SUNRISE

Strategies and Technologies for **Un**ited and **R**esilient Critical **I**nfrastructures and Vital **S**ervices in Pandemic-Stricken **E**urope

D6.3 Cyber-physical resilience tool and training guide V2

Document Identification			
Status	Final	**Due Date**	31/05/2024
Version	1.0	**Submission Date**	30/05/2024

Related WP	WP6	**Document Reference**	D6.3
Related Deliverable(s)	D6.1, D6.2	**Dissemination Level (*)**	PU
Lead Participant	XLB	**Lead Author**	Justin Činkelj (XLB)
Contributors	ATS, INS, CAF, PIL, SZ, TS	**Reviewers**	Olga Segou (INT) José M. del Álamo (UPM)

Keywords:

Critical infrastructure, cyber-physical resilience, artificial intelligence, threat intelligence, risk assessment, incident reporting, user manual

This document is issued within the frame and for the purpose of the SUNRISE project. This project has received funding from the European Union's Horizon Europe Programme under Grant Agreement No.101073821. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the European Commission.

The dissemination of this document reflects only the author's view, and the European Commission is not responsible for any use that may be made of the information it contains. This deliverable is subject to final acceptance by the European Commission.

(*) Dissemination level: **(PU)** Public, fully open, e.g., web (Deliverables flagged as public will be automatically published in CORDIS project's page). **(SEN)** Sensitive, limited under the conditions of the Grant Agreement. **(Classified EU-R)** EU RESTRICTED under the Commission Decision No2015/444. **(Classified EU-C)** EU CONFIDENTIAL under the Commission Decision No2015/444. **(Classified EU-S)** EU SECRET under the Commission Decision No2015/444.

Document Information

List of Contributors	
Name	**Partner**
Tomaž Martinčič	XLB
Justin Činkelj	XLB
Pablo de Juan	ATS
Miguel Martín	ATS
Susana González	ATS
Jorge Martínez	ATS
Mario Triviño	ATS
Aljosa Pasić	ATS
Gilda De Marco	INS
Daniele Fabro	CAF
Blaž Jemenšek	PIL
Tomaž Ramšak	SZ
Andreja Markun	TS

Document History			
Version	**Date**	**Change editors**	**Changes**
0.1	15/03/2024	Justin Činkelj (XLB)	First version of the document (ToC). Initial inputs to sections.
0.2	08/04/2024	Justin Činkelj (XLB)	Modified LOMOS section
0.2	11/4/2024	Daniel Vladušić (XLB)	Document check and modification
0.2	11/4/2024	Pablo De Juan (ATS)	Modifications
0.3	11/4/2024	Daniel Vladušić (XLB)	Merge of inputs
0.3	15/4/2024	Justin Činkelj (XLB)	Modify pilot trials preamble
0.3	15/4/2024	Pablo De Juan (ATS)	Modifications
0.4	21/4/2024	Daniel Vladušić (XLB)	Merge of inputs
0.6	02/05/2024	Daniel Vladušić (XLB)	Final merge of the inputs and submission into internal review
0.7	10/05/2024	Daniel Vladušić (XLB)	Implementing corrections - review
0.8	14/05/2024	Daniel Vladušić (XLB)	Merge of the corrections.
0.9	16/05/2025	Pablo De Juan (ATS)	Style checks.
0.95	21/05/2024	Daniel Vladušić (XLB)	Final merge of inputs and corrections
0.96	30/05/2024	Juan Alonso (ATS)	Quality Assessment
1.0	30/05/2024	Aljosa Pasic (ATS)	Final version

Quality Control		
Role	**Who (Partner short name)**	**Approval Date**
Deliverable leader	Justin Činkelj (XLB)	28/05/2024
Quality manager	Juan Andrés Alonso (ATS)	30/05/2024
Project Coordinator	Aljosa Pasic (ATS)	30/05/2024

Table of Contents

List of Tables

List of Figures

List of Acronyms

Abbreviation / acronym	Description
AIRE	Atos Incident Report Engine
API	Application Programming Interface
BERT	Bidirectional Encoder Representations from Transformers
BGL	BlueGene/L supercomputer
BPMN	Business Process Model and Notation
CERCA	CybEr Risk assessment CAlculator
CERT	Computer Emergency Response Team
CI	Critical Infrastructure
CNA	CVE Numbering Authorities
CPR	Cyber Physical Resilience
CPU	Central Processing Unit
CSIRT	Computer Security Incident Response Teams
CTI	Cyber Threat Intelligence
CUDA	Compute Unified Device Architecture
CVE	Common Vulnerabilities and Exposures
D6.1	Deliverable number 1 belonging to WP 6
D6.2	Deliverable number 2 belonging to WP 6
D6.3	Deliverable number 3 belonging to WP 6
D6.4	Deliverable number 4 belonging to WP 6
DB	Database
EC	European Commission
EC2	(Amazon) Elastic Compute Cloud
FN	False Negative
FP	False Positive
FTP	File Transfer Protocol
GB	Gigabyte
GDPR	General Data Protection Regulation
GPU	Graphics Processing Unit
GUI	Graphical User Interface
HDD	Hard Disk Drive
HDFS	Hadoop Distributed File System
HTTP	Hypertext Transfer Protocol
ICT	Information and Communications Technology
INCIBE	Instituto Nacional de Ciberseguridad de España
IP	Internet Protocol (address)
IRM	Integrated Risk Management
JSON	JavaScript Object Notation
LOMOS	LOg MOnitoring System
MS	Milestone – Milestones as defined in DoA

MISP	Malware Information Sharing Platform
NIS	Network and Information Security Directive
REST	Representational State Transfer
SIEM	Security Information and Event Management
SOC	Security Operations Centre
SQL	Structured Query Language
SSD	Solid State Drive
TIE	Threat Intelligence Engine
TINTED	Threat Intelligence Node inTEgrated with Data enrichment services
TP	True Positive
TRL	Technical Readiness Level – TRL1 to TRL9
VM	Virtual Machine
VPN	Virtual Private Network
WP	Work Package
WFH	Work From Home

Executive Summary

This deliverable presents the cyber-physical resilience (CPR) tool. The goal of the tool is to improve critical infrastructure (CI) cyber-physical security capabilities. The importance of improving the cyber-security is evident in extreme situations such as a pandemic, where the CIs may face other issues, like absenteeism, which reduces the manpower required to defend the increasingly digital and connected critical infrastructure.

The CPR tool (concept, architecture, initial testing on publicly available data and the piloting scenarios, envisaged for validation) was presented in deliverables D6.1[1] and D6.2[2]. This iteration thus presents improvements of the tool:

- validation of the anomaly detection tool with the real, CI provided, logs;
- improvements in usability of the anomaly detection too;
- threat intelligence scoring module extended with source confidence evaluation for better management of intelligence sources;
- mapping of Indicators of Compromise (IoC) with MITRE ATT&CK matrix techniques in threat intelligence tool;
- risk assessment allows new input to include temporary conditions;
- risk assessment digests alarms from physical activity monitoring (connection with WP7);
- a comprehensive and detailed evaluation of NIS 2 Directive and its impact on the incident reporting module;

The tool was tested with public data (former deliverables) and, as we report in this deliverable, with actual CI provided data. Using real data and setting up the facility to receive live data (through FileBeat), we validated the CPR tool (TRL5). We will proceed with validation and demonstration in M21-M22 of the project (June and July 2024), when the CPR tool is installed locally, at the premises of CIs (validation and demonstration on multiple CI deployments from different sectors). We thus achieved TRL4 in previous deliverables, and we achieved TRL5 with this deliverable - connected with MS4, MS7 (this point in the project's lifetime) and with MS8 - First Pilot Trials Complete (upgraded and integrated tool demonstrated and validated, first pilot trials successfully completed). The demonstration and further validation results will be reported in D6.4.

The architecture of the CPR tool did not change throughout its evolution – it follows the one set in D6.2[2]. We provide a summary of the component's descriptions, to keep the good understanding of the deliverable.

The initial testing results with the CI provided data logs strongly suggest that we can identify relevant events for cyber-physical resilience in different layers of cyber infrastructure. An example is a problem (bug) in the upper layer (application layer). The anomalies in the infrastructure may be a result of tampering with the application, the virtual resources' infrastructure, even the network issues. Each anomaly may not be directly connected with the cyberattacks. However, their existence or combination with other indicators, may show that a threat is imminent. This is an innovative approach, where not just focusing on demonstrably security-related incidents, but also on observation of a wider threat landscape that includes anomalies or indicators of compromise (IoC), we may detect more subtle attacks. In this sense, improvements such as threat intelligence scoring or mapping of Indicators of Compromise (IoC) with MITRE ATT&CK matrix techniques, is another important advance that gives better situational awareness to CI cybersecurity operators. Both detected anomalies and information received from cyber threat intelligence tool, are treated as risk indicators, next to the already existing indicators whether organisational, technical, physical or workforce related. New input to automated risk (re)assessment also includes temporary conditions related to pandemics, such as changes of priority in impact assessment, availability and awareness level of workforce, etc. The results of risk assessments, in its turn, are used to help in orientation and making decisions, including decisions related to incident reporting. In this way, we follow the OODA loop approach (Observe, Orient, Decide, Act) that has a focus on contextualization of the available information, while also making sense of newly arrived data and changing circumstances. It is particularly suitable approach for volatile, uncertain, complex, and often ambiguous inflow of data, such as the case of cybersecurity decision making systems during temporary conditions such as pandemics.

For each module, we describe its deployment in the infrastructure, which serves as guidance towards the installation of the whole CPR tool on the target (CI) infrastructure. We also provide a user manual, to describe the configuration and management of the components and the CPR tool itself.

