ANASTACIA

Advanced Networked Agents for Security and Trust Assessment in CPS/IoT Architectures

D2.8

Secure Software Development Guidelines Final Report

This document presents the evaluation of the software components developed in ANASTACIA following the evaluation methodology presented in D2.4 that permits to exhaustively follow development activities by defining preventive actions within the implementation of components and mechanisms included in a IoT/CPS infrastructure. This document is to be used as reference for ANASTACIA developers to evaluate the protection against threats and the backwards traceability of requirements.

Distribution level	PU
Contractual date	30.06.2019 [M30]
Delivery date	30.06.2019 [M30]
WP / Task	WP2 / T2.4
WP Leader	UMU
Authors	Ruben Trapero (ATOS), Stefano Bianchi (SOFT), Enrico Cambiaso (CNR), Elisabetta Punta (CNR), Ivan Vaccari (CNR), Alejandro. Molina (UMU), Sofianna Menesidou (UBITECH), Rafael Marin-Perez (ODINS), Miloud Bagaa (AALTO), Eunah Kim (DG)
EC Project Officer	Carmen Ifrim carmen.ifrim@ec.europa.eu
Project Coordinator	Softeco Sismat SpA Stefano Bianchi Via De Marini 1, 16149 Genova – Italy +39 0106026368 stefano.bianchi@softeco.it
Project website	www.anastacia-h2020.eu

ANASTACIA has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement N° 731558 and from the Swiss State Secretariat for Education, Research and Innovation.

Table of contents

Index of figures

Index of tables

PUBLIC SUMMARY

This deliverable is the final report of the definition of guidelines to develop secure software. This deliverable continues with the work carried out in D2.4 (Secure Software Development Guidelines Initial Report), where a methodology for the development of secure software was created. This report starts by briefly revisiting the methodology included in D2.4 and evaluating the new input derived from the second period of the project, which considers additional security threats and the final set of requirements elicited.

The new set of input (requirements and threats) is evaluated and used in the methodology to obtain the impact and criticality of the requirements and also the severity of the new threats. Special emphasis is given in this document to the evaluation of the ANASTACIA components developed since the delivery of the initial report on security software development guidelines. To this end, it is specified the requirements related to every component of the ANASTACIA architecture, indicating what has been done to fulfil with those requirements.

Finally, the last part of this report is focused on the analysis of the development activities, supported by the evaluation methodology created in D2.4 and used in the current document. Such analysis allows to trace back requirements and threats, allowing to identify to what extent the ANASTACIA components are protected against those threats and what implementation activities have been done to achieve such protection. The prevention actions listed in D2.4 was used in this report to check if every component is being protected against all the security threats that they are supposed to cover and check whether any security threat have been left behind during the implementation activities.

1 INTRODUCTION

1.1 AIMS OF THE DOCUMENT

This document presents the evaluation of the software components developed in ANASTACIA following the evaluation methodology presented in D2.4 that permits to exhaustively follow development activities by defining preventive actions within the implementation of components and mechanisms included in an IoT/CPS infrastructure. This document is to be used as reference for ANASTACIA developers to evaluate the protection against threats and for the backwards traceability of requirements.

1.2 APPLICABLE AND REFERENCE DOCUMENTS

This document refers to the following documents:

- D1.4: Final User-centred Requirements Analysis
- D2.4: Secure Software Development Guidelines Initial Report
- D2.6: Attack Threats Analysis and Contingency Actions Final Report

1.3 REVISION HISTORY

Version	Date	Author	Description
0.1	12.4.2019	ATOS	Table of contents
0.2	23.4.2019	ATOS	Added assignment and organized inputs
0.3	10.5.2019	ATOS	Added content to Section 2
0.4	13.5.2019	CNR	Added content to Section 3.2
0.5	31.5.2019	UMU	Added content to Section 3.1
0.6	03.6.2019	ATOS	Added content to Sections 3.2.1 and 3.2.2
0.7	14.6.2019	ATOS	Added introductions to Sections 3.2.1, 3.2.2 and Annex I
0.8	16.6.2019	ATOS	Added tables for threat and components evaluation in Section 4
0.9	16.6.2019	UMU	Added input to table 4-2
0.9.1	16.6.2019	ATOS	Added input to Section 4
0.9.2	20.6.2019	UMU	Updated content to Section 3.1
0.9.3	21.6.2019	UBI	Added input to Section 3.2.1 and 4
0.9.4	24.6.2019	ATOS	Added content to Section 1.1, 1.2, 4, public summary and Annex II
0.9.5	24.6.2019	DG	Added content to Section 3.4
0.9.6	24.6.2019	ATOS	Added content to Section 4
0.9.7	25.6.2019	AALTO	Added content to Section 3.3 and Section 4
1.0	25.6.2019	ATOS	Produced first version ready for review by UBI
1.0.1	28.6.2019	ATOS	Produced final version ready for delivery

1.4 ACRONYMS AND DEFINITIONS

Acronym	Meaning
AAA	Authentication Authorization Accounting
CA	Certification Authority
CPS	Cyber Physical Systems
DNS	Domain Name Service
DREAd	Damage Potential, Reproducibility, Exploitability, Affected Users, Discoverability

DSPS	Dynamic Security and Privacy Seal
DTLS	Datagram Transport Layer Security
ECC	Elliptic-curve cryptography
GUI	Graphic User Interface
IMPI	Intelligent Platform Management Interface
IoT	Internet of Things
NIDS	Intrusion detection system
OWASP	Open Web Application Security Project
P2M	Peer2Mail
PANA	Protocol for Carrying Authentication for Network Access
SDN	Software Defined Network
SSL	Secure Socket Layer
VNF	Virtual Network Function

2 PROGRESS BEYOND PREVIOUS WORK

This section describes the progress that this deliverable represents with respect to the work presented in D2.4. This deliverable goes in depth in the methodology that was created in D2.4 for guiding the development of secure software for IoT/CPS. In this iteration such methodology is applied to the updated set of results obtained during the second half of the project, considering not just new requirements but also with to prevent additional threats.

Figure 2-1 represents the different phases of the methodology created in D2.4. Several stages are defined, each belonging to a different phase of the implementation life cycle.

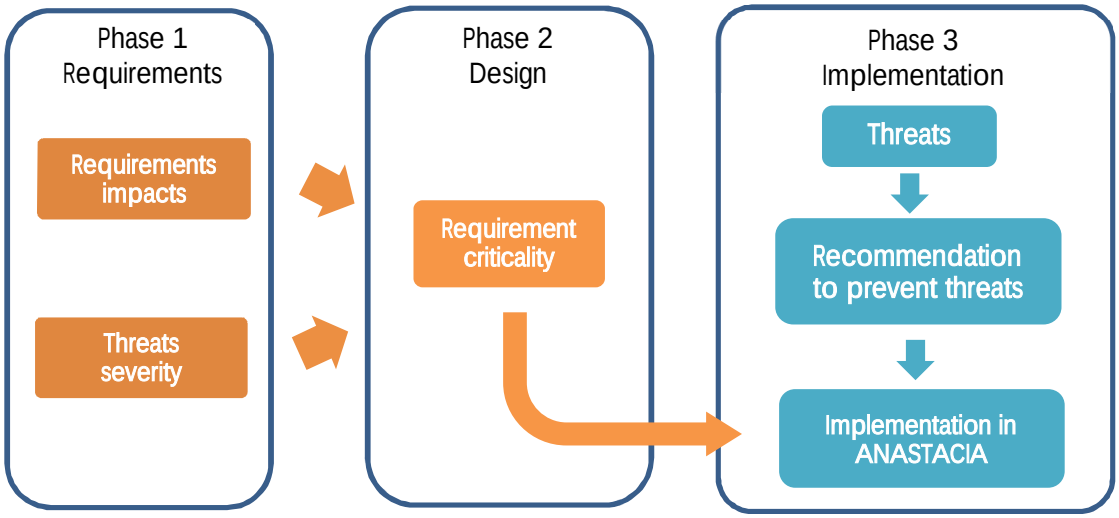

Figure 2-1. Evaluation steps

During the first phase an evaluation of the requirements and potential threats was done. On the one side, the evaluation of the requirements is done by selecting the subset of requirements related to security aspects, both functional and non-functional, and also the requirements for privacy. The impact of these requirements is evaluated by classifying their relevance in integrity, availability and confidentiality aspects. Depending on the partial scores obtained in these three categories every requirement is assigned with an impact level. This impact level is used in further stages to determine how critical is to cover certain requirement.

In parallel to the evaluation of requirements it is also carried out an elicitation of the main threats that the system can be exposed to. The severity of every threat is also analysed by evaluating different aspects: damage caused, reproducibility, how easy to exploit, quantity of users effected and how easy is to discover the threat. All these aspects determine the severity of the threat, which is used to prioritize implementation activities to prevent them.

During the second phase both requirements and threats are evaluated together. Every requirement is assigned to the related threats. Combining the impact of the requirements and the severity of the threats that are related to the requirement results in a value representing the criticality of every requirement.

In the third phase it is detailed the implementation activities that help to prevent the identified threats. This step depends on the type and number of components to implement. Therefore, with the threats identified it is analysed which ones might affect to the components of the architecture to implement.

This deliverable stresses on the third phase of the process, focusing mainly on the implementation actions to incorporate when developing the ANASTACIA components. During the second half of the project many implementation activities have been carried out, which have been used for the analysis done in this deliverable.

Additionally, the final iteration of this document applies the two first phases of the evaluation methodology to the updated set of requirements produced in D1.4 and with the emerging new threats evaluated in D2.6.

The methodology developed in D2.4 allows to trace back the fulfilment of the requirements specified and estimate the level of protection against the threats identified. Keeping track of specific implementation actions to fulfil security requirements and being them linked to identified security threats is a powerful tool to guarantee that the system is protected against these threats by design.

2.1 IMPACT OF UPDATED SECURITY REQUIREMENTS ON IOT/CPS

With the methodology created in D2.4 the new set of requirements elicited from D1.4 are analysed in this section in terms of its relationship to integrity, availability and confidentiality aspects. The impact level is given by the individual scores in these three aspects and given by the Table 3-1 in D2.4. For the sake of completeness and to facilitate the reading, these requirements have been incorporated to the Annex I of this document. Table 2-1 shows the scored for the list of requirements, which appears just with their corresponding requirements ID (Req ID). The impact level, shown in the top right column, will be used in later sections to calculate the criticality of the requirements with respect to the security threats that they are related to.

