

RESISTO:

D4.3 _TECHNIQUES AND PROCEDURES FOR CYBER/PHYSICAL THREATS DETECTION



RESISTO

D4.3 – TECHNIQUES AND PROCEDURES FOR CYBER/PHYSICAL THREATS DETECTION

Document Manager:	Giuseppe CELOZZI	TEI	Editor
--------------------------	------------------	-----	--------

Project Title:	RESilience enhancement and risk control platform for communication infraSTructure Operators
Project Acronym:	RESISTO
Contract Number:	786409
Project Coordinator:	LEONARDO
WP Leader:	TEI

Document ID N°:	RESISTO_D4.3_191219_01	Version:	1.0
Deliverable:	D4.3	Date:	19/12/2019
		Status:	APPROVED

Document classification	Public
--------------------------------	---------------

Approval Status	
Prepared by:	Giuseppe CELOZZI (TEI)
Approved by: (WP Leader)	Giuseppe CELOZZI (TEI)
Approved by: (Coordinator)	Bruno SACCOMANNO (LDO)
Advisory Board Validation (Advisory Board Coordinator)	N.A.
Security Approval (Security Advisory Board Leader)	Paolo DI MICHELE (LDO)

CONTRIBUTING PARTNERS

Name	Company / Organization	Role / Title
Giuseppe CELOZZI, Antonio NICOLETTI, Giovanna SPADACCIO, Rosa CATAPANO, Cosimo ZOTTI	TEI	Telecommunications Experts, Senior Researchers, Senior Project Manager
Moisés VALEO, Jose SANCHEZ, Javier VALERA	INT	Senior Researchers, Electrical Engineers, Defence and Security Specialists
Risto LAANOJA, Kadri ISAKAR	GT	Security Engineer, Technical Writer
Andrei AVADANEI Florina DUMITRACHE Lucian NITESCU	BSS	CEO & Senior Security Specialist, Senior Security Specialist, Communication Specialist
Rodoula MAKRI, Panos KARAIVAZOGLU	ICCS	Telecommunications Experts, Senior Researchers

DISTRIBUTION LIST

Name	Company / Organization	Role / Title
PMT	RESISTO CONSORTIUM	NA
Markus MULLER	EC DG REA	EC Programme Officer
General Public	NA	NA

REVISION TABLE

Version	Date	Modified Pages	Modified Sections	Comments
0.1	15.11.2018	All	All	Table of contents and draft sections
0.2	01.07.2019	All	All	Additions and partners contributions
0.3	16.08.2019	All	All	Reviewed with all WP partners
0.4	30.10.2019	All	All	Reworked based on comments
0.8	30.10.2019	All	All	Final release for review
0.9	26.11.2019	All	All	Submitted to SAB Review
1.0	19.12.2019	All	All	Final release

COPYRIGHT STATEMENT



© 2018-2021 This document and its content are the property of the RESISTO Consortium. All rights relevant to this document are determined by the applicable laws. Access to this document does not grant any right or license on the document or its contents. This document or its contents are not to be used or treated in any manner inconsistent with the rights or interests of the RESISTO Consortium or the Partners detriment and are not to be disclosed externally without prior written consent from the RESISTO Partners. Each RESISTO Partner may use this document in conformity with the RESISTO Consortium Grant Agreement provisions.

The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Program, under the Grant Agreement No 786409.

The views and opinions in this document are solely those of the authors and contributors, not those of the European Commission.

PROJECT CONTACT



LEONARDO
Via Puccini 2 – Genova (GE) – 16154 – Italy
Tel.: +39 348 6505565
E-Mail: bruno.saccomanno@leonardocompany.com

RESISTO PROJECT – PUBLISHABLE EXTENDED ABSTRACT

Communications play a fundamental role in the economic and social well-being of the citizens and on operations of most of the CIs. Thus, they are a primary target for criminals having a multiplier effect on the power of attacks and providing enormous resonance and gains. Also, extreme weather events and natural disasters represents a challenge due to their increase in frequency and intensity requiring smarter resilience of the Communication CIs, which are extremely vulnerable due to the ever-increasing complexity of the architecture also in light of the evolution towards 5G, the extensive use of programmable platforms and exponential growth of connected devices. The fact that most enterprises still manage physical and cyber security independently represents a further challenge. RESISTO platform is an innovative solution for Communication CIs holistic situation awareness and enhanced resilience (aligned with ECSO objectives). Based on an Integrated Risk and Resilience analysis management and improvement process availing all resilience cycle phases (prepare, prevent, detect, absorb, etc.) and technical resilience capabilities (sense, model, infer, act, adopt), RESISTO implements an innovative Decision Support System to protect communication infrastructures from combined cyber-physical threats exploiting the Software Defined Security model on a suite of state of the art cyber/physical security components (Blockchain, Machine Learning, IoT security, Airborne threat detection, holistic audio-video analytics) and services (Responsible Disclosure Framework) for detection and reaction in presence of attacks or natural disasters. Through RESISTO Communications Operators, will be able to implement a set of mitigation actions and countermeasures that significantly reduce the impact of negative events in terms of performance losses, social consequences, and cascading effects in particular by bouncing efficiently back to original and forward to operational states of operation.

EXECUTIVE SUMMARY

This deliverable report collects techniques and procedures for cyber and physical threats detection.

A novel holistic approach to event correlation that is based on the collection of data using several sources. RESISTO collects and correlates several sources: Alarms from Telecommunication systems, OSINT events, weather channels information, seismic networks events, RESISTO IoT sensors networks, to provide a more exact interpretation of state of the telecom infrastructure leading to a correct course of corrective action.

High level description of the relevant Alarms from Telecommunication systems and how this are collected via the management network is reported.

Procedure to perform threat detection using IoT sensors integrity breach detection using MIDA and threat disclosure using the “Responsible Disclosure Framework” shall also be described.

CONTENTS

ABBREVIATIONS	10
1. INTRODUCTION – PURPOSE OF THE DOCUMENT.....	13
2. FAULT MANAGEMENT IN TELECOM INFRASTRUCTURES	14
2.1. TMN	14
2.2. NFV.....	15
2.3. Telecom alarms.....	17
2.4. Telecom alarms analysis procedure.....	21
2.4.1. IDEA alerts.....	23
3. NATURAL EVENTS SENSOR NETWORKS.....	24
3.1. Seismic networks.....	24
3.2. Weather Channel API.....	25
4. OSINT PLATFORMS FOR MONITORING THREATS AND VULNERABILITIES	26
4.1. MISP	26
4.2. Crawlers.....	27
4.3. IVRE framework.....	28
4.4. Machine Learning in threat Intelligence processes	28
4.5. Collecting data for threats propagation.....	29
5. THREAT DETECTION BASED ON IOT SENSORS.....	30
6. KSI BLOCKCHAIN MONITORING TECHNIQUES AND PROCEDURES.....	42
6.1. KSI Blockchain.....	42
6.2. XDAL and Dockets	42
6.3. Guardtime MIDA.....	42
6.3.1. MIDA Overview	43
6.3.2. MIDA Agent.....	44
6.3.3. MIDA State Management Services.....	45
6.3.3.1. Sentry.....	45
6.3.3.2. Broker	46
6.3.3.3. Venture	46
6.3.3.4. MIDA Dashboard	46
6.4. Why KSI Blockchain?	47
7. RESPONSIBLE DISCLOSURE FRAMEWORK	48
8. CONCLUSION	51
REFERENCES	52

LIST OF FIGURES

Figure 1 TMN Layers	15
Figure 2 NFV interfaces	16
Figure 3 MISP dash board	27
Figure 4 OSINT Service	29
Figure 5 Guardtime MIDA	44
Figure 6 Guardtime MIDA deployment in the RESISTO project	45
Figure 7 RDF architecture	49
Figure 8 Disclosure Framework Process	50

ABBREVIATIONS

API	Application Programming Interface
APT	Advanced persistent threat
ARCA	Alarm Root Cause Analysis
AWS	Amazon Web Services
CIRCL	Computer Incident Response Center Luxembourg
CSIRT	Computer Security Incident Response Services
CVE	Common Vulnerability Exposure
DDoS	Distributed Denial of Service
DL	DL
DoS	Denial of Service
EIDA	European Integrated Data Archive
EM	ELEMENT MANAGER
EMS	ELEMENT MANAGEMENT SYSTEM
EPOS	European Plate Observing System
FDSN	Freedom Scientific Developer Network
FM	Fault Management
FCAPS	Fault Configuration Accounting Performance Security
IDEA	Intrusion Detection Extensible Alert – a message schema
IDMEF	Intrusion Detection Message Exchange Format
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
IoC	Indicator of Compromise
IODEF	Incident Object Description and Exchange Format
IoT	Internet of Things
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
ISP	Internet Service Provider

ITU	International Telecommunication Union
KSI	Keyless system infrastructure
MANO	Management and Orchestration
MIDA	Machine Integrity, Defense and Awareness – a software framework
MISP	Malware Information Sharing Platform
ML	Machine Learning
NATO	North Atlantic Treaty Organization
NCIRC TC	NATO Computer Incident Response Center Technical Center
NFV	Network Function Virtualization
NFVO	Network Function Virtual Orchestrator
NLP	Natural Language Processing
NS	Network Service
O&M Network	Operation and Maintenance Network
OS	Operating system
OSINT	Open Source Intelligence
OSS/BSS	Operation Support System / Business Support System
RAT	Remote Access Trojans
RCA	Root Cause Analysis
RFC	Request for Comments
SDN	Software Defined Networking
SE	Social Engineering
SSH	Secure Socket
STCL	Short Term Control Loop
TCP	Transmission Control Protocol
TI	Threat Intelligence
TLC	Telecommunication
TMN	Telecom Management Network (Note: TMN indicates both the standard and the management systems that implement it)
UC	Use Case

UE	User Equipment
VNF	Virtual Network Function
VNFC	Virtual Network Function Component
VNFM	Vitrual Network Function Manager
VPN	Virtual Private Network
WP	Work Package
XDAL	eXtensible Data Attribution Language – a message or container schema
XML	eXtensible Markup Language
XMPP	Extensible Messaging and Presence Protocol

1. INTRODUCTION – PURPOSE OF THE DOCUMENT

The present Deliverable D4.3 is the third report of WP4 “Tools and techniques for Monitoring and Detection of cyber-physical threats”. This WP deals with the implementation of a variety of hardware and software tools and technologies for detection and monitoring of anomalous conditions, intrusions and threats.

Procedure and tools to collect standard telecom alarms and security alerts from Telecommunication systems deployed and how this data can be correlated to report possible cyber and or physical attacks will be included. More specifically this deliverable purpose is to describe techniques and procedures regarding the alarm handling of cyber and physical threats detection that will be considered in RESISTO.

Telecom system alarms is highly standardized and supported by all telecom equipment and by network virtual function, this standardization makes possible a common analysis of the data and root cause analysis (RCA); that is the standard procedure used in telecom organization to handle faults on equipment. This approach, though, does not consider other events that can be collected and used to perform an improved root cause analysis, for this purpose RESISTO will propose a set of additional tools and modules.

