800-61, Revision 2: Computer Security Incident Handling Guide NIST, US Department of Commerce (2012).

[31] C. Macabante, S. Wei, D. Schuster. Elements of cyber-cognitive situation awareness in organizations, Proceedings of the Human Factors and Ergonomics Society Annual Meeting, SAGE Publications Sage, CA: Los Angeles, CA (2019), pp. 1624-1628.

[32] ETSI NFV-SEC 024: Security Management specification.

[33] P4 Language and Related Specifications, P4 Language Consortium.

[34] Structured Threat Information Expression, Cyber Threat Intelligence Technical Committee, OASIS.

[35] Trusted Automated Exchange of Intelligence Information, Cyber Threat Intelligence Technical Committee, OASIS.

[36] Risk Management, Approaches for SMEs, ENSIA.

[37] The Hive Project.

[38] MIG: Mozilla InvestiGator.

[39] AlienVault, AT&T.

[40] Cyphon.

[41] SIFT, SANS Institute.

[42] Sarbanes-Oxley Act, United States federal law, 2002.

[43] Health Insurance Portability and Accountability Act, United States federal, 1996.

[44] Payment Card Industry Data Security Standard, Payment Card Industry Security Standards Council.

[45] ISO/IEC 27001 Information security management, ISO.

[46] National Vulnerability Database, Special Publication 800-53, NIST.

Annex A.: End-user questionnaire and results collected

The goal of this End-user Questionnaire is to gather advice on the PALANTIR architecture, services, user experience and operational model.

Presentation of PALANTIR

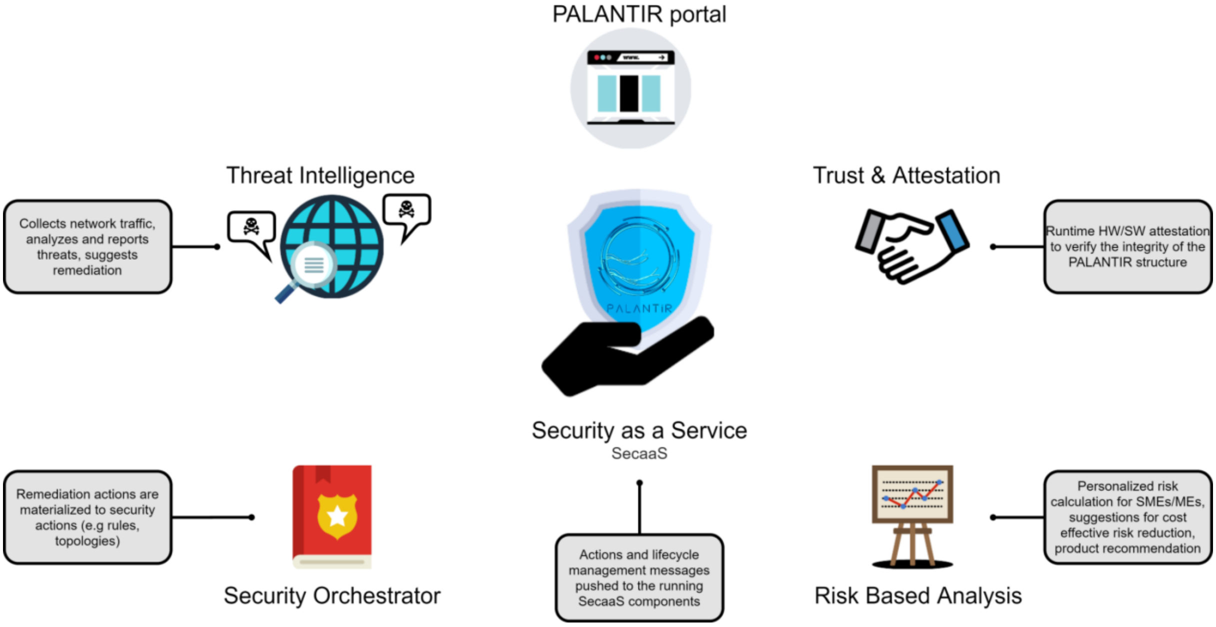

PALANTIR portal
Threat Intelligence
Collects network traffic, analyzes and reports threats, suggests remediation
Trust & Attestation
Runtime HW/SW attestation to verify the integrity of the PALANTIR structure
PALANTIR
Security as a Service
SecaaS
Remediation actions are materialized to security actions (e.g rules, topologies)
Security Orchestrator
Actions and lifecycle management messages pushed to the running SecaaS components
Personalized risk calculation for SMEs/MEs, suggestions for cost effective risk reduction, product recommendation
Risk Based Analysis

Figure 12: Overview of PALANTIR components

Presentation of PALANTIR

Throughout the course of the PALANTIR project, the consortium will create a technical framework enabling the provision of next-generation, cost-effective Security-as-a-Service (SecaaS) services to Small and Medium Enterprises (SME) and Micro-Enterprises (ME), by leveraging novel technologies such as Network Function Virtualisation (NFV), Security Orchestration, Remote Attestation, Machine Learning (ML), Policy-based Remediation and Multi-attribute Risk Assessment. A general vision on the PALANTIR SecaaS platform for cyber-resiliency is depicted in Figure 1, showing the main operational blocks.

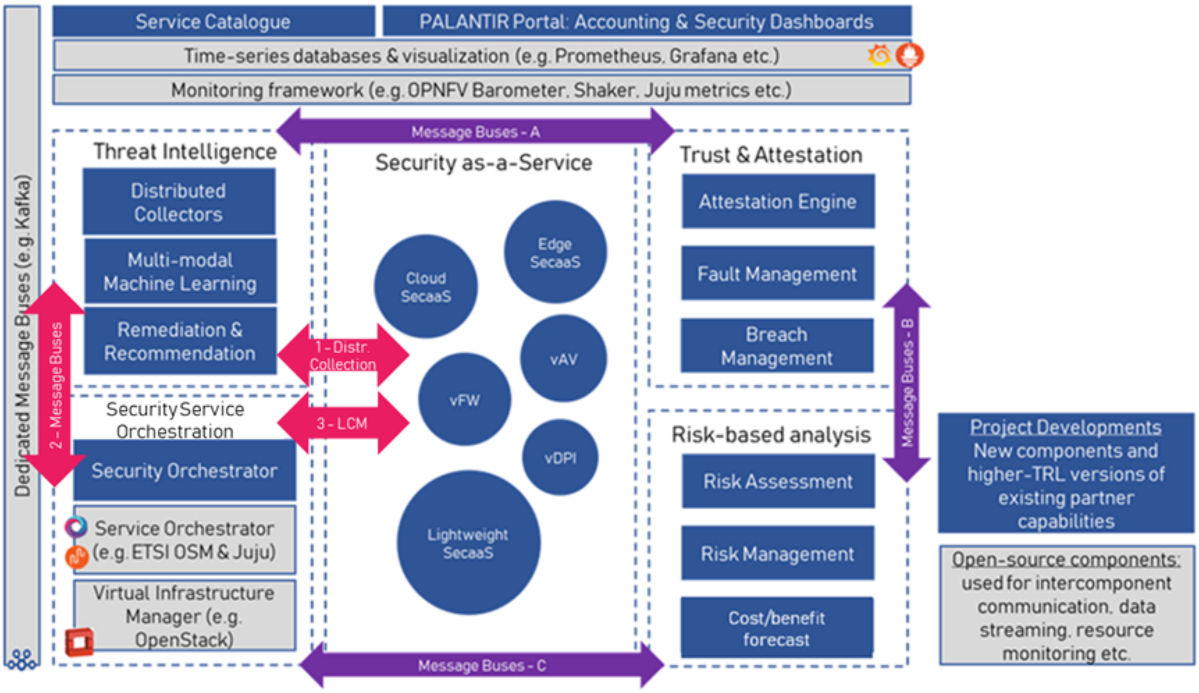

Service Catalogue
PALANTIR Portal: Accounting & Security Dashboards
Time-series databases & visualization (e.g. Prometheus, Grafana etc.)
Monitoring framework (e.g. OPNFV Barometer, Shaker, Juju metrics etc.)
Dedicated Message Buses (e.g. Kafka)
Message Buses - A
Threat Intelligence
Distributed Collectors
Multi-modal Machine Learning
Remediation & Recommendation
2 - Message Buses
Security Service Orchestration
Security Orchestrator
Service Orchestrator (e.g. ETSI OSM & Juju)
Virtual Infrastructure Manager (e.g. OpenStack)
1 - Distr. Collection
3 - LCM
Security as-a-Service
Cloud SecaaS
Edge SecaaS
vAV
vFW
vDPI
Lightweight SecaaS
Message Buses - C
Trust & Attestation
Attestation Engine
Fault Management
Breach Management
Message Buses - B
Risk-based analysis
Risk Assessment
Risk Management
Cost/benefit forecast
Project Developments
New components and higher-TRL versions of existing partner capabilities
Open-source components:
used for intercomponent communication, data streaming, resource monitoring etc.

Figure 13: Overview of the PALANTIR proposed architecture

The security services are hosted on top of a NFV architecture, whose management and orchestration layer is enhanced with a dedicated Security Orchestration and Service Catalogue.

The Threat Intelligence component provides advanced analytics capabilities, based on ML and distributed collectors that can be part of the security services or monitoring the client network. The Remediation and Recommendation Module is responsible for defining the threat mitigation solution; it can deploy new security services or reconfigure existing ones.

The Trust and Attestation component is responsible for monitoring the integrity of the security services – and the underlying hosting infrastructure – to ensure the correct operation of PALANTIR. In case of attack or breach detection, a remediation procedure is deployed, which includes notification if needed.

Use case presentation

The consortium aims at demonstrating the PALANTIR solution in the following 3 use cases:

1. Securing private medical practices with lightweight SecaaS: Private medical practices are prime examples of MEs with high security and data protection needs. Private practices frequently suffer from critical data breaches and the staff is usually not in the position to handle a cyber-attack. PALANTIR will illustrate at minimum two cases of attacks prevented by the Lightweight SecaaS gateway and/or Cloud SecaaS in this use case.
2. Uninterrupted Electronic Commerce with Cloud SecaaS: Small businesses with e-commerce operations are increasingly leveraging cloud services along with local infrastructure for expense savings, yet they do not always ensure that these services use strong online security measures. In this use case, PALANTIR will demonstrate a personalized enterprise grade solution offered to the end-user at affordable cost by minimizing cost of licenses, software and hardware.
3. Live Threat Intelligence Sharing in a large-scale Edge scenario: In this use case, the PALANTIR provider would be able to i) jointly analyse information from multiple clients to detect incidents which would remain unnoticed if each client was treated individually and ii) exploit the live threat intelligence feedback from the community of users directly into the local network of the user, through its provided gateway or in the network infrastructure.

Methodology

The PALANTIR project has identified 5 criteria and their respective sub-criteria that can potentially affect the development and adoption if its proposed services. Please answer the questions using the following instructions:

Each criterion will be rated according to its degree of relative importance to the other criteria within the group using pair wise comparisons to rank them. The method is able to test the consistency of the replies. Please indicate your preference between two criteria by providing a range of values between 0 and 8 [lower bound, upper bound], utilising increments of 1.