Table 2-1. Evaluation of updated security requirements

Req ID	Integrity	Availability	Confidentiality	Impact Level
FR-21	H	M	M	3
FR-22	H	M	H	4
FR-23	L	L	L	0
FR-24	H	H	L	3
FR-25	H	M	M	3
FR-26	H	H	M	4
FR-27	H	H	H	5
FR-28	H	M	H	4
FR-29	H	L	L	1
FR-30	H	L	L	1
FR-31	H	H	H	5
FR-32	H	H	H	5
FR-33	M	M	L	1
FR-34	M	M	L	1
FR-35	H	M	L	2
FR-36	H	M	L	2
FR-37	H	M	L	2
FR-38	M	M	L	1
FR-39	M	M	M	2
FR-40	M	M	M	2
FR-41	M	M	H	3
FR-42	M	M	L	1
FR-43	M	M	L	1
FR-44	M	M	M	2

Req ID	Integrity	Availability	Confidentiality	Impact Level
FR-45	M	M	L	1
FR-46	M	M	L	1
FR-47	M	M	L	1
FR-48	M	M	M	2
FR-49	M	M	L	1
FR-50	M	M	H	3
FR-51	M	M	H	3
FR-52	M	M	H	3
FR-53	H	H	H	5
FR-54	M	M	H	3
FR-55	M	M	H	3
FR-56	M	M	M	2
FR-57	M	M	M	2
NFR-16	H	H	H	5
PR-1	H	H	H	5
PR-2	M	H	H	4
PR-3	M	M	H	3
PR-4	M	M	H	3
PR-5	M	M	H	3
PR-6	M	M	H	3
PR-7	M	M	H	3
PR-8	M	M	H	3
PR-9	H	M	H	3
PR-10	H	H	H	5

2.2 GUIDELINES FOR PREVENTION OF EMERGING THREATS ON IOT/CPS

In this section, guidelines, assessment and evaluation of the emerging threats described in D2.6 are described. Also, a DREAd[1] score (which evaluates risk considering five categories: Damage, Reproducibility, Exploitability, Affected users and discoverability) is associated to each threat in order to evaluate the risk of the threats against IoT and CPS scenarios. Each use case is analysed and finally the DREAd risk table is reported. Details about the DREAd evaluation methodology can be obtained in D2.4.

2.2.1 Use Case O.1

In this use case, an attacker exploits CCTV security cameras in order to compromise data confidentiality. When the attack starts, the network is characterized by anomalous traffic due to the effect of the attack.

[1] Microsoft. Improving web application security: Threats and countermeasures. Available online http://msdn2.microsoft.com/en-us/library/ms994921.aspx, June 2003

In order to detect the attack, network monitoring activities can be accomplished in order to detect the anomalous traffic generated by the cameras. The monitoring activities could be based on anomaly-based detection or machine learning algorithms. In particular, it is therefore important to train the anomaly detection algorithm by deeply analysing a set of legitimate situations, in order to characterize a legitimate behaviour. Once such characterization is accomplished, it is possible to identify anomalies, often ensuring a predefined success rate.
Regarding the mitigation plan, two different level approaches could be implemented:

- at the network level, it is possible to temporarily block communications of the affected devices (or close the connection where external nodes/services are involved). This can be done by deploying specific rules on the involved firewall or by working at SDN level.
- at the host level, the camera could be temporarily reconfigured in order to close/reset the communications.

In order to prevent the proposed threat, the network camera traffic should be monitored and implement authentication mechanisms to control network access to the devices.

2.2.2 Use Case MEC.1

The threat analysed in this scenario is a spoofing attack, aimed to impersonate a smart camera data collector in order to retrieve sensitive videos from the security cameras. The attack is implemented at IP layer of the ISO/OSI stack.
The detection phase should be accomplished by using SNMP data analysis and by implementing network route controllers bound to the legitimate IP addresses communications, in order to detect traffic from suspicious sources.
In order to mitigate the threat, three different approaches should be implemented:

- Encrypt data and communication through strong client-to-server and server-to-client authentication methods, between the smart security cameras and the collector service
- Routes configuration and packets filtering techniques to detect and block traffic from suspicious sources (for instance, by working at network firewall level to bind communications only on legitimate nodes)
- Once the attack is detected, it is dynamically updated the IP address of the collector server, with consequent update of the related references on the hosts communicating with the server. Using a similar approach, the IP address of the collector server may be frequently updated, through a pseudo-casual algorithm based on a random seed shared between the collector service and the smart cameras.

2.2.3 Use Case MEC.2

This scenario is focused on a man-in-the-middle attack against security cameras. The attacker is an employee of the targeted company, and his aim is to retrieve sensitive videos to store them illegally and/or share them outside of the network. The attack is accomplished by exploiting credentials, certificates and video decryption keys owned by the attacker. In addition, the attack exploits a man-in-the-middle approach to impersonate the smart camera management server system, to the eyes of the security cameras in order to retrieve videos and sensitive information.
The detection of the man-in-the-middle attack may be accomplished by adopting and combining different solutions:

- By logging certificates to check validity, origin and owner of the certificates (authorization level)
- By monitoring host-to-host communications of the security cameras (e.g. at IP or MAC levels)
- By analysing network traffic and communications (e.g. through NIDS) to identify man-in-the-middle attacks

- By analysing communications and related flows (we suppose that videos are shared/exfiltrated outside of the organizations by exploiting the network, and by avoiding low-rate transfers), in order to identify anomalous traffic generated from the host operating as the MITM

In order to mitigate the MiTM attack, a first approach is based on filtering the communication of the smart security cameras in order to allow them to communicate with legitimate devices by using a firewall device. Regarding the data exfiltration attack, a solution could be to block connectivity of the affected devices when the attack is detected and to avoid packets encapsulation by implementing a deep packet inspection.

2.2.4 Use Case MEC.4

This scenario is focused on the exploitation of vulnerabilities affecting IoT camera systems with the aim to perpetrate cameras in order to execute malicious cyber-attacks against third parties such as DoS, scanning, or other well-known threats.
The detection phase may be executed in two different temporal periods:

- At exploitation time, in case a known-vulnerability is exploited, it is possible to identify (and mitigate) the exploitation. This is possible only on known vulnerabilities and if known detection patterns are present. In this case, by using a NIDS (e.g. Snort[2]) it is possible to detect (and block) the exploitation of the affected vulnerability.
- At post-exploitation time, hence, only after the IoT cameras are exploited by analysing network traffic flows and communications, to identify known threats (for instance, through signature-based detection, combined with Deep Packet Inspection (DPI)), or unknown threats (for instance, by adopting network anomaly- based IDS)

Instead mitigation may be accomplished by blocking outgoing traffic from the affected IoT cameras, or by redirecting malicious traffic to secure locations (under the control of the network administrator) through network reconfiguration by adopting SDN/NFV approaches.
In order to identify known threats, vulnerability assessment activities may be executed periodically to identify novel potential vulnerabilities on the system.

2.2.5 Use Case BMS.1

This scenario is focused on the execution of an advanced attack based on the exploitation of a 0-day vulnerability. Once the attacker obtains access to the network, different malicious activities are accomplished (activation of emergency in several floors of the building, switch-off of emergency units, overwrite of heating and cooling configurations, etc.), also including the gaining of physical unauthorized access to the facilities, needed to install malicious applications on specific network nodes, making them exfiltrate sensitive data outside of the organization and, simultaneously, perpetrate network attacks (e.g. SQLi) against management services.
In this scenario, different detection statements should be considered:

- By definition, it is not possible to detect 0-day vulnerabilities. Nevertheless, it is possible to deploy anomaly-based NIDS (by adopting machine learning algorithms) to identify and detect anomalies on the system by focusing on analysing network communications
- Malicious activities executed by the attacker can be detected by implementing an appropriate logging systems
- The unauthorized access to the facilities can be detected by implementing authentication and access control lists on the services adopted for access management and access to physical locations, combined with a physical identification of intrusions through the adoption of physical security systems
- Exfiltration outside the organization of sensitive data may be identified by deploying anomaly-based NIDS in order to monitor the network traffic and flows
- Running attacks (e.g. SQLi) can be identified by NIDS through DPI approaches

[2] https://www.snort.org/

Mitigation of the advanced attack considered can be accomplished as follows:

- The malicious activities can be mitigated by restoring systems and configuration to previous secure backup
- The possibility to obtain physical unauthorized access to the facilities can be prevented by implementing proper authentication and access control lists on the services (for instance, also considering timing accesses), adopted for access management and access to physical locations
- Exfiltration attack of sensitive data may be mitigated by blocking or redirecting network communications
- Running attacks (e.g. SQLi) can be mitigated at the network level, by NIDS and/or by redirecting the network traffic to harmless nodes

In the following, based on the attacks described in this section, we will report the related DREAd table, which extends table 5-3 of D2.4 with additional threats.

Threat ID	Threat	Partial scores for severity {0, 5, 10}					Severity (risk)
		D	R	E	A	d	
T45	Compromise data confidentiality	10	5	10	5	5	7
T46	Spoofing attack	10	10	5	5	5	7
T47	Man-in-the-middle attack	5	5	5	5	5	5
T48	Exploitation of vulnerabilities of IoT device to execute attacks	5	10	5	0	0	4
T49	0-day vulnerability	10	10	10	5	10	8

Table 2-2. Evaluation of additional threats

3 EVALUATION OF THE ANASTACIA PLATFORM

The following section evaluates the ANASTACIA platform in terms of the requirements covered by each of the main components that are part of the ANASTACIA architecture. To this extent, the evaluation carried out in the following subsections also provides with information about the implementation activities that supports the fulfilment of every related requirement. The requirements considered in the following subsections are derived from the final set of requirements reported in deliverable D1.4.

3.1 SECURITY POLICIES

ANASTACIA security policy models allow administrators to define pro-active and reactive behaviour of the whole system at two different level of abstractions, high-level Security Policy Language (HSPL) and Medium-level Security Policy language (MSPL). HSPL is the policy language suitable for expressing the general protection requirements of typical non-technical end-users, such as "do not permit access to illegal content" or "block access to peer-to-peer networks". MSPL is an abstract language with statements related to the typical actions performed by various security enablers but expressed independent of the final devices, it means, it expresses specific configurations in a device-independent format, such as "deny *.sex", "deny src 192.168", or "inspect HTTP traffic". Both policy languages were defined within the European project SECURED and now ANASTACIA's security policy models extends them by the unification of relevant, new and extended capability-based security policy models (including Event-Condition-Action features), as well as policy orchestration and conflict detection mechanisms. All the former under a unique policy framework.

Table 3-1. Evaluation of security policies: requirements and implementation

Subcomponent	Security Requirements Covered	Implementation details to cover the requirements
Policy Editor Tool	FR-21	The GUI allows defining multiple security policies as a policy for orchestration to manage multiple attack scenarios.
	FR-23	It has been deployed as distributed system
	FR-24	Policy Editor tool allows defining IoT control security policies to manage proactively IoT devices
	FR-26	Policy Editor tool allows defining IoT control security policies for manual attack mitigation purposes
	FR-28	Policy Editor tool allows defining priorities and dependencies for the policy conflict detection process
	FR-31	Policy Editor tool allows defining different combinations of security policies in order to mitigate 0-day attacks
	FR-32	Policy Editor tool allows defining different combinations of filtering, forwarding and IoT control policies in order to mitigate DDoS attacks.
	NFR-16	The friendly GUI allows configuration of security policies, enhancing the usability of the system.
	PR-1	Proactive/Reactive Privacy policies definition
	PR-3	GUI allows defining authentication policies
	PR-5	GUI allows defining data privacy policies
	PR-7	GUI allows defining authorization policies
	PR-9	GUI allows provide encryption by default by instantiating proactive/reactive channel protection and privacy policies.