Special consideration is given to the AIRE component – The Incident Reporting Module. Due to the changes in legal requirements (NIS 2 Directive [7]), we enhanced this module compared to its description in deliverable D6.2[2] with the additional communication capabilities.

The main contributions of this deliverable are therefore related to validation on the real, data logs provided by the CI operators, improvement of the CPR tool components, and finally, the updated user manual. The piloting activities and their results will be reported in deliverable D6.4, while the updated CPR tool (based on the results of piloting) will be reported in D6.5.

1 Introduction

1.1 Purpose of the document

The purpose of D6.3 is to publicly present the cyber-physical resilience (CPR) tool, initially presented in D6.1 - *Cyber-physical resilience conceptualization* [1] and improved in D6.2 - *Cyber-physical resilience tool and training guide V1* [2]. The deliverable presents the tool's architecture and deployment process. The outcomes of the tests conducted on the submodules in a lab environment on public datasets were presented in detail in D6.2[2]. We summarize the D6.2[2] to achieve completeness of the document and present new results that rely on testing with the sample log files provided by CI operator partners. In the annex, we present a user guide as envisaged at this stage. The final iteration of the user guide will follow the first piloting phase and will be reported in D6.5.

This section provides the necessary contextual information, like relation to other project work, organization of the whole document, the intended use of the tool at the CI premises, what are the differences between previous (D6.2[2]) and this (D6.3) deliverable, etc.

1.2 Relation to other project work

This deliverable reports the results of ongoing tasks of WP6: *T6.1 Cyber-physical security risk assessment, T6.2 AI-powered log monitoring,* and *T6.3 Incident response and threat intelligence sharing*. It provides results of validation with the real data from the SUNRISE partners, albeit conducted without installing the CPR tool at the CI's premises. These activities will follow in M21 and M22 of the project, providing validation of the tool in the operational environment. Following the tasks in WP6, the D6.3 reports also on T6.4 and T6.5 – integration and demonstration, throughout deployment of the tool and the usage guidelines of the CPR tool modules presented in D6.1[1] and D6.2[2]: anomaly detection (LOMOS), threat intelligence (TINTED), risk assessment (CERCA), and incident reporting (AIRE).

However, we address other WPs, providing them with a way to observe, report and protect in the physical realm. An example is WP7, where physical security of the drone is monitored, providing a way to monitor any possible tampering with the potentially dangerous equipment.

The tool follows requirements from D3.2 – *Requirements and designs V2* [3]. Deliverable D6.3 is the second version of the *Cyber-physical resilience tool and training guide*; it follows the first version (D6.2[2]) and will be iterated in D6.5.

1.3 Structure of the document

This document is structured in 6 major chapters and annex.

Chapter 1 (this chapter) presents the purpose and contextual information of this (D6.3) deliverable.

Chapter 2 presents the overview of the Cyber-Physical Resilience Tool. The focus is on the architecture and deployment of the four modules. The data, needed for swift understanding of the modules and, architecture, is summarized, alleviating the reader's task.

Chapter 3 presents the evaluation of log data provided by CI operator partners, to provide insight to CI operators how modules perform, and to show how they can complement their existing tools. Please note that this deliverable does not report the results of the piloting, but rather reports on the tests, conducted on the data, provided by CIs. The results of the piloting (the first iteration) will be reported in D6.4.

Chapter 4 is dedicated to describing possible issues regarding pilots due to legal restrictions related to CI and outlines the testing methodology, as these are tightly connected, with the possible legal issues which we expect to be relevant, when we start actual piloting and involve more of the CI technical personnel.

Chapter 5 presents four CI pilot trials related to public administration, water, telecommunication, and transport.

Chapter 6 outlines the main findings of this WP so far, and provides conclusions - the body of work produced, and which will be used to validate our approach and developments.

To summarise, the main focus is on the first tests of tool with the CI-provided data, to show the CI the capabilities of the CPR tool and to get the acceptance, which is sorely needed for testing in piloting phase.

Annex offers a user manual for the modules presented in previous chapters. The manual is in the step-by-step descriptive format with screenshots from demo deployments.

1.4 Differences to the deliverable D6.2[2]

The differences between section of D6.2[2] and his successor D6.3 (this document) are shown in Table 1. With bold, we mark new sections and major updates. Besides this presentation of differences, se also summarize the advancements in the work, as bullet list below the table.

Table 1: D6.3 - changes in Sections compared with D6.2[2]

Section in D6.3		Section in D6.2[2]		Difference
Executive Summary		Executive Summary		Updated
1	Introduction	1	Introduction	Updated
1.1	Purpose of the document	1.1	Purpose of the document	Unchanged
1.2	Relation to other project work	1.2	Relation to other project work	Updated
1.3	Structure of the document	1.3	Structure of the document	Unchanged
1.4	Differences to the deliverable D6.2[2]			**New subsection**
1.5	Personas used in the document			**New subsection**
2	Cyber-Physical Resilience Tool	2	Cyber-Physical Resilience Tool	Unchanged
2.1	General Context	2.1	General Context	Unchanged
2.2	Architecture	2.2	Architecture	Unchanged
2.3	Operational Prerequisites			**New subsection**
2.4	Deployment	2.3	Deployment	Updated
3	Cyber-Physical Resilience Tool Tested in Labs	3	Cyber-Physical Resilience Tool Methods Tested in Labs	Updated
3.1	Monitoring System (LOMOS)	3.1	Monitoring System (LOMOS)	**Major Change**
3.2	Threat Intelligence (TINTED)	3.2	Threat Intelligence (TINTED)	Updated
3.3	Risk Assessment (CERCA)	3.3	Risk Assessment (CERCA)	Updated
3.4	Incident Reporting (AIRE)	3.4	Incident Reporting (AIRE)	**Major Change**

Section in D6.3		Section in D6.2[2]		Difference
4	Legal Compliance and Testing Methodology	4	Management and What-If Analysis	**Major Change**
5	Pilot trials execution	5	Pilot trials execution (feasibility analysis)	**Major Change**
5.1	Pilot Execution Plans	5.1	Proofs of concepts	**Major Change**
5.2	Description of End-Users' Roles			**New subsection**
6	Conclusions	6	Conclusions	Updated
7	References	7	References	Updated
Annex I	Training guide and user manual	Annex I	Training guide and user manual	Updated
I.I	Anomaly Detection	I.I	Anomaly Detection	**Major Change**
I.II	Threat Intelligence	I.II	Threat Intelligence	**Major Change**
I.III	Risk Assessment	I.III	Risk Assessment	Updated
I.IV	Incident Reporting	I.IV	Incident Reporting	**Major Change**

Summarisation of the advancements in the work, achieved from delivery of D6.2[2] up to D6.3 is given in the list below:

- Anomaly detection tool was extended with lomos-cli tool for easier repeated training.
- Anomaly detection tool was extended with lomos-api2 service to retrieve more easily detected anomalies in programmatic way.
- Anomaly detection tool has certain requirements regarding input log content. Those requirements are now more explicitly listed.
- A preliminary test of Anomaly detection tool on data provided is presented.
- Threat intelligence scoring module was extended with source confidence evaluation for better management of intelligence sources.
- Threat intelligence tool also includes mapping of IoCs with MITRE ATT&CK matrix techniques and contextual health events following Google Trends results.
- Risk assessment allows new input to include temporary conditions.
- Risk assessment digests alarms from physical activity monitoring triggered by WP7 Computer Vision Tool and threat score from threat intelligence module.
- A comprehensive and detailed evaluation of NIS 2 Directive and its impact in the incident reporting module.

Besides the technical changes, we introduce Personas – the CI personnel's profile, as provided by CIs, who will use the CPR tool. This is to address the possible confusion of who the end-user is, its profile and what is needed for the end-user to understand and operate the tool.

Personas are modelled after our description and presentations of the tool to the CIs, which means, they might slightly change after the piloting in the first year.

The CIs reported the roles, profiles, and skills based on their internal organization.

1.5 Personas used in the document

In terms of the WP6 tool Cyber-physical resilience (CPR), the term “end-user” refers strictly to the final operators of the tool, which belong to operators/personnel of the different Critical Infrastructures (CI).

The tool will be demonstrated and potentially used at the following CIs:

- Health (Italy): Health digital services INS-FVG.
- Water (Italy): Water providers CAF.
- Public Sector (Italy): Local Administrations in the Friuli Venezia Giulia region INS-FVG.
- Telecommunications (Slovenia): Telecom company TS
- Transport (Slovenia): Transport operator SZ-PIL

We provide the end-user manual in Annex and intend to provide additional training where needed.

Target audience for this document includes end-users for tools developed in WP6. In the context of WP6 definition of end-users refers to different teams inside organisations TS, ELS, FVG, CAF and SZ (5 CIs). More specifically, under WP6, these CIs have similarities, but also differences in the ways they manage cybersecurity and give name to roles in the IT department. In addition, the CPR is a complex tool divided in several submodules (LOMOS, CERCA, TINTED, AIRE) that each comes with its own specificities and end user types. More details about user roles and profiles are given in the Section 5.2 in the table that summarizes our best effort to define the “end-user” roles in WP6.

2 Cyber-Physical Resilience Tool

2.1 General Context

The CPR tool contains four modules, which are introduced in the sections below. The modules are:

- The Anomaly detection module (LOMOS) utilizes machine learning for log-based anomaly detection.
- The Threat intelligence module (TINTED) is used for sharing the threat intelligence information with external stakeholders, including pandemics/health related threat intelligence, scoring of threats and their sources, and mapping of low-level technical information, such as indicators of compromise (IoC), to higher level techniques, tactics and procedures (TTP).
- Risk assessment module (CERCA) ingests different types of inputs (real time feeds from existing cybersecurity tools such as anomalies or incidents, events related to physical threats, changes in temporary conditions, threat intelligence, organisational and workforce related information etc) and is automatically (re)assessing risks, based on pre-defined risk models.
- The Incident reporting module (AIRE) is responsible for automating the reporting process to the relevant authorities in the event of a security incident.