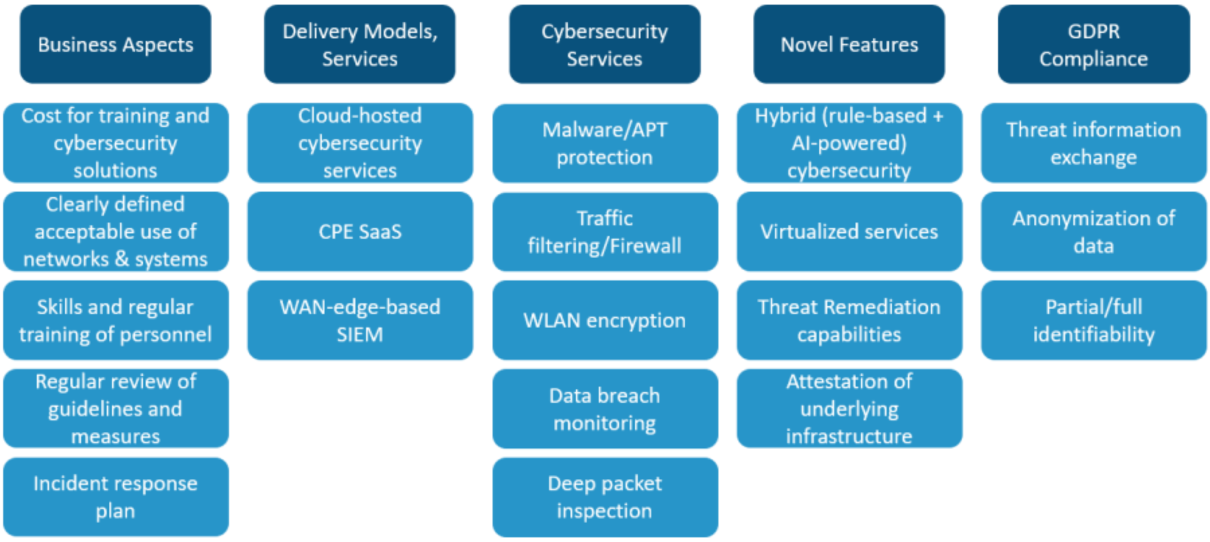
As shown in the table below when two criteria are of equal importance, they should take a score of 0. When one criterion is more important than another criterion, then it should take a score between 2 and 8, depending on how much more important it is compared to the other criterion, with 0 indicating that is much more important.

The scale used to find pair wise relative importance between the different criteria is a nine-point scale as follows:

Importance	Definition	Explanation
0	Equal importance	The two criteria are of equal importance
2	Moderate importance	Experience and judgment favours one criterion
4	Strong importance	One criterion is strongly favoured
6	Very strong importance	One criterion is dominant over the other
8	Extreme importance	One criterion is favoured by at least an order of magnitude over the other
1,3,5,7	intermediate values	Used as a compromise between two of the above numbers

Figure 14: AHP scale definition

The criteria and sub-criteria identified are depicted in the following figure.



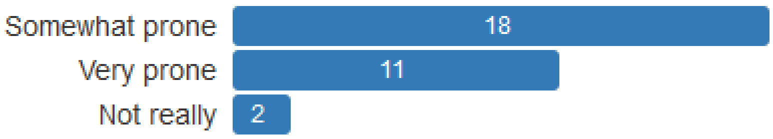
Business Aspects	Delivery Models, Services	Cybersecurity Services	Novel Features	GDPR Compliance
Cost for training and cybersecurity solutions	Cloud-hosted cybersecurity services	Malware/APT protection	Hybrid (rule-based + AI-powered) cybersecurity	Threat information exchange
Clearly defined acceptable use of networks & systems	CPE SaaS	Traffic filtering/Firewall	Virtualized services	Anonymization of data
Skills and regular training of personnel	WAN-edge-based SIEM	WLAN encryption	Threat Remediation capabilities	Partial/full identifiability
Regular review of guidelines and measures		Data breach monitoring	Attestation of underlying infrastructure	
Incident response plan		Deep packet inspection		

Figure 15: Factors affecting PALANTIR adoption and evolution

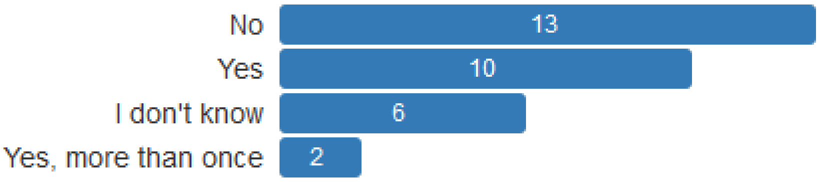
Business-type related questions (13 questions)

Question 1: Do you consider your business sector as being prone to cyberattacks?

Possible responses*: Not really, Somewhat prone, Very prone, I don't know*



Question 2: Has your organisation suffered any cyberattack or other type of security breach over the last two years?
Possible responses: *No, Yes, Yes-more than once, I don't know*



Question 3: Which do you consider the most dangerous type of attack for your organisation?

Possible responses: *Volumetric/DDoS, Man-in-the-middle, APTs, Malware, Phishing, I don't know, Other (Free text option)*

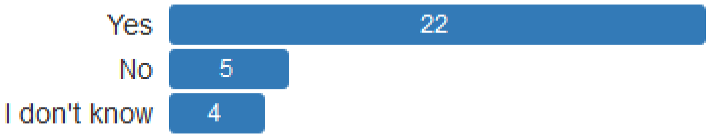
Attack type	Number of answer selection (is considered the most dangerous)	Number of answer deselection (is not considered the most dangerous)
Volumetric/DDoS	10	25
Man-in-the-Middle	10	25
APTs	11	24
Malware	22	13
Phishing	22	13
I don't know	1	35
Other: Ransomware	2	0
Other: Cryptomining	1	0

Question 4: Have you received any notifications and/or complaints with regard to the security of the IT system over the last year?
Possible responses: *Volumetric/DDoS, Man-in-the-middle, APTs, Malware, Phishing, I don't know, Other (Free text option)*

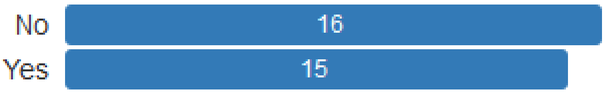
Attack type	Number of answer selection (have received)	Number of answer deselection (have not received)
Volumetric/DDoS	4	25
Man-in-the-Middle	0	29
APTs	2	27
Malware	9	20
Phishing	13	16
I don't know	7	29
Other: No	2	0

Attack type	Number of answer selection (have received)	Number of answer deselection (have not received)
Other: Cryptomining	1	0
Other: Potential open ports and non-up-to-date exposed services	1	0

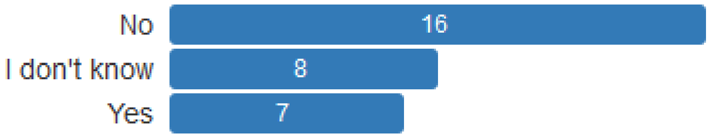
Question 5: Have you determined who is responsible for cybersecurity in your company?
Possible responses: *Yes, No, I don't know, Other (Free text option)*



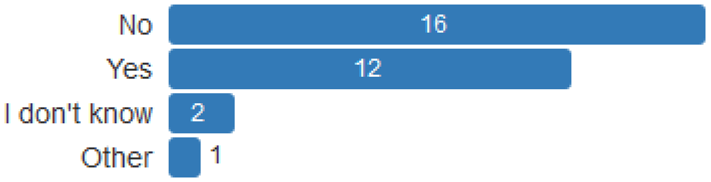
Question 6: Have you applied restrictions to prevent users downloading 3rd party apps?
Possible responses: *Yes, No, I don't know, Other (Free text option)*



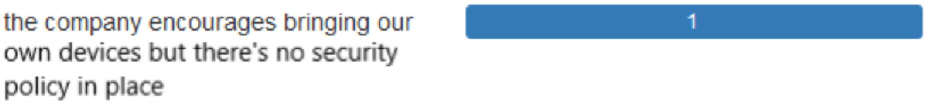
Question 7: Have you ever had a vulnerability assessment or penetration test conducted on your network or websites?
Possible responses: *Yes, No, I don't know, Other (Free text option)*



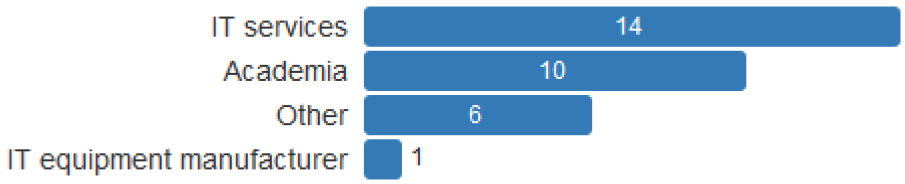
Question 8: Do you have a Bring Your Own Device (BYOD) Policy in place for employees who use personal devices for work?
Possible responses: *Yes, No, I don't know, Other (Free text option)*



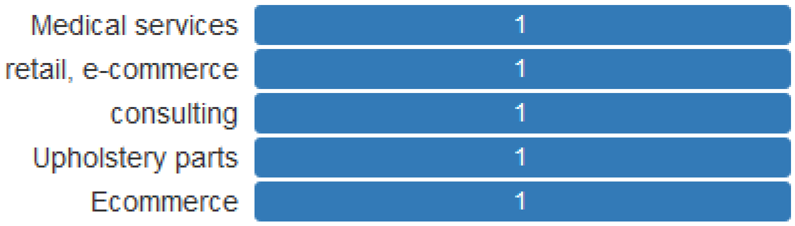
Other responses:



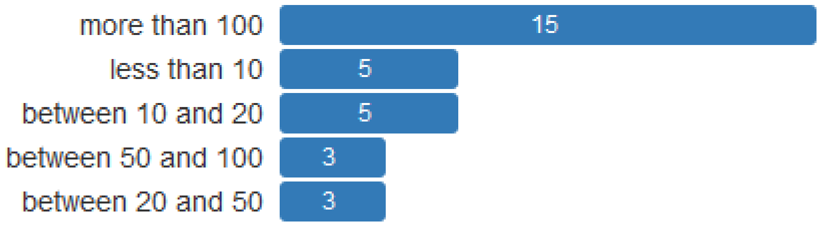
Question 9: What is the business sector of your company?
Possible responses: *IT services, IT equipment manufacturer, Academia, Other (Free text option)*



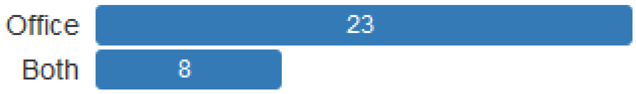
Other responses:



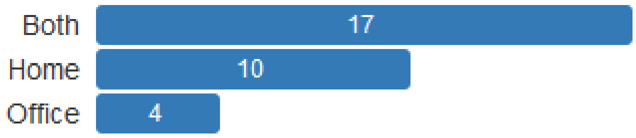
Question 10: How many employees does your company have?
Possible responses: *less than 10, between 10 and 20, between 20 and 50, between 50 and 100, more than 100*



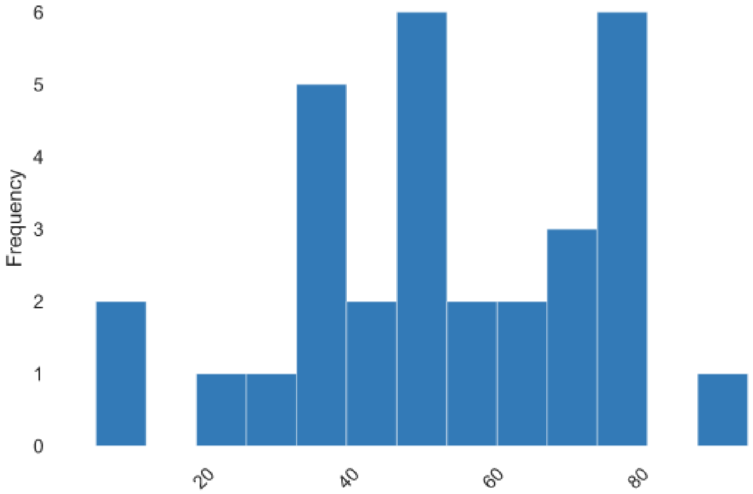
Question 11: Pre-COVID, where did the employee of your company work from (home, office, both, other)?
Possible responses: *Home, Office, Both, Other (Free text option)*



Question 12: Post-COVID, where do you envision the employee of your company will work from (home, office, both, other)?
Possible responses: *Home, Office, Both, Other (Free text option)*

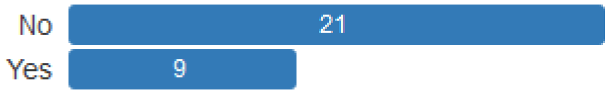


Question 13: What balance would you like between the CAPEX and OPEX costs of the solution? (0% being no CAPEX, 100% being no OPEX)
Possible responses: *Percentage (0-100) %*

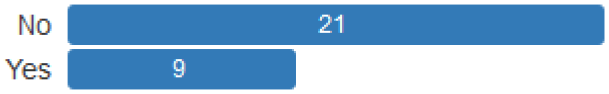


Use case related questions (4 questions)

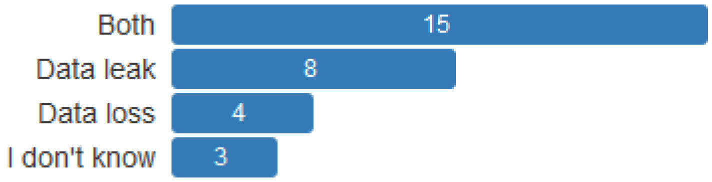
Question 14: Do you offer Open Wi-Fi / Open networks?
Possible responses: *Yes, No, I don't know.*



Question 15: Do you block access to some services, i.e. Google Drive?
Possible responses: *Yes, No, I don't know.*



Question 16: What has a more negative impact for you organisation, data loss or data leak?
Possible responses: *Data loss, Data leak, Both, I don't know.*



Question 17: What are the possible results of an attack on a computer network of your organisation?
Possible responses: *Loss or corruption of sensitive data that is essential for a company's survival and success, Diminished reputation and trust among customers, The decline in value with shareholders, Reduced brand value, Reduction in profits, Other (Free text option)*

Result of an attack	Number of answer selection (is possible result)	Number of answer deselection (is not possible result)
Loss or corruption of sensitive data that is essential for a company's survival and success	23	7
Diminished reputation and trust among customers	20	10
The decline in value with shareholders	6	24
Reduced brand value	11	19
Reduction in profits	9	21

Result of an attack	Number of answer selection (is possible result)	Number of answer deselection (is not possible result)
Other: GDPR risk	1	0

Services related questions (10 questions)

Question 18: How is the following software managed and installed on your organisation's computer system?