OSINT, weather channels, seismic networks available that can be used to correlate events coming from equipment alarms or the sensors networks can be correlated with the purpose of an exact interpretation of the events.

Security issues collected by open source intelligence, OSINT, and tools to recon data from a network will be collected and used to identify possible threats.

Natural events coming from sensors network deployed to monitor weather conditions and seismic events can also be collected connecting to public or private web API on the internet. Specific RESISTO modules will be used to collect those events and forward them to the event correlator.

Events collected by the active and passive sensors described in the deliverable D4.1 – ACTIVE AND PASSIVE SENSOR DEFINITION of Task 4.1 will be adapted to a common format and forwarded to the event correlator.

Novel data integrity tools and techniques to report storage integrity violations of the code and data present on both equipment and sensors are described and detailed.

A set of tools and a feature-rich system allows security researcher, independent contractors and other 3rd party security providers to report discovered vulnerabilities on the end user’s infrastructure using RESISTO.

2. FAULT MANAGEMENT IN TELECOM INFRASTRUCTURES

Telecom Equipment deployed in a telecom network are constantly monitored by management software and for this purpose the equipment are always providing a fault management interface that can be integrated by a management software. The high level standard that telecom equipment are compliant with is called TMN, see the next section for more details on how this standard describes the management software that is controlling a telecom infrastructure.

5G networks have been implemented according to the ETSI Network Function Virtualization standard that has a different management model with its own management software, nevertheless NFV is integrated with the standard TMN model and also the newly introduced virtualized functions can generate, in case of malfunctions, alarms indications, how this is done is described in section 2.2 below.

A fault in a telecom equipment or in a virtualized function can be used as an indication of a possible security issue, a taxonomy of the typical alarms generated by the equipment and how this can be correlated to a security issue is reported in section 2.3.

A fault generates an alarm indication on a standard interface, i.e. FM interface and this indication is used by the telecom operators to identify the root cause of the problem according to a procedure that is called root cause analysis, which is briefly described in section 2.4, RESISTO will complement this procedure with a correlation procedure by which the faults collected from the network are forwarded to the event correlator, via a properly implemented adapter, that converts the standard telecom alarm in a RESISTO event. The events generated in this way can be used by the event correlator together with other events to identify a security issue and suggest the proper corrective procedure.

RESISTO approach to correlation of faults reported via standard FM interface will take into account also external actions and events, for instance the ones coming from sensors and the ones coming from other events like the ones related to natural conditions that can be correlated using the equipment location info and the weather or seismic information coming from external event engines.

2.1. TMN

Telecom Management Network – (TMN) is a standard developed within ITU-T, “M.3000 is the Overview of TMN Recommendations” document gives an overview of the recommendation. TMN defines interfaces and the specification of interface protocols between OSs and transmission terminals (a.k.a. equipment or nodes) and information network operating for the management of all telecommunication networks and services.

TMN provides a framework for achieving interconnectivity and communication across heterogeneous operations system and telecommunication networks. To achieve this, TMN defines a set of interface points for elements which perform the actual communications processing (such as a call processing switch) to be accessed by elements, such as management workstations, to monitor and control them. The standard interface allows elements from different manufacturers to be incorporated into a network under a single management control. Thus, TMN indicates both the standard and the management systems that implement it.

TMNs are the corresponding systems and they provide the means to transport, store and process information that support the management of telecommunication networks and services. When telecommunication networks relate to each other, their TMNs provide the means of exchanging information required to manage end-to-end telecommunication services.

The TMN is a layered model that includes from top to bottom Network Elements, Element Management handled via the EMS, Network Management handled by the NMS, Services and Businesses handled by the Operator OSS/BSS. The management systems (EMS, NMS, OSS/BSS) will act on five areas of functionality: Fault, Configuration, Accounting, Performance and Security. In particular it's interesting to see how Faults are handled by this model and collected by the management systems.

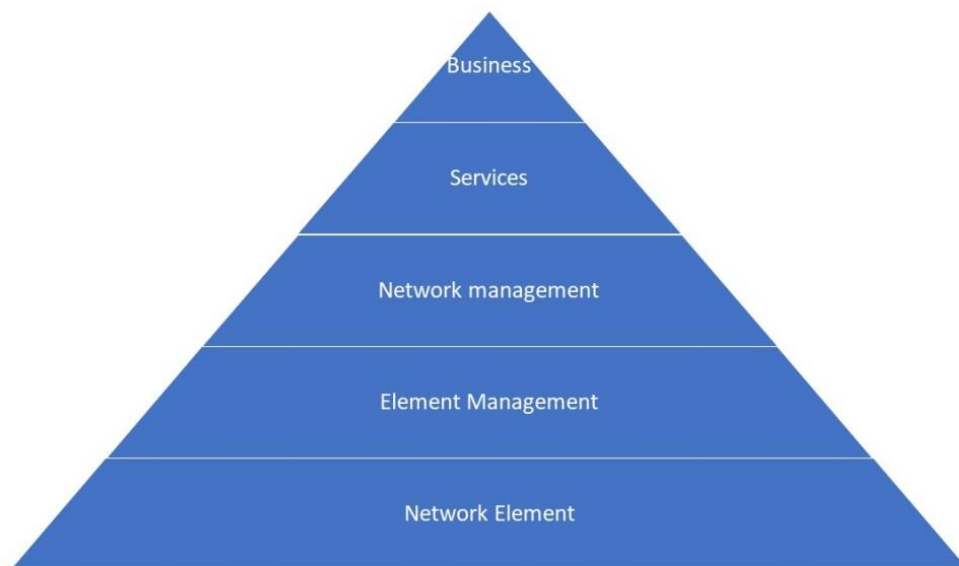


Figure 1 TMN Layers

2.2. NFV

Since RESISTO is considering also the novel 5G architecture we need to also consider a different management and orchestration standard because of the virtualization of some of the Network Elements (NEs).

This standard is based on the NFV (Network Function Virtualization) reference model depicted in Figure 2 below. Thus, we have to consider these additional management elements to the TMN model which furthermore are actually interconnected to it.

In Figure 2 the interfaces for fault management and performance monitoring between the TMN elements (OSS/BSS and EMS) towards the orchestration components of the NVF architecture are shown.

The same interfaces can be accessed with a RESISTO adapter to collect alarms from the virtual functions and forward them to the event correlator.

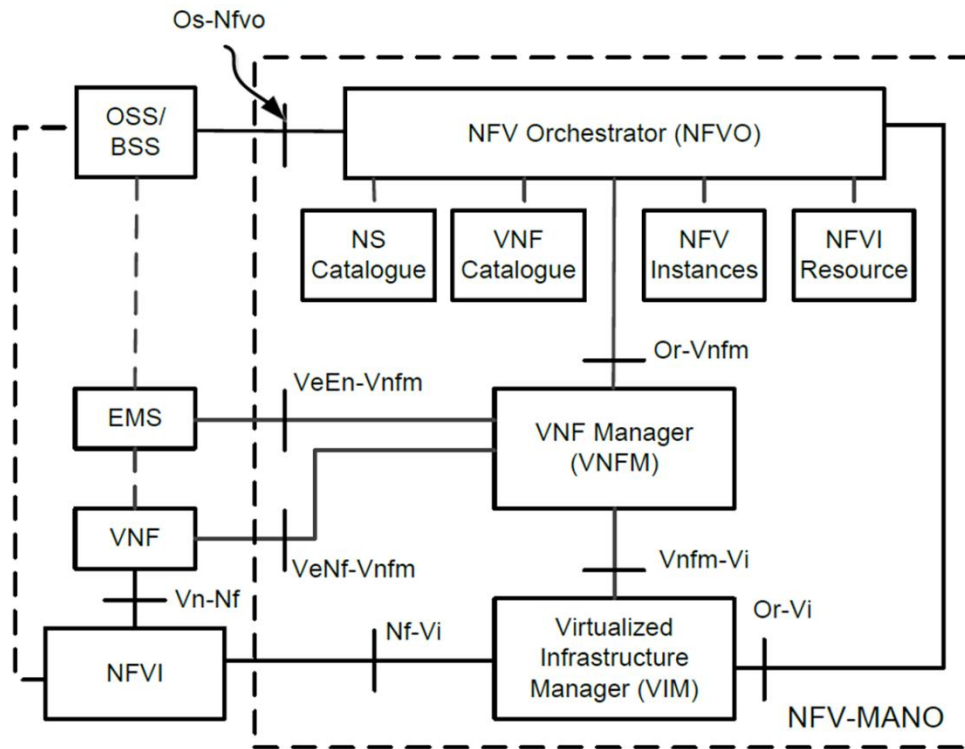


Figure 2 NFV interfaces

NFV poses a Fault Management interface at Network Service (NS) level. This interface shall allow the Network Function Virtualization Orchestrator, NFVO, to provide alarms related to the Network Services visible to the consumer. An alarm on a given Network Service results from either a collected virtualised resource fault impacting the connectivity of the Network Service instance or a Virtual Network Function, VNF, alarm, resulting from a virtualised resource alarm, issued by the Virtual Network Function Manager, VNFM, for a Virtual Network Function, that is part of this Network Service instance.

The fault management interface shall support subscription of OSS/BSSs with the NFV Orchestrator for the notifications related to the alarms, notifications of alarms or alarm state change from NFV Orchestrator to OSS/BSS and accessing active alarms from the NFV Orchestrator.

At Virtual Network Function Manager, VNFM, level the Fault Management interface allow the Virtual Network Function Manager to provide alarms related to the Virtual Network Function(s) and its Virtual Network Function Component(s) visible to the consumer. Virtualised resource alarms collected by the Virtual Network Function Manager well be filtered, correlated and modified by the Virtual Network Function Manager and mapped to the corresponding Virtual Network Function instance, resulting in alarms on the corresponding Virtual Network Function and its Virtual Network Function Components(s). The operations will include, as before a subscribe operation (Element Manager, EM, and Virtual Network Function with the Virtual Network Function Manager) for the notifications related to the alarms, notify operation (Notifications of alarms or alarm state change from Virtual Network Function Manager to Element Manager and Virtual Network Function) and accessing active alarms from the Virtual Network Function Manager to Element Manager and Virtual Network Function .

2.3. Telecom alarms

From the security point of view the most important types of alarms are those relevant to the “Equipment” (that indicates an equipment fault: hardware or software related), as this also can be derived from Deliverable D4.1.

The Probable Causes field of the alarm in ITU-T X.733 results in further qualification of the alarms, specifying a probable cause, following a classification of most probable causes described in this Standard that could indicate a physical-attack or cyber-attack. Indicative examples of this manner are given in the following table. The last column indicates possible connections with other events that can be used in the event correlator. A concise indicator was also added through a three level scale (HIGH, MEDIUM, LOW) on the probability that the fault indicates certain attacks or external events; suggestions on possible actions that should be taken is also reported. (Note that threshold alarms can be defined on performance and the generated alarms can be collected using the Fault interface).