The modules are designed to allow integration of legacy systems that are currently used by CI.

2.2 Architecture

The CPR tool is designed to enhance the resilience of CI during pandemics by considering both technical and human aspects. It comprises four modules: Detection, Threat Intelligence, Risk Assessment, and Incident Reporting. The tool's architecture and data flow are illustrated in Figure 1.

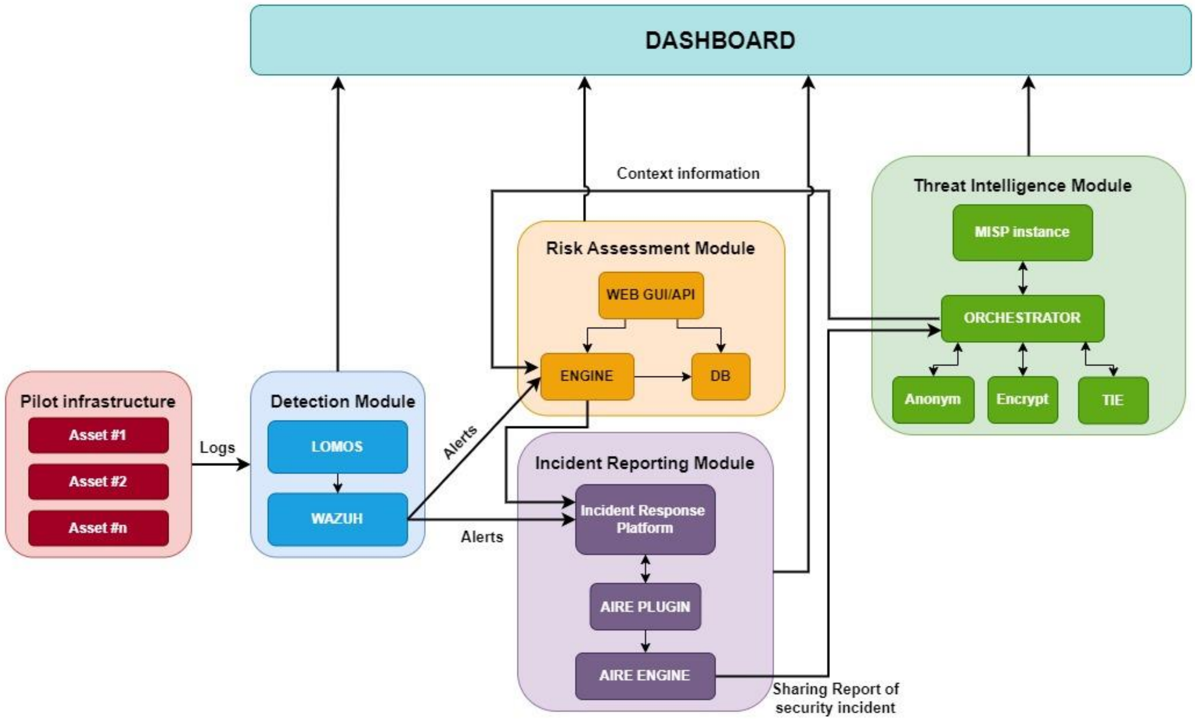


Figure 1. Overall architecture of the CPR tool.

The Detection module oversees CI assets and generates security events and low-level alerts. It comprises the two main components: an anomaly detector named LOMOS, which uses application logs and raw data to train an AI in recognizing normal system behaviour and triggering alerts for deviations, and a SIEM called Wazuh[1], which identifies event sequences related to known threats and raises alarms correlating LOMOS' output. These alerts and events are sent to the Risk Assessment and Incident Reporting Modules.

The Risk Assessment Module evaluates incoming input to assess the risk associated with the system's assets. The outcome is a risk report that quantifies cyber risk exposure in monetary terms. This report includes the likelihood of the security incidents based on many inputs, including real-time cyber environment data, and an estimation of monetary impact related to the incident and based on the currently estimated values of the digital assets, that might change during pandemics in so called "temporary conditions". It is also sent to the Incident Reporting Module, which evaluates events and alarms from the SIEM to determine security incident presence and severity for potential reporting to authorities. This module also ensures the orderly completion of reporting steps.

The Threat Intelligence Module has two primary roles: secure sharing of Cyber Threat Intelligence (CTI) information and enhancing external threat intelligence data, in order to improve estimations of incident likelihood. It employs a common MISP[2] instance to share relevant attack and threat information. After a security incident and notifying authorities, CIs may choose to share this information with others. Input from the Incident Reporting Module is integrated, ensuring appropriate context in the information flow. Before sharing, data can be encrypted or anonymized. The module employs a threat score generated by the Threat Intelligence Engine (TIE) module, using heuristics on incoming external events to provide context-aware data to the Risk Assessment module.

The logic behind this architecture follows the need for adaptivity, collaboration and dealing with absenteeism, scenarios that have been also identified and described in WP2, as especially relevant for the temporary operational conditions such as those during pandemics.

During these periods, SUNRISE users observed the fast-changing cybersecurity landscape, systems, and behaviours, where the existing static practices were not enough anymore. Plan-do-check-act (PDCA) approach, for example, follows linear process, which has some drawbacks during these periods with very dynamic changes. Its strength is that it is simple, yet effective manner to plan, structure and implement risk controls through corrective and preventive actions. "Plan" and "Do" phases were identifying assets, models, impacts, assessing the risks, proposing mitigation etc., while "check" phase was assessing how well the risks have been controlled (usually by audits). This was separated from the operational cybersecurity management that was focused on real-time monitoring and detection of suspicious events. The main weakness is its static nature, inappropriate for steady reduce of "time to react", one of the most important metrics for cyber-physical resilience.

More recently, real time risk engines such as the one used in CERCA were introduced, leading to a possibility to trigger risk (re)assessments automatically, for example after detection of an incident or vulnerability, or when temporary conditions change.

The OODA loop (Observe, Orient, Decide, Act) is also a four-step approach to decision-making, but unlike PDCA, it focuses on contextualization of the available information, while also making sense of newly arrived data and changing circumstances. It is particularly suitable approach for volatile, uncertain, complex, and often ambiguous inflow of data, such as the case of pandemics. Here, rule-based detection, used in cybersecurity operational management tools, is combined with expert-based risk assessment, that prioritizes and optimizes mitigation actions and re-adjusts risk baselines.

This is why CPR tool architecture proposes to combine sensing ("observation") of external environment (anomalies from LOMOS, incidents from SIEM, threats from TINTED etc.), with a cognitive process of "orientation", to make an optimal decision. Observation works with outside- in sensory information, even if it uses rules for correlation of events, or signatures for detection of an intrusion. Orientation works with inside-out created cyber risk landscape, which includes changes in temporary conditions,

[1] https://wazuh.com

[2] https://www.misp-project.org

such as for example availability of cybersecurity workforce, or a higher priority and value for health-related digital assets.

Our approach and architecture work better with uncertainties, partial information, diversity or degree of randomness and disorder. While availability of incoming data in observation is compulsory, calculated values such as likelihood of an attack, based on this data, vary depending on the actual context, including confidence in the sources of threat intelligence, timeliness or relevance of incoming information etc. The same holds for the calculation of impact, which is better aligned with priorities and changes at strategic and tactical level (e.g. due to the interruption in supply chain or unavailability of workforce). As the result of “Action” phase in OODA loop, there will be a risk mitigation decision, and feedback loop goes towards the external observation environment through sharing of threat intelligence, that can also help to correct cognitive bias in relation to risks from other CI operators.

2.3 Operational Prerequisites

2.3.1 The content and format of logs for successful anomaly detection

It was clear from the very beginning that there are operational prerequisites regarding what logs LOMOS can process. Examples are included to further clarify the subject. This will help prevent a few potential problems that were identified during initial testing. It allows CI partners to check their logs are suitable for anomaly detection tool before actual deployment of the anomaly detection tool.

2.3.1.1 Logs must be human-readable

The LOMOS tool was designed to process human-readable logs. Counterpart to human-readable logs are more structured machine-readable logs. Machine-readable logs are more suitable for machine processing, and tools for this do exist. Thus, LOMOS focuses on human-readable logs only.

The human-readable logs represent the trove of information that is very frequently neglected, while on the other hand, represent the actual operation and the actual state, messages from the creators of the application. Creators of the application will often write a message (log line) if an unusual situation is detected.

To illustrate what is each log type, two examples are shown below.

Human-readable:

```
2024-03-04T09:58:49.796963Z 0 [Note] Found ca.pem, server-cert.pem and server-key.pem in data directory.
Trying to enable SSL support using them.

2024-03-04T09:58:49.797517Z 0 [Note] Skipping generation of SSL certificates as certificate files are present in
data directory.
```

Machine-readable:

```
{ "timestamp": "2024-03-07T11:07:27+00:00", "remote_addr": "172.18.0.10", "body_bytes_sent": 5,
"request_time": 0.000, "response_status": 200, "request": "POST /broker_auth/api/v2/auth/rabbitmq/topic/
HTTP/1.1", "request_method": "POST", "host": "rproxy","upstream_cache_status": "HIT","upstream_addr": "-
","http_x_forwarded_for": "-","http_referrer": "-", "http_user_agent": "-" }
```

The human-readable logs are generated by an application when the programmer decided there is something interesting to show, as this detail might help later. Typically, the main part of the content is text in natural language.

This is different to structured logs. The example above is from a JSON file; other common formats are CSV or TSV files. The amount of natural language is small. In the example above, there is no natural language in JSON values (only JSON keys are in natural language).