Policy Repository	FR-21	The service stores and provides all the information regarding the current available security policies, capabilities and templates in the system to handle multiple attacks.
	FR-23	Deployed as distributed system
	NFR-16	Policy templates allows enhancing the usability of the system.
Policy interpreter	FR-21	Reactive policies for orchestration refinement and translation in order to mitigate attacks.
	FR-23	Deployed as distributed system
	FR-24	Policy Interpreter refines and translates IoT control security policies in order to manage proactively/reactively IoT devices
	FR-26	Policy Interpreter refines and translates monitoring and IoT control security policies.
	FR-28	Policy Interpreter refines and translates policies for orchestration which contains priorities and dependencies for the policy conflict detection process
	FR-31	Policy Interpreter can refine/translate different combinations of security policies in order to mitigate 0-day attacks
	FR-32	Policy interpreter can refine/translate different combinations of filtering, forwarding and IoT control policies in order to mitigate DDoS attacks.
	FR-42	Proactive/Reactive filtering and forwarding policies refinement and translation
	FR-47	Policy interpreter can translate reactive monitoring policies
	FR-49	Policy interpreter can use plugins in order to translate monitoring policies into final configurations.
	PR-1	Proactive/Reactive Privacy policies refinement and translation
	PR-3	Authentication policies refinement and translation
	PR-5	Data privacy policies refinement and translation
	PR-7	Refinement and translation of authorization policies
	PR-9	Channel protection and privacy policies refinement and translation.
Policy conflict detector	FR-21	Conflict and dependencies detection in reactive security policies for orchestration.
	FR-23	Deployed as distributed system
	FR-27	Proactive and reactive security and privacy conflict detection
IoT Controller	FR-23	Deployed as distributed system
	FR-24	IoT Controller implements IoT control policies enforcement so to avoid unexpected impacts in the operational context
	FR-26	IoT Controller implements IoT control policies enforcement for attack mitigation

3.2 MONITORING AND REACTION PLANE

This section includes the evaluation of the Monitoring or Reaction plane which have been grouped in two different subsections, covering individually the two main sub modules of this plane: Monitoring and Reaction.

3.2.1 Monitoring components

The ANASTACIA monitoring components retrieve the monitoring data generated by the IoT infrastructure. Several security probes are analysing the network traffic (i.e., the MMT probe) or reporting about authentication related events (i.e., AAA activity in IoT controllers). The components of the monitoring plane filter and process such information to report about incidents detected. The Data Filtering and pre-processing broker centralizes, filters and normalizes the information received from monitoring probes, acting as a proxy for the Incident Detector. The Incident Detector interprets the monitoring data, applying correlation rules that result in incidents alerts. Additionally, a Data Analysis component retrieves operational data from IoT devices (for example, temperature measurements) to identify anomalous behaviour of the devices by checking patterns in the values measured, reporting the anomalies identified to the Incident Detector. Table 3-2 describes the components of the monitoring module and the requirements that those components are covered. The table also indicates implementation activities carried out to fulfil with the associated requirements.

Table 3-2. Evaluation of monitoring components: requirements and implementation

Subcomponent	Security Requirements Covered	Implementation details to cover the requirements
Data Filtering and pre-processing Broker	FR-21	The Data Filtering and pre-processing broker is filtering and aggregating events from multiple sources, therefore it can assist the monitoring and reaction components to handle multiple attack scenarios.
	FR-26	The Data Filtering and pre-processing broker is using Apache Kafka and Apache Storm, in order provide real-time filtering from multiple monitoring sources (IoT devices, MMT agent, etc) and providing the processed stream to the monitoring and reaction components.
	FR-49	Newly added monitoring instances can provide monitoring data that will be aggregated and provided to the monitoring and reaction components. Unsupported monitoring data types can be added through the creation of new topics, and if needed the implementation a service that collects monitoring data and acts as a Kafka Consumer.
	PR-2	As this component is used to make filtering of the events, the non-processing of special categories is supported, as we ignore any unneeded and possibly sensitive data and the processed outputs is not including any sensitive data.
	PR-4	As we use Apache Kafka for the storage and sharing of data, we use the retention policies available for Kafka in order to have perioding deletion of the data that have been processed. Also, it is possible to manually remove data that has been processed.
	PR-5	As this component is used to make filtering and pre-processing of the events, Deidentification of personal data supported, as with Apache Storm we replace sensitive data at real time. In our scenarios the removal of specific data was sufficient, and we didn't execute anonymization scenarios.
Data Analysis	FR-34	The Data Analysis module is capable of analysing, using machine learning algorithms, operational data to evaluate
	FR-44	

		anomalies on the values captured from IoT sensors, detecting patterns that might denote a potential incident.
Incident Detector	FR-21	The Incident Detector is capable of managing different events from different security probes by incorporating a plugin-based approach that process individual events, extract relevant information from them and convert into a common format. Several correlation rules are used to trigger alerts by matching certain conditions (i.e., type of events) based on several factors (i.e., frequency of events, timestamp), etc.
	FR-23	The Incident detector is capable of being deployed on a distributed approach with different nodes carrying out different specific activities. This allows the isolation of data from the processing engine. TLS mechanisms were used for the transfer of data between nodes.
	FR-26	TLS mechanisms were used for transferring data between monitoring agents and the incident detector. Additionally, every agent is uniquely identified at the Incident Detector by the exchange of tokens.
	FR-33	Different correlation rules at the Incident Detector allows to find incident by combining operational and network data. The Apache Storm correlation-based engine isolate correlation in different workers which might run in different nodes.
	FR-46	Only authorized agents can be configured at the Incident Detector to receive monitoring data. Different certificates can be used by the monitoring agents to report in a secure way information from the IoT infrastructure.
	FR-49	Only authorized agents can be configured at the Incident Detector to receive monitoring data. Different certificates can be used by the monitoring agents to report in a secure way information from the IoT infrastructure.
	NFR-16	The Incident Detector GUI allows to set up different users with different permissions depending on the information allowed to be visualized by each.
	PR-4	Data backups can be done at the Incident Detector, which can be scheduled to be removed

3.2.2 Reaction components

The Reaction module carries out the decision about the mitigations to react to a security incident. The Reaction module feeds from the alerts generated by the Monitoring module and from information received from the infrastructure about the mitigations supported by the infrastructure and about the IoT devices affected by the incident. The Verdict and Decision Support System (VDSS) contains the logic that decides about the most convenient mitigation depending on several factors, namely the type of incident to mitigate, the risk associated to the incident, the impact of the incident in the infrastructure, the importance of the assets affected by the incident and cost associated to every mitigation. The Asset Model provides with information about the current set up of the IoT infrastructure, updating the Reaction module with information about the type of devices, the importance, the configuration details and other aspects relevant for the decision on the reaction to enforce. The Security Alert Service (SAS) centralizes the information about incidents and reactions, reporting it to the Dynamic Security and Privacy Seal. The Mitigation Action Service

(MAS) receives the verdict about the suitability of the mitigations that can react to a certain security incident, triggering the enforcement of the chosen one by interfacing with the Security Orchestrator. Table 3-3 includes the analysis of the Reaction components, evaluating the requirements covered and the implementation actions taken to meet them.

Table 3-3. Evaluation of reaction components: requirements and implementation

Subcomponent	Security Requirements Covered	Implementation details to cover the requirements
Verdict and Decision Support System (VDSS)	FR-22	The VDSS communicates with the Incident Detector with TLS channels and with other relevant components by using Secure REST API.
	FR-31	
	FR-32	
	FR-37	The algorithms for the quantitative analysis of risk uses raw data, not linked to any concrete organization. Additionally, the data used for the reasoning is based on TLS channels and RabbitMQ queues secured with TLS certificates.
	FR-38	
	FR-39	The system model is retrieved by using secure REST API
	FR-40	The information about the effectiveness of a mitigation is obtained by using a secure REST API.
Assets Model	FR-39	The system model is retrieved by using secure REST API
Mitigation Action Service (MAS)	FR-28	The MAS reports mitigations by using secure RabbitMQ queues secured with TLS certificates
	FR-31	
	FR-32	
Security Alert Service (SAS)	FR-21	The SAS reports information to the DSPS by using secure RabbitMQ queues based on TLS certificates.
	FR-40	The SAS will retrieve the information about mitigations from a secure RabbitMQ queues based on TLS certificates.

3.3 ORCHESTRATION PLANE

ANASTACIA orchestration system leverages the strength of SDN technology to interconnect the cloud domain with IoT domain, whereby different IoT services are running. Formally, the communication between a user and an IoT domain happens through a list of chains of virtual network functions (VNFs) named service function chaining (SFCs) which consists of three parts the ingress point, the intermediate VNFs and the egress point.

The security orchestrator oversees orchestrating the security enablers according to the security policies generated and forwarded from other ANASTACIA's components taking into consideration the policies requirements and the available resources in different cloud providers, as well as the communication network characteristics including the use of secure channels with different levels including IPsec, SSL and TLS.
The order of the communications between the VNFs is defined according to the different SDN rules enforced thanks to the SDN controller. The nature and the size of the SFCs would be defined according to the nature of the user (a normal or a suspicious). Table 3-4 describes the components of the orchestration plane, as well as their requirements. The table also indicates implementation activities carried out to fulfil with the associated requirements.

Table 3-4. Evaluation of orchestration plane components: requirements and implementation

Subcomponent	Security Requirements Covered	Implementation details to cover the requirements
Security Orchestrator Engine (SOE)	FR-21 FR-32 FR-45 NFR-16	The security orchestrator engine (SOE) considers multiple attacks at the same time. To mitigate those attacks the SOE applies variant counter measures by deploying multiple security VNFs using OSM[3] and Openstack[4], as well as rerouting the traffics through those VNFs using ONOS[5] SDN controllers.
	FR-22	The SOE is able to mitigate the attack in an autonomous fashion by deploying different mitigation actions after receiving the successful detection of attacks thanks to MAS component. each request received from MAS is considered as an independent request that should be treated independently and parallel
	FR-23	Security Orchestrator communicates with other components through REST API for enabling micro services architecture. Although SOE is running with other orchestration plane components on top of the same bare-metal server, SOE could be also deployed on different a separate machine or a container (i.e., Docker).
	FR-42 FR-43	SOE includes also a smart routing functionality that consider also the changes of data traffic in the routes and the amount of resources used in different VNFs. According to the information received from Performance Data Analytics (PDA) component.
Security Orchestrator Optimizer (SOO)	FR-26 FR-32 FR-35	Security Orchestrator Optimizer (SOO) process the SOE reaction in order to avoid conflict with the existed architecture configuration. This process requires communication system model and policy interpreter.
	FR-29 FR-44 FR-45	SOO explores optimal strategies for selecting the appropriate and optimal SDN/NFV-based security mechanisms for preventing different attacks. ANASTACIA system leverages different mathematical techniques, such as mathematical optimization and machine learning techniques, to provide optimal SDN/NFV-based mitigation plane.
	FR-45	SOO executes the optimal reaction by updating SFCs through OSM and ONS.
System Model Service (SMS)	FR-22 FR-39 FR-46	The System model flexible autonomous component ensures consistent context for the different system parts with REST API interface.
Security Resource Planning (SRP)	FR-26	Security Resource Planning ensure resources availability in difference network functionalities besides the application of the rules and policy restriction.

[3] https://osm.etsi.org/
[4] https://www.openstack.org/
[5] https://onosproject.org/

Performance Data Analytics (PDA)	FR-26 FR-29 FR-37	Performance Data Analytics guarantees optimal decision using ML methods based on the collected data and monitoring context to better define appropriate mitigation plans for the Security Orchestrator Engine.
	FR-40	Performance Data Analytics evaluate with the increase of collected data furthermore processing complex criteria develops the significant effectiveness.
	FR-42 FR-43	PDA component keeps monitoring the network for detecting any over or under estimation of the resource utilization. Also, this component is responsible for detecting any bottleneck in the network or violation of the service level agreement. If so, PDA informs SOE about the anomalies.