Probable Causes		
SW or HW module has been tampered causing intentionally failures in the overall system		
Fault	Description	Correlation Level
application subsystem failure:	A failure in an application subsystem has occurred (an application subsystem may include software to support the Session, Presentation or Application layers);	HIGH: This could be caused by corruption of the code and failure of a SW module, so could be caused by an attack on the code on the system; action: system logs should be analysed
file error:	The format of a file (or set of files) is incorrect and thus cannot be used reliably in processing;	HIGH: This could be caused by corruption of the data, so could be caused by an attack on the data present on the system; action: integrity check is needed
configuration or customization error:	A system or device generation or customization parameter has been specified incorrectly, or is inconsistent with the actual configuration;	HIGH: Intentional mis-configuration could be caused by an attacker; action: log analysis should be performed to verify the type of commands performed
corrupt data:	An error has caused data to be incorrect and thus unreliable;	HIGH: This could be caused by corruption of the data, so could be caused by an attack on the data present on the system; action: integrity check is needed
processor problem:	An internal machine error has occurred on a Central Processing Unit;	LOW: This could be caused mostly by a HW fault in the unit so should more rarely indicate a problem related to security; action: systems logs should be analysed depending on the recurrence
software error:	A software error has occurred for which no more specific Probable cause can be	HIGH: This could be caused by unexpected behaviour which could have been caused intentionally; action: system

	identified;	logs should be analysed
software program abnormally terminated:	A software program has abnormally terminated due to some unrecoverable error condition;	HIGH: This could be caused by unexpected behaviour which could have been caused intentionally; action: system logs should be analysed
software program error:	An error has occurred within a software program that has caused incorrect results;	HIGH: This could be caused by unexpected behaviour which could have been caused intentionally; action: system logs should be analysed
version mismatch:	There is a conflict in the functionality of versions of two or more communicating entities which may affect any processing involving those entities.	HIGH: This could be caused by code that was maliciously replaced; action: system configuration should be compared with expected one, configuration actions should be analysed to check if the system has been reconfigured by intruders
Congestion or overload of the system or network caused by a DOS attack		
bandwidth reduced:	The available transmission bandwidth has decreased;	HIGH: this could be caused by congestion due to DoS attack; action: network logs should be analysed
call establishment error:	An error occurred while attempting to establish a connection;	HIGH: this could be caused by congestion due to DoS attack; action: network logs should be analysed
communications protocol error:	A communication protocol has been violated;	HIGH: data plane messages could have been altered; "man in the middle" could also be the cause; action: network logs should be analysed
communications subsystem failure:	A failure in a subsystem that supports communications over telecommunications links, these may be implemented via leased telephone lines, by X.25 networks, token-ring LAN, or otherwise;	HIGH: data plane messages could have been altered; "man in the middle" could also be the cause; action: network logs should be analysed
I/O device error:	An error has occurred on the I/O device;	MEDIUM: device error could be caused by overload due to congestion; action: system logs should be analysed
congestion:	A system or network component has reached its capacity or is approaching it;	HIGH: this could be caused by congestion due to DoS attack; action: network logs should be analysed
CPU cycles limit exceeded:	A Central Processing Unit has issued an unacceptable number of instructions to accomplish a task;	MEDIUM: could be caused by overload due to congestion; action: behaviour should be analysed to verify if an attack is on going

degraded signal:	The quality or reliability of transmitted data has decreased;	HIGH: this could be caused by congestion due to DoS attack trying to occupy the media; action: network logs should be analysed, and weather conditions should also be checked
local node transmission error:	An error occurred on a communications channel between the local node and an adjacent node;	LOW: this could be a transient communication error; action: verify frequency and analyse logs for HW and SW faults
loss of frame:	An inability to locate the information that delimits the bit grouping within a continuous stream of bits;	LOW: this could be a transient synchronization error; action: verify frequency and analyse logs for HW and SW faults
loss of signal:	An error condition in which no data is present on a communications circuit or channel;	HIGH: this could be a transient communication error or a permanent fault of the system that cannot operate root causes can be all the disruption caused by a physical attack to the communication media; action: verify if the communication with the equipment is still possible over the O&M network and perform the analysis
out of memory:	There is no program-addressable storage available;	HIGH: this could be caused by overload due to DoS attack; action: network and system logs should be analysed
output device error:	An error has occurred on the output device;	MEDIUM: this could be caused by congestion due to DoS attack; action: network logs should be analysed
performance degraded:	Service agreements or service limits are outside of acceptable limits;	MEDIUM: this could be caused by congestion due to DoS attack, but also adverse weather conditions could be the cause of performance degradation in case of microwave transmission; action: network logs should be analysed, and weather conditions in the location verified
resource at or nearing capacity:	The usage of a resource is at or nearing the maximum allowable capacity;	MEDIUM: this could be caused by overload due to DoS attack; action: network and system logs should be analysed
response time excessive:	The elapsed time between the end of an inquiry and beginning of the answer to that inquiry is outside of acceptable limits;	MEDIUM: this could be caused by overload due to DoS attack; action: network and system logs should be analysed
retransmission rate excessive:	The number of repeat transmissions is outside of	HIGH: this could be caused by overload due to DoS attack; action: network and

	acceptable limits;	system logs should be analysed
storage capacity problem:	A storage device has very little or no space available to store additional data;	MEDIUM: this could be caused by overload due to DoS attack; action: system logs should be analysed
Physical intrusion or natural disaster		
enclosure door open;		HIGH: this could be caused by an-authorized access; action: on site visit is needed
excessive vibration:	Vibratory or seismic limits have been exceeded;	HIGH: depending on the level and damage occurred proper action should be taken; action: seismic information should be collected on the area where the equipment is located. on site visit is needed to fix depending on the priority
fire detected;		HIGH: depending on the level and damage occurred proper action should be taken; action: on site visit is needed to fix depending on the priority
flood detected;		HIGH: depending on the level and damage occurred proper action should be taken; action: weather information should be collected on the area where the equipment is located. on site visit is needed to fix depending on the priority
heating/ventilation/cooling system problem;		LOW: this could be caused by intentional physical damage; action: cross check for site intrusion and plan an on site visit is needed to fix depending on the priority
humidity unacceptable:	The humidity is not within acceptable limits;	MEDIUM: depending on the level and damage occurred proper action should be taken; action: weather information should be collected on the area where the equipment is located, there might be a related issue on the site air conditioning system, on site visit is needed to fix depending on the priority
leak detected:	A leakage of (non-toxic) fluid or gas has been detected;	MEDIUM: depending on the level and damage occurred proper action should be taken; action: possible intrusion should be checked on site visit is needed to fix depending on the priority
material supply exhausted:	A supply of needed material has been exhausted;	MEDIUM: this should be a normal refurbishment issue; action: on site visit is needed to fix depending on the priority

power problem:	There is a problem with the power supply for one or more resources;	HIGH: depending on the autonomy level of auxiliary power supply proper action should be taken; this could be a cascading effect of a damage to the power-grid action: on site visit is needed to fix depending on the priority
pressure unacceptable:	A fluid or gas pressure is not within acceptable limits;	MEDIUM: depending on the level and damage occurred proper action should be taken; action: possible intrusion should be checked on site visit is needed to fix depending on the priority
pump failure:	Failure of mechanism that transports a fluid by inducing pressure differentials within the fluid;	MEDIUM: depending on the level and damage occurred proper action should be taken; action: possible intrusion should be checked on site visit is needed to fix depending on the priority
temperature unacceptable:	A temperature is not within acceptable limits;	MEDIUM: depending on the level and damage occurred proper action should be taken; action: weather information should be collected on the area where the equipment is located, there might be a related issue on the site air conditioning system, on site visit is needed to fix depending on the priority
toxic leak detected:	A leakage of toxic fluid or gas has been detected.	HIGH: depending on the level and damage occurred proper action should be taken; action: on site visit is needed to fix depending on the priority

2.4. Telecom alarms analysis procedure

Telecom Standards and Recommendations are targeting mainly faults that can be generated by hardware and software in normal operation. The functional requirements for the alarm management interface include the management functions for alarm forwarding and filtering, clearing of alarms, storage and retrieval of alarms in/from the agent, configuration of alarms, alarm acknowledgement and alarm notification failure. The TMN standard provides a detailed information model supporting the above functions across the management interface. The root cause is always related to ordinary operation and security alarms are not well specified.

Furthermore, they do not specifically foresee recommendations related to risks, alarms and events caused by direct physical or cyber-physical threats. Instead, any kind of problem or malfunction in the overall telecom network and facilities (either physical, cyber or combined) is being defined as a "fault" and as such is being treated within the relevant telecom standards. In this respect, for example, errors in the overall system are being considered as faults; the same stands for problems and malfunctions that are caused by physical or other threats.

If an incident causes the generation of several notifications providing correlation among them is utterly important and helpful in the alarm handling. Correlation of events, though, is typically limited to the cases where this is somehow expected by design, like correlation of faults in different layers of a protocol stack or where a dependency among systems is there by design, i.e. a cable that connects 2 physical ports, and all the layers using the physical port.

A typical procedure that is followed in finding a solution to such problems in a telecom infrastructure is the process of Root Cause Analysis (RCA).

In Telecom networks all equipment is under management, and in case of services not performing several alarms can be raised. In fact, the entities involved in a network fault can be several. Moreover, as time elapses, issues can also spread over a geographical area or into different layers up to the applications that are using them. It is not easy for the operator to identify the entity and the reason of a network fault.

It is also possible that a fault is caused by a cyber security attack. Several attacks are just aimed at creating a fault in the network. A classic example is the DoS attack type. A DoS attack creates a congestion in the network practically simulating an abnormal usage level of the network.

Rapid and accurate determination of faulty entity will allow proper course of action that would lead to a different path if the alarm root cause is due to errors caused by internal design of the network or external misbehaviours put in place by cyber/physical attackers; this will in turn reduce the effort and the effect of the attack on final users.

As a result of the above it is seen that, alarm correlation and Alarm Root Cause Analysis (ARCA) process should be widened in scope to include all security fault effects. A new set of root causes must be considered in the process, in order to identify the proper cause of a degraded service.

Alarm correlation in general should drive the identification of the root cause which is the basic scope of fault management. The standard suggests the fault management implementation on the nodes that the alarms shall be compiled in such a way as to report whenever possible indication of the correlation.

Another type of correlation is used by operators just to prioritize repair actions and does not lead to a root cause. This type of function could be useful to assess the resilience of the network. In fact, examples of properties shared by a group of alarms are:

- Number of affected sites over a certain number;
- Number of affected subscribers over a certain number;
- Affected site is designated as important (e.g. holding special event).

Priority level designation for groups shall be though defined as part of the process of the Operator of the network and is not defined in the standard. Not all actions that can cause a fault are intentional, but it is very important to improve the capacity to detect and report such actions targeting mainly faults that can be generated by hardware and software in normal operation.

As already stated in the introduction RESISTO approach towards a more refined correlation of faults needs to take into account also external actions and events coming from external event engines.