2.3.1.2 Logs should contain a timestamp with high resolution

LOMOS searches for anomalies by looking at N sequential log lines. This requires preservation of time order in which log lines were generated.

The used database can sort log lines using timestamp, which requires timestamp to be present. If two log lines have identical timestamp, then we cannot tell which line was first. This problem usually happens if a timestamp with small resolution (like 1 second or 1 millisecond) is used - the application can easily generate more than 1 log line in a single millisecond. The application logging should thus be configured with high-resolution timestamp (microsecond or nanosecond).

A possible workaround is to artificially extend timestamp if the application cannot be easily reconfigured with high-resolution timestamp. We usually do this only if logs were exported to file, where order in file is the same as order in time. In this case, three messages with timestamp “20240102T11:22:33” will be stored as “20240102T11:22:33.000000”, “20240102T11:22:33.000001” and “20240102T11:22:33.000002”. This is difficult to use with log shipping applications (FileBeat sending logs to ElasticSearch, or OpenTelemetryCollector agent). Therefore it has limited use and will likely not work with automated real-time log shipping.

2.3.2 Anomaly Detection

LOMOS is a self-supervised machine-learning system for log-based anomaly detection, comprising a log parser, anomaly detector trainer, and anomaly detector. It extracts log events using Drain, trains models with LogBERT, and assigns anomaly scores per log. The architecture includes components for log storage, parsing, anomaly detection, and visualization. New components like lomos-cli and lomos-api2 facilitate training and inference tasks, see Figure 2. The system utilizes Celery for job distribution, MLflow for experiment tracking, and Grafana for dashboard development. lomos-api2 offers anomaly detection without direct database access. lomos-cli aids in frequent training with stored parameters for repeatability. For a more in-depth look into LOMOS, please refer to D6.2[2].

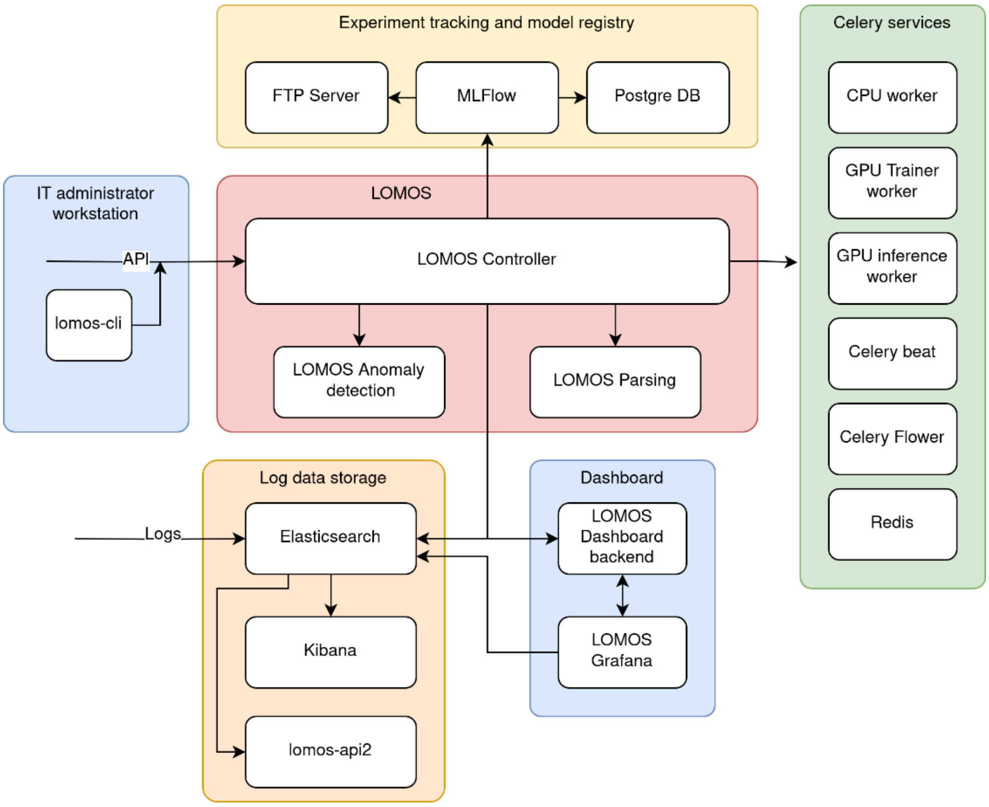


Figure 2. LOMOS architecture.

Service lomos-api2 was developed to provide a list of detected anomalies in a given time window. It is implemented as a REST API. It isolates the consuming application from the LOMOS internal working. The consuming application also does not need direct access to LOMOS internal database to find anomalies.

During experimental LOMOS training we need to frequently retry experiments, which involves tasks of log parsing, model training and inference. The provided GUI dashboard is primary a tool for all three tasks. But the CI operator’s IT administrator needs to input many parameters, and this makes usage difficult, inefficient and prone to human error.

For frequent LOMOS training, an additional CLI tool named lomos-cli was developed. The needed parameters are stored in JSON files and can be committed to source versioning system (git). This allows experiment repeatability. The needed credentials to access LOMOS deployment need to be provided separately. The tool can load credentials from repository used to deploy LOMOS (env/.env and env/.secrets files).

2.3.3 Threat Intelligence

TINTED, the threat intelligence module, facilitates secure CTI exchange and enhances cyber risk calculation. Its layers include authentication, transport, and privacy/enrichment as shown in Figure 3. **MISP Instance** serves as the transport layer, ensuring secure CTI exchange with granular sharing controls. **Keycloak** ensures secure user authentication and authorization. **MongoDB** handles data storage, storing configuration, user, and infrastructure information. The **Orchestrator** facilitates communication among modules and provides an API for user interaction. The **WEB-GUI** simplifies tool usage and integrates authentication mechanisms. Privacy modules include **Encryption** and **Anonymization**. The Threat Intelligence Engine (TIE) consists of ZMQClient and HeuristicEngine, which calculate event scores based on heuristics. An in-depth look into TINTED is provided in D6.2[2].

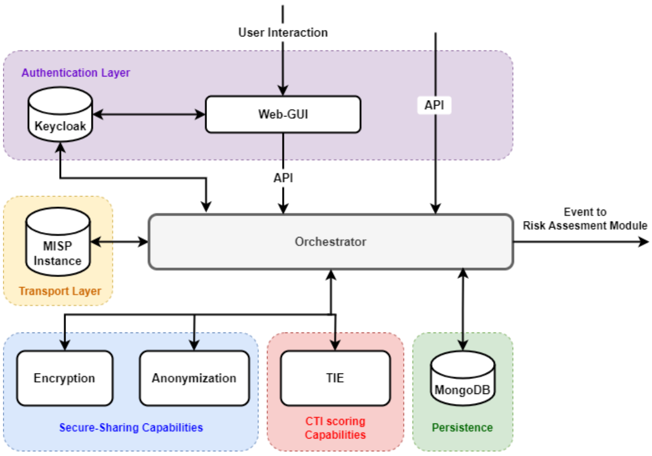


Figure 3. TINTED architecture.

2.3.4 Risk Assessment

The risk assessment module, CERCA, comprises several submodules that generate reports sent to the incident reporting module for evaluation, see Figure 4. The **WEB-GUI/API** facilitates tool configuration, while the **Indicator Value Generator** creates or modifies indicators based on user input and threat intelligence data. The **Triggering Detector** activates the **Risk Model Executors**, which execute algorithms to generate reports on risk per target. These reports are aggregated by the **Aggregator** and stored in **PostgreSQL**. Static information from questionnaires and target configurations, along with dynamic data like alarms, events, vulnerability reports, and indicators of compromise, feed into the assessment process. Outputs include a comprehensive Global Report, Reports per Target and Risk, Reports per Model, and Reports per Target, providing insights into the organization's threat landscape at various levels of granularity. An in-depth look into CERCA is provided in D6.2[2].

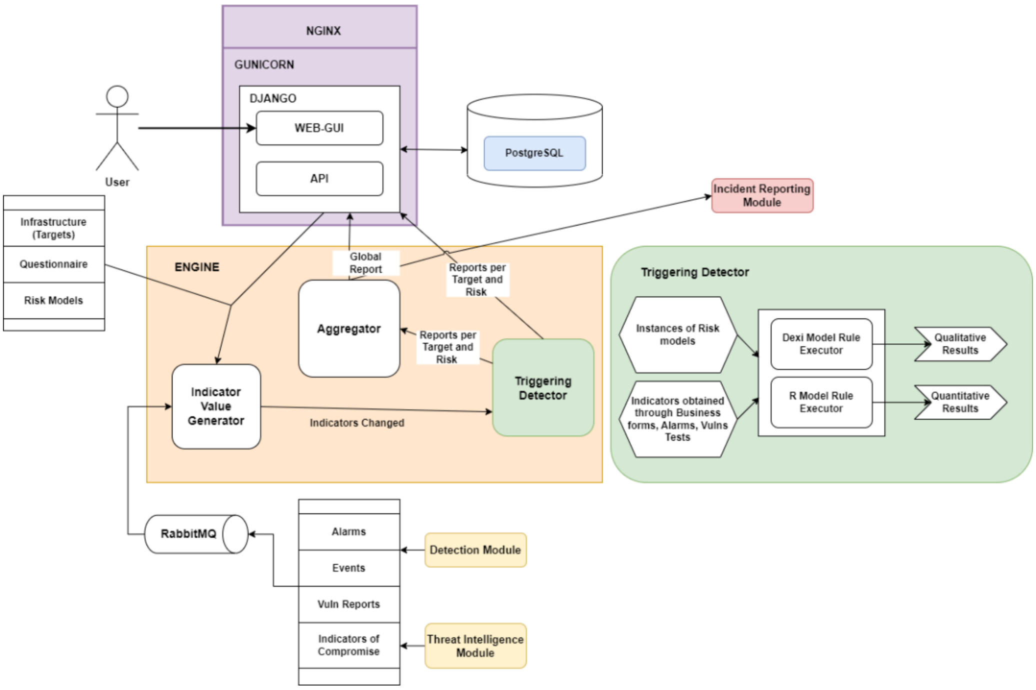


Figure 4. CERCA architecture.