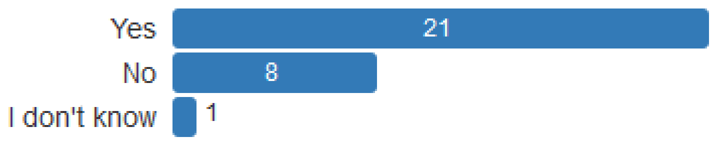
- Firewall
- Updates on the Operating System (e.g., Microsoft Windows)
- Third-party updates (e.g., Adobe, Java)

Possible responses: *Automatically (organisation), Mix of automatic and manual (organisation), Mix of automatic and manual (end-user), Automatic (user), Manual (user)*

Software	Automatically (organisation)	Mix of automatic and manual (organization)	Mix of automatic and manual (end-user)	Automatic (user)	Manual (user)
Firewall	8	14	0	2	6
Updates on the Operating System (e.g., Microsoft Windows)	10	4	3	4	9
Third-party updates (e.g., Adobe, Java)	7	4	1	6	12

Question 19: Is there a separate WLAN for employees and guests?

Possible responses: *Yes, No, I don't know.*



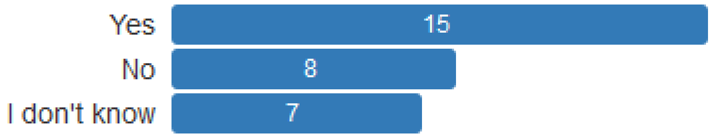
Question 20: How often do you do perform the following?

- Use secure and encrypted communication connections on the Internet
- Perform data backup processes
- Check functionality and readability of the backup
- Change default passwords on networking equipment

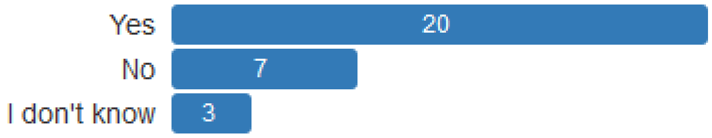
Possible responses: *Never, Seldom, Occasionally, Frequently, Always, N/A*

Activity	Never	Seldom	Occasionally	Frequently	Always	N/A
Use secure and encrypted communication connections on the Internet	0	3	8	11	8	0
Perform data backup processes	1	2	11	9	6	0
Check functionality and readability of the backup	3	10	10	4	1	0
Change default passwords on networking equipment	1	11	9	5	2	0

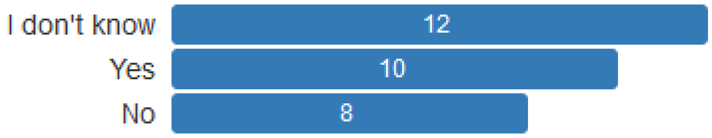
Question 21: Is the storage of the backup physically separate (offline)?
Possible responses: *Yes, No, I don't know.*



Question 22: Is it possible to provide access to an internal personal data processing system through the internet (e.g. for certain users or groups of users)?
Possible responses: *Yes, No, I don't know.*



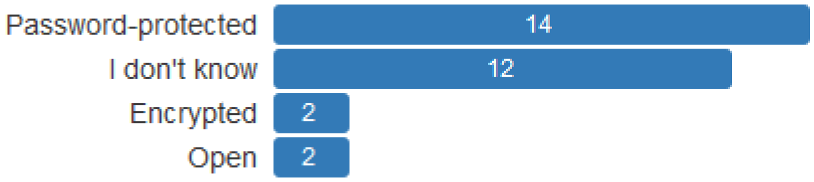
Question 23: Can personal data processing activities be performed without log files being created?
Possible responses: *Yes, No, I don't know.*



Question 24: What level of password secrecy/complexity is being enforced at your organization (check all that apply)?
Possible responses: *Minimum length, Mix of characters, Restrict password reuse, Mandatory Password Resets, Authentication manager*, Other (Free text option)

Password secrecy/complexity	Number of answer selection (is enforced)	Number of answer deselection (is not enforced)
Minimum length	15	15
Mix of characters	23	7
Restrict password reuse	9	21
Mandatory Password Resets	12	18
Authentication manager	6	24
Other: None	1	0

Question 25: How is financial, medical and/or PII (Personally Identifiable Information) stored on your computers, and what kind of security is in place to protect it?
Possible responses: Open, Password-*protected,* Encrypted*, I don't know.*



Question 26: Which of the following do you or your organisation apply?

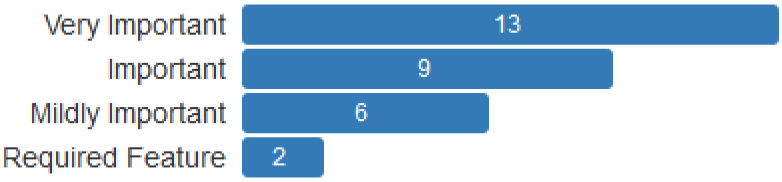
- Secure, encrypted way for employees working from home to access your corporate network
- Log activity on your network and have the capability to identify suspicious behaviour
- External cloud services or are the services hosted only within your private network

Possible responses: *Yes, Partially, No, I don't know*

Organisation Measures	Yes	Partially	No	I don’t know
Secure, encrypted way for employees working from home to access your corporate network.	22	3	5	0
Log activity on your network and have the capability to identify suspicious behaviour.	10	7	8	5
External cloud services or are the services hosted only within your private network.	15	9	4	2

Question 27: How important is to you to have visibility into the health of the underlying infrastructure hosting the services?

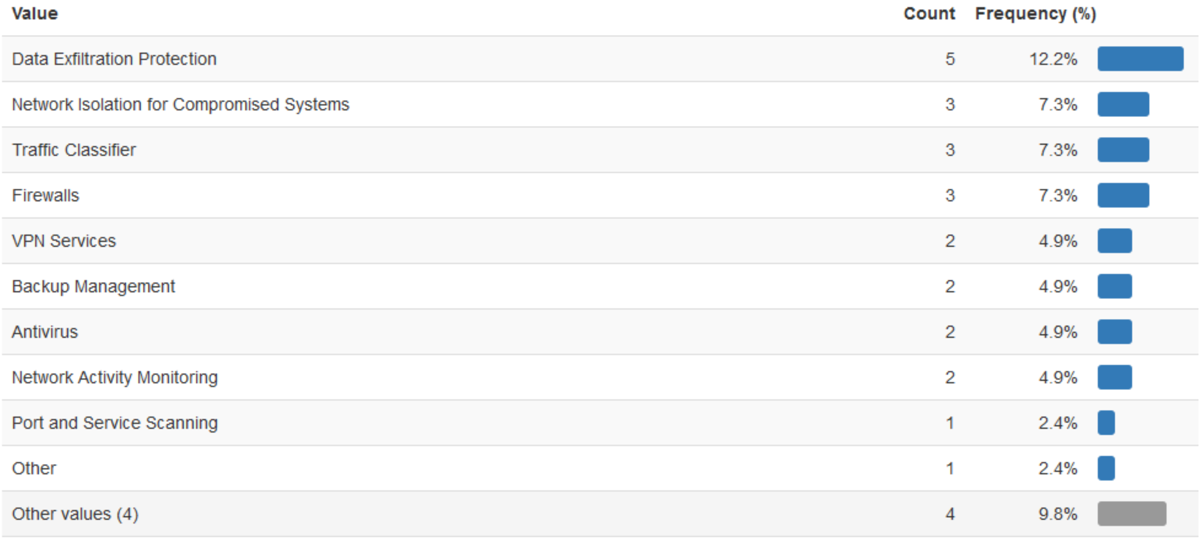
Possible responses: *Not important, Mildly Important, Important, Very Important, Required Feature.*



Feature related questions (3 questions)

Question 28: Which do you consider the most important security feature currently lacking from the cybersecurity software used in your organisation?

Possible responses: *Antivirus, Application-based Policies, Availability and Overloading Analysis, Backup Management, Data Exfiltration Protection, Filtering, Firewalls, Honeypots, IDPS, Network Activity Monitoring, Network Isolation for Compromised Systems, Port and Service Scanning, Remote Attack Detection, Traffic Classifier, VPN Services, Other.*



Value	Count	Frequency (%)
Data Exfiltration Protection	5	12.2%
Network Isolation for Compromised Systems	3	7.3%
Traffic Classifier	3	7.3%
Firewalls	3	7.3%
VPN Services	2	4.9%
Backup Management	2	4.9%
Antivirus	2	4.9%
Network Activity Monitoring	2	4.9%
Port and Service Scanning	1	2.4%
Other	1	2.4%
Other values (4)	4	9.8%

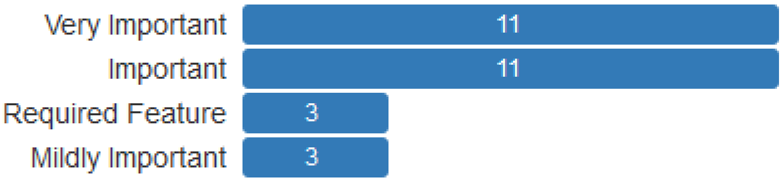
Question 29: Do you (or your company) care about:

- The solution being proprietary?
- Based on open-source software?
- Being compliant with the relevant industry standards?

Possible responses: *Not important, Mildly Important, Important, Very Important, Required Feature, I don’t know*

Feature	Not important	Mildly important	Important	Very important	Required	I don't know
The solution being proprietary.	7	8	6	3	0	4
Based on open-source software.	4	8	7	6	0	2
Being compliant with the relevant industry standards.	0	1	10	10	7	0

Question 30: How important is it for you (or your company) to know the security state of the underlying infrastructure (e.g. have proof that it is running up-to-date firmware, OS)?
Possible responses: *Not important, Mildly Important, Important, Very Important, Required Feature, I don't know*



GDPR compliance questions

Question 31: What do you consider as personal network data?
Possible Responses: (IP, application identification, user identification, service classification, traffic prioritization) *Check one or more of the suggestions.*

Network data	Number of answer selection (is considered)	Number of answer deselection (is not considered)
IP	20	7
Application identification	11	16
User identification	26	1
Service classification	4	23
Traffic prioritization	1	26

The following questions were implemented using the AHP methodology detailed in section 1.1.1.