2.4.1. *IDEA alerts*

In order to present a common information model and format to RESISTO correlation module IDEA: Designing the Data Model for Security Event Exchange has been selected. General description of IDEA and considerations that lead to this choice and some alternative formats that have been also proposed and can be found in the literature are reported in the rest of the section.

Intrusion Detection Extensible Alert (IDEA) is the format chosen for the RESISTO project. IDEA is a security event model that tries to overcome limitations and drawbacks of other models proposed for communication between different components that are part of a security system like honeypots, agents, detection probes, etc.

RESISTO needs to receive security events from a variety of sources to perform intrusion detection systems and has selected IDEA for event description because it's compact and contains the relevant information needed for threat analysis and reaction.

3. NATURAL EVENTS SENSOR NETWORKS

RESISTO event collection will implement specific modules, that will connect to public and private sensor networks, in order to implement the holistic approach to event correlation and detect abnormal weather conditions and relevant seismic events.

In the rest of the section environmental event channels are reported. The channels shall be used to correlate with other events reported by the TMNs and the sensors deployed in the attack trees that are related to natural disasters. In order these modules to be implemented, connection to seismic databases and to weather channels are needed; these would also include some filtering based on the geographical area of interest and the addition of significant parameters useful for the correlator to cross-check. Although these channels would be useful, their correlation is beyond the current scope of the RESISTO project. However, they are been briefly described herein, so that to indicate the future potential of holistic platforms like RESISTO.

3.1. Seismic networks

A seismic station consists of a seismometer for sensing ground motion, a clock for determining time, and a recorder for collecting data. Multiple stations are deployed in regional (focus is on small to moderate sized earthquakes at regional distances) and global networks (used to investigate both Earth structure and the phenomena that create seismic signals, i.e., earthquakes and explosions anywhere in the world) to locate seismic events accurately and determine their nature. If the primary interest in the network is for earthquake location, a concentration of stations in areas of known seismicity is appropriate.

One of such networks with the corresponding public data interface is EPOS, the European Plate Observing System, is a long-term plan to facilitate integrated use of data, data products, and facilities from distributed research infrastructures for solid earth science (geologists) in Europe.

ORFEUS EIDA implements various web services¹ to provide standardized and open access to data. The specifications and the usage of parameters of each service can be on the Orfeus page².

Note: ORFEUS EIDA consists of multiple data centres with unique data holdings and webservices. Data exposed at one data centre may not be available at another, therefore the appropriate node should be selected in your request. Please consult the EIDA networks page to discover the appropriate node(s) for data requests and citation.

Example of the data that can be retrieved is the following:

- TimeOrigin time of the event in UTC
- LatitudeEvent latitude in degrees
- LongitudeEvent longitude in degrees
- Depth/kmEvent depth in kilometers
- AuthorIdentifier of event origin author
- CatalogIdentifier of source catalog
- ContributorIdentifier of event information contributor
- ContributorIDEvent ID as reported by the contributor
- MagTypeMagnitude scale identifier (e.g. mb, ML, Mw)

¹ <https://www.orfeus-eu.org/data/eida/webservices/>

² <https://www.orfeus-eu.org/data/eida/networks/>

- MagnitudeMagnitude value
- MagAuthorIdentifier of magnitude author
- EventLocationNameGeographic description of event location (e.g. Flinn-Engdahl region name)
- EventTypeEvent type classification string as of QuakeML 1.2
- EventType enumeration

Note besides public API like the one exposed by EPOS, a number of twitter channels that can also be monitored to collect up to date information. For instance the: ISTITUTO NAZIONALE DI GEOFISICA E VULCANOLOGIA (INGV) has both a web interface and via twitter³.

3.2. Weather Channel API

Several platforms provide weather info on the web, in line with other external sources of information a specific module will be implemented to collect information based on the location information of the areas where the infrastructures are located, this can span over an entire nation so the area to cover is very large. However, in certain cases this presupposes that the operator has equipment installed on meteo conditions (alert), proper location info (latitude, longitude), severity of the event, wind speed, water level for flood. The modules will connect to a public channel like baron weather⁴ or open weather maps⁵ and filtering based on coordinates will be implemented.

It is assumed that the natural disasters threats to be handled by RESISTO will be based on already existing sensors (i.e. fire or flood alarms) in the telecom infrastructures or in order to use results from already existing networks the connection to the service or public web API could be used. Depending on the type of site they could be or not damaged in case values are above a certain level. The scope of the event collection is to correlate with other input to the system for instance from the network management to identify specific natural disaster conditions (e.g. in case of very strong wind some antennas could be tilted). Only events of a certain magnitude shall be considered and correlated.

³ <http://www.ingv.it/it/>

4. OSINT PLATFORMS FOR MONITORING THREATS AND VULNERABILITIES

Threat Intelligence is the analysis of internal and external threats to an organization performed in a systematic way. The threats that Threat Intelligence attempts to defend against include zero-day threats, exploits and Advanced Persistent Threats (APTs). Threat intelligence includes in-depth analysis of both internal and external threats.

RESISTO approach to integration of OSINT events is to anticipate incidents with threat intelligence practices shared among telecom companies, to result in a holistic security process.

Monitoring and staying ahead against risks is a complex activity: even if there are well-known and reputable threat intelligence feeds, it is still a challenge to manage and prioritize potential threats.

The use of open source intelligence (OSINT) techniques will provide necessary information on the evolution of the threat landscape surrounding the telecom network and all devices connected through it.

One of the use cases that will be considered is botnets. Among the others, botnets can be used as a mean to perform a direct DDoS attacks which can reduce network capacity, degrade performance, increase traffic exchange costs, disrupt service availability and even bring down Internet access if ISPs are hit. Besides, DDoS attacks can be a cover for a deeper, more damaging secondary attack, such as large-scale ransomware campaigns. DDoS attacks are often related to the exploitation of vulnerabilities in network and consumer devices, in fact there have been several cases of botnets composed by IoT devices such as home routers or IP cameras. The attackers are targeting these kinds of devices, due to their lack of security, most of the time they have software vulnerabilities or misconfigurations such as default or weak passwords.

In order to face this, the RESISTO OSINT solution can be used for identifying devices exposed to the internet and able to detect if they have any known vulnerability or misconfigurations are implemented in the Telecom network and will be reported to the event correlator.

The main features of the crawler will be collect information regarding CVE and potential misconfigurations and known vulnerabilities. A second step will be to identify devices exposed to the Internet that are also connected on the operator network using tools from the IVRE framework. The information collected by IVRE will be: the IP of the device, the software running on it, the potential misconfigurations/vulnerabilities, the country, the geolocation, among other data.

So in summary RESISTO approach will be based of integration of different tools and OSINT platforms:

- a crawler based on Twitter API to collect threat intelligence events evolution
- a machine learning platform to process the events collected by the crawlers
- IVRE framework will be used to perform network « recon » (i.e. gathering information) to correlate the data collected on the internal operator network with the events found by the crawler.

4.1. MISP

MISP (Malware Information Sharing Platform) is a knowledge base on malware, initially built to support NATO Computer Incident Response Capability Technical Centre (NCIRC TC) missions, whose purpose is to speed up the detection of incidents and the production of defence countermeasures, especially for malware that is not blocked by anti-virus protection, or that is part of sophisticated targeted intrusion attempts.

MISP platform is used by a number of organizations to store and share security related events it in fact allows sharing of technical characteristics of malware within a trusted community. The events comprise a number of information but avoid to share information about the context of the incident. The platform includes a web-based platform, a searchable repository with a multidirectional information

sharing mechanism. MISP repository provides also mechanisms to perform automatic import and export of data and interfacing with other systems.

MISP when used as Threat intelligence platform, results in a quite big volume of data in a short period of time. For instance, MISP will provide a set of IoC (Indicator of Compromise) that are widely used in TI. The IoC's are entities such as Hashes, IPs, domain names, emails, emails subject lines, filenames or registry keys.

Published	Org	Id	Clusters	Tags	#Attr	#Corr	#Sightings	#Post
✓	CERTBW	63428	Threat Actor TA505	PAP:WHITE ttp:white malware_classification:malware-category="Downloader"	75	2		
✓	CERT-RLP_1185	63434		ttp:green	2			
✓	CERT-RLP_1185	63435		ttp:green osint:lifetime=ephemeral	2			
✓	CERT-RLP_1185	63429		ttp:green osint:lifetime=ephemeral	189	84		
✓	CERTBW	63427	Malpedia Geodo Tool Emotet	malware:emotet ttp:white	684			
✓	CERT-RLP_1185	63430		ttp:green	389	17		
✓	CIP	63425	Attack Pattern	ttp:white osint:source-type="blog-post"	38			

Figure 3 MISP dash board

4.2. Crawlers

The data collected will be analysed using Machine Learning algorithms. More than one alternative approach based on ML algorithms can be used. One approach which has been also considered in several cases is to use tweets, a large number of security organizations are publishing news using twitter that seems quite interesting.

Tweeter is the platform most used to share data in the communities and practitioners about security issues, therefore we decided to use only this as crawling mean to collect data. RESISTO implemented a module that will connect to the Tweeter API and collect tweets related to CVE (common vulnerability exposure) the crawler will select tweets according to a dictionary that will be configurable and that will be enriched during time with new terms that can be used in selecting the tweets. The output will be a dataset of tweets that will be forwarded to the ML modules for elaboration.

4.3. IVRE framework

IVRE⁶ is an open-source framework for network recon. It relies on open-source well-known tools (Nmap, Zmap, Masscan, Bro and p0f) to gather data (network intelligence), stores it in a database (MongoDB), and provides tools to analyze it.

It includes a Web interface aimed at analyzing Nmap scan results (since it relies on a database, it can be much more efficient with huge scans than a tool like Zenmap, the Nmap GUI, for example).

IVRE includes tools to run Nmap or Masscan against targets like a network or an address range, a whole country, a specific AS, or the full IPv4 connected address space. It can use Zmap for a fast pre-scan, and collect info from network traffic (passively) using Bro, Argus, Nfdump & p0f.

Use the CLI tools, the Python API or the Web interface to browse the results.

Filter, look for specific services or vulnerable versions, within a specific country or network, quickly access to previous results for a specific host, etc. We shall collect information in the internal network of the Operator to detect devices that can be interested by vulnerabilities collected with the crawlers.

4.4. Machine Learning in threat Intelligence processes

The volume of information regarding cyber threats can be very difficult to process on time, therefore it is necessary to filter the noise in order to analyse the relevant information.

For this purpose, the data collected with the tweet crawler will be separated in 2, one will select only a reliable source of CVE from specific accounts that were selected based on their timeliness in reporting CVE information and will be used as a control flow, the other will collect all tweets based on the dictionary and will be feed to the ML because will generate a large amount of tweets to identify the trends of the attacks that are going on the networks.

Moreover, on top the crowdsourced data gathered by the crawler, Machine Learning techniques will be used to filter and adapt to the telecommunications sector the Intelligence information shared.

The tweets will be feed to ML and/or DL to analyse potential IoCs. TI information DDos attacks where botnets of devices will be considered.