2.3.5 Incident Reporting

AIRE, the incident reporting tool, features a modular design to adapt to diverse regulations. Its structure, see Figure 5, includes Springboot microservices **aire-reports-generators** and **aire-workflow-enforcement**, along with the **aire-thehive-plugin** for integration with TheHive.

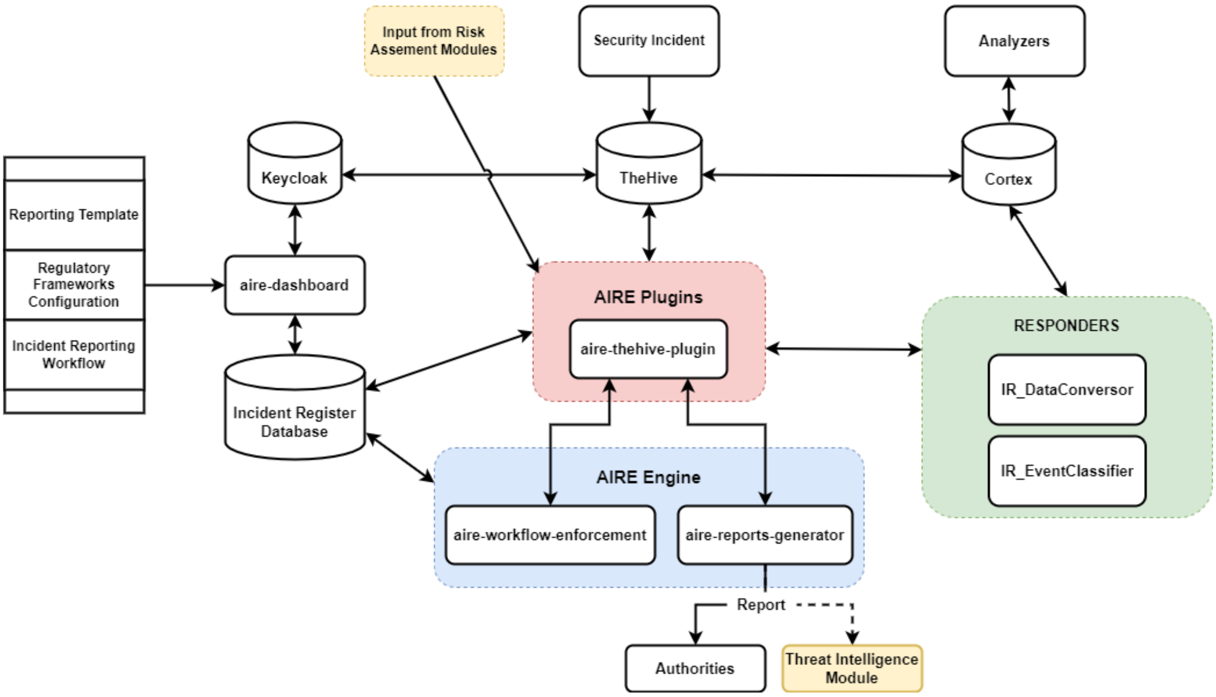


Figure 5. AIRE architecture.

The architecture includes an Incident Register Database and **aire-dashboard** for configuration. The **aire-workflow-enforcement** orchestrates incident reporting workflows following a BPMN framework, ensuring compliance and managerial oversight. The aire-reports-generator tailors incident data to different report templates mandated by Competent Authorities, utilizing Apache POI for Microsoft formats and Apache PDFBox for PDFs.

2.3.6 Dashboard

The CPR tool consolidates modules into a central dashboard for Critical Infrastructure monitoring. It features sections for risk assessment (CERCA), anomaly detection (LOMOS), SIEM data (Wazuh), threat intelligence (TINTED), and regulatory reporting (AIRE). Each section offers real-time charts and tables summarizing CI metrics, with options for detailed views and configuration. The CERCA section prioritizes risk scores for monitored assets, while LOMOS showcases anomaly events. SIEM data displays alarms per asset, and TINTED presents event types. AIRE tracks ongoing reports and tasks for regulatory reporting. The dashboard provides a comprehensive overview of CI performance, enhancing decision-making and operational efficiency.

2.4 Deployment

2.4.1 Pre-requisites

All the modules are containerized using Docker. Consequently, the deployment environment must have Docker (version 20.10.14 or newer) to facilitate component deployment.

Testing of the application has been conducted on Ubuntu 22.04 LTS, Ubuntu 20.04 LTS and Ubuntu 18.04 LTS operating systems.

2.4.2 Anomaly Detection Module

The source code, the built docker images and the docker compose based deployment scripts for LOMOS are stored in the XLB internal GitLab repository. For the piloting, planned at M21 and M22 of the project, a copy of the deployment scripts and the access token for built docker images are required. This means the piloting (i.e., installation of the module at the CI's premises, on their infrastructure) is very straightforward and does not require any significant changes of the code or significant installation procedures. Optionally XLB can also store a copy of built docker images to CI operator controlled docker image registry.

2.4.2.1 Hardware requirements

LOMOS requires a GPU for training the neural network (transformer) model used for anomaly detection. GPUs are not mandatory for inference; however, they significantly improve the throughput. The hardware requirements depend on the mode:

Training mode:

- 8 core CPU.
- 64 GB RAM.
- 1x GPU (11 GB+ VRAM).

Inference mode:

- 8 core CPU.
- 32 GB RAM.

There should be enough disk space to store at least three copies of log data, to enable normal system operation.

2.4.2.2 Installation procedure

The system has two configuration files, one for secrets, and another one for the rest of the parameters. The secrets are located in a separate file to enable sharing and storing non-sensitive configuration parameters in a repository. Example of the non-sensitive parameters configuration file:

```
# Configuration
SERVER_IP=10.44.18.214
# Docker
DOCKER_RESTART=unless-stopped
DOCKER_LOGGING_MAX_SIZE=5g
DOCKER_LOGGING_MAX_FILE=4
# Celery
CELERY_BROKER_URL=redis://${SERVER_IP}:6379
CELERY_RESULT_BACKEND=redis://${SERVER_IP}:6379
CELERY_REDIS_SCHEDULER_URL=redis://${SERVER_IP}:6379
REDBEAT_REDIS_URL=redis://${SERVER_IP}:6379
FLOWER_PORT=5555
# Flask
LOMOS_CONTROLLER_URL=http://flask:25000
# Grafana
GRAFANA_URL=https://${GRAFANA_USER}:${GRAFANA_PASS} @${SERVER_IP}/grafana
GRAFANA_URL_NO_CREDENTIALS=https://${SERVER_IP}/grafana
GRAFANA_BACKEND_URL=https://${SERVER_IP}/grafana-backend
GRAFANA_BACKEND_API_PORT=25001
# FTP
FTP_PUBLIC_HOST=${SERVER_IP}
FTP_20=20
FTP_21=21
# MLflow
MLFLOW_PORT=5000
MLFLOW_TRACKING_URI=http://${SERVER_IP}:${MLFLOW_PORT}
# LOMOS
INFERENCE_DEVICE=cpu
LOMOS_PARSING_VERSION=
LOMOS_ANOMALY_DETECTION_VERSION=
LOMOS_ELASTIC_VERSION=
# Nginx
HTTP_PORT=80
HTTPS_PORT=443
```

```
API_PORT=25000

# Elasticsearch

ELASTICSEARCH_PORT=9200

ELASTICSEARCH_URL=http://${SERVER_IP}:${ELASTICSEARCH_PORT}

KIBANA_PORT=5601

KIBANA_URL=http://${SERVER_IP}:${KIBANA_PORT}
```

To deploy the system, execute the *deploy.sh* bash script. The script sets up the environment and starts the system with “docker compose”. The components are grouped into three groups. The first one is actual LOMOS – the controller, workers, celery services, and dashboard. The second one is model registry – Mlflow with FTP server and Postgre database. The third group consists of Elasticsearch and Kibana. The script can start a new Elasticsearch and model registry deployment, or hook to an existing one.

2.4.3 Threat Intelligence Module

2.4.3.1 Hardware requirements

The suggested hardware requirements are as follows:

- CPUs: 4 or more.
- RAM: 6GB or more.
- Disk space: 64GB or more.

2.4.3.2 Installation procedure

The configuration details for the tool are found within the .env file. It is crucial to verify the accuracy of this information before deploying the tool.

In the overarching configuration segment, the DEBUGGING_FLAG and TUNNELING_FLAG indicators must both be set to 0. These flags determine whether the tool is being deployed on a production server. The subsequent part focuses on the individual configurations of specific tool modules. This involves defining container names and the associated ports they utilize. The TIE configuration segment is particularly noteworthy, as it holds environment variables essential for proper tool functioning:

- MISP_URL: This refers to the URL of the MISP instance, particularly relevant if the MISP instance is located outside the docker deployment.
- MISP_SERVICE_NAME: In cases where the MISP instance is part of the same docker deployment, this variable designates the service name of the MISP instance container.
- MISP_API_KEY: This API key is indispensable for interactions with the MISP instance.
- ZMQ_CONTAINER_NAME: The zmq_client module connects to the ZMQ Server, which is situated within the MISP instance. Thus, this variable contains the name of the MISP Instance container.
- ZMQ_CONTAINER_PORT: This variable stores the port at which the zmq server is active, enabling the zmq_client to subscribe to the queue.