3.4 DYNAMIC SECURITY AND PRIVACY PLANE

The DSPS plane will keep track of the security and privacy status of a system monitored by ANASTACIA. The derived information of each status change is stored with two different techniques: one based on permissioned blockchain and one based on Shamir secret sharing scheme[6].
The Security and Privacy Manager Analysis is composed by three services: the DSPS Seal Creation service, responsible of the creation of the security/privacy status, the DSPS Privacy Mappings service, responsible of computing the privacy risks associated to a security alert and the DSPS Storage service, responsible of the storage of public and private data.
The DSPS Agent role is to connect with the SAS and receive security alert messages. After converting the messages in STIX[7] (Structured Threat Information Expression) format, the Agent will use the Seal Creation and Privacy Mappings services to update the status of the system.
The DSPS GUI allow the users involved in the monitored system to inspect its current and past status. It is also used by auditor users (DPO and CISO) to update the status of the system by providing, for example, reports on performed Privacy Impact Assessments.

Table 3-5. Evaluation of dynamic security and privacy plane components: requirements and implementation

Subcomponent	Security Requirements Covered	Implementation details to cover the requirements
DSPS Storages	FR-16	The DSPS Storage service is based on blockchain and Shamir secret sharing scheme.
	FR-23	The DSPS Storage service which is based on blockchain and Shamir secret sharing scheme are distributed by definition.
	FR-50	Every change of the status system is stored in the DSPS Storage service.
Security and Privacy Manager Analysis	FR-17	DSPS Privacy seal agent includes mapping of security risk and privacy risk.
	PR-9	All personal information is encrypted by default.
Dynamic Security and Privacy Seal Agent	FR-46	The Agent can be deployed as Docker container.
	FR-15	The DSPS User Interface provides real-time seal information.

[6] Shamir, Adi. "How to share a secret." *Communications of the ACM* 22.11 (1979): 612-613.
[7] https://oasis-open.github.io/cti-documentation/

Dynamic Security and Privacy Seal User Interface	FR-52	It includes DPOs and CISOs inputs on seal update.
	FR-50 FR-51 FR-52	This component allows the users to graphically inspect the information contained in the DSPS Storage service.
	PR-10	It includes periodic check-up/update of organizational measure related to privacy policies.

4 TRACEABILITY OF IMPLEMENTATION, REQUIREMENTS AND THREATS

The following sections aggregate and provide insights about the information gathered about the implantation activities of the ANASTACIA framework. More specifically the outcomes of Deliverable D2.4 are combined with the information included in Sections 2 and Sections 3 of the current document, in order to evaluate the level of fulfilment of requirements by the ANASTACIA components and level of protection against the threats identified in D2.4 and the new threats identified in Section 2.2.

4.1 EVALUATION OF THREATS AND REQUIREMENTS

Derived from the new security threats identified in D2.6, five new IoT specific threats are included in this analysis. According to the DREAd evaluation carried out in Section 2.2, the severity of these new threats is included in Figure 4-1, which integrate the severity of the new threats (in blue) with the severity of the threats identified in D2.4 (in orange). As we can see, the new threat T49, which deals with the 0-day vulnerabilities, rises to the top three threats. This is quite consistent given the high impact of such threats and the difficulty to address the protection against unknown vulnerabilities.

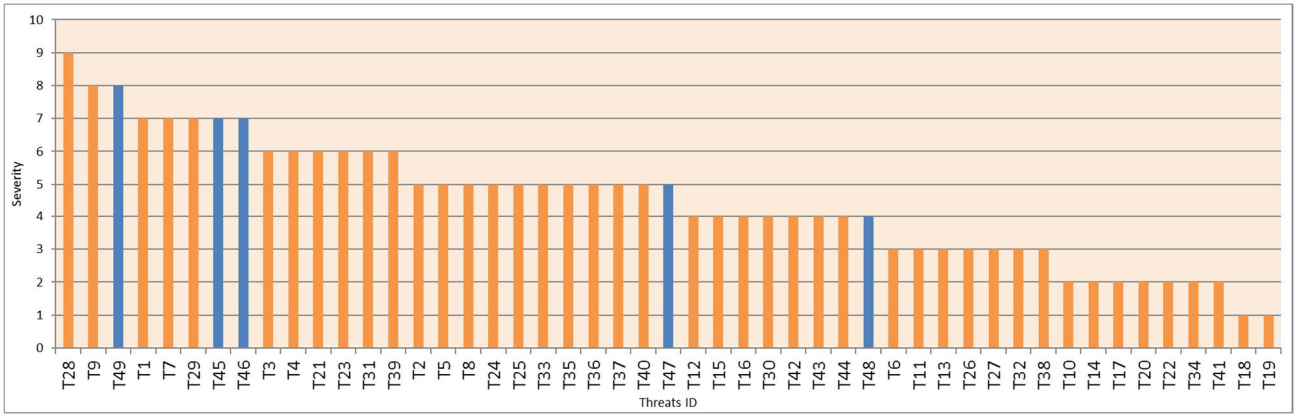

Figure 4-1. Threat severity highlighting (in blue) the new ones

Following the methodology described in D2.4, the severity scores are used to calculate the criticality of the requirements. To this end, the latest set of requirements produced in D1.4 are used provide with the latest possible evaluation. In order to calculate the criticality of the new set of requirements it is necessary to link the security threats to the requirements. Table 4-1 maps every security threat (the former ones elicited in D2.4 and the new ones elicited in D2.8) with the new set of requirements elicited in D1.4 (which have been added to the Annex I of the current deliverable). This mapping is used to evaluate what requirements are, to some extent, capable, or at least contribute to, minimize the identified security threats. It is important to notice that just functional requirements have been used in this mapping, as it is considered non-functional and privacy requirements are transversal to the platform, and therefore, to be fulfilled by all the components.

Table 4-1. Link between the updated set of security threats (from D2.6) and the new set of requirements (from D1.4)

Thread id	Security Threats	Related requirements from the final set
T1	Data flow from device is interrupted	FR-22, FR-25, FR-26, FR-33, FR-40, FR-42, FR-43, FR-46, FR-47, FR-55
T2	Code execution due to buffer overflow vulnerability	FR-21, FR-22, FR-25, FR-26
T3	Unauthorized access to the platform by malicious users	FR-21, FR-22, FR-25, FR-26, FR-41, FR-45, FR-53, FR-56, FR-57

T4	Denial of Service attacks (Spoofing, Flooding, Ping of Death, WinNuke, XDoS)	FR-21, FR-22, FR-25, FR-26, FR-32, FR-35, FR-36, FR-37, FR-38, FR-46
T5	SQL Injection	FR-21, FR-22, FR-24, FR-25, FR-26, FR-35, FR-36, FR-37, FR-38
T6	0-day vulnerability to remotely target a device	FR-21, FR-22, FR-25, FR-26, FR-31, FR-55
T7	Malware spread via network to exploit sensitive sensors	FR-21, FR-22, FR-25, FR-26
T8	Identity fraud	FR-21, FR-22, FR-25, FR-26, FR-41, FR-53
T9	Unsolicited & infected e-mail	FR-21, FR-22, FR-25, FR-26
T10	Malicious code/software activity	FR-21, FR-22, FR-25, FR-26
T11	Abuse of information leakage	FR-21, FR-22, FR-25, FR-26
T12	SSL CA infiltration	FR-21, FR-22, FR-25, FR-26, FR-27, FR-28, FR-29, FR-30, FR-35, FR-36, FR-37, FR-38, FR-39, FR-49, FR-50, FR-51, FR-52, FR-53, FR-54, FR-57
T13	Manipulation of hardware & software	FR-21, FR-22, FR-23, FR-25, FR-26, FR-34
T14	Routing table manipulation	FR-21, FR-22, FR-23, FR-25, FR-26, FR-33, FR-42
T15	DNS spoofing	FR-21, FR-22, FR-23, FR-25, FR-26, FR-46, FR-47
T16	DNS poisoning	FR-21, FR-22, FR-23, FR-25, FR-26, FR-46, FR-47
T17	Falsification of configuration	FR-21, FR-22, FR-25, FR-26, FR-27, FR-28, FR-29, FR-30, FR-35, FR-36, FR-37, FR-38, FR-39, FR-42, FR-43, FR-44, FR-45, FR-48 FR-49, FR-50, FR-51, FR-52, FR-54
T18	Autonomous System hijacking	FR-21, FR-22, FR-25, FR-26, FR-45
T19	Misuse of audit tools	FR-21, FR-22, FR-25, FR-26, FR-35, FR-36, FR-37, FR-38, FR-39, FR-42, FR-43, FR-50, FR-51, FR-52, FR-54
T20	Falsification of records	FR-21, FR-22, FR-25, FR-26, FR-41, FR-44, FR-50, FR-51, FR-52, FR-54
T21	Unauthorised use of administration of devices & systems	FR-21, FR-22, FR-25, FR-26, FR-35, FR-36, FR-37, FR-38, FR-42, FR-48, FR-53, FR-55
T22	IMPI Protocol	FR-21, FR-22, FR-25, FR-26
T23	DNS Register Hijacking	FR-21, FR-22, FR-25, FR-26
T24	Unauthorised installation and use of software	FR-21, FR-22, FR-25, FR-26, FR-34, FR-35, FR-36, FR-37, FR-38, FR-40
T25	Unauthorised installation of software	FR-21, FR-22, FR-25, FR-26, FR-35, FR-36, FR-37, FR-38, FR-40

T26	Abuse of personal data compromising confidential information	FR-21, FR-22, FR-24, FR-25, FR-26, FR-39, FR-41
T27	Abuse of authorizations	FR-21, FR-22, FR-24, FR-25, FR-26, FR-35, FR-36, FR-37, FR-38, FR-45, FR-53
T28	Hoax	FR-21, FR-22, FR-25, FR-26, FR-47
T29	Badware (Virus, Worm, Trojan, Rootkit, Botnets, Spyware, Scareware)	FR-21, FR-22, FR-25, FR-26, FR-47
T30	Remote activity (execution)	FR-21, FR-22, FR-25, FR-26, FR-34, FR-45
T31	Targeted attacks (including ATP)	FR-21, FR-22, FR-25, FR-26, FR-45
T32	War driving	FR-21, FR-22, FR-25, FR-26
T33	Interception compromising emissions	FR-21, FR-22, FR-25, FR-26
T34	Targeted espionage attempts to obtain sensitive information	FR-21, FR-22, FR-25, FR-26
T35	Rogue hardware	FR-21, FR-22, FR-25, FR-26
T36	Interfering radiations	FR-21, FR-22, FR-25, FR-26
T37	Replay of messages	FR-21, FR-22, FR-23, FR-25, FR-26, FR-48
T38	Network reconnaissance and information gathering	FR-21, FR-22, FR-25, FR-26, FR-33, FR-39, FR-42, FR-43, FR-45, FR-48
T39	Man in the middle/ session hijacking	FR-21, FR-22, FR-25, FR-26, FR-39, FR-46, FR-47
T40	Repudiation of actions	FR-21, FR-22, FR-25, FR-26, FR-34, FR-40, FR-41
T41	Damage caused by a third party (External or internal)	FR-21, FR-22, FR-25, FR-26
T42	Loss of (integrity of) sensitive information	FR-21, FR-22, FR-25, FR-26, FR-39, FR-41, FR-48
T43	Loss of information in the cloud or destruction of devices, storage media and documents	FR-21, FR-22, FR-25, FR-26
T44	Information leakage	FR-21, FR-22, FR-24, FR-25, FR-26, FR-39, FR-41, FR-48
T45	Compromise data confidentiality	FR-21, FR-22, FR-24, FR-25, FR-26, FR-39, FR-41
T46	Spoofing attack	FR-21, FR-22, FR-25, FR-26, FR-46, FR-47
T47	Man-in-the-middle attack	FR-21, FR-22, FR-25, FR-26, FR-39, FR-46, FR-47, FR-55
T48	Exploitation of vulnerabilities of IoT device to execute attacks	FR-21, FR-22, FR-25, FR-26, FR-55
T49	0-day vulnerability	FR-21, FR-22, FR-25, FR-26, FR-31, FR-55