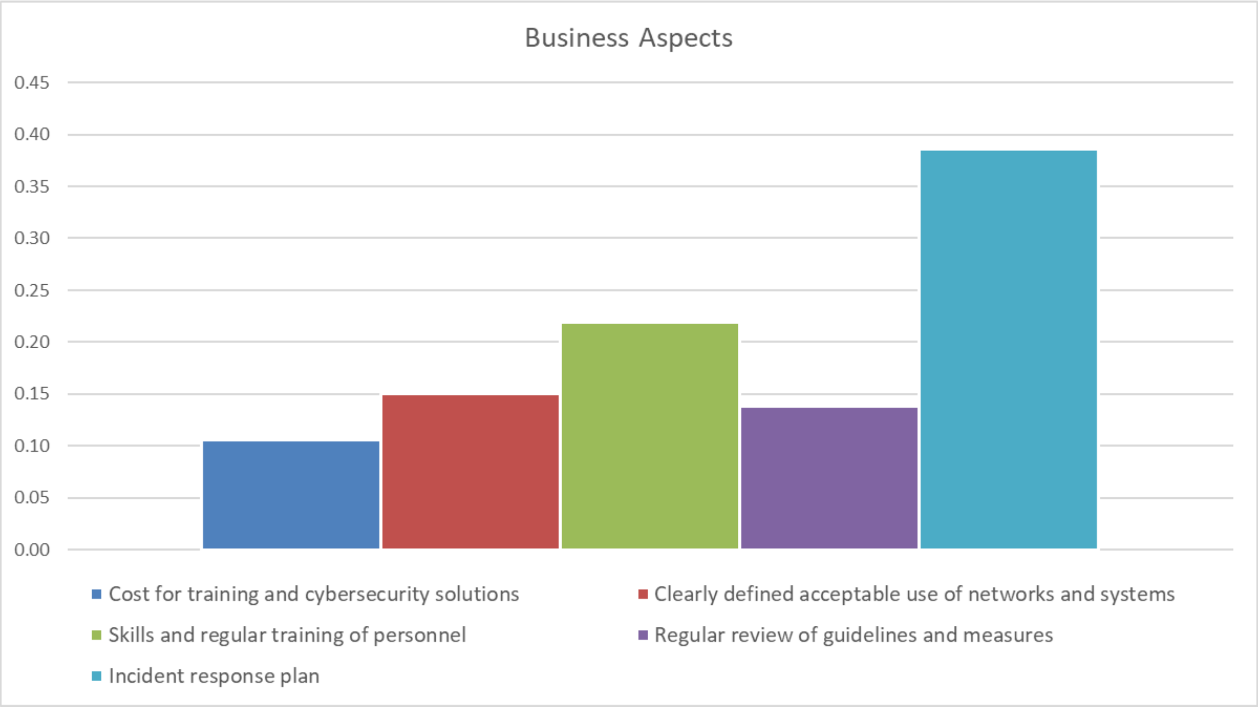
Business aspects

Question 32: Which of the following do you consider more important?

Cost for training and cybersecurity solutions	8	7	6	5	4	3	2	1	0	1	2	3	4	5	6	7	8	Clearly defined acceptable use of networks & systems
Cost for training and cybersecurity solutions	8	7	6	5	4	3	2	1	0	1	2	3	4	5	6	7	8	Skills and regular training of personnel
Cost for training and cybersecurity solutions	8	7	6	5	4	3	2	1	0	1	2	3	4	5	6	7	8	Regular review of guidelines and measures
Cost for training and cybersecurity solutions	8	7	6	5	4	3	2	1	0	1	2	3	4	5	6	7	8	Incident response plan
Clearly defined acceptable use of networks & systems	8	7	6	5	4	3	2	1	0	1	2	3	4	5	6	7	8	Skills and regular training of personnel

Clearly defined acceptable use of networks & systems	8	7	6	5	4	3	2	1	0	1	2	3	4	5	6	7	8	Regular review of guidelines and measures
Clearly defined acceptable use of networks & systems	8	7	6	5	4	3	2	1	0	1	2	3	4	5	6	7	8	Incident response plan
Skills and regular training of personnel	8	7	6	5	4	3	2	1	0	1	2	3	4	5	6	7	8	Regular review of guidelines and measures
Skills and regular training of personnel	8	7	6	5	4	3	2	1	0	1	2	3	4	5	6	7	8	Incident response plan
Regular review of guidelines and measures	8	7	6	5	4	3	2	1	0	1	2	3	4	5	6	7	8	Incident response plan

Sub-criterion	Weight	Rank
Cost for training and cybersecurity solutions	0.106	5
Clearly defined acceptable use of networks & systems	0.150	3
Skills and regular training of personnel	0.219	2
Regular review of guidelines and measures	0.139	4
Incident response plan	0.368	1

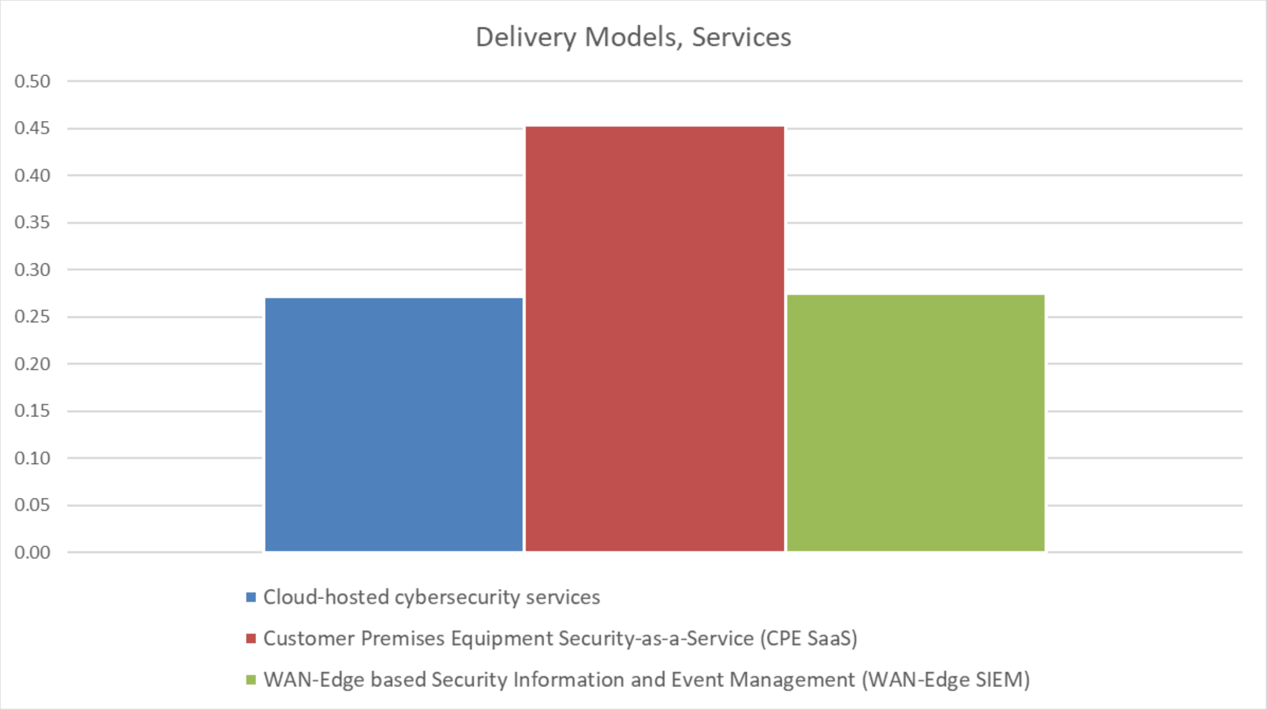


Delivery Models, Services

Question 33: Which of the following do you consider more important?

Cloud-hosted cybersecurity services	8	7	6	5	4	3	2	1	0	1	2	3	4	5	6	7	8	Customer Premises Equipment Security-as-a-Service (CPE SaaS)
Cloud-hosted cybersecurity services	8	7	6	5	4	3	2	1	0	1	2	3	4	5	6	7	8	WAN-Edge based Security Information and Event Management (WAN-Edge SIEM)
Customer Premises Equipment Security-as-a-Service (CPE SaaS)	8	7	6	5	4	3	2	1	0	1	2	3	4	5	6	7	8	WAN-Edge based Security Information and Event Management (WAN-Edge SIEM)

Sub-criterion	Weight	Rank
Cloud-hosted cybersecurity services	0.271	3
Customer Premises Equipment Security-as-a-Service (CPE SaaS)	0.454	1
WAN-Edge based Security Information and Event Management (WAN-Edge SIEM)	0.275	2



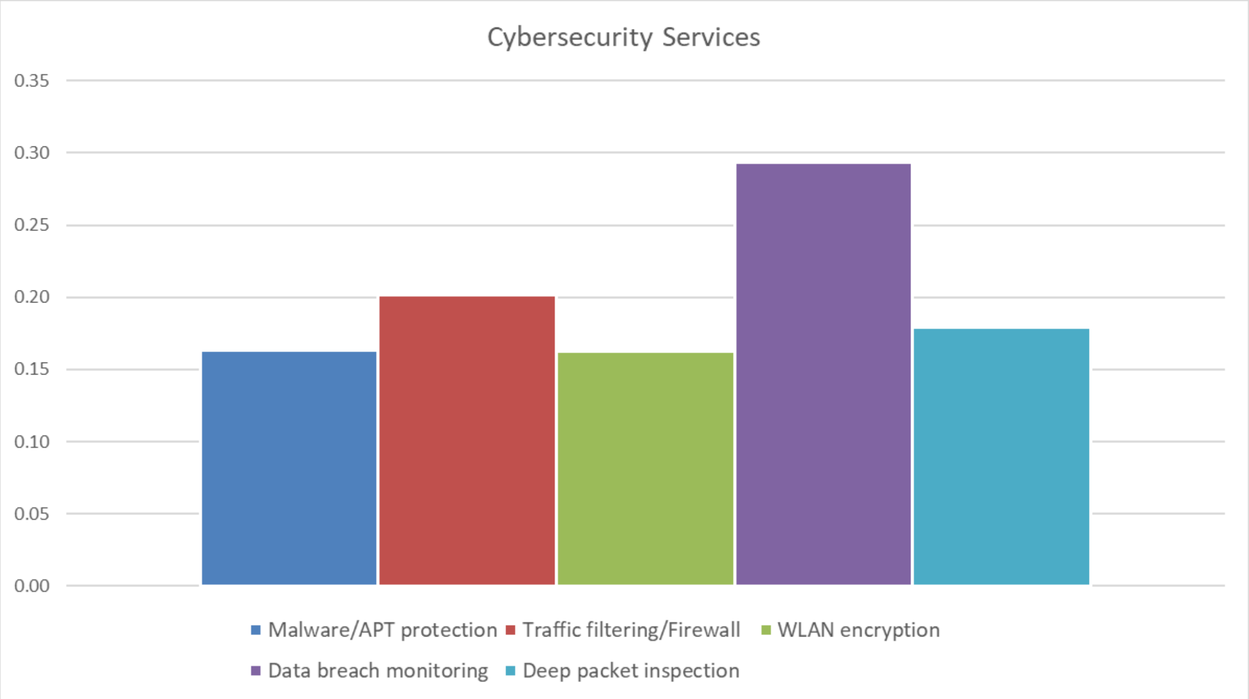
Cybersecurity Services

Question 34: Which of the following do you consider more important?