The output of this analysis will be used to configure dynamically the scan using the appropriate tools from IVRE framework to verify if the new threats apply in the specific network of the operator. The positive cases will then be sent to the Event Correlator to trigger proper additional correlation and trigger proper workflow actions.

⁶ <https://ivre.rocks/>

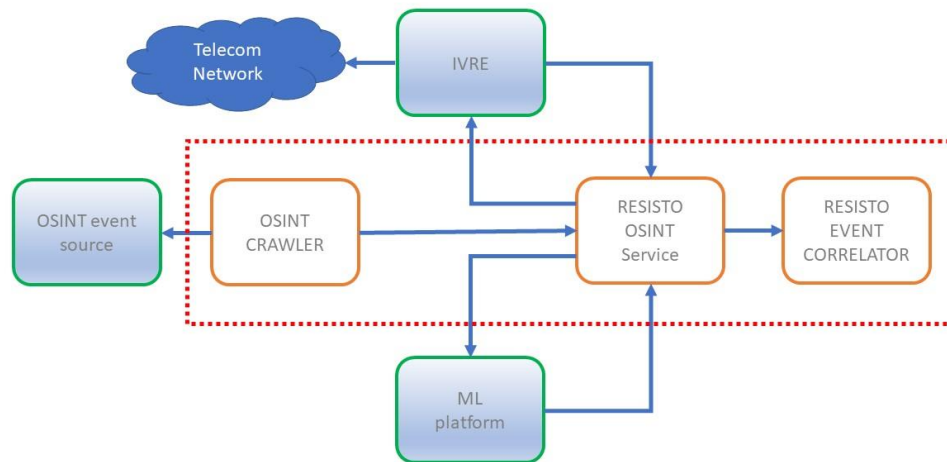


Figure 4 OSINT Service

4.5. Collecting data for threats propagation

In case one or more vulnerabilities are exploited by any malware looking for victims to add to their botnet the data collected by the Tweet crawler will help estimating the propagation of botnets in the IoT devices connected to the telecom provider network.

IVRE framework will be used to scan the network to obtain the approximated number of IoT devices (cameras, routers) of a certain model and firmware version installed that can be the target of the botnet.

The data collected by the crawler and the number of devices found using IVRE scan will be used Task 4.4 “Threats propagation in the TLC infrastructure”, to determine the parameters the possible impact could have on the telecom services chain and how they are propagated within the TLC infrastructure.

The number of devices can be used to estimate the impact of a DDoS attack, in case they are compromised, and TI information collected by the crawlers could be used to find out how a DDoS attack is going to be spread or what are the targets of the cybercriminals.

This all process should produce an estimate of the growth of the botnet. As an example this could be done as follows, if there are a lot of particular IP Surveillance Cameras in a certain nation, called nation 1, exposed and there is a botnet compromising the same devices in another nation, called nation 2, this might be an indication that the attackers are starting to target also devices located in the nation 1.

5. THREAT DETECTION BASED ON IOT SENSORS

There are two complementary tools that are part of RESISTO which make use of IoT sensors for the detection of physical events/threats. These tools, being developed by INTEGRASYS in the context of RESISTO project, are the following:

- **RADIOFILTER**: Standalone system used for the detection of non-authorized access points, devices and connections in manned facilities as well as intrusion detection in unmanned facilities.
- **RANMONITOR**: Standalone system used for the detection of IMSI-catchers/rogue base stations, misconfigured small cells and interferences to the cellular network (intentional and non-intentional)

The physical events detected by RADIOFILTER and RANMONITOR are published as IDEA messages with JSON data format. In IDEA (Intrusion Detection Extensible Alert) messages each line is in the form KEY: TYPE. The keys "Format", "ID", "DetectTime" and "Category" are mandatory. The rest of the keys are optional (non-existent key indicates that information is not applicable or unknown).

Each creator of an IDEA message is encouraged to do their best to describe a security event by existing fields already included in the data model definition, however completely new fields name may be used if none existing are applicable. This is the case in the physical events (threats) detected by RADIOFILTER and RANMONITOR. Given the physical nature of these events based on radio spectral monitoring, new fields (whether KEY or TYPE) needed to be defined.

The following keys are used in RADIOFILTER and RANMONITOR generated messages (new custom fields, whether key or type, are written in *italics*):

KEY	Description	TYPE [range of possible sent values]	Sent
Format	Identifier of the IDEA container	Version	Always
ID	Unique message identifier	ID	Always
CreateTime	Timestamp of the creation of the IDEA message. May point out delay between detection and processing of data	Timestamp	Always
DetectTime	Timestamp of the moment of detection of event (not necessarily time of the event taking place). This timestamp is mandatory, because	Timestamp	Always

	every detector is able to know when it detected the information - for example when line about event appeared in the logfile, or when its information source says the event was detected, or at least when it accepted the information from the source.		
Confidence	Confidence of detector in its own reliability of this particular detection. If key is not presented, detector does not know (or has no capability to estimate the confidence).	number [0 – surely false, 1 – no doubts]	in some events
Category	Category of event. Category name consists of one or two abbreviated parts - category and optional subcategory, separated by dot. If unsure of more precise nature of the incident, subcategory and dot may be omitted	EventTag [Intrusion.UnauthorizedDevice Intrusion.UnauthorizedAP Fraud.Phishing Fraud.Masquerade Information.UnauthorizedConnection Service.NonIntentionalInterference Service.Jamming]	Always
Description	Short free text human readable description	string	Always
Source / Target	Information concerning the threat source / target	Array of object	Always
Type	Type of source / target	[UnknownDevice UnknownAP Device Cell Jammer NonintentionalInterferer]	Always

<i>Freq</i>	Center frequency of the source/target signal (AP, device, cell...) in MHz	number	Always
<i>RSSI</i>	Received –from the source/target –Signal Strength Indicator in dBm	number	in some events
<i>Location</i>	Room level approximate location of the source device/AP	string	in RADIOFILTER events only
<i>MAC</i>	Source device/AP MAC address	string	in RADIOFILTER events only
<i>Tech</i>	Source/target cell 3GPP Technology (i.e. GSM, UMTS, LTE...)	string	in RANMONITOR events only
<i>MCC</i>	Source/target cell Mobile Country Code	string	in RANMONITOR events only
<i>MNC</i>	Source/target cell Mobile Network Code	string	in RANMONITOR events only
<i>TAC</i>	Source/target cell Tracking Area Code (this attribute is only for LTE cells, in case of other technologies an analogue attribute could be used)	string	in RANMONITOR LTE events only
<i>ENBI</i>	Source/target cell eNodeB Identifier (this attribute is only for LTE cells, in case of other technologies an analogue attribute could be used)	string	in RANMONITOR LTE events only
<i>CI</i>	Source/target Cell Identifier (this attribute is only for LTE cells, in	string	in RANMONITOR LTE events only

	case of other technologies an analogue attribute could be used)		
<i>PCI</i>	Source/target Physical Cell Identifier (this attribute is only for LTE cells, in case of other technologies an analogue attribute could be used)	string	in RANMONITOR LTE events only
<i>RSRP</i>	Source/target cell Reference Signal Received Power in dBm (this attribute is only for LTE cells, in case of other technologies an analogue attribute could be used)	number	in RANMONITOR LTE events only
Node	Detector description	Array of object	Always
Name		string	Always
Type		string [<i>Spectrum.Monitor</i>]	Always

In the following table an indicative list has been compiled with all the physical security events that RADIOFILTER and RANMONITOR are able to detect; a description and a basic JSON serialized IDEA Message example is given as it would be sent to the RESISTO platform (Short Term Control Loop –STCL- correlator). In addition, the IDEA messages shown are basic examples that could be modified in further stages.

Physical Security Event	Description	IoT Sensors Detection Tool	Basic JSON serialized IDEA Message
Non-whitelisted device MAC address inside infrastructure	A device MAC address (BSSID) which is not whitelisted is detected inside the infrastructure.	RADIOFILTER	<pre>{ "Format": "IDEA0", "ID": "00000000-0000-0000-0000-000000000000", "CreateTime": "2019-07-24T09:00:08Z", "DetectTime": "2019-07-24T09:00:07Z", "Category": ["Intrusion.UnauthorizedDevice"], "Description": " Non-whitelisted device MAC address inside infrastructure", "Source": [{ "Type": ["UnknownDevice"], "MAC": ["00:00:00:00:00:00"], "Freq": 2452, "RSSI": -67, "Location": "Room A" }], "Node": [{ "Name": "eu.resisto.radiofilter", "Type": ["Spectrum", "Monitor"], "SW": ["Radiofilter v1.0"], }] }</pre>
Non-whitelisted Access Point MAC address inside infrastructure	An AP MAC (BSSID) address which is not whitelisted is detected inside the infrastructure. This could be a rogue AP.	RADIOFILTER	<pre>{ "Format": "IDEA0", "ID": "00000000-0000-0000-0000-000000000000", "CreateTime": "2019-07-24T09:00:08Z", "DetectTime": "2019-07-24T09:00:07Z", "Category": ["Intrusion.UnauthorizedAP"], "Description": " Non-whitelisted AP MAC address inside infrastructure", "Source": [{</pre>

```

    "Type": ["UnknownAP"],
    "SSID": ["Corporate Telco WLAN"],
    "MAC": ["00:00:00:00:00:00"],
    "Freq": 2447,
    "RSSI": -60,
    "Location": "Room A"
  }
],
"Node": [
  {
    "Name": "eu.resisto.radiofilter",
    "Type": ["Spectrum", "Monitor"],
    "SW": ["Radiofilter v1.0"],
  }
]
}

```

**Access Point
with repeated
SSID detected
inside
infrastructure**

An AP with a RADIOFILTER repeated SSID is detected inside the infrastructure. This could be an evil twin attack.

```

{
  "Format": "IDEA0",
  "ID": "000000000-0000-0000-0000-000000000000",
  "CreateTime": "2019-07-24T09:00:08Z",
  "DetectTime": "2019-07-24T09:00:07Z",
  "Category": ["Fraud.Phishing"],
  "Description": " AP with repeated SSID detected inside infrastructure ",
  "Source": [
    {
      "Type": ["UnknownAP"],
      "SSID": ["Corporate Telco WLAN"],
      "MAC": ["00:00:00:00:00:00"],
      "Freq": 2442,
      "RSSI": -63,
      "Location": "Room A"
    }
  ],
  "Node": [
    {
      "Name": "eu.resisto.radiofilter",
      "Type": ["Spectrum", "Monitor"],
      "SW": ["Radiofilter v1.0"],
    }
  ]
}