With the threats vs requirements mapping carried out above we are able to calculate the criticality of the new set of requirements. Again, following the methodology created in D2.4, we can use the impact of the

new requirements (which values are included in Section 2.1 of the current deliverable) with the threat severity obtained with the DREAd analysis carried out in D2.4 and D2.8. Annex II includes the complete table that shows all the scores, the mapping and the partial values used to obtain the criticality. Figure 4-2 summarizes these scores, which groups in different colours the most critical ones. It is worth noticing that the most critical requirements are related to the mitigation of the 0-day vulnerabilities and the mitigation of slow DDoS attacks, which are in fact directly related to two of the new security threats analysed in Section 2.2.

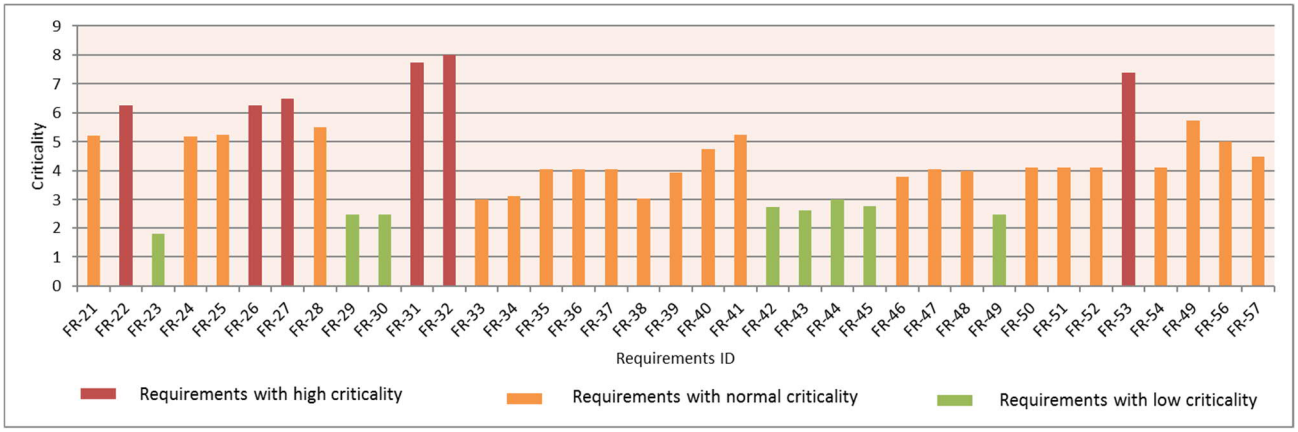

Figure 4-2. Evaluation of criticality for the new set of functional requirements

4.2 PREVENTING THREATS THROUGH THE ANASTACIA FRAMEWORK

Having included the new set of requirements and the new threats in the evaluation methodology created in D2.4, next step is the traceability of the requirements with respect to the ANASTACIA components, their implementation, the security threats and the prevention recommendations elicited in D2.4. The complete evaluation is included in Table 4-2. The three first columns of Table 4-2 are obtained directly from D2.4 and shows the prevention actions to include in the implementation of the ANASTACIA components, with details about how to include it in the development activities. The additional columns detail whether such prevention recommendation has been incorporated to the concerned ANASTACIA components, explaining also how it has been included (or in case it is not a justification of why it was not). Also, a mapping about the threats prevented is included, which is obtained directly from D2.4 (where a mapping between preventions and threats was done. This will be used later to perform the traceability of the threats covered or not covered by every ANASTACIA component). The last column of Table 4-2 incorporates a mapping between the requirements that are related to every threat prevented. This information is taken from Table 4-1 and can be used to better evaluate the fulfilment of every requirement with the implementation actions included when developing every ANASTACIA component, and to analyse to what extent these implementation actions are capable of prevent every related threat.

In the next subsection it is included an example of evaluation of the traceability of one of the components of the ANASTACIA framework, which allows to identify threats covered and threats not covered.

Table 4-2. Final analysis of the ANASTACIA platform and threat prevention activities

Prevention	ANASTACIA approach	ANASTACIA components	Incorporated (YES/NO/Partially)	Explanation (How, reason)	Threats prevented	Related requirements for the set of threats prevented
P1 - Log access activities to detect the attack and prevent unauthorized access	• Trusted communication among ANASTACIA components using encrypted data and PKI to manage trust among components • GUIs built over HTTPS, with valid certificates issued by a trusted CA. ANASTACIA deployed AAA controllers that logs the access activity to IoT devices • ANASTACIA has deployed with agents compiling the access activities log and monitors anomalous access attempts	All components	YES	Logs are distributed from the agents to the incident detector filtered by the Data filtering component. These logs are the basic unit of evidence that is used to detect security incidents. Special importance for this prevention is the AAA agent which log about unauthorized access to IoT devices. Additionally, the Data Filtering and pre-processing Broker has been created in order to assist the monitoring from multiple sources.	T1 T4 T10	FR-21, FR-22, FR-25, FR-26, FR-32, FR-33, FR-35, FR-36, FR-37, FR-38, FR-40, FR-42, FR-43, FR-46, FR-47, FR-55
P2 - Perform scheduled	• Distributed sensors provide monitoring	Incident detector	NO	Automatic vulnerability assessment was not	T2 T11	FR-21, FR-22, FR-25, FR-26

vulnerability assessments based on latest updates on discovered vulnerabilities	agents with logs (i.e., NIDS sensors such as snort) • Dynamic deployment of virtual sensors through VNFs (i.e., virtual honeypots) providing with events • ANASTACIA counts with reaction capabilities to mitigate incidents detected at the IoT platform, including also the mitigation of known or discovered vulnerabilities by scheduling the patching or update of the firmware of IoT devices	Verdicts and Decision Support System	NO	included in the platform, but the platform is compatible with vulnerability assessment report, which would notify about vulnerable devices. The incident detector would report about the vulnerabilities reported in the infrastructure and recommend any mitigation to minimize the impact (i.e., proposing patching the IoT device or isolating the device till the update is done)		
		Security Enabler Repository	NO			
P3 - Apply the latest updates on software and firmware for devices and computers deployed in the targeted infrastructure.	• Mitigation actions are designed at the orchestrator in order to guarantee the compatibility of the actions with the IoT platform and interfaces. • ANASTACIA plans to execute periodic	Policy Editor Tool	YES	Policy Editor Tools allows defining IoT control security policies in order to update IoT devices behaviours.	T2 T7	FR-21, FR-22, FR-25, FR-26
		Policy Interpreter	YES	Policy Interpreter is able to translate IoT control policies into IoT Controller configurations.		

	secure update procedures in order to keep the systems updated, without compromising the functionalities.	IoT Controller	YES	IoT Controller is able to enforce IoT updates in the IoT devices.		
		Orchestrator	YES	Security orchestrator is able to prevent different attacks using NFV and SDN enablers without creating conflicts.		
		Security Enabler Repository	YES	Security Enabler Repository is responsible for providing various capabilities can be offered by the system.		
P4 - Provide distributed authorization mechanisms to control the access of devices & systems	• In AAA architecture, DCAPBac protocol provides a distributed scheme for the generation and verification of capability tokens which will be used to send the authorizations with the query from the user to subscribe to a topic or request an actuation in IoT devices.	IoT nodes	YES	IoT devices are deployed in a secured way, always requesting authorization mechanisms to operate, logging unauthorized activities which can be used to detect security incidents	T3 T21 T35 T40	FR-21, FR-22, FR-25, FR-26, FR-35, FR-36, FR-37, FR-38, FR-34, FR-40, FR-41, FR-42, FR-48, FR-53, FR-55
		Policy Editor tool	YES	Policy Editor Tool allows model high-level authorization security policies.		
		Policy Interpreter	YES	Policy Interpreter translates high-level authorization policies into medium-level authorization policies as well as medium-level		

				authorization policies into DCAPBac configurations.		
P5 - Use input validation	• The development of ANASTACIA components relies on secure software practices, which includes implementation of data validation mechanisms to prevent code injection or buffer overflow vulnerabilities. Additionally, ANASTACIA includes detection capabilities for code injection such as SQL injection.	All components	YES	Several components of the ANASTACIA platform require validation of the data inserted by the system administrator. Several GUI are available to monitor the incident detector, to check the status of the Seal or to configure mitigation rules used by the Verdict and decision support system. All those GUIs count with mechanisms to validate the data inserted during the operation of the tool and to prevent code injection incidents.	T4 T6	FR-21, FR-22, FR-25, FR-26, FR-32, FR-35, FR-36, FR-37, FR-38, FR-46, FR-31, FR-55
P6 - Use the principle of least privilege	• ANASTACIA plans to design security policies and authorization procedures through the adoption of least privilege approaches.	User plane components	YES	Policy Editor Tool allows policy definition according on the organisation policies.	T4 T13	FR-21, FR-22, FR-23, FR-25, FR-26, FR-32, FR-34, FR-35, FR-36, FR-37, FR-38, FR-46
		Incident detector	YES	The incident detector includes several correlation policies that optimize the usage of information received from agents, considering just the events coming from authorized sources.		

		Verdict and Decision Support System	YES	The capabilities of the verdict and decision support system are deployed as part of the incident detector, applying the same actions as the ones mentioned above for the incident detector		
		IoT nodes	YES	The protection of the IoT devices is based upon the definition of security policies		
P7 - Block network traffic from the attack source based on IP filtering	• SDN controller provides IPv4 and IPv6 filtering of network traffic from the attack source. • ANASTACIA reaction component plans to deploy IP filtering policies/rules on network nodes in order to mitigate running threats, by dropping packets coming from malicious source IP addresses using SDN	Security orchestrator	YES	Security orchestrator is able to provide the communication between different peers using both IPv4 and IPv6 protocols. Also, it is able to deploy an IPv4 and IPv6 based filtering virtual function that able to filter the traffic by allowing or denying some ongoing connections.	T5	FR-21, FR-22, FR-24, FR-25, FR-26, FR-35, FR-36, FR-37, FR-38
		Security policies repository	YES	Policy repository provides filtering policies templates		
		Policy Editor Tool	YES	Policy Editor tool allows defining filtering policies		
		Policy Interpreter	YES	Policy Interpreter translates filtering policies		

				to different enabler configurations.		
		Verdict Reactions	YES	The verdict reactions only apply to the affected devices, either affected directly or indirectly.		
		Security Enabler Repository	YES	This component is able to provide different capabilities can be supported by the system.		
P8 - Testing activities will allow to minimize the insertion of malicious code in the system	• ANASTACIA includes sensors capable to detect code injection, such as SQL injection. The ANASTACIA agents and incident detector are capable of correlating events received from such sensors and alert about them	User plane components	YES	User plane components are namely GUI for managing several components of the ANASTACIA infrastructure. All of them include input validation strategies to prevent inject code injection attacks.	T8	FR-21, FR-22, FR-25, FR-26, FR-41, FR-53
		Databases of the infrastructure	YES	All databases used in the ANASTACIA platform are updated to the latest version, protecting them against SQL injection attempts. Supported by the input data validation forced at GUIs and other components allows to guarantee the protection against this type of attacks.		