For the configuration of Keycloak, the appropriate adjustments should be made within the *docker/app/controller/keycloak_controller.py* file.

Ultimately, deploying the tool is straightforward and accomplished with a single command:

```
docker compose --env-file .env up -d –build
```

2.4.4 Risk Assessment Module

2.4.4.1 Hardware requirements

The suggested hardware requirements are as follows:

- CPUs: 2 or more.
- RAM: 16 GB or more.
- Disk space: 30 GB or more.

2.4.4.2 Installation procedure

To appropriately set up and deploy the Risk Assessment module, the following applications must be installed [8]:

- The Risk Assessment Engine, which serves as the central element of the tool. It's responsible for executing rules and performing risk assessments. This component is developed as a Python application with multi-threading capabilities.
- The Graphical Interface, which functions as the visualization part of the tool. It's created using the Django framework for Python. This interface offers a control dashboard to exhibit input and output data concerning the security of the target infrastructure.
- The Database, serving as the storage element of the tool. It's built using SQL and contains data related to risk models, indicators, data processing activities, mitigation measures, and all security-related information about the infrastructure and its components.
- The Message broker, responsible for facilitating communication among various components using a RabbitMQ server.
- Nginx load balancer

A Docker container is created for each application: Dashboard (Django), Engine (Python), message broker (RabbitMQ), load balancer (Nginx), and the database server (PostgreSQL). These containers are initiated with specific port bindings on the host system, enabling access to internal application components (such as the web application or the broker) from the external network.

Immediately after launching the Dashboard web application, a script is run to populate use case data. This data is sourced from JSON files located within the directory "*rae_dashboard/rae_dashboard/dashboard/db_test_data/*". This script, in turn, utilizes an internal Python function called "*load_initial_data()*" to parse and load the existing JSON files into the database tables. The local SQLite3 database is stored in the file "*rae_dashboard/db.sqlite3*", and this file is fully compatible with SQLite tools.

In essence, each of the four application directories encompasses source code, configuration files, and a Docker file. This Docker file defines the base image, dependencies, source deployment, and a startup script (commonly referred to as an entry point) for the respective application.

Before creating the Docker containers, the Python script "*parser_configurator.py*" (located in the root of the sources) needs to be executed. This script copies specific configuration files, environment files containing necessary variables, and cryptographic certificates utilized by the applications for secure communication. This preparation is essential for subsequent dockerization:

```
sudo python3 parser_configurator.py
```

To simplify the creation and execution of the Docker containers, a configuration file named "docker-compose.yml" is included in the root directory of the code. This file facilitates building the containers, launching them, or stopping the services:

```
sudo docker-compose up --build --detach --force-recreate

sudo docker-compose down # to stop the running containers
```

Additionally, the accompanying script "*manage_docker_compose.sh*" can achieve the same outcomes:

```
chmod 755 manage_docker_compose.sh
sudo ./manage_docker_compose.sh up build
sudo ./manage_docker_compose.sh down
```

Creating container images from scratch might take some time due to dependency installation. However, these images will be cached at the layer level, leading to quicker recreation of containers in the future. Furthermore, cached images can be exported or uploaded to third-party repositories, like a Docker registry. To obtain a list of currently cached images:

```
sudo docker images
```

Alternatively, a config file named "*docker-compose-images.yml*" has been provided. This script relies solely on existing system images and constructs and launches containers using those images, requiring no source files:

```
sudo docker-compose -f docker-compose-images.yml up --detach
```

2.4.5 Incident Reporting Module

AIRE component requires a user account with sudo privileges.

2.4.5.1 Aire-reports-generator service

To deploy the module, we need to follow these steps:

Run the following commands in the directory containing the *docker-compose.yml* file to construct and deploy the Docker image:

```
sudo docker-compose build && docker-compose up -d
```

Below is the content of the *docker-compose.yml* file:

```
services:
  dashboard:
    build:
      context: ../dashboard/aire_dashboard
      dockerfile: ./Dockerfile
      args:
        DOCKER_DJANGO_DEBUG: "False"
    command: gunicorn config.wsgi:application -c ./config/gunicorn_configuration.py
    volumes:
      - ../cs4e-media:/usr/src/app/aire_dashboard/media
    expose: # exposed internally to other Docker services
      - 5602
    env_file: ../dashboard/aire_dashboard/.envs/.env
    container_name: aire_dashboard
    restart: unless-stopped
    depends_on:
      - db
    networks:
      - "aire-net"
  db:
    image: postgres:12.4-alpine
    #image: postgres:11.2-alpine
    volumes:
      - postgres_data:/var/lib/postgresql/data/
    env_file: ../dashboard/aire_dashboard/.envs/.env
    container_name: aire_database
    restart: unless-stopped
  ports:
   - 5432:5432
  networks:
   - "aire-net"
aire-reports-generator:
  build:
   context: ./aire-reports-generator
   dockerfile: ./Dockerfile
  #image: aire-reports-generator:0.1
  #ports:
  #  - 8083:8083
  expose: # exposed internally to other Docker services
   - 8083
  volumes:
   - ../cs4e-media/templates:/opt/aire/config/templates
   - ../cs4e-media/reports:/opt/aire/reports
  container_name: aire-reports-generator
  restart: unless-stopped
  depends_on:
   - db
   - dashboard
  networks:
   - "aire-net"
volumes:
 postgres_data:
 static_volume:
networks:
 aire-net:
   external: true
```

For log verification (with the default file location at */opt/aire/log/aire-reports-generator.log*) employ the command:

```
sudo docker logs -f aire-reports-generator
```

For altering the configuration file, establish a connection with the container:

Execute:

```
sudo docker exec -u 0 -it aire-reports-generator bash
```

Subsequently, modify the file located at */opt/aire/config/application.properties*. Upon completion, restart the container:

Use:

```
sudo docker restart aire-reports-generator
```

2.4.5.2 Aire-thehive-plugin service

Execute the following commands from the folder where the *docker-compose.yml* file is to build and deploy the docker image:

```
sudo docker-compose build && docker-compose up -d
```

This is the *docker-compose.yml* file:

```
version: "3.3"

 # every container should be in the same network
 services:
  dashboard:
    build:
      context: ../dashboard/aire_dashboard
      dockerfile: ./Dockerfile
      args:
        DOCKER_DJANGO_DEBUG: "False"
     command: gunicorn config.wsgi:application -c ./config/gunicorn_configuration.py
    volumes:
      - ../cs4e-media:/usr/src/app/aire_dashboard/media
    expose: # exposed internally to other Docker services
      - 5602
    env_file: ../dashboard/aire_dashboard/.envs/.env
    container_name: aire_dashboard
    restart: unless-stopped
    depends_on:
      - db
    networks:
      - "aire-net"
  db:
    image: postgres:12.4-alpine
    #image: postgres:11.2-alpine
    volumes:
      - postgres_data:/var/lib/postgresql/data/
    env_file: ../dashboard/aire_dashboard/.envs/.env
    container_name: aire_database
    restart: unless-stopped
    ports:
      - 5432:5432
    networks:
      - "aire-net"
aire-thehive-plugin:
    build:
      context: ./aire-thehive-plugin
      dockerfile: ./Dockerfile
    expose: # exposed internally to other Docker services
      - 8081
    container_name: aire-thehive-plugin
    restart: unless-stopped
    depends_on:
      - db
      - dashboard
    networks:
      - "aire-net"
volumes:
  postgres_data:
  static_volume:
networks:
  aire-net:
      external: true
```

To check the logs (by default file */opt/aire/log/aire-thehive-plugin.log*):

```
sudo docker logs -f aire-thehive-plugin
```

To change the configuration file, connect to the container:

```
sudo docker exec -u 0 -it aire-thehive-plugin bash
```

and edit file */opt/aire/thehive-plugin/config/application.properties*

3 Cyber-Physical Resilience Tool Tested in Labs

This section describes the validation of components, modules and ultimately, the whole CPR tool using the data provided by Cis and in lab conditions. The validation in operational environment will follow in M21 and M22 of the project.

The purpose of these experiments (validation using the CI-obtained data) was to provide better insight into how the tool behaves with real CI operator data, what anomalies could be detected in this data, and what problems could happen when using the tools later in operational environment.

The following subsections provide clear descriptions of the experiment's implementation, along with summary description of the tool's functionality, provided to improve the understanding of the reader. We emphasize that in-depth description of the tools is given in previous deliverables, e.g. D6.2[2].

3.1 Monitoring System (LOMOS)

We provide a short description of the experiments with LOMOS, along with a brief description of the methods used this component. For a more in-depth look into LOMOS component, please consult D6.2[2].

In D6.2[2] the performance of log-based anomaly detection methods was assessed. Evaluation was performed on two public datasets, namely BGL [9] and HDFS [10], labelled by the experts responsible for the system maintenance. One of the datasets contains logs from the BlueGene/L supercomputer, while the other contains logs from multiple hundred EC2 nodes in the Hadoop Distributed File System cluster. The datasets were captured from the actual systems running in production. They capture both, software, and hardware problems. As such, they more than adequately represent behaviour captured in logs in complex systems and can serve as an indication of the expected performance of the methods in our pilots. The datasets are well accepted in the log-based anomaly detection research community, as they are used as benchmark datasets in the field.

LOMOS primarily employs the **LogBERT** method [5] for log-based anomaly detection. LogBERT is a self-supervised approach that draws the main architecture and training ideas from BERT [6]. While BERT uses subword tokens, LogBERT employs log keys (log template IDs) as tokens. We **extended LogBERT** to be able to predict anomalies on a per-log basis.