```

			<pre>] } </pre>
Whitelisted device connection with non-whitelisted AP outside the infrastructure	A whitelisted device has a connection established with a non-whitelisted (i.e. unauthorized) AP outside the infrastructure.	RADIOFILTER	<pre> { "Format": "IDEA0", "ID": "00000000-0000-0000-0000-000000000000", "CreateTime": "2019-07-24T09:00:08Z", "DetectTime": "2019-07-24T09:00:07Z", "Category": ["Information.UnauthorizedConnection"], "Description": " Whitelisted device connection with non-whitelisted AP outside the infrastructure ", "Source": [{ "Type": ["Device"], "MAC": ["00:00:00:00:00:00"], "Freq": 2442, "RSSI": -59, "Location": "Room A" } { "Type": ["UnknownAP"], "SSID": ["Corporate Telco WLAN"], "MAC": ["00:00:00:00:00:00"], "Freq": 2442, "RSSI": -81, "Location": "Outside" }], "Node": [{ "Name": "eu.resisto.radiofilter", "Type": ["Spectrum", "Monitor"], "SW": ["Radiofilter v1.0"], }] } </pre>
Whitelisted device connection with non-whitelisted AP inside the	A whitelisted device has a connection established with a non-whitelisted (i.e. unauthorized)	RADIOFILTER	<pre> { "Format": "IDEA0", "ID": "00000000-0000-0000-0000-000000000000", "CreateTime": "2019-07-24T09:00:08Z", </pre>

infrastructure	AP inside the infrastructure	<pre> "DetectTime": "2019-07-24T09:00:07Z", "Category": ["Information.UnauthorizedConnection"], "Description": " Whitelisted device connection with non-whitelisted AP inside the infrastructure ", "Source": [{ "Type": ["Device"], "MAC": ["00:00:00:00:00:00"], "Freq": 2442, "RSSI": -59, "Location": "Room A" } { "Type": ["UnknownAP"], "SSID": ["Corporate Telco WLAN"], "MAC": ["00:00:00:00:00:00"], "Freq": 2442, "RSSI": -55, "Location": "Room A" }], "Node": [{ "Name": "eu.resisto.radiofilter", "Type": ["Spectrum", "Monitor"], "SW": ["Radiofilter v1.0"], }] } </pre>
Whitelisted device unauthorized peer-to-peer connection with whitelisted device	A whitelisted device inside or outside the infrastructure has an unauthorized peer-to-peer connection established with a whitelisted device inside or outside the infrastructure.	<pre> RADIOFILTER { "Format": "IDEA0", "ID": "00000000-0000-0000-0000-000000000000", "CreateTime": "2019-07-24T09:00:08Z", "DetectTime": "2019-07-24T09:00:07Z", "Category": ["Information.UnauthorizedConnection"], "Description": " Whitelisted device unauthorized peer-to-peer connection with whitelisted device", "Source": [{ "Type": ["Device"], </pre>

```

    "MAC": ["00:00:00:00:00:00"],
    "Freq": 2412,
    "RSSI": -64,
    "Location": "Room A"
  }
  {
    "Type": ["Device "],
    "MAC": ["00:00:00:00:00:00"],
    "Freq": 2412,
    "RSSI": -67,
    "Location": "Outside"
  }
],
"Node": [
  {
    "Name": "eu.resisto.radiofilter",
    "Type": ["Spectrum", "Monitor"],
    "SW": ["Radiofilter v1.0"],
  }
]
}

```

Unknown cell detected A cell is detected in the operator frequency bands with an unknown ID. This cell could be a rogue eNodeB or an IMSI-catcher

```

RANMONITOR {
  "Format": "IDEA0",
  "ID": "00000000-0000-0000-0000-000000000000",
  "CreateTime": "2019-07-24T09:00:08Z",
  "DetectTime": "2019-07-24T09:00:07Z",
  "Category": ["Fraud.Masquerade"],
  "Description": " Unknown cell detected",
  "Confidence": 0.7,
  "Source": [
    {
      "Type": ["Cell"],
      "Freq": 796,
      "Tech": ["LTE"],
      "MCC": ["000"],
      "MNC": ["1"],
      "TAC": ["1234"],
      "ENBI": ["1122334455"],
      "CI": ["9"],
      "PCI": ["100"],
      "RSRP": -92
    }
  ]
}

```

```

    }
  ],
  "Node": [
    {
      "Name": "eu.resisto.ranmonitor",
      "Type": ["Spectrum", "Monitor"],
      "SW": ["Ranmonitor v1.0"],
    }
  ]
}

```

High level of interference in a specific cell from a non-intentional source

High level of non-intentional interference (including noise) causing service degradation or outage in a specific cell

RANMONITOR {

```

  "Format": "IDEA0",
  "ID": "00000000-0000-0000-0000-000000000000",
  "CreateTime": "2019-07-24T09:00:08Z",
  "DetectTime": "2019-07-24T09:00:07Z",
  "Category": ["Service.NonIntentionalInterference"],
  "Description": " High level of interference in a specific cell from a non-intentional source ",
  "Confidence": 0.7,
  "Source": [
    {
      "Type": ["NonIntentionalInterferer"],
      "Freq": 796,
      "RSSI": -80,
    }
  ],
  "Target": [
    {
      "Type": ["Cell"],
      "Freq": 796,
      "Tech": ["LTE"],
      "MCC": ["000"],
      "MNC": ["1"],
      "TAC": ["1111"],
      "ENBI": ["333333333"],
      "CI": ["7"],
      "PCI": ["300"],
      "RSRP": -92
    }
  ]
}

```

```

    ],
    "Node": [
      {
        "Name": "eu.resisto.ranmonitor",
        "Type": ["Spectrum", "Monitor"],
        "SW": ["Ranmonitor v1.0"],
      }
    ]
  }
}

```

High level of interference in a specific cell from a jammer

High level of jamming interference (including noise) causing service degradation or outage in a specific cell

```

{
  "Format": "IDEA0",
  "ID": "00000000-0000-0000-0000-000000000000",
  "CreateTime": "2019-07-24T09:00:08Z",
  "DetectTime": "2019-07-24T09:00:07Z",
  "Category": ["Service.Jamming"],
  "Description": "High level of interference in a specific cell from a jammer",
  "Confidence": 0.7,
  "Source": [
    {
      "Type": ["Jammer"],
      "Freq": 796,
      "RSSI": -70,
    }
  ],
  "Target": [
    {
      "Type": ["Cell"],
      "Freq": 796,
      "Tech": ["LTE"],
      "MCC": ["000"],
      "MNC": ["1"],
      "TAC": ["1111"],
      "ENBI": ["3333333333"],
      "CI": ["7"],
      "PCI": ["300"],
      "RSRP": -90
    }
  ],
  "Node": [
    {

```



```
"Name": "eu.resisto.ranmonitor",  
"Type": ["Spectrum", " Monitor"],  
"SW": ["Ranmonitor v1.0"],  
}  
]  
}
```

Based on the correlation rules available at the platform and the information about the event detected by the sensors, the correlator will decide whether a physical security alarm should be raised or not.

6. KSI BLOCKCHAIN MONITORING TECHNIQUES AND PROCEDURES

IoT device cybersecurity monitoring solution is based on *Guardtime MIDA* framework, extended with RESISTO specific message formats and IoT device security policies. First the main underlying technologies are described, followed by more thorough description of the MIDA platform, its adaptation for IoT cybersecurity use-case and integration into the RESISTO project.

6.1. KSI Blockchain

KSI Blockchain provides data authenticity, time and participant identity. These are achieved through the creation of the KSI Signature that seals the MIDA Snapshot. Each of the Agents and Services supporting the creation of the MIDA Snapshots will be provisioned a unique identity associated with the KSI Blockchain.

KSI Blockchain is described in more detail in “RESISTO: D4.1_ACTIVE AND PASSIVE SENSOR DEFINITION”, section 5.3 (KSI Blockchain overview and use in telecom network monitoring).

The KSI infrastructure implements the functions of KSI Blockchain. It provides high availability and scalability ensuring that any number of signatures can be requested worldwide and the time to get the signature is always approximately one second.

6.2. XDAL and Dockets

XDAL, or the eXtensible Data Attribution Language, provides the basic data structure for the MIDA State Captures. XDAL is used by MIDA Agents and Services to normalize and format data in specific ways. This allows for the transmission and verification of the State Captures as well as the ability to imbue the data with context or policy inputs. XDAL defines the syntax and semantics of the MIDA construct called “Dockets”. These “Dockets” provide an interoperable and self-contained construct to cryptographically link data authenticity, identities, and contextual based information using the KSI Signature. The KSI Signature is the output of participating in the KSI Blockchain, and cryptographically proves the data has not been altered, provide the identity of the participant, and includes system agnostic time. Once sealed with a KSI Signature, these Dockets enable the state captures from the MIDA Agents and Services to be portable, allowing them to be verified across boundaries and in perpetuity. In MIDA, the dockets are used to encapsulate and protect the identities of the agents or services, data authenticity of the state capture and time associated with the capture. These can then be cryptographically verified by the State Management Services, owners, and auditors.

6.3. Guardtime MIDA

Guardtime MIDA (Machine Integrity, Defense and Awareness) provides capabilities for machine and environmental integrity state capture, defense, and remediation for distributed, cloud, and IoT environments. The main capabilities of MIDA are providing awareness and reporting, remediation techniques, malicious or accidental state change detection, and enhanced analytics. These basic capabilities are valuable across many environments such as cloud, IoT, virtualized environments, and even host-based systems such as laptops, desktops, and mobile devices. The MIDA product suite is used to streamline development and reuse as much knowledge, investment, and resources as possible across the various environments.

6.3.1. MIDA Overview

Guardtime MIDA provides adaptive state capture and event correlation through what are called MIDA Snapshots. These snapshots allow system owners and operators to significantly cut the time from accidental or malicious event to remediation. Along with cryptographically sealing more traditional system and transaction log events, MIDA provides an adaptable platform for capturing and correlating the systemic state of infrastructure and machine instances. MIDA enables the ability to containerize this information through the creation of these resilient data objects or MIDA Snapshots. These infrastructure snapshots leverage the KSI Blockchain to gain accountability, immutability and time of creation. The Snapshots contain the various types of state data and are sealed with a KSI Signature. Leveraging the KSI Blockchain, these snapshots provide true cryptographic verification, allowing them to become truly portable and durable for cross organizational distribution, event correlation and analysis, and long-term storage.

Using Guardtime's unique approach to Provable State Capture, the Guardtime MIDA product is designed to provide unprecedented and provable insights into the operation of infrastructures, namely:

- Realtime Discovery of Misconfiguration or Malicious Changes,
- Cryptographically Immutable Inputs for Audit, Certification and Accreditation,
- Provable and Real-Time Continuous State and Integrity Monitoring,
- Trusted and Portable Data,
- Granular Accountability and Chain of Custody of Events,
- Enhanced Durable Data for Analytics.

The primary components of the MIDA are:

- Guardtime KSI Blockchain – provides the distributed trust anchor for Docket Verification.
- MIDA Services – provide distributed data capture for AWS/Azure events such as instance creation or security group changes and KSI Blockchain integration (not used in the RESISTO project).
- MIDA Agents – provide distributed data capture for system state and configuration changes. These reside within the actual IoT sensors and devices and monitor events such as file changes, directory changes, and processes.
- MIDA State Management Services – provides backend event analysis, correlation, exchange and storage management. Consists of the Sentry, Broker, and Venture that are highlighted later in the document.
- MIDA Dashboard – provides visualization, event correlation and alerting

A (high level) logical overview of the MIDA is depicted in the following picture.