Malware/APT protection	8	7	6	5	4	3	2	1	0	1	2	3	4	5	6	7	8	Traffic filtering/Firewall

Malware/APT protection	8	7	6	5	4	3	2	1	0	1	2	3	4	5	6	7	8	WLAN encryption
Malware/APT protection	8	7	6	5	4	3	2	1	0	1	2	3	4	5	6	7	8	Data breach monitoring
Malware/APT protection	8	7	6	5	4	3	2	1	0	1	2	3	4	5	6	7	8	Deep packet inspection
Traffic filtering/Firewall	8	7	6	5	4	3	2	1	0	1	2	3	4	5	6	7	8	WLAN encryption
Traffic filtering/Firewall	8	7	6	5	4	3	2	1	0	1	2	3	4	5	6	7	8	Data breach monitoring
Traffic filtering/Firewall	8	7	6	5	4	3	2	1	0	1	2	3	4	5	6	7	8	Deep packet inspection
WLAN encryption	8	7	6	5	4	3	2	1	0	1	2	3	4	5	6	7	8	Data breach monitoring
WLAN encryption	8	7	6	5	4	3	2	1	0	1	2	3	4	5	6	7	8	Deep packet inspection
Data breach monitoring	8	7	6	5	4	3	2	1	0	1	2	3	4	5	6	7	8	Deep packet inspection

Sub-criterion	Weight	Rank
Malware/APT protection	0.164	4
Traffic filtering/Firewall	0.202	2
WLAN encryption	0.162	5
Data breach monitoring	0.293	1
Deep packet inspection	0.179	3



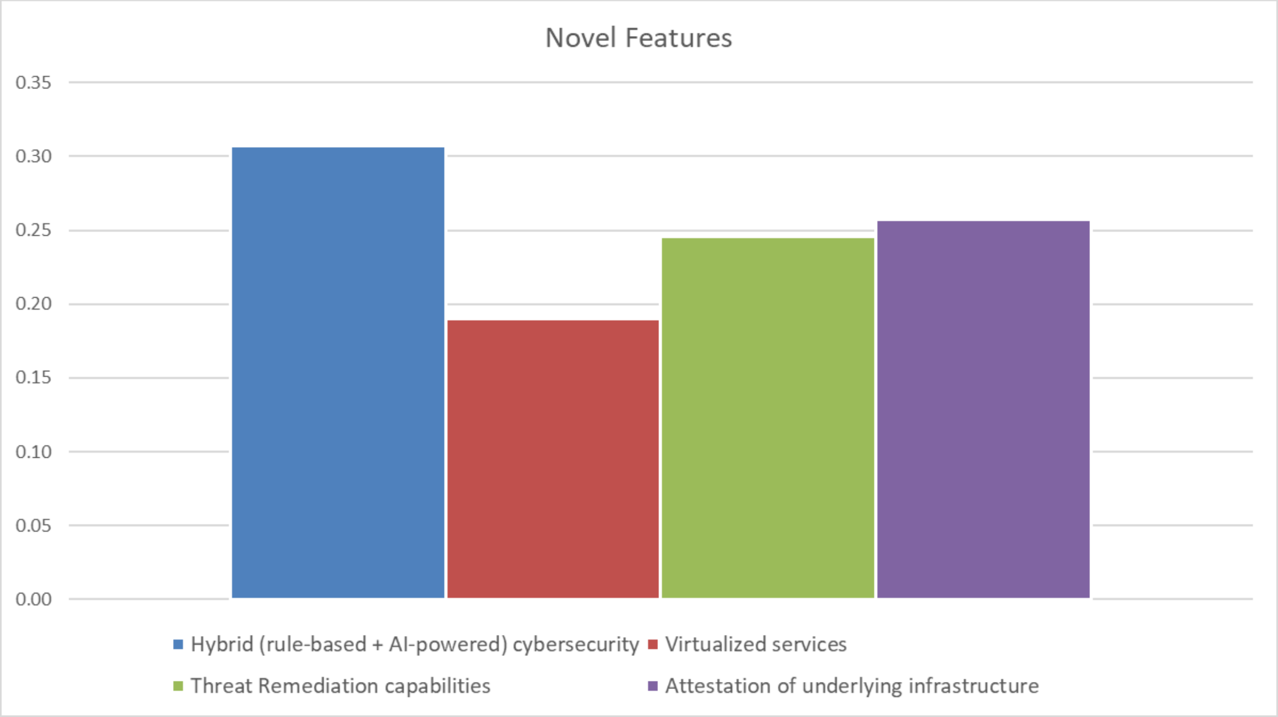
Novel Features

Question 35: Which of the following do you consider more important?

Hybrid (rule-based + AI-powered) cybersecurity	8	7	6	5	4	3	2	1	0	1	2	3	4	5	6	7	8	Virtualized services
Hybrid (rule-based + AI-powered) cybersecurity	8	7	6	5	4	3	2	1	0	1	2	3	4	5	6	7	8	Threat Remediation capabilities

Hybrid (rule-based + AI-powered) cybersecurity	8	7	6	5	4	3	2	1	0	1	2	3	4	5	6	7	8	Attestation of underlying infrastructure
Virtualized services	8	7	6	5	4	3	2	1	0	1	2	3	4	5	6	7	8	Threat Remediation capabilities
Virtualized services	8	7	6	5	4	3	2	1	0	1	2	3	4	5	6	7	8	Attestation of underlying infrastructure
Threat Remediation capabilities	8	7	6	5	4	3	2	1	0	1	2	3	4	5	6	7	8	Attestation of underlying infrastructure

Sub-criterion	Weight	Rank
Hybrid (rule-based + AI-powered) cybersecurity	0.307	1
Virtualized services	0.190	4
Threat Remediation capabilities	0.246	3
Attestation of underlying infrastructure	0.257	2

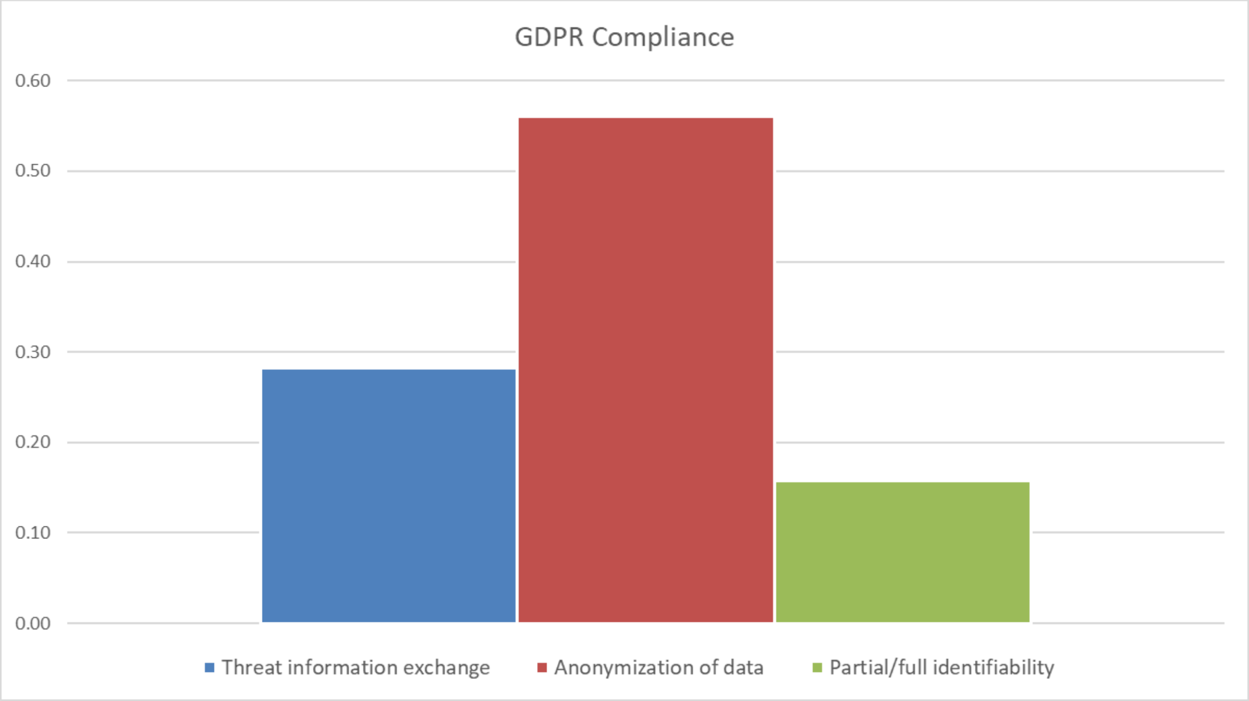


GDPR Compliance

Question 36: Which of the following do you consider more important?

Threat information exchange	8	7	6	5	4	3	2	1	0	1	2	3	4	5	6	7	8	Anonymization of data
Threat information exchange	8	7	6	5	4	3	2	1	0	1	2	3	4	5	6	7	8	Partial/full identifiability
Anonymization of data	8	7	6	5	4	3	2	1	0	1	2	3	4	5	6	7	8	Partial/full identifiability

Sub-criterion	Weight	Rank
Threat information exchange	0.282	2
Anonymization of data	0.560	1
Partial/full identifiability	0.158	3



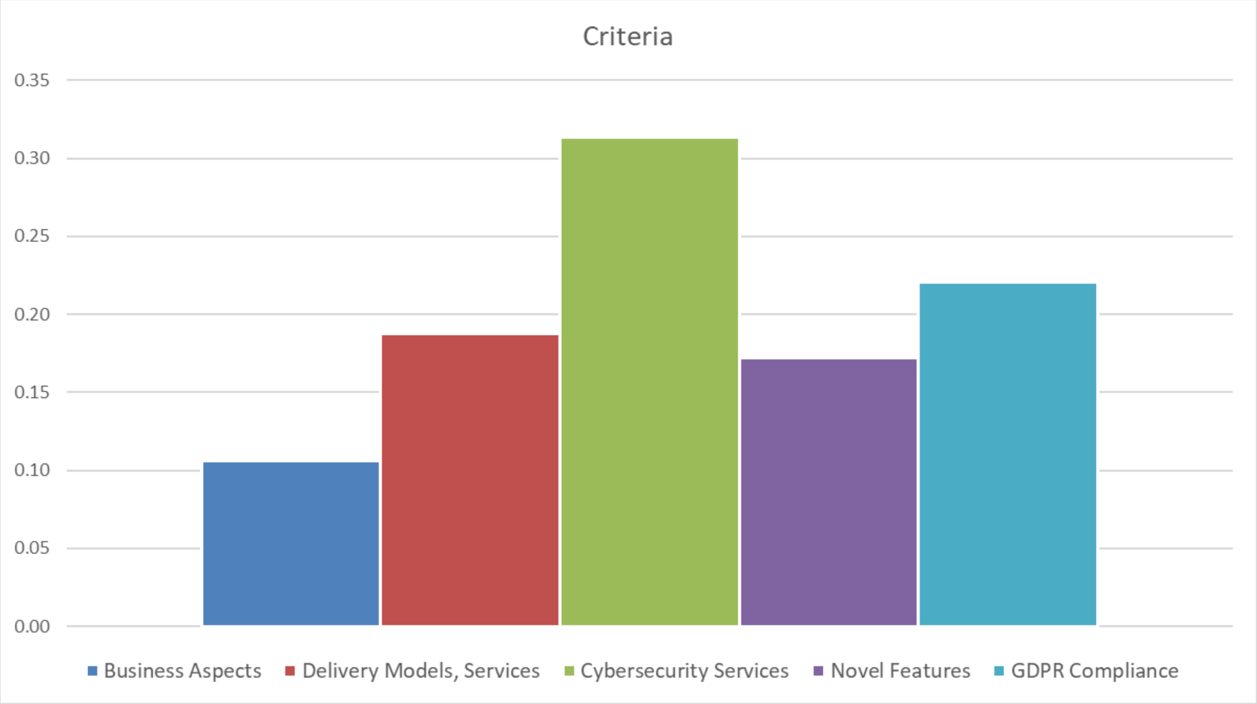
Criteria comparison

Question 37: Which of the following do you consider more important?