The **per log LogBERT** performs a bit worse than the normal LogBERT in the sense of precision and therefore also the F1 score. The reason for this is a much harder task, to classify each single log message as normal or anomalous. LogBERT must classify if any of the log templates in a sequence of multiple (e.g., 100) logs are anomalous. However, by evaluating each log in the stream, it can detect more anomalies. For this reason, it has a higher recall than LogBERT. More details are available in D6.2[2].

3.1.1 Throughput

Classification performance is only one of the relevant metrics for log-based anomaly detection. Another important performance indicator is speed. This was evaluated on two different machines, one physical machine, called Turbo, with four CUDA-supported GPUs, and one virtual machine (VM) without GPU support. It should be noted that even VM without GPUs did still run GPU processing jobs on the physical machine with GPUs (i.e. hybrid deployment).

The first million logs from the BGL dataset were used. The log-based anomaly detection can be divided into training and inference modes. Training on Turbo using 4 GPUs took 1,310 s, and inference took 465 s if GPUs were used and 5,000 s if only CPUs were used. Running inference on VM using VM CPUs and disk as storage took 11,092 s. The main reasons for slow inference were use of less CPU cores, slower CPU cores and slower disk storage. This demonstrated that inference can be run on machine without GPUs. It also demonstrated that slowest option could process more than 7.5 million logs per day, while the fastest more than 185 million logs per day. More details are available in D6.2[2].

3.1.2 Evaluation on log data for CI partners

After testing on a public dataset to evaluate performance, additional testing was performed on dataset provided by CI partners. This was to provide insight into how the tool behaves with real CI operator data, what anomalies will be detected in this data, and what problems could happen when using the tools.

LOMOS was preliminarily tested on a dataset of 1M lines from Insiel SESAMO backend application. The dataset covered a period of 10 days, from 2024-01-22 to 2024-01-31. The dataset was anonymized and provided as a set of text files.

The timestamp had 1 second resolution and was extended to 1 microsecond during pre-processing. Pre-processing also fixed log lines that were split over multiple lines.

No anomalies were known in advance, and all log lines were initially treated as normal. We decided to split the dataset into two chunks:

- 2024-01-22 – 2024-01-30 is used for training

- 2024-01-30 – 2024-01-31 is not used for training

Inference is run over the whole dataset. Small number of anomalies should not adversely affect training, and such anomalies should still be detected during inference.

The results are displayed in Figure 6 below. Data from all 10 days are shown. The mean anomaly score has some peaks, but they are quite low, and a value of 0.04 just indicates something did happen. The mean anomaly score is an average value, so a single anomalous event gets hidden, as other normal events with near zero anomaly score lower mean anomaly score.

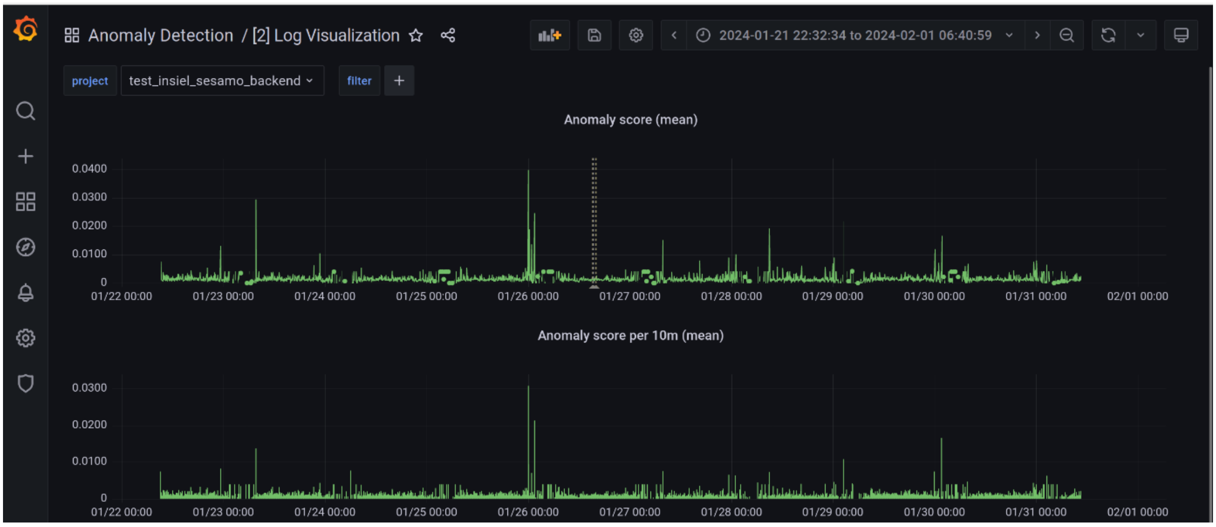


Figure 6. Overview of detected anomalies over all 10 days.

On next Figure 7 is shown maximum anomaly score graph. The timeline is zoomed in for easier visual inspection. The interesting events are now clearer to see.

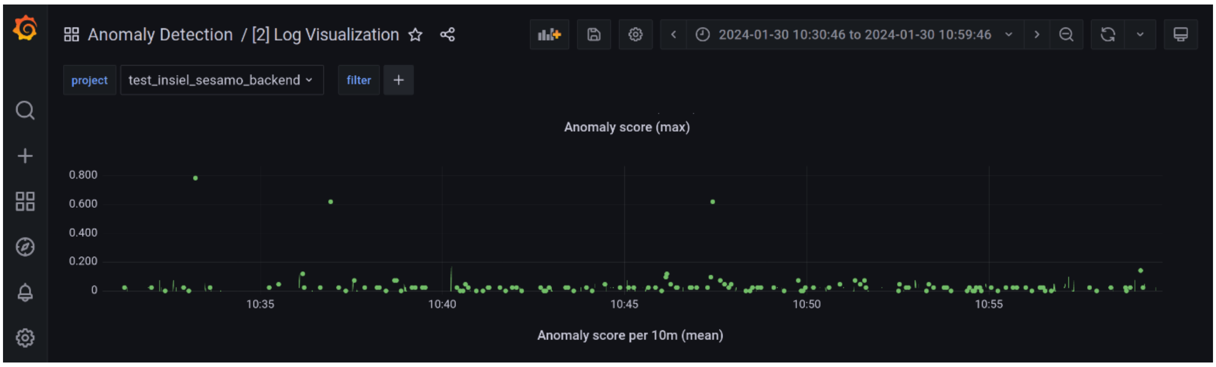
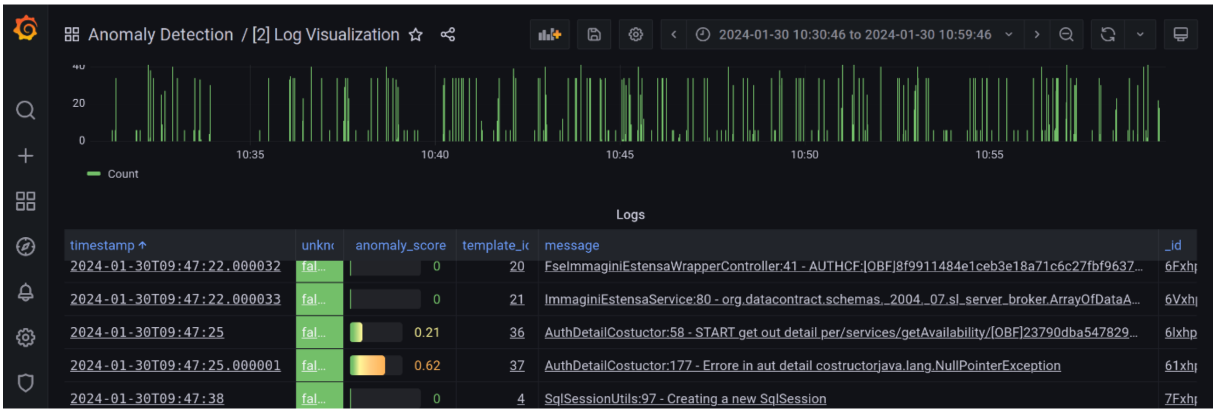

Anomaly Detection / [2] Log Visualization
2024-01-30 10:30:46 to 2024-01-30 10:59:46
project
test_insiel_sesamo_backend
filter
Anomaly score (max)
0.800
0.600
0.400
0.200
0
10:35
10:40
10:45
10:50
10:55
Anomaly score per 10m (mean)

Figure 7. Highest anomaly score in selected time window.

One relevant anomaly was detected, it was a java.lang.NullPointerException. The relevant log lines are shown in Figure 8 below. It looks like a bug in the application that triggers occasionally. Since this seems to be a bug, it is of interest, even if it is not a security related event per se since bugs in general can affect security of the application. A wider look to detect arbitrary anomalies and not just security incidents can also help to improve security.


Anomaly Detection / [2] Log Visualization
2024-01-30 10:30:46 to 2024-01-30 10:59:46
40
20
0
10:35
10:40
10:45
10:50
10:55
Count
Logs

timestamp ↑	unkn(	anomaly_score	template_ic	message	_id
2024-01-30T09:47:22.000032	fal...	0	20	FselmmaginiEstensaWrapperController:41 - AUTHCF:[OBF]8f9911484e1ceb3e18a71c6c27fbf9637...	6Fxh(
2024-01-30T09:47:22.000033	fal...	0	21	ImmaginiEstensaService:80 - org.datacontract.schemas._2004._07.sl_server_broker.ArrayOfDataA...	6Vxh(
2024-01-30T09:47:25	fal...	0.21	36	AuthDetailCostuctor:58 - START get out detail per/services/getAvailability/[OBF]23790dba547829...	6lxhp
2024-01-30T09:47:25.000001	fal...	0.62	37	AuthDetailCostuctor:177 - Errore in aut detail costructorjava.lang.NullPointerException	61xh(
2024-01-30T09:47:38	fal...	0	4	SqlSessionUtils:97 - Creating a new SqlSession	7Fxh(

Figure 8. Anomalous Null Pointer exception.