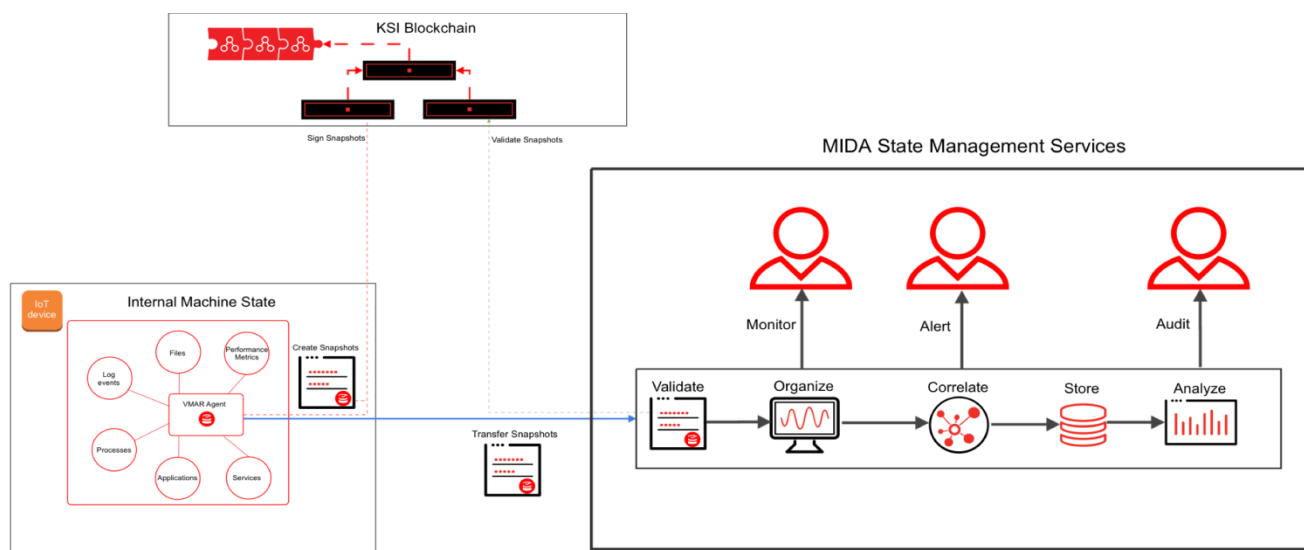


Figure 5 Guardtime MIDA

6.3.2. MIDA Agent

MIDA Machine Awareness and Reporting Agents are deployed to a local machine (or device). These are commonly deployed onto edge devices, switches, routers, or host systems.

The following pollers have been implemented:

Auth log	Monitors and captures SSH events from auth.log.
Directory change poller	Watches directories for changes and periodically creates and routes docketts for each captured event. Event type can be ENTRY_CREATE, ENTRY_DELETE or ENTRY_MODIFY. If for some reason an event is lost or discarded, OVERFLOW event will be captured. Period of which the events are routed depends on the polling interval.
File change poller	Watches files for changes and periodically creates and routes docketts for each captured event. Event type can be ENTRY_CREATE, ENTRY_DELETE or ENTRY_MODIFY. If for some reason an event is lost or discarded, OVERFLOW event will be captured. Period of which the events are routed depends on the polling interval.
File system ownership	Watches files and directories for ownership changes.
File system permissions	Watches files and directories for permission changes.
Processes	Captures the number of currently running processes and for each process its ID, user and command.
Performance	Captures CPU and Memory usage.

6.3.3. MIDA State Management Services

Potential deployment scheme depicting MIDA State Management Services is provided in the following figure.

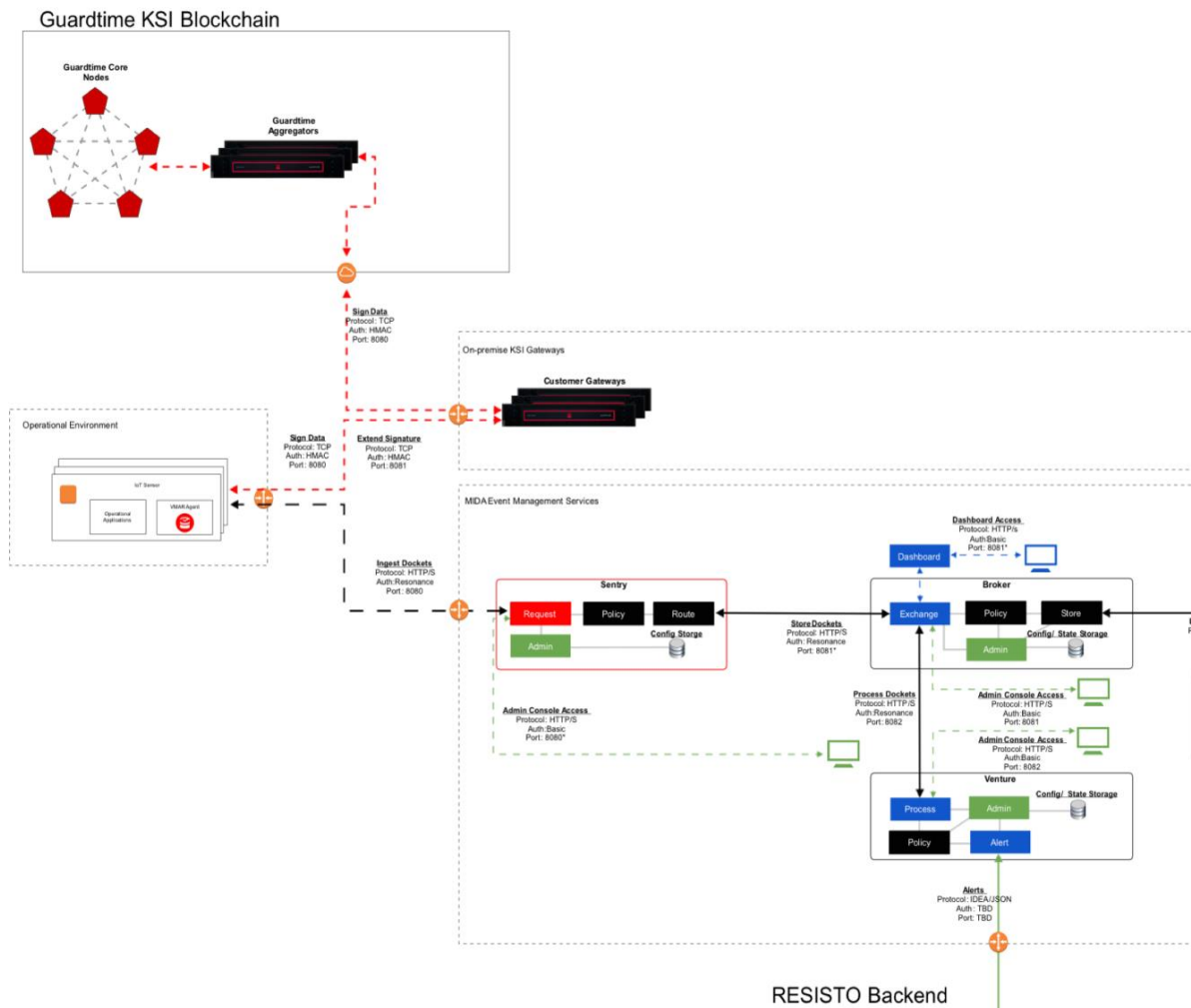


Figure 6 Guardtime MIDA deployment in the RESISTO project

6.3.3.1. Sentry

Sentry provides a configurable policy enforcement and decision point focused on validating only authentic and relevant Dockets are stored in the MIDA platform. Sentry achieves this by leveraging the XDAL Patterns, attributes, and contextual information to validate the Docket relevancy and KSI Signatures to cryptographically validate the authenticity. Sentry also provides secure Docket

exchange by providing KSI Authorization and Authentication enabling distributed and granular access control and rights management to resources.

In order to protect the infrastructure from bad actors or misconfigured clients sending Dockets to an incorrect instance, the Dockets needed to be processed to verify they were authentic, authorized and relevant. The processing of these Dockets needed to include the identity of the creator, verify the business process was performed correctly, and make sure the Docket was constructed in a correct manner. These types of rules processing are what makes up the Sentry Policy.

6.3.3.2. *Broker*

Broker provides Docket storage and exchange between data stores and other MIDA components. Broker provides configurable features to enable these types of capabilities through Broker Administration Console and through manual configuration on the server. The primary capabilities and features include modular storage configuration, tailored storage parameters and configurable triggers.

6.3.3.3. *Venture*

Venture combines traditional "Secure Workflows" with the ability to perform these in a distributed manner, and include important business functions such as cross organizational consensus and data processing.

Venture provides support for business processes that are modelled using Dockets. Venture watches for dockets entering the platform, and when it detects one that is part of a defined workflow, it notifies participants of the workflow that they need to perform the appropriate task in order to move the docket through the workflow.

Many of the use cases required the ability to perform some business processing or consensus around the Dockets being stored. These were commonly realized through processes such as "Voting" or what we now call Multi-Signature Processing Rules where multiple end users were required to perform actions. Due to the nature of the Dockets this could be performed across boundaries and with granular visibility since the identities, time and relationships between the Dockets remained intact across organizations.

Within the RESISTO Project Venture is configured to detect illegitimate state changes in monitored devices and forward alarms to RESISTO-specific backend services.

6.3.3.4. *MIDA Dashboard*

The MIDA Dashboard aims to provide multiple levels of visualization and data to the end user in the MIDA Dashboard Rollup and MIDA Dashboard Details views.

The purpose of the MIDA Dashboard Rollup view is to provide a high-level overview of the current state captures in MIDA. This view aims to visualize the overall state of the system or systems being monitored. It has various graphs and aggregated metrics to present centralized high-level state of all of the assets associated with the state management for that deployed instance of MIDA. This aggregate view will allow an operator of the system to visualize and understand, for example, how many times the state of instances have changes recently or over time. The data aggregated in the

Rollup view also is useful as a "real-time reports" function where a user can quickly navigate to the view and glean useful information at a higher level.

The purpose of the MIDA Dashboard Details view is to provide a "drill down" capability for each of the unique state captures within the MIDA instance. This view will provide the end user with the ability to select individual state captures, the data associated with that Docket, and other useful features such as exporting an individual Docket. The Details view provides the end user with data useful for investigating details of a state capture and have the ability to sort through the Dockets to perform basic queries or sorting functions such as showing all Dockets of specific event type.

Extent of MIDA Dashboard integration and functionality within the RESISTO project is determined during the project execution.

6.4. Why KSI Blockchain?

In providing protection against cyber threats to IoT sensors in the RESISTO project the KSI Blockchain provides auxiliary function. By capturing monitored system's state changes in dockets and anchoring dockets in blockchain we achieve following benefits:

- data is immutable and associated with producing system's identifier,
- data is cryptographically time-stamped,
- integrity is protected for long term, measured in tens of years; even if efficient quantum computer materializes,
- signed containers are exportable and transferrable without key management efforts,
- signed containers are suitable for audit and forensics; even privileged users cannot fabricate data,
- process Integrity of data capture, transfer, processing and storage processes can be demonstrated,
- key leaks do not have catastrophic effects.