P9 - Use strong authentication algorithms, preferably based on PKI	• Usage of trusted certificates when accessing dashboards and other management tools • In AAA architecture, ECC protocol is an elliptic curves solution for constrained IoT devices to enables authentication based on PKI. The approach provides security mechanisms such as encryption and digital signature.	User plane components	YES	Policy Editor tool allows defining authentication policies. Policy models allows PKI based authentication policies instantiation.	T9	FR-21, FR-22, FR-25, FR-26
		Policy interpreter	YES	Policy Interpreter allows authentication policies translation into final authentication configurations.		
		IoT nodes	YES	IoT devices are deployed in a secured way, always requesting authorization mechanisms to operate, logging unauthorized activities which can be used to detect security incidents		
P10 - Provide with antivirus/antimalware scans	• ANASTACIA attaches different kinds of sensors and detection tools to the IoT platform. The ANASTACIA agents, in charge of collecting events from these sensors and detection tools, can be extended to receive events from antivirus/antimalware tools that might be	All components	NO	No antivirus has been included in the ANASTACIA platform or testbed. However, in case this tool is included the approach would be the same as for the rest of the tools, collecting reports about virus detection and processed by the incident detector to notify about an ongoing incident.	T10 T11 T12 T29 T31	FR-21, FR-22, FR-25, FR-26, FR-27, FR-28, FR-29, FR-30, FR-35, FR-36, FR-37, FR-38, FR-39, FR-45, FR-47, FR-49, FR-50, FR-51, FR-52, FR-53, FR-54, FR-57

	installed in the platform to protect					
P11 - Apply periodic updates of SSL CA	• This prevention will not apply during the project development although remains as a good practice for all components requiring user authentication or the usage of a secure communication channel	Policy Editor Tool	NO	ANASTACIA provides easily extensible operational models but the implementation effort has been focused on other capabilities like authentication, authorization, channel protection, filtering, forwarding, IoT control, monitoring and data privacy.	T12	FR-21, FR-22, FR-25, FR-26, FR-27, FR-28, FR-29, FR-30, FR-35, FR-36, FR-37, FR-38, FR-39, FR-49, FR-50, FR-51, FR-52, FR-53, FR-54, FR-57
		Security sensors	YES	The communication between sensors and agents is secured using TLS, with periodic updates of the certificates used		
		Data Filtering and pre-processing broker	YES	For collecting data from the IoT sensors (through the IoT Broker) the token should be regularly updated.		
		Dynamic Security and Privacy Seal User Interface	YES	The communication between all components is secured using TLS, with periodic updates of the certificates used		
P12 - Provide authentication protocol for new	• This prevention will not apply during the project development	IoT nodes	NO	Not being a priority, this prevention was not considered to be included.	T13	FR-21, FR-22, FR-23, FR-25, FR-26, FR-34

hardware connected to the network with identification and sequence number.	although remains as a good practice for all connected devices	Policy Editor tool	YES	Policy Editor Tool allows defining policy for orchestration as a set of policies for bootstrapping		
		Policy Interpreter	YES	Policy interpreter is able to translate policies for orchestration, e.g., a set of authentication policies for bootstrapping.		
P13 - Schedule recurring assessments of authorizations	• PANA is a network authentication protocol for constrained IoT device ANASTACIA plans to periodically review authorization procedures and authorized accounts for the protected components.	IoT nodes	YES	IoT nodes use PANA for authentication by default.	T13 T17 T19	FR-21, FR-22, FR-25, FR-26, FR-27, FR-28, FR-29, FR-30, FR-34 FR-35, FR-36, FR-37, FR-38, FR-39, FR-42, FR-43, FR-44, FR-45, FR-48 FR-49, FR-50, FR-51, FR-52, FR-54
		Policy Editor tool	YES	Policy Editor Tool allows defining PANA authentication policies.		
		Policy Interpreter	YES	Policy interpreter is able to translate PANA authentication policies.		
P14 - Manage privileged sessions (such as control outbound traffic)	• In AAA architecture, DCAPBac protocol provides recurring assessments of authorizations. • ANASTACIA plans to guarantee quality of service for privileged hosts (e.g. sensitive services requiring high availability), by working on network nodes configuration.	IoT nodes		IoT devices are deployed in a secured way, always requesting authorization mechanisms to operate, logging unauthorized activities which can be used to detect security incidents	T13 T14	FR-21, FR-22, FR-23, FR-25, FR-26, FR-33, FR-34, FR-42
		IoT network	NO	Quality of service from/to IoT nodes was not considered due to priority on the development of		

				security related objectives.		
P15 - Provide secure routing mechanism based on SDN, software definition network in the control plane	ANASTACIA provide with SDN/NFV orchestration based on security policy which allows to deploy security enablers to react to incidents and enforce the fulfilment of the security policy	Security orchestrator	YES	Security orchestrator is able to manage the communication between different peers by either allowing or denying some ongoing connections.	T14	FR-21, FR-22, FR-23, FR-25, FR-26, FR-33, FR-42
		Security Enabler Repository	YES	This repository contains references to enablers based on SDN/NFV functions		
		IoT network	YES	SDN/NFV capabilities were included as one of the main objectives of ANASTACIA to interact with the IoT infrastructure for the enforcement of mitigations and security policies.		
P16 - Use access control mechanisms	In AAA architecture, DCAPBac protocol provides access control mechanisms to resources of IoT devices and IoT-Broker ANASTACIA plans to deploy strong authentication procedures/protocols to access sensitive nodes.	All components	YES	Policy Editor tool and Policy Interpreter allows defining and translate authentication and authorization policies.	T14 T21 T22 T24 T25 T30 T32	FR-21, FR-22, FR-23, FR-25, FR-26, FR-33, FR-42, FR-35, FR-36, FR-37, FR-38, FR-40, FR-42, FR-48, FR-53, FR-55

P17 - Use anomaly detection techniques	ANASTACIA deployed an Incident Detector that correlates events monitored and generate alerts for the anomalies detected	IoT network	YES	ANASTACIA has deployed with network sniffers that analyse traffic to detect anomalies and potential incidents.	T14 T33 T34 T37 T44	FR-21, FR-22, FR-23, FR-25, FR-26, FR-33, FR-41, FR-42, FR-48
		IoT nodes	YES	Network traffic generated and consumed by IoT is sniffed and analysed by network sniffers.		
		Monitoring components	YES	The results of the network sniffing is evaluated by monitoring components to detect incidents.		
P18 - Use DNSSEC	This prevention will not apply during the project development although remains as a good practice to be considered in a real production environment	IoT network	NO	Not being a priority, this prevention was not included in the ANASTACIA platform.	T15 T16 T23	FR-21, FR-22, FR-23, FR-25, FR-26, FR-46, FR-47
P19 - Provide assessments for configuration values	Configuration schemes for ANASTACIA components will be documented and tested before committing them	All components	YES	Data Filtering and pre-processing Broker is composed by a specially configured Kafka, an application using Storm for parallel and real time processing, and applications that act as adapters to the various components or sensors. All tools are deployable through docker-compose files to ensure the proper	T17	FR-21, FR-22, FR-25, FR-26, FR-27, FR-28, FR-29, FR-30, FR-35, FR-36, FR-37, FR-38, FR-39, FR-42, FR-43, FR-44, FR-45, FR-48 FR-49, FR-50, FR-51, FR-52, FR-54

				testing and the stability of the component.		
P20 - Use TPM to provide mutual attestation	This prevention will not apply during the project development although remains as a good practice to be considered in a real production environment	IoT network	NO	Not being a priority, this prevention was not included in the ANASTACIA platform.	T18	FR-21, FR-22, FR-25, FR-26, FR-45
P21 - Provide data analysis tools to validate records according to historical data	ANASTACIA provides with anomalous behaviour analysis capabilities by incorporating deep learning techniques that feed from current and past data to infer potential anomalies on IoT devices.	Data Analysis	YES	Machine learning algorithms are used to analyse operational data to infer potential anomalies.	T20	FR-21, FR-22, FR-25, FR-26, FR-41, FR-44, FR-50, FR-51, FR-52, FR-54
P22 - Schedule recurring assessments and validation of records	UTRC Data analysis can provide assessments and validation of temperature values in real time.	Data Analysis	YES	Machine learning algorithms use current and past data to detect anomalies on the data produced by IoT sensors.	T20	FR-21, FR-22, FR-25, FR-26, FR-41, FR-44, FR-50, FR-51, FR-52, FR-54
P23 - Log activities to detect modifications	ANASTACIA has deployed agents compiling the access activities logs	Incident Detector	YES	Logs are distributed from the agents to the incident detector filtered by the Data filtering component. These logs are the basic unit of evidence that is used to detect security incidents.	T20	FR-21, FR-22, FR-25, FR-26, FR-41, FR-44, FR-50, FR-51, FR-52, FR-54
		Data filtering and pre-processing broker	YES			
P24 - Use integrity mechanisms	DTLS protocol provides the security services such as integrity, authentication and confidentiality in P2M	All components	YES	Policy Editor Tool and Policy interpreter allows defining and translate DTLS security policies in	T20	FR-21, FR-22, FR-25, FR-26, FR-41, FR-44, FR-50, FR-51, FR-52, FR-54

	communication. ANASTACIA uses TCP based communications to guarantee network level integrity of the exchanged data.			order to guarantee confidentiality and integrity.		
		IoT network	Yes	Data Filtering and pre-processing Broker, collects, aggregates, filters, pre-process and temporarily stores, monitoring data, sensor data and log activities.		
P25 - Enabling HTTPS for all web apps and services	ANASTACIA uses HTTPS connections for all the components deployed at the user plane: seal manager GUI, incident dashboard and policy editor tool	User plane components	YES	All GUI used in ANASTACIA are secured with HPPS	T23 T39	FR-21, FR-22, FR-25, FR-26, FR-39, FR-46, FR-47
		All components	YES	All components which implements HTTP APIs can be HTTPS enabled.		
		IoT network	YES	All HTTP based traffic exchange uses HTTPS		
P26 - Provide privacy mechanism based on encryption scheme of personal data	ANASTACIA provides with a Data Management plan that regulates the use of personal data	IoT nodes	Partially	Data is encrypted for IoT nodes, but for those devices supporting data encryption.	T26	FR-21, FR-22, FR-24, FR-25, FR-26, FR-39, FR-41
		User plane components	YES	Policy Editor Tool and Policy interpreter allows defining data privacy policies.		
		Policy Interpreter	YES	Policy Editor Tool and Policy interpreter allows translating data privacy policies into final privacy configurations		