Business Aspects	8	7	6	5	4	3	2	1	0	1	2	3	4	5	6	7	8	Delivery Models, Services
Business Aspects	8	7	6	5	4	3	2	1	0	1	2	3	4	5	6	7	8	Cybersecurity Services
Business Aspects	8	7	6	5	4	3	2	1	0	1	2	3	4	5	6	7	8	Novel Features
Business Aspects	8	7	6	5	4	3	2	1	0	1	2	3	4	5	6	7	8	GDPR Compliance
Delivery Models, Services	8	7	6	5	4	3	2	1	0	1	2	3	4	5	6	7	8	Cybersecurity Services
Delivery Models, Services	8	7	6	5	4	3	2	1	0	1	2	3	4	5	6	7	8	Novel Features
Delivery Models, Services	8	7	6	5	4	3	2	1	0	1	2	3	4	5	6	7	8	GDPR Compliance
Cybersecurity Services	8	7	6	5	4	3	2	1	0	1	2	3	4	5	6	7	8	Novel Features
Cybersecurity Services	8	7	6	5	4	3	2	1	0	1	2	3	4	5	6	7	8	GDPR Compliance
Novel Features	8	7	6	5	4	3	2	1	0	1	2	3	4	5	6	7	8	GDPR Compliance

Criterion	Weight	Rank
Business Aspects	0.106	5
Delivery Models, Services	0.187	3
Cybersecurity Services	0.314	1
Novel Features	0.172	4

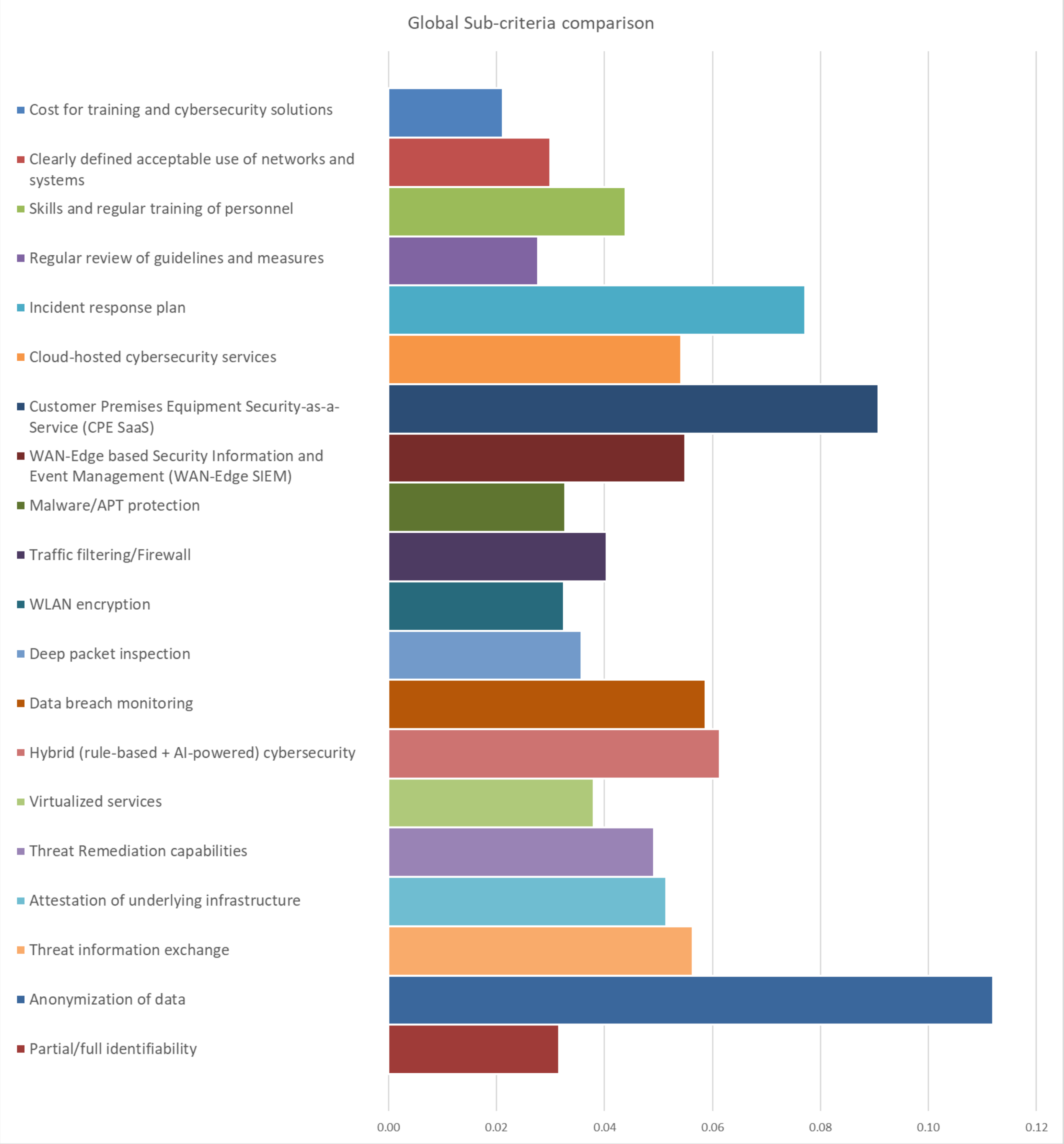
Criterion	Weight	Rank
GDPR Compliance	0.221	2



Global Sub-criteria comparison

Criterion	Rank	Sub-criterion	Weight	Rank
Business Aspects	5	Cost for training and cybersecurity solutions	0.021	20
		Clearly defined acceptable use of networks & systems	0.030	18
		Skills and regular training of personnel	0.044	11
		Regular review of guidelines and measures	0.028	19
		Incident response plan	0.077	3
Delivery Models, Services	3	Cloud-hosted cybersecurity services	0.054	8
		Customer Premises Equipment Security-as-a-Service (CPE SaaS)	0.091	2
		WAN-Edge based Security Information and Event Management (WAN-Edge SIEM)	0.055	7

Criterion	Rank	Sub-criterion	Weight	Rank
Cybersecurity Services	1	Malware/APT protection	0.033	15
		Traffic filtering/Firewall	0.040	12
		WLAN encryption	0.032	16
		Data breach monitoring	0.059	5
		Deep packet inspection	0.036	14
Novel Features	4	Hybrid (rule-based + AI-powered) cybersecurity	0.061	4
		Virtualized services	0.038	13
		Threat Remediation capabilities	0.049	10
		Attestation of underlying infrastructure	0.051	9
GDPR Compliance	2	Threat information exchange	0.056	6
		Anonymization of data	0.112	1
		Partial/full identifiability	0.032	17


Global Sub-criteria comparison
Cost for training and cybersecurity solutions
Clearly defined acceptable use of networks and systems
Skills and regular training of personnel
Regular review of guidelines and measures
Incident response plan
Cloud-hosted cybersecurity services
Customer Premises Equipment Security-as-a-Service (CPE SaaS)
WAN-Edge based Security Information and Event Management (WAN-Edge SIEM)
Malware/APT protection
Traffic filtering/Firewall
WLAN encryption
Deep packet inspection
Data breach monitoring
Hybrid (rule-based + AI-powered) cybersecurity
Virtualized services
Threat Remediation capabilities
Attestation of underlying infrastructure
Threat information exchange
Anonymization of data
Partial/full identifiability
0.00
0.02
0.04
0.06
0.08
0.10
0.12

Annex B.: Technical questionnaire and results collected

The goal of this Technical Questionnaire is to gather Subject-Matter Expert (SME) advices on the PALANTIR architecture, services, user experience and operational model.

Presentation of PALANTIR

Throughout the course of the PALANTIR project, the consortium will create a technical framework enabling the provision of next-generation, cost-effective Security-as-a-Service (SecaaS) services to Small and Medium Enterprises (SME) and Micro-Enterprises (ME), by leveraging novel technologies such as Network Function Virtualisation (NFV), Security Orchestration, Remote Attestation, Machine Learning (ML), Policy-based Remediation and Multi-attribute Risk Assessment. A general vision on the PALANTIR SecaaS platform for cyber-resiliency is depicted in Figure 16, showing the main operational blocks.

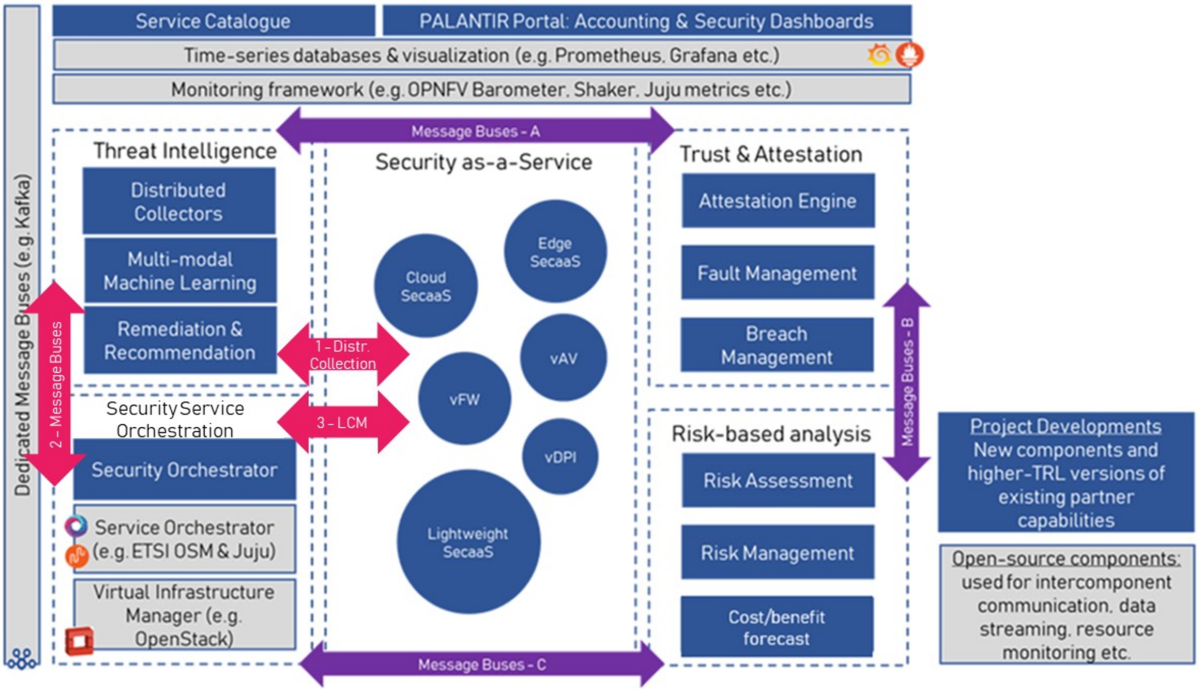

Service Catalogue
PALANTIR Portal: Accounting & Security Dashboards
Time-series databases & visualization (e.g. Prometheus, Grafana etc.)
Monitoring framework (e.g. OPNFV Barometer, Shaker, Juju metrics etc.)
Dedicated Message Buses (e.g. Kafka)
Message Buses - A
Threat Intelligence
Distributed Collectors
Multi-modal Machine Learning
Remediation & Recommendation
2 - Message Buses
Security Service Orchestration
Security Orchestrator
Service Orchestrator (e.g. ETSI OSM & Juju)
Virtual Infrastructure Manager (e.g. OpenStack)
1 - Distr. Collection
3 - LCM
Security as-a-Service
Cloud SecaaS
Edge SecaaS
vAV
vFW
vDPI
Lightweight SecaaS
Message Buses - C
Trust & Attestation
Attestation Engine
Fault Management
Breach Management
Message Buses - B
Risk-based analysis
Risk Assessment
Risk Management
Cost/benefit forecast
Project Developments
New components and higher-TRL versions of existing partner capabilities
Open-source components:
used for intercomponent communication, data streaming, resource monitoring etc.

Figure 16: Overview of the PALANTIR proposed architecture

The security services are hosted on top of an NFV architecture, whose management and orchestration layer is enhanced with a dedicated Security Orchestration and Service Catalogue.

The Threat Intelligence component provides advanced analytics capabilities, based on ML and distributed collectors that can be part of the security services or can be monitoring the client network. The Remediation and Recommendation Module is responsible for defining the threat mitigation solution; as it can trigger deployment of new security services or reconfiguration of existing ones.

The Trust and Attestation component is responsible for monitoring the integrity of the security services – and the underlying hosting infrastructure – to ensure the correct operation of PALANTIR. In case of an attack or breach detection, a remediation procedure is deployed, which includes notification if needed.

Demonstration use cases

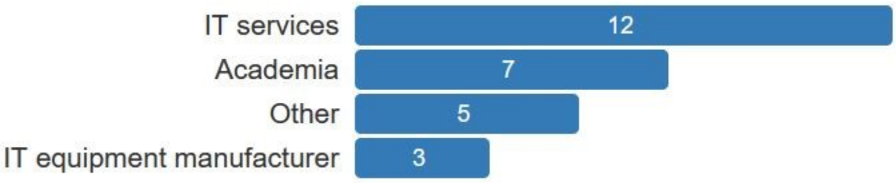
The consortium aims at demonstrating the PALANTIR solution in the following 3 use cases:

1. Securing private medical practices with lightweight SecaaS: Private medical practices are prime examples of MEs with high security and data protection needs. Private practices frequently suffer from critical data breaches and the staff is usually not in the position to handle a cyber-attack. PALANTIR will illustrate at minimum two cases of attacks prevented by the Lightweight SecaaS gateway and/or Cloud SecaaS in this use case.
2. Uninterrupted Electronic Commerce with Cloud SecaaS: Small businesses with e-commerce operations are increasingly leveraging cloud services along with local infrastructure for expense savings, yet they do not always ensure that these services use strong online security measures. In this use case, PALANTIR will demonstrate a personalised enterprise-grade solution offered to the end-user at affordable cost by minimising cost of licenses, software and hardware.
3. Live Threat Intelligence Sharing in a large-scale Edge scenario: In this use case, the PALANTIR provider would be able to i) jointly analyse information from multiple clients to detect incidents which would remain unnoticed if each client was treated individually and ii) exploit the live threat intelligence feedback from the community of users directly into the local network of the user, through its provided gateway or in the network infrastructure.