There are other anomalies detected. In this case, we need to know that any event that was not present in training data (for example application restart) will generate log lines that will likely be identified as an anomaly. This needs to be addressed to reduce false positives. The recommended approach is to include these events into the training data. The operator should first review logs to ensure they indeed do not contain anomalies, so that the data can be used as normal data for training.

3.2 Threat Intelligence (TINTED)

The threat intelligence module uses MISP underneath. This platform allows users to share and store security events that contain IoCs. The way MISP is envisioned, therefore TINTED, is to facilitate the information on threat intelligence data.

As expressed in D6.2[2] and following the requirements that were listed in D3.2, TINTED has been enhanced with different developments. Besides testing with some real threat intelligence data, in this section, an assessment of functional and business requirements will be done.

First, and considering the requirement FR.WP6.03, the size of the Docker containers that are deployed have been reduced by 40% as Python Slim version is now included. This reduces the amount of storage needed and facilitates the deployment of the threat intelligence module in machines with less resources.

Throughout the SUNRISE workshops and in insightful interviews with end users, the importance of collaboration and the establishment of circles of trust were recurrent themes. Participants stressed the critical role of collaboration not only in everyday operations but also in navigating the unique challenges posed by pandemics, as highlighted in the strategic scenarios outlined in deliverables D2.2 and D2.3. These documents provided overarching strategies for fortifying CI resilience during times of crisis.

In the specific context of CTI sharing, collaboration stands as a cornerstone principle. Effective collaboration is essential for timely and accurate threat detection, analysis, and response. Understanding the paramountcy of collaboration, we have developed a comprehensive set of mechanisms aimed at facilitating CTI sharing while ensuring the utmost security and privacy, covering the requirement NFR.WP6.02 (D3.2) and described in Annex I.III.I.

At the forefront of these mechanisms is the implementation of fine-grained data sharing policies. These policies allow organizations to delineate precisely which intelligence assets are shared and with whom, enabling granular control over the dissemination of sensitive information. By tailoring access permissions based on the need-to-know principle, organizations can strike a delicate balance between sharing intelligence and safeguarding confidentiality.

Moreover, we have incorporated advanced anonymization techniques into our CTI sharing framework. By anonymizing sensitive data, such as source identities and specific incident details, we safeguard the privacy of contributors while still enabling meaningful collaboration. This anonymization process ensures that participants can share critical intelligence without fear of compromising their confidentiality.

In tandem with anonymization, robust encryption protocols are employed to secure shared CTI data in transit and at rest. Encryption guarantees the confidentiality and integrity of shared intelligence, shielding it from unauthorized access or tampering. By leveraging state-of-the-art encryption technologies, we uphold the trustworthiness of shared CTI data, instilling confidence in collaborative efforts.

Through the seamless integration of these collaborative mechanisms, stakeholders can exchange CTI insights with confidence, bolstering collective defences against cyber threats. By fostering a culture of trust, transparency, and cooperation, we empower organizations to proactively address emerging threats and fortify the resilience of critical infrastructure ecosystems against evolving cyber risks.

One critical aspect where collaboration is indispensable is in the sharing of strategic CTI pertaining to threat actors and their methodologies. Following this principle, we have developed another feature that will empower SOC related activities, such as threat hunting, is the development of a mapping between IoC and techniques from MITRE ATT&CK framework. This functionality covers FR.WP6.10 and is described with more detailed in Annex I.II.III.

Strategic CTI encompasses insights into threat actors' motivations, objectives, and the tools and tactics they employ in cyber-attacks. Collaborative efforts to share this strategic intelligence among cybersecurity stakeholders are essential for developing a comprehensive understanding of the threat landscape.

By aggregating intelligence from various sources and sharing strategic information about threat actors, organizations can gain valuable insights into emerging trends and recurring patterns in cyber-attacks. This collective intelligence facilitates the identification of potential threats and enables proactive measures to mitigate risks before they materialize into full-fledged attacks.

Moreover, sharing strategic CTI empowers organizations to adopt a proactive defence posture. Armed with knowledge about threat actors and their methodologies, cybersecurity teams can pre-emptively implement security controls and countermeasures to thwart potential attacks. This proactive approach enhances the resilience of organizations against evolving cyber threats. This functionality not only enhances threat detection and mitigation but also strengthens the resilience of CI systems against evolving cyber threats, which leads to the idea of Pyramid of Pain, which is a concept used in cybersecurity to illustrate the relative difficulty for an attacker to overcome various defensive measures. It is often depicted as a pyramid with different layers, each representing a level of defence.

At the bottom of the pyramid are indicators of compromise (IOCs) such as IP addresses, domain names, and file hashes. These are relatively easy for attackers to change or evade once they are detected, making them less effective for defenders. Unfortunately, these are the most common pieces of information that threat intelligence feeds provides, that is why CI needs stronger mechanisms. Moving up the pyramid, we will find tactics, techniques, and procedures (TTPs) used by attackers. These include things like attack patterns, malware families, and specific methods used in cyber-attacks. TTPs are more valuable to defenders because they provide insight into the behaviour and motivations of attackers, allowing for more proactive defence measures. At the top of the pyramid are the attacker's infrastructure and tools. These are the hardest for attackers to change or replace, since they often require considerable time and resources to develop or acquire.

The idea behind the Pyramid of Pain is that defenders should focus on detecting and mitigating threats at higher levels of the pyramid, as these are more persistent and difficult for attackers to change. By targeting these higher-level indicators, defenders can disrupt attackers' operations more effectively and make their attacks less viable.

Currently, TINTED can map the techniques that the different malware samples have in a campaign from single IP addresses, domain names, URLs, and file hashes. This set of information is attached to the specific IoC in MISP, allowing security engineers to understand which threat actor is behind of an attack.

During pandemics, absenteeism in the workforce due to illness poses a significant challenge for critical infrastructure sectors, potentially disrupting essential services and operations. However, by leveraging external threat intelligence sources, the critical infrastructure entities can proactively manage employee absenteeism and ensure operational continuity during periods of heightened health risks.

Google Trends, for example, is one of the open intelligence sources that provides valuable insights into public interest and search behaviour, offering real-time data on topics related to illness, symptoms, and sick leave. By monitoring trends in search queries related to COVID-19 symptoms, sick leave policies, and healthcare resources, critical infrastructure organizations can anticipate potential surges in employee absenteeism linked to illness outbreaks.

By analysing social network or Google Trends data alongside other relevant indicators such as local infection rates and public health advisories, critical infrastructure operators can make informed decisions regarding workforce management strategies. For example, they can adjust staffing levels, implement remote work arrangements, or allocate resources to areas experiencing spikes in absenteeism due to illness.

Furthermore, proactive utilization of open intelligence data, next to pandemics relevant data shared by the CI operators, enables critical infrastructure entities to enhance their response capabilities, such as implementing targeted interventions to prevent further spread or improving assignments according to the risk level and the actual priority. By staying ahead of absenteeism trends through data-driven insights, critical infrastructure organizations can effectively manage employees on specific periods of time, mitigate operational disruptions, and improve the resilience of essential services during pandemics and other public health emergencies.

A new feature, described in Annex I.II.III, shows how the threat intelligence module can also monitor this kind of events and produce a new alarm to the system.

Finally, the module also provides evaluation of threat intelligence sources considering different criteria (FR.WP6.21) which allows CI operators to build a network with different “circles or levels of trust” and to manage the information given accordingly to the confidence in specific source. In the realm of CTI, adaptivity emerges as a crucial aspect addressed within WP2. This facet is approached through the introduction of two innovative functions: the calculation of trust scores and, notably, the aspect of timeliness, alongside the dynamic adjustment of score confidence, which are described in Annex I.II.III. A scenario contemplated within WP2 revolves around the fluidity of trust assessment, where external factors, such as the availability of qualified personnel during pandemics, can influence the reliability and relevance of information sources for trust scoring.

During temporary circumstances like pandemics, the availability of qualified staff may fluctuate, potentially impacting the credibility of certain sources within the CTI ecosystem. Consequently, some sources may be deemed less trustworthy or pertinent for trust scoring purposes. This fluctuation underscores the necessity for adaptivity within CTI frameworks, where systems must dynamically adjust their trust assessments based on evolving contextual factors.

The dynamic adjustment of score confidence allows CTI systems to recalibrate their trust scores in real-time, accounting for changes in source reliability and relevance. By incorporating this adaptive approach, CTI frameworks can maintain the integrity and efficacy of trust scoring mechanisms, even amidst fluctuating conditions. This adaptivity ensures that decision-makers can rely on timely and accurate threat intelligence insights, bolstering their ability to effectively mitigate cyber threats and safeguard critical assets.

3.3 Risk Assessment (CERCA)

The risk assessment module considers static and dynamic data to perform a global risk assessment with multiple levels of granularity. Dynamic data includes alarms from the SIEM and, as a novelty for SUNRISE, also includes "temporary conditions" or data considered on the "temporary conditions model", such as:

- Pandemic events: in the event of a pandemic, an asset, or an employee may become critical, thus needing to increase its value and/or risk exposure:
  - VPN server that must accept a sudden increase in connections due to a sudden increase in work from home (WFH) situations. SIEM application that needs to register more events as near 100% WFH is temporarily established.
  - Critical personnel that normally work in the office is displaced to WFH or must stay on site with a higher risk.
  - Equipment use variations, such as laptops, tablets, and phones.
  - An asset may become compromised or destroyed (backup asset), halting operations totally or partially, or