		All databases of the platform	YEs	All data is stored encrypted		
P27 - Security awareness and continuous education of all the involved users	ANASTACIA includes security guidelines and privacy risk modelling and contingency assessment that provides with a useful source of information for system admin training and continuous education.	Incident Detector	YES	The Incident Detector counts with a Knowledge Base that provide with information about the incidents detected.	T26 T28	FR-21, FR-22, FR-24, FR-25, FR-26, FR-39, FR-41
		Verdict and Decision Support System	NO	Being added a Knowledge Base to the incident detector, it was not included again to toe VDSS.		
P28 - Provide a maximum lifetime for using authorization keys	In AAA architecture, DCAPBac protocol provides a maximum lifetime for using capability tokens that are authorization keys. Periodically schedule change of authorization keys. This is a good practice that is not a priority during the project development although it remains very relevant for a real environment.	IoT nodes	Partially	DCAPBac protocol was included depending on the capabilities of the IoT device	T27	FR-21, FR-22, FR-24, FR-25, FR-26, FR-35, FR-36, FR-37, FR-38, FR-45, FR-53
		User plane components	NO	Not being a priority, the scheduled change of authorizations was not included to the ANASTACIA platform.		
P29 - Enforcing short lifetime of authorization keys	In AAA architecture, DCAPBac protocol provides short time of authorization keys.	User plane components	NO	Not being a priority, the scheduled change of authorizations was not included to the ANASTACIA platform.	T27	FR-21, FR-22, FR-24, FR-25, FR-26, FR-35, FR-36, FR-37, FR-38, FR-45, FR-53

	Periodically schedule change of authorization keys. This is a good practice that is not a priority during the project development although it remains very relevant for a real environment.	IoT nodes	Partially	DCAPBac protocol was included depending on the capabilities of the IoT device		
P30 - Provide authenticated wireless access points	IoT devices with wireless access will be protected with secure authentication, adding also AAA logging to detect unauthorized access attempts	IoT nodes	Partially	AAA capabilities was included depending on the capabilities of the IoT device	T32	FR-21, FR-22, FR-25, FR-26
P31 - Provide secure communication channel for integrity and confidentiality	DTLS protocol provides the security services such as integrity, authentication and confidentiality in P2M communication. ANASTACIA components will communicate each other by using secure connections	IoT nodes	Partially	DTLS protocol was included depending on the capabilities of the IoT device	T33 T37 T38	FR-21, FR-22, Fr-23, FR-25, FR-26, FR-33, FR-39, FR-42, FR-43, FR-45, FR-48
		All components	YES	Policy Editor Tool and Policy interpreter allows defining and translate DTLS security policies in order to guarantee confidentiality and integrity.		
P32 - Obfuscate or encrypt data	In AAA architecture, ECC protocol provides security mechanisms such as encryption and digital signature.	IoT nodes	Partially	Obfuscation and encryption of data was included depending on the capabilities of the IoT device	T34 T42	FR-21, FR-22, FR-25, FR-26
		All components	YES	Policy Editor Tool and Policy interpreter allows		

	ANASTACIA will encrypt sensitive communications and stored data through the adoption of well-known encryption protocols able to guarantee confidentiality.			defining and translate data privacy policies.		
P33 - Use TPM make sure that hardware is trusted	This prevention will not apply during the project development although remains as a good practice to be considered in a real production environment	IoT nodes	NO	Not being a priority, this feature was not included in the ANASTACIA platform	T35	FR-21, FR-22, FR-25, FR-26
P34 - Apply dynamic scheme to detect interferences and change radio channel	This prevention will not apply during the project development although remains as a good practice to be considered in a real production environment	IoT nodes	NO	Not being a priority, this feature was not included in the ANASTACIA platform	T36	FR-21, FR-22, FR-25, FR-26
P35 - Provide secure channel with sequence number for M2M communication	DTLS protocol provides security services such as integrity, authentication and confidentiality in P2M communication.	All components	Partially	Secure communication channels were used between all components of the platform. Its applicability to IoT nodes depends on the capabilities of the device.	T37 T39	FR-21, FR-22, FR-23, FR-25, FR-26, FR-39, FR-46, FR-47, FR-48
P36 - Use of timestamps	DTLS protocol provides the security services such as integrity, authentication and confidentiality in P2M communication.	All components	Yes	One of the pre-processing reasons is that data without timestamps can be removed or timestamp can be added by the Data Filtering and pre-processing Broker.	T37	FR-21, FR-22, FR-23, FR-25, FR-26, FR-48

P37 - Enforcing short session timeouts	This prevention will not apply during the project development although remains as a good practice to be considered in a real production environment	User plane components	NO	Not being a priority, this feature was not included in the ANASTACIA platform	T39	FR-21, FR-22, FR-25, FR-26, FR-39, FR-46, FR-47
P38 - Use digital signatures on the performed actions	In AAA architecture, ECC protocol provides security mechanisms such as encryption and digital signature.	User plane components	YES	TLS certificates were used at the user side GUIs.	T40	FR-21, FR-22, FR-25, FR-26, FR-34, FR-40, FR-41
P39 - Schedule recurring backup of the information in multiple places	ANASTACIA plans to execute periodic backups, prior to updates (if any).	All databases of the platform	YES	Periodic backups are done at the Incident Detector when a maximum size is reached.	T41 T42 T43 T44	FR-21, FR-22, FR-24, FR-25, FR-26, FR-39, FR-41, FR-48

4.3 CASE STUDY: CHECKING IMPLEMENTATION, PREVENTIONS AND THREATS WITH AN ANASTACIA COMPONENT

All the information included both in D2.4 and D2.8 can be used to trace back the level of protection that the ANASTACIA components have against the security threats identified. The final purpose of the methodology created in T2.4 is to be able to identify the effectiveness of the implementation activities, providing with security guidelines to produce components protected by design against threats. However, it is not enough with just providing those guidelines. It is also required a way to identify whether those guidelines have been finally incorporated. This subsection shows an example of such trace-back evaluation, considering one of the components of the ANASTACIA platform: the incident detector. The same exercise can be done with the rest of the components of the ANASTACIA platform. However, for the sake of simplicity it was shown just one example. The summary of the traceability evaluation is shown in Table 4-3. Using the information included in D2.4 and in Table 4-2 of the current document it has been listed the prevention actions related to the Incident Detector. With this list of prevention actions, we can go to table D2.4 where a mapping between preventions and threats was done. The resulting threats are the ones that this component should cover if the prevention recommendations are followed when developing the component. The column "Threat covered" shows the threats that, according to the analysis done in Table 4-2 of the current document, have been finally covered after developing the component. Mapping the columns "Threats to cover" and "Threats covered" shows that there are additional threats covered by the component which were not supposed to be covered (for example, T38). However, it is more important to identify the threats that are supposed to be covered and, according to the methodology here presented, was not finally covered. Analysing that we can check that T9 was initially planned to be covered for the incident detector. However, checking the evaluation done during the development activities, we can see that T9 is not considered.

Next step would be the evaluation of the threat not covered, checking the related requirements (by looking at Table 4-1) and identifying possible flows when evaluating the fulfilment of the requirements. Looking at the description for T9 we can see that it is related to "Unsolicited & infected email". Checking the criticality of such threat we can see that it is very high. This is consistent with the attacks associated to such threats, which benefit of social engineering actions to infect infrastructures via email with malicious attachments. While this is critical in infrastructures using active usage of emails and attachments, the impact on a platform like ANASTACIA, which special focus on IoT infrastructures, is very minor as there is no usage of email or attachments. So, although it is true that such threat seems not to be covered during the implementation of the ANASTACIA platform, we consider that it is not relevant to revisit both requirements and implementation activities to cover it.

Table 4-3. Traceability analysis for the Incident Detector

Component	Related Preventions	Threats to cover	Threats covered	Threats not covered
Incident Detector	P1 P2 P5 P6 P10 P19 P23 P24 P25	T1 T2 T4 T6 T9 T10 T11 T17 T20 T23 T29 T31	T1 T2 T4 T6 T10 T11 T12 T13 T17 T20 T23 T29	T9

		T39	T31 T37 T38 T39	

As we have mentioned, a similar exercise can be done with the rest of the components of the infrastructure. In all cases it is not enough to rely just on the results of the evaluation, but it is also required expert knowledge (from analysts and developers) to check whether identified threats are relevant enough to modify implementations or revisit some requirements. In any case, this methodology allows to focus the efforts on certain parts of the development activities, which allows to optimize resources devoted to the developing secure software.

5 CONCLUSIONS

This document has continued the work presented in D2.4, where a methodology for developing secure software based on the evaluation of requirements and threats was created. In this deliverable it was refined the analysis, incorporating additional threats that was included from D2.6, and including also the latest set of requirements produced in D1.4. Additionally, this deliverable has put more emphasis on the implementation activities carried out during the second period of the ANASTACIA project. More specifically it has been checked the fulfilment of the requirements for every component of the ANASTACIA framework with regards to the threats that those requirements are related to.

The evaluation of the latest requirements and the new threats, together with the implementation details of the components of the ANASTACIA framework, were used to detail the protection level of the components developed. It was analysed the prevention activities identified in D2.4 with respect to the implementation activities done in the second period, obtaining the level of protection against the threats identified in the analysis.

In summary, in this deliverable it has been validated the methodology created in D2.4, by applying it to the implementation of the ANASTACIA components. It has allowed to identify which prevention recommendations have been addresses, which ones were not addressed and why they were not. Also, the methodology has allowed to perform a traceability analysis which has permitted to know whether there the implementation activities were included to prevent the threats that might affect to every component of the architecture. The methodology also allows to know if there has been any threat not addressed by the implementation activities. This helps to identify gaps in the development activities, which allows to further consider revisiting some requirements or the development of any component, in case the threat not covered is relevant enough not to be left behind.

6 ANNEX I. FINAL REQUIREMENTS TAKEN FROM D1.4

The following annex bring, for the sake of completion, the list of functional, non-functional and privacy requirements described in D1.4.