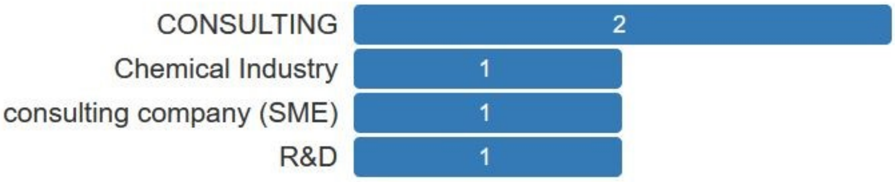
Company & position (4 questions)[1]

Question 1: What business sector does your company operate in?

Possible responses: IT services, IT equipment manufacturer, Academia, Other (free text).

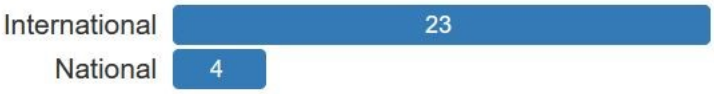


Other responses:



Question 2: What is the scope of your company?

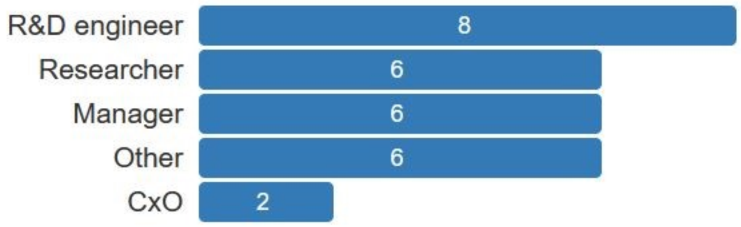
Possible responses: Local, National, International



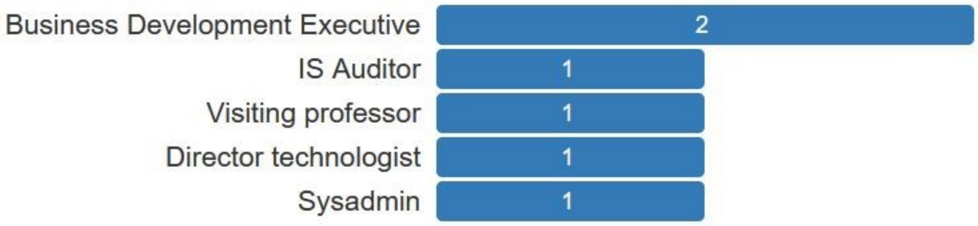
Question 3: What position do you have in your company?

Possible responses: R&D Engineer, Researcher, Product Manager, CxO, Manager, Other (free text).

[1] For every question in the Technical questionnaire, the SMEs have the option to choose not to answer.

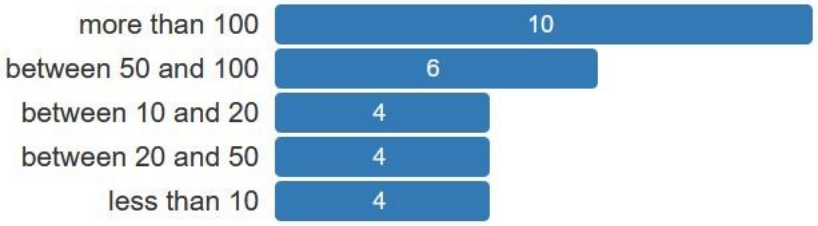


Other responses:



Question 4: How many employees does your company have?

Possible responses: less than 10, between 10 and 20, between 20 and 50, between 50 and 100, more than 100.



Infrastructure-related questions (4 questions)

Question 5: Which attacks against the PALANTIR infrastructure should be prioritised (up to 3)?

Possible responses: Rootkit, Cryptojacking, Ransomware, Supply Chain attack, Counterfeit Products, Hardware Tampering (e.g. plugging USB device, changing components), Runtime OS or Software attacks, Network Configuration Tampering.

Attack type	Number of answer selection (should be prioritize)	Number of answer deselection (should not be prioritize)
Ransomware	16	10
Runtime OS or software attack	13	13
Rootkit	11	15
Network Configuration Tampering	9	17
Cryptojacking	7	19
Supply Chain attack	7	19
Hardware Tampering	4	22
Counterfeited Products	0	26

Question 6: How important are the following features for the PALANTIR infrastructure?

Possible responses: Not important, Mildly Important, Important, Very Important, Required Feature.

- Patch level
- Software signature (the kernel, containers, etc. needs to be signed and the signature is validated before execution)
- Hardware authentication
- Service authentication
- Attestation (measurement and continual verification)
- Using best practices

Feature	Not important	Mildly important	Important	Very Important	Required
Best practices	0	2	3	4	14
Service authentication	0	0	6	7	10
Patch level	0	5	5	4	8
Attestation	0	3	5	8	6
Software signature	0	3	9	6	5
Hardware authentication	1	6	9	4	2

Question 7: Which deployment model should PALANTIR prioritise between on-premise or cloud-based?

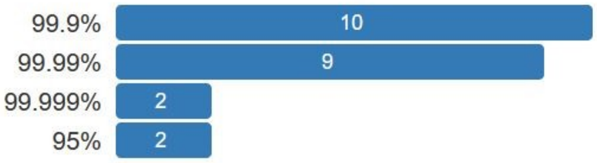
Possible responses: On-Premise, On-Premise and Cloud-Based, Cloud-Based.

- For the Cybersecurity Services.
- For the PALANTIR orchestration.
- For the Threat Intelligence (e.g. AI/ML engine).
- For the Service Catalogue.
- For the PALANTIR portal.
- For the Trust & Attestation component.
- For the Risk-based analysis component.

Component	On-Premise	On-Premise and Cloud-Based	Cloud-Based
Cybersecurity Services	7	12	4
Trust & Attestation	6	12	3
Threat Intelligence	4	15	4
Service Orchestration	4	12	7
Risk-based analysis	3	13	5
PALANTIR Portal	2	10	10
Service Catalogue	0	12	10

Question 8: What availability do you expect from the PALANTIR infrastructure (network, services)?

Possible responses: 99.999%, 99.99%, 99.9%, 95%



Services-related questions (3 questions)

Question 9: Which services (up to 3) should PALANTIR prioritise?

Possible responses: Antivirus, Application-based Policies, Availability and Overloading Analysis, Backup Management, Data Exfiltration, Filtering, Firewalls, Honeypots, IDPS, Network Activity Monitoring, Network Isolation for Compromised Systems, Port and Service Scanning, Remote Attack Detection, Traffic Classifier, VPN Services, Other (free text).

Service	Yes (should be considered)	No
Firewalls	11	13
Network Activity Monitoring	10	14
IDPS	8	16
Remote Attack Detection	8	16
Port and Service Scanning	7	17
Traffic Classifier	6	18
Data Exfiltration	5	19
Antivirus	4	20
Network Isolation for Compromised Systems	4	20
Backup Management	3	21
Honeypots	1	23
VPN	1	23
Application-based Policies	0	24
Availability and Overloading Analysis	0	24
Filtering	0	24

Question 10: Which services (up to 3) should PALANTIR not consider (e.g., they should stay under direct control of the end-user)?

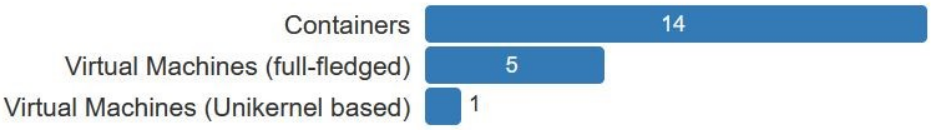
Possible responses: None, Antivirus, Application-based Policies, Availability and Overloading Analysis, Backup Management, Data Exfiltration, Filtering, Firewalls, Honeypots, IDPS, Network Activity Monitoring, Network Isolation for Compromised Systems, Port and Service Scanning, Remote Attack Detection, Traffic Classifier, VPN Services, Other (free text).

Service	Yes (should not be considered)	No
Antivirus	12	9
Backup Management	7	14
VPN	7	14
Firewalls	5	16
Honeypots	3	18
Application-based Policies	2	19
Filtering	2	19
Traffic Classifier	2	19
Data Exfiltration	1	20
Network Activity Monitoring	1	20
Port and Service Scanning	1	20

Service	Yes (should not be considered)	No
Remote Attack Detection	1	20
Availability and Overloading Analysis	0	21
IDPS	0	21
Network Isolation for Compromised Systems	0	21

Question 11: What infrastructure abstraction technology should the PALANTIR services use?

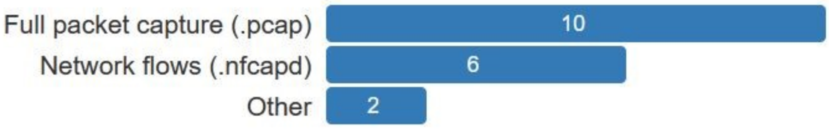
Possible responses: Containers, Virtual Machines (full-fledged), Virtual Machines (Unikernel based).



Threat Intelligence questions (7 questions)

Question 12: Which format should PALANTIR use when collecting network traffic?

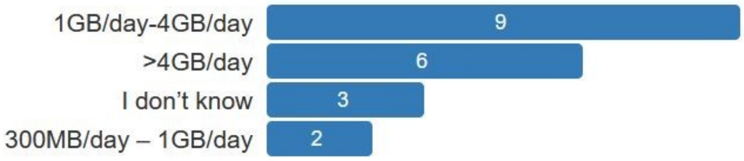
Possible responses: Network flows (.nfcapd), Full packet capture (.pcap), Other (free text)



Other response: "Both".

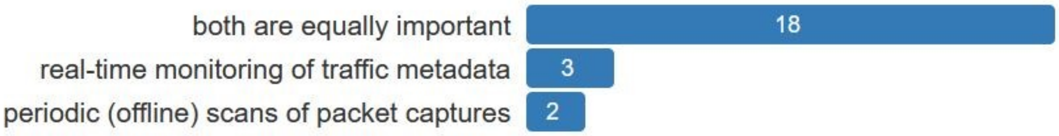
Question 13: What average amount of network traffic should PALANTIR expect in a day?

Possible responses: <300MB/day, 300MB/day – 1GB/day, 1GB/day-4GB/day, >4GB/day, I don't know



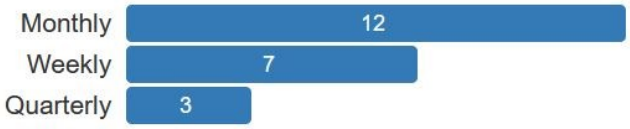
Question 14: Should PALANTIR consider AI-powered analytics solution that performs real-time monitoring of traffic metadata or periodic (offline) scans of packet captures?

Possible responses: real-time monitoring of traffic metadata, periodic (offline) scans of packet captures, both are equally important



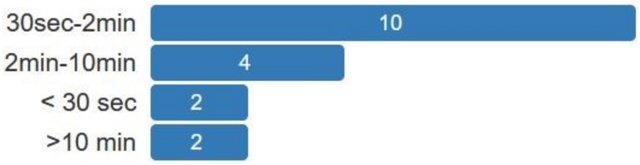
Question 15: How often does PALANTIR need to retrain its analytics models (to address network changes for example)?

Possible responses: Weekly, Monthly, Quarterly, Yearly, Never.



Question 16: What do you consider an acceptable inference time for PALANTIR with regards to newly discovered threats using ML?