Due to relatively simple use-case the data provenance aspect, i.e. cryptographically linking related data captures, is not demonstrated.

7. RESPONSIBLE DISCLOSURE FRAMEWORK

Responsible Disclosure Framework provides tools and a feature-rich system that allows security researcher, independent contractors and other 3rd party security providers to report discovered vulnerabilities on the end user's infrastructure & while they stay in contact with stakeholders responsible for the system in scope throughout the internal Software Development Life Cycle (SDLC) & Patch Management procedures. The process followed is described in

The framework has several critical modules:

Configuration and administration	Scope Definition & Management of Assets	allows end users to define what is the scope of testing for security teams, vulnerabilities to be ignored, responsible disclosure & bug bounty policies
	Vulnerability Triage	allows end users to define teams and pre-verify any reported vulnerability against duplicates, false positive before opening a fix procedure
Vulnerability life cycle	Threat Classification engine	allows both security research and end users team to classify or re-classify findings during the patch management process using Risk Rating Methodologies identified during RESISTO project such as OWASP Risk Rating Methodology or Common Vulnerability Scoring System
	Vulnerability lifecycle GUI & Rewarding module	Vulnerability lifecycle via a user friendly GUI to register and track the progress of the vulnerability, this in turn will trigger the Rewarding module to reward security contractors (which includes the Hall of Fame module update) depending on the finding type and impact which would allow teams to prioritise the findings and track the patch process progress

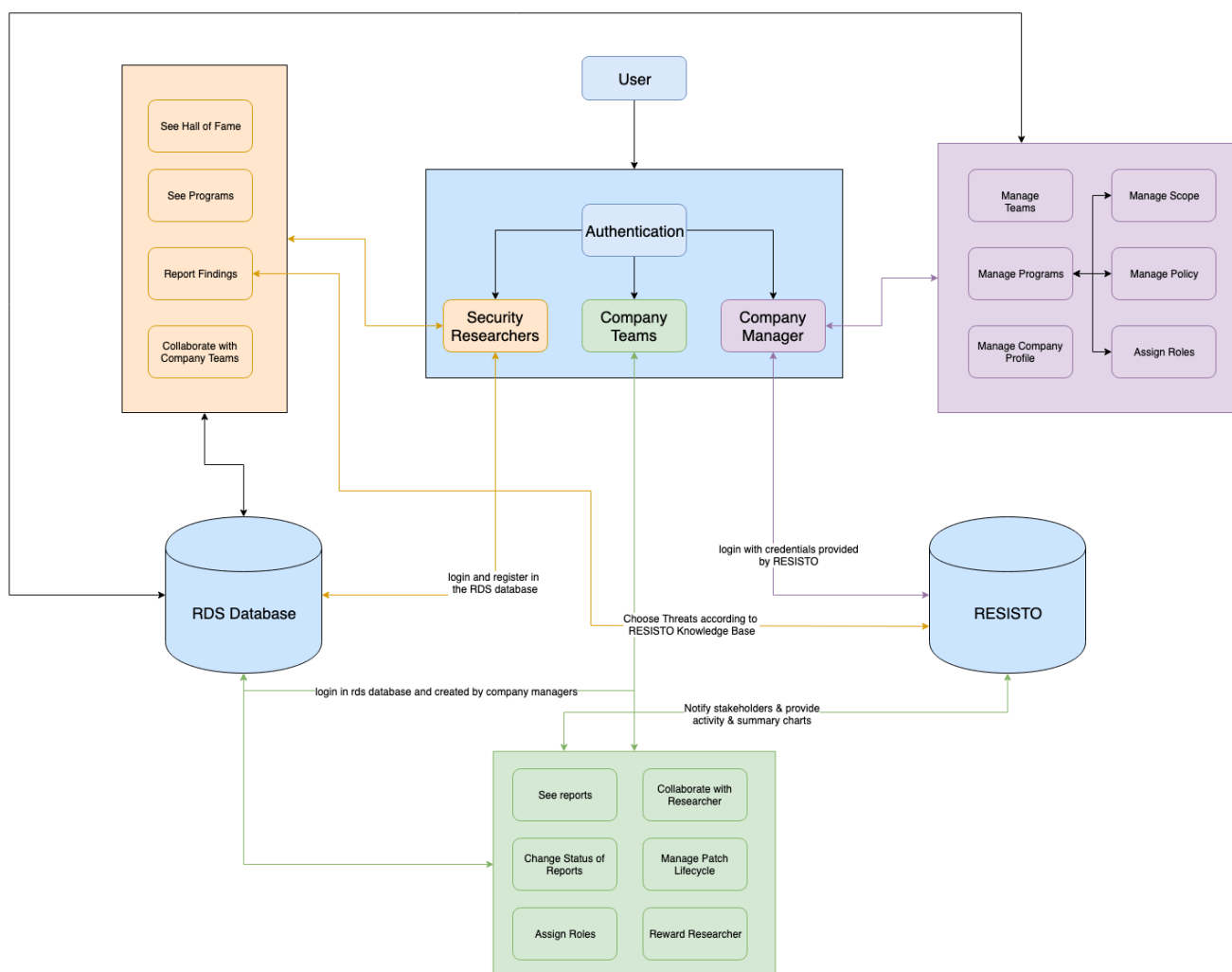


Figure 7 RDF architecture

The Responsible Disclosure Framework proposed by BSS will provide a series of benefits for parties involved in this process:

- For security researchers, independent contractors and other cyber security services:
 - A disclosure guideline and a program policy designed to guide security research into a particular service, product or IoT device
 - a simple interface to report and follow the fixing process during the whole lifecycle
- For end users:
 - Establish a compliant process for receiving and acting on vulnerabilities discovered by third-parties during any penetration testing engagement
 - Align with NIST best practices for accepting and managing security feedback

- Allow teams to prioritise the findings and initiate, supervise and close patching process for individual vulnerabilities while staying in contact with security researchers
- Functionalities to integrate internal or third-parties triage team do the heavy-lifting
- Promote a positive relationship with the security researcher community.

The framework will have to integrate with external sources to achieve the following

- a) Functionalities to integrate internal or third-parties triage team do the heavy-lifting
- b) Promote a positive relationship with the security researcher community.

RDF is integrated in the flow of RESISTO as a tool/system to collect discovered vulnerabilities in the telecom provider development organization. The vulnerabilities once collected will need to be corrected and the tool allows tracking of the corrections throughout the internal Software Development Life Cycle & Patch Management procedures (Note for sw that the telecom provider outsources the framework can be used to handle only the registration/patch management).

For instance one of the events from the OSINT flow can report a new vulnerability to the knowledgebase , if there is not already a patch for the vulnerability the patch lifecycle must start, if a patch is already available a plan must be made to deploy it.

The process followed, which is summarized in figure 6, includes 5 different steps:

1. Definition of the disclosure policy and the attack surface and assets in the scope for testing. This will have to be defined by the operator according to the type of vulnerability involved.
2. Submit the vulnerability to the Responsible Disclosure Framework in order to manage it.
3. Involve the correct organization in the triage, this can be an internal security team, a 3rd party or the asset owner itself.
4. Integrate the triaged vulnerability into the patching process during the Software Development Life Cycle
5. Incentive results with a Hall of Fame for security researchers or sending rewards to foster the research and solution of vulnerabilities activity within the organization.

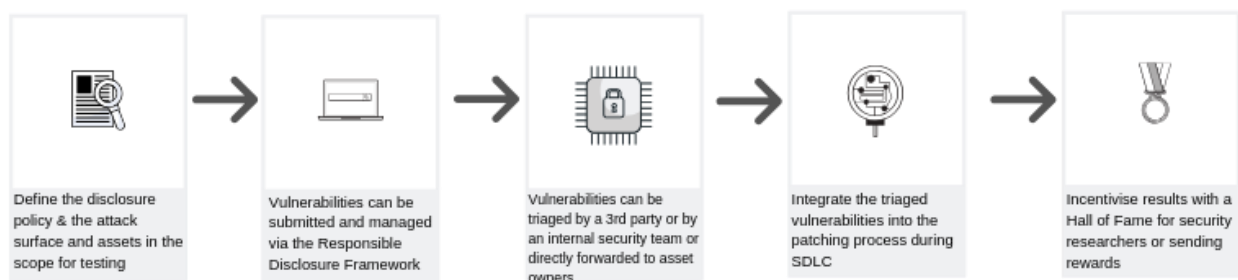


Figure 8 Disclosure Framework Process

8. CONCLUSION

The present Deliverable reports a collection of techniques and procedures that will be collected as alarms and alerts regarding cyber and physical threats detected by RESISTO. The complete set of techniques and the fact that they can be correlated in RESISTO represent a novel holistic approach to root cause analysis.

Alarms from Telecommunication systems via the management network that can be correlated to suspicious activities will be the base for the alarms that will be generated and treated in the use case scenarios.

Alerts formats have also been evaluated and IDEA has been chosen as the standard format in case of threats.

Procedures and techniques are described in detail and will be used by the event correlator to detect relevant events reported by the deployed sensor network. Furthermore, procedures and techniques from data integrity implemented in MIDA - Blockchain have been described in detail.

The Responsible Disclosure Framework will support disclosure guideline, aligned with NIST practices, and a program policy with a simple interface to support the process for the whole lifecycle.

Several other sources of events have been integrated in a number of modules that will be connected to several sources external to RESISTO over the internet they are OSINT platforms, weather channels, seismic networks,

The events collected can be used to correlate internal reported events from the sensor's networks and the network monitoring applications to provide the correct event and therefore mitigation action later in the RESISTO pipeline.

RESISTO correlation process will be based on a holistic approach. Since alarms can be caused by multiple actions or events, alarms shall be correlated with other external events in RESISTO, for instance the ones coming from sensors as event sources and the results of the OSINT analysis.

REFERENCES

Apart from the references already denoted within the txt, the following ones were also considered:

INDEX	REFERENCE
1	RESISTO – Grant Agreement. Project Starting Date: May, 1 st 2018
2	MANO Network Functions Virtualisation (NFV); Infrastructure Overview https://www.etsi.org/deliver/etsi_gs/NFV-INF/001_099/001/01.01.01_60/gs_NFV-NF001v010101p.pdf
3	ETSI GS NFV-SEC 001 (V1.1.1) (10-2014): "Network Functions Virtualisation (NFV); NFV Security; Problem Statement https://www.etsi.org/deliver/etsi_gs/NFV-SEC/001_099/001/01.01.01_60/gs_NFV-SEC001v010101p.pdf
4	M3000 Overview of TMN Recommendations
5	M3016 Security for the management plane: Overview
6	M3400 TMN management functions
7	D4.1 – ACTIVE AND PASSIVE SENSOR DEFINITION