Table 6-1. Final set of functional requirements (source: D1.4)

ID	Name/Description	Priority*
FR-21	The ANASTACIA system will handle complex (e.g. multiple attack) scenarios	HIGH
FR-22	The ANASTACIA system will include novel reasoning capabilities for autonomous mitigation of attacks	HIGH
FR-23	The ANASTACIA system will be deployed as a distributed architecture (appropriate guidelines/instructions to be issued)	MEDIUM
FR-24	The ANASTACIA system will enforce policies that interfere with CPS status so to avoid unexpected impacts in the operational context	HIGH
FR-25	The ANASTACIA system will not introduce additional potential points of failure during the orchestration/enforcement of mitigation plans	HIGH
FR-26	The ANASTACIA system will support real-time monitoring and control of IoT for attack mitigation purposes devices	HIGH
FR-27	The ANASTACIA system will include security and privacy policy conflict detection to support orchestration and enforcement of mitigation plans	HIGH
FR-28	The ANASTACIA system will manage security and privacy policy dependencies to support orchestration and enforcement of mitigation plans	HIGH
FR-29	The ANASTACIA system will adopt optimal selection criteria for SDN/NFV-based security mechanisms to enforce	HIGH
FR-30	The ANASTACIA system will adopt optimal orchestration criteria for SDN/NFV-based security mechanisms to enforce	HIGH
FR-31	The ANASTACIA system will allow to mitigate 0-day attacks	HIGH
FR-32	The ANASTACIA system will allow to mitigate slow DDoS attacks	HIGH
FR-33	The ANASTACIA system will find correlation between operational attacks and network attacks	MEDIUM
FR-34	The ANASTACIA system will design and develop algorithm for learning the evolving nature of attack	MEDIUM
FR-35	The ANASTACIA system will include advanced decision models (included in the Monitoring Plane) to detect suspect IoT malicious activities and potential associated risks/attacks	HIGH
FR-36	The ANASTACIA system will include advanced reasoning capabilities (to be included in the Monitoring Plane) to leverage event correlation and enhance IoT security	HIGH
FR-37	The ANASTACIA system will include advanced reasoning capabilities (to be included in the Reaction Plane) based on mathematical models for quantitative evaluation of risks/attacks to better define appropriate mitigation plans	HIGH
FR-38	The ANASTACIA system will define list of suggested mitigation actions with associated score based on quantitative evaluation of risks/attacks	HIGH
FR-39	The ANASTACIA system will consider context-awareness (system model) in the quantitative evaluation of risks/attacks	HIGH
FR-40	The ANASTACIA system will support the evaluation of the effectiveness of applied reaction and mitigation plans (reinforcement)	HIGH
FR-41	The ANASTACIA system will support accountability as for compliance with GDPR, with a focus on DPIA activities and on non-repudiable proof	HIGH

ID	Name/Description	Priority*
FR-42	The ANASTACIA system will include smart routing functionalities for service & network management	HIGH
FR-43	The ANASTACIA system will include a dynamic Service Function Chain (SFC) requests placement to reduce routing	HIGH
FR-44	The ANASTACIA system will include learning methods to enhance routing and prevent attacks by supervised and/or reinforcement learning techniques	HIGH
FR-45	The ANASTACIA system will leverage SDN and NFV 5G-enabler technology for cyberattack mitigation	HIGH
FR-46	The ANASTACIA system will support flexible and dynamic deployment of monitoring agents	MEDIUM
FR-47	The ANASTACIA system will support reaction policies containing monitoring capabilities	MEDIUM
FR-48	The ANASTACIA system will embed SDN and NFV technologies in MMT IoT Sniffer	MEDIUM
FR-49	The ANASTACIA system will include translation plugins to support the deployment of new monitoring instances	MEDIUM
FR-50	The ANASTACIA system will include a DSPS as an internal/external audit and transparency tool	HIGH
FR-51	The ANASTACIA system will include a DSPS as a tool to support Privacy and Security Certification Monitoring	HIGH
FR-52	The ANASTACIA system will a DSPS for auditing data processing activities and data escrow	HIGH
FR-53	The ANASTACIA system will allow end user feedback to support organizational compliance / due-diligence tracking	MEDIUM
FR-54	The ANASTACIA system will support streamline feedback process by enabling end-users to raise alerts to DSPS	MEDIUM
FR-55	The ANASTACIA system will support streamline feedback process by integrating DPIA tools	MEDIUM
FR-56	The ANASTACIA system will support streamline feedback process by enabling data upload functionalities	MEDIUM
FR-57	The ANASTACIA system will support streamline feedback process by ensuring correct integration of digital signature for data validation	MEDIUM

Table 6-2. Final set of non-functional requirements (source: D1.4)

ID	Name/Description	Priority*
NFR-16	Usability – the ANASTACIA system will generally hide complexity by providing differentiated views/UIs • Improve the DSPS GUI to: o Easily convey complex privacy and security information to end-user o Exploring graphical and symbolic mechanisms for data conveyance o Adding custom visualizations/views o Generating a distinct graphical identity for the DSPS o Determining and showcasing the most relevant information for end-users • Overhead and complexity associated to the implementation/deployment/use of the ANASTACIA framework should be generally minimized	HIGH

ID	Name/Description	Priority*
	• Usability of Security Orchestrator UI/console should be improved • Usability of Mitigation Action Service and Security Orchestrator UI/console should be improved • Complexity should be mitigated by usability for configuration and deployment processes • Usability should be addressed and improved (terminology for non-technical users) • Information about orchestrated/enforced mitigation plans should be duly provided in plain language for non-technical users	

Table 6-3. Final set of privacy requirements (source: D1.4)

ID	Name/Description	Priority*
PR-1	Enable privacy safeguards by default Privacy safeguards shall be enabled by default, without requiring further intervention by the user.	HIGH
PR-2	Identification of data categories, non-processing of special categories, and protection of traffic and location data ANASTACIA should incorporate express organizational and technical measures to avoid the processing of sensitive data and/or the identification of sensitive data from any of the datasets and measurements available to the system (apply the data minimization principle and storage limitation principles, among others). Special care must be taken to identify the categories of data which might have been involved in a potential breach in the monitored system, to ensure that the correct remedial and informational measures are adopted.	HIGH
PR-3	Data management and respect of data subject rights This requirement aims to fulfil several of the rights granted by the GDPR to data subjects, including the rights of access, rectification, opposition and deletion of personal data. This requirement has several additional implications: a) In compliance with the right of information, the data subject is to be informed as soon as possible after a breach to his/her personal data has taken place; b) the right of access entails also the requirement to ensure that the system upon which such right is to be exercised is available as soon as possible after facing a data breach, so as to ensure the data subject remains in control of his personal data. Finally, all necessary measures are to be incorporated to ensure that whenever a request for deletion has been received from the data subject, any controllers or processors which possess copies of the information should be informed, asked to comply with such request.	HIGH
PR-4	Data retention A reasonable retention period should be set, after the expiration of which, data should be erased or de-identified. Unnecessary personal data should be erased by the system without undue delays. All processes related to ANASTACIA end-users should utilize reasonable or non-	MEDIUM

	extensive data retention periods as well as implement any technical measures as necessary to ensure that unnecessary personal data are neither requested nor registered by the system (storage limitation and data minimization principles). Effective deletion of the data should be ensured and transparency on the followed procedures kept towards the end-users.	
PR-5	Deidentification of Personal Data (Anonymization, Pseudonymization, Non-identifiability) The GDPR recognizes that the rights of access, rectification and erasure (including the right to be forgotten), restriction of processing, and data portability shall no longer be applicable when the controller of personal data is able to demonstrate that it is not able to identify a data subject. This requirement then focuses on the information and practices that are necessary to ensure that identifiability is no longer possible.	HIGH
PR-6	Records and audit of processing activities and disclosures This requirement should be introduced and considered for all monitoring activities for which ANASTACIA is utilized "based on the assumption that the ANASTACIA framework would be deployed in the context of personal data processing activities which are not defined by ANASTACIA itself, yet by the entity deploying ANASTACIA's system as a service; in that regard, ANASTACIA will typically fulfil the tasks of a Data Processor, and in so doing it provides some means to achieve the purposes set by another entity, the Data Controller"(Bianchi et al., 2017, p. 62).	HIGH
PR-7	Security of processing (prevention of unauthorized access, alteration, disclosure and destruction of personal data) This high-level requirement aims to ensure the introduction of technical and organizational security safeguards to protect personal data by both the monitored IT systems and ANASTACIA. From an organizational point of view, the requirement addresses the need to define, implement (and update) security mechanisms and policies to the very design of the system.	HIGH
PR-8	Data breach information In direct relation with the transparency and accountability principles enshrined by the GDPR, the ANASTACIA system must immediately inform its users of any breach to personal data leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed, in order to enable that user to fulfil its obligations to notify data breaches to competent Data Protection Authorities and concerned data subjects.	HIGH
PR-9	Encryption of personal data by default All personal data should be encrypted whenever it is stored or transferred, and strong encryption mechanisms should always be used.	HIGH
PR-10	Update and review privacy measures Technical and organizational measures to ensure the privacy of end-users should be implemented and periodically updated/reviewed as necessary to ensure their effectiveness. Organizational and technical processes to ensure the effectiveness of security measures are required	HIGH

by the GDPR and constitute part of ANASTACIA's principal objectives. Generally, this requirement calls for audits and cross-verification of the security measures that have been implemented, and of the verification mechanisms themselves to maximize accountability and transparency and ensure the security and confidentiality of personal data.

7 ANNEX II. DETAILED EVALUATION OF CRITICALITY FOR THE NEW SET OF REQUIREMENTS

Table 7-1. Complete evaluation of the complete list of threats and the new set of requirements

		T1	T2	T3	T4	T5	T6	T7	T8	T9	T10	T11	T12	T13	T14	T15	T16	T17	T18	T19	T20	T21	T22	T23	T24	T25	T26	T27	T28	T29	T30	T31	T32	T33	T34	T35	T36	T37	T38	T39	T40	T41	T42	T43	T44	T45	T46	T47	T48	T49		
Req ID	Impact (N)	7	5	6	6	5	3	7	5	8	2	3	4	3	2	4	4	2	1	1	2	6	2	6	5	5	3	3	9	7	4	6	3	5	2	5	5	5	3	6	5	2	4	4	4	7	7	5	4	8	Threat Severity	Criticality
FR-21	6		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	4,44	5,22
FR-22	8	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	4,49	6,24
FR-23	0													x	x	x	x																						x														3,60	1,80
FR-24	6					x																					x	x																		x	x					4,40	5,20
FR-25	6	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	4,49	5,24
FR-26	8	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	4,49	6,24
FR-27	10												x					x																																		3,00	6,50
FR-28	8												x					x																																		3,00	5,50
FR-29	2												x					x																																		3,00	2,50
FR-30	2												x					x																																		3,00	2,50
FR-31	10						x																																												x	5,50	7,75
FR-32	10				x																																														6,00	8,00
FR-33	2	x													x																								x												4,00	3,00
FR-34	2													x											x						x									x											4,25	3,13
FR-35	4				x	x							x					x		x		x			x	x		x																						4,11	4,06
FR-36	4				x	x							x					x		x		x			x	x		x																						4,11	4,06
FR-37	4				x	x							x					x		x		x			x	x		x																						4,11	4,06
FR-38	2				x	x							x					x		x		x			x	x		x																						4,11	3,06
FR-39	4												x					x		x							x												x	x			x		x	x		x			3,90	3,95
FR-40	4	x																							x	x															x										5,50	4,75
FR-41	6			x					x												x						x														x		x			x	x				4,50	5,25
FR-42	2	x													x			x		x		x																	x												3,50	2,75
FR-43	2	x																x		x																			x												3,25	2,63
FR-44	4																	x			x																														2,00	3,00
FR-45	2			x														x	x								x				x	x							x											3,57	2,79
FR-46	2	x			x											x	x																							x	x										5,57	3,79
FR-47	2	x														x	x												x	x											x	x									6,13	4,06
FR-48	4																	x				x																	x	x			x		x							4,00	4,00
FR-49	2												x					x																																		3,00	2,50
FR-50	6												x					x		x	x																															2,25	4,13
FR-51	6												x					x		x	x																															2,25	4,13
FR-52	6												x					x		x	x																															2,25	4,13
FR-53	10			x					x				x									x						x																								4,80	7,40
FR-54	6												x					x		x	x																															2,25	4,13
FR-49	6	x					x															x																													x	x	x	5,50	5,75
FR-56	4			x																																																6,00	5,00
FR-57	4			x									x																																								5,00	4,50