Possible responses: < 30 sec, 30sec-2min, 2min-10min, >10 min



Question 17: How important is it for PALANTIR to protect from the following types of attacks?

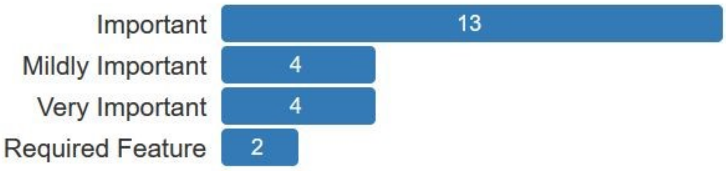
Possible responses: Not important, Mildly Important, Important, Very Important, Required Feature.

- Volumetric/DDoS
- Man-in-the-middle
- APTs
- Malware
- Phishing

Attacks	Not important	Mildly important	Important	Very Important	Required
Malware	1	1	3	8	10
Man-in-the-middle	1	2	2	8	10
Volumetric/DDoS	0	5	6	5	7
Phishing	1	4	5	8	5
APTs	1	2	8	7	4

Question 18: Should PALANTIR present feedback regarding anomalies of network activity (potentially malicious behaviour), even if they are not labelled as specific/well-known threats?

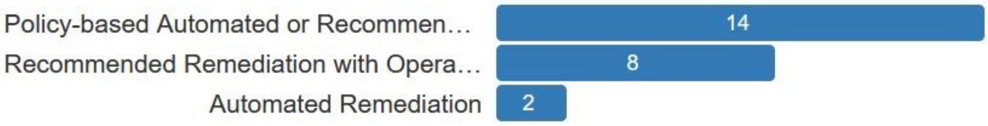
Possible responses: Not important, Mildly Important, Important, Very Important, Required Feature.



Threat Remediation (2 questions)

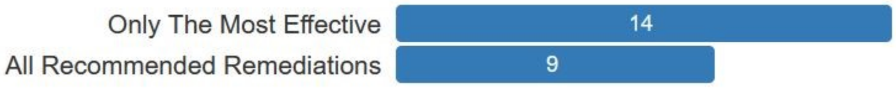
Question 19: How should PALANTIR remediate failures or attacks?

Possible responses: Automated Remediation, Recommended Remediation with Operator Authorisation, Policy-based Automated or Recommended Remediation.



Question 20: How many possible remediation/mitigation actions – ordered by effectiveness (as calculated by PALANTIR) - should PALANTIR present?

Possible responses: All Recommended Remediations, Only The Most Effective.



Risk-based Analysis (5 questions)

Question 21: What are the threats (up to 3) that PALANTIR must consider?

Possible responses: Unauthorised Access (attacker or employee error), Misuse of Information by Authorised Users, Data Leakage, Data Loss, Service Disruption.

Threats	Yes (should be considered)	No
Unauthorised Access	21	3
Data Leakage	19	5
Service Disruption	14	10
Data Loss	9	15
Misuse of Information	5	19

Question 22: Are there financial or legal penalties associated with those threats?

Possible responses: Financial, Legal, Both, No

- Unauthorised Access (attacker or employee error)
- Misuse of Information by Authorised Users
- Data Leakage
- Data Loss
- Service Disruption

Threats	Both	Financial	Legal	No
Unauthorised Access	13	5	4	1
Data Leakage	20	0	2	1
Service Disruption	Due to a technical error, this question did not appear in the survey.			
Data Loss	12	9	1	1
Misuse of Information	16	2	4	1

Question 23: Would there likely be a revenue or profitability impact associated with those threats?

Possible responses: No, Unlikely, Likely, Very Likely.

- Unauthorised Access (attacker or employee error)
- Misuse of Information by Authorised Users
- Data Leakage
- Data Loss
- Service Disruption

Threats	No	Unlikely	Likely	Very Likely
Unauthorised Access	0	3	10	10
Data Leakage	0	3	7	13
Service Disruption	0	4	14	5

Threats	No	Unlikely	Likely	Very Likely
Data Loss	0	3	9	11
Misuse of Information	0	7	8	8

Question 24: Would there likely be an impact to the day-to-day business operations associated with those threats?

Possible responses: No, Unlikely, Likely, Very Likely.

- Unauthorised Access (attacker or employee error)
- Misuse of Information by Authorised Users
- Data Leakage
- Data Loss
- Service Disruption

Threats	No	Unlikely	Likely	Very Likely
Unauthorised Access	0	9	9	4
Data Leakage	0	14	4	4
Service Disruption	0	2	2	18
Data Loss	0	2	7	13
Misuse of Information	0	14	7	1

Question 25: Would there likely be a reputational or brand impact associated with those threats?

Possible responses: No, Unlikely, Likely, Very Likely.

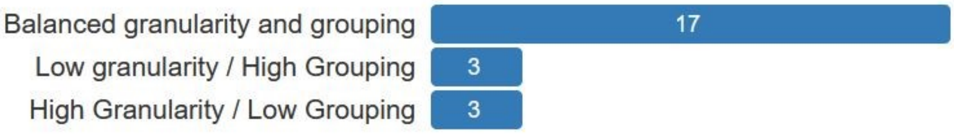
- Unauthorised Access (attacker or employee error)
- Misuse of Information by Authorised Users
- Data Leakage
- Data Loss
- Service Disruption

Threats	No	Unlikely	Likely	Very Likely
Unauthorised Access	0	4	8	9
Data Leakage	0	2	6	13
Service Disruption	0	3	6	12
Data Loss	0	3	8	10
Misuse of Information	0	1	13	7

User Interface and Experience (6 questions)

Question 26: Which level of granularity should the security alerts have?

Possible responses: Low granularity / High Grouping, Balanced granularity and grouping, High Granularity / Low Grouping, Specific Alerts / No Grouping.



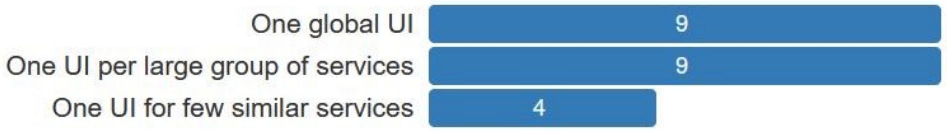
Question 27: Which means/media do you prefer to receive security alerts?

Possible responses (multiple answers allowed): Web Application, Mobile Notifications, e-mail, SMS, CLI, Desktop GUI.

Media	Yes (preferred)	No
Web Application	15	8
Mobile Notifications	14	9
e-mail	14	9
CLI	5	18
Desktop GUI	5	18
SMS	3	20

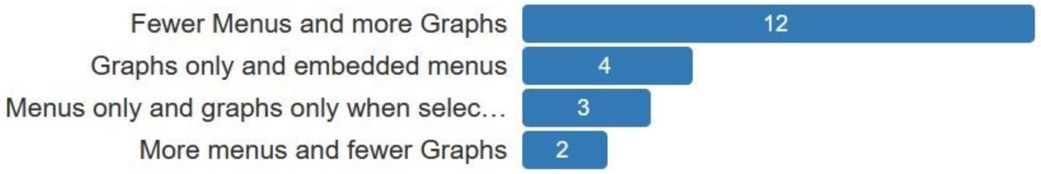
Question 28: Which UX should PALANTIR implement between a global unified security management UI, or a distinct management UI for each service?

Possible responses: One global UI, one UI per large group of services, one UI for few similar services, one UI per service.



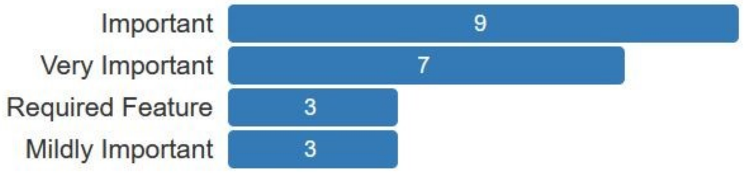
Question 29: Which UX is preferable for cybersecurity: a management view based on graphs and visualizations, or one based on menus?

Possible responses: Menus only and graphs only when selected, More menus and fewer Graphs, Fewer Menus and more Graphs, Graphs only and embedded menus.



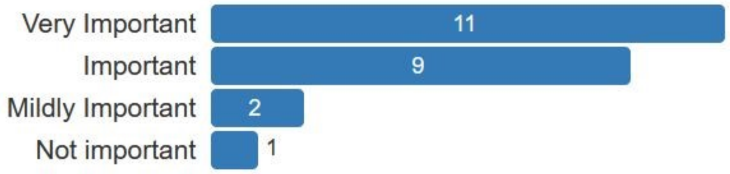
Question 30: How important is access to history of past threats?

Possible responses: Not important, Mildly Important, Important, Very Important, Required Feature.



Question 31: How important is it to you the threat knowledge sharing between users (SME, ME)?

Possible responses: Not important, Mildly Important, Important, Very Important, Required Feature.



GDPR compliance (5 questions)

Question 32: Should PALANTIR perform the following data processing?

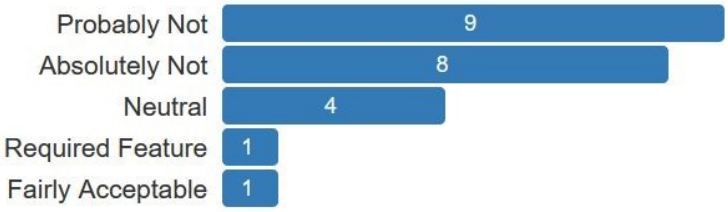
Possible responses: Absolutely Not, Probably Not, Neutral, Fairly Acceptable, Required Feature.

- Cloud-based processing of plaintext data.
- Cloud-based processing of anonymised data.
- On-Premise (hosted by PALANTIR) processing of plaintext data.
- On-Premise (hosted by PALANTIR) processing of anonymised data.
- Implement full identifiability of data.
- Implement partial identifiability of data.

Data processing	Absolutely Not	Probably Not	Neutral	Fairly Acceptable	Required Feature
On-Premise of anonymised data	0	0	7	7	8
Cloud-based of anonymised data	0	2	6	11	3
Implement partial identifiability	0	2	14	4	1
On-Premise of plaintext data	2	4	7	6	3
Cloud-based of plaintext data	6	6	5	4	1
Implement full identifiability	8	9	4	1	1

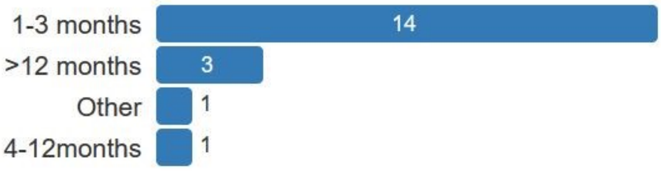
Question 33: Should PALANTIR extract or track personal information from the monitored networks?

Possible responses: Absolutely Not, Probably Not, Neutral, Fairly Acceptable, Required Feature.



Question 34: Which retention period for network data should PALANTIR implement?

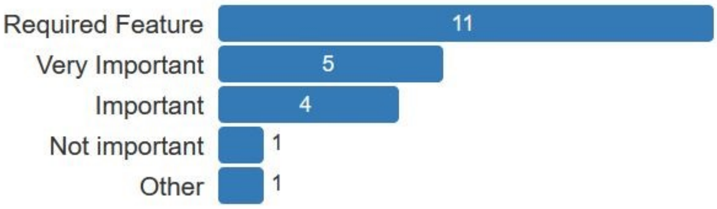
Possible responses: No data retention, <14 days, 1-3 months, 4-12months, >12 months, Other (free text).



Other response: “Configurable option”.

Question 35: How important is GDPR compliance for PALANTIR?

Possible responses: Not important, Mildly Important, Important, Very Important, Required Feature.



Other response: “This is equal to the question if it will be legal or not”.

Question 36: In addition to GDPR, which regulation should PALANTIR be compliant with (or facilitating)?

Possible responses: EU Open Internet Regulation, ePrivacy Directive, BEREC’s Net Neutrality, EU Lawful Interception resolution, ISO27001 (Security audit), Other (free text), None.

Regulation	Yes (should be compliant with)	No
ISO27001 (Security audit)	12	4
EU Open Internet Regulation	7	9
ePrivacy Directive	7	9
EU Lawful Interception resolution	4	12
BEREC’s Net Neutrality	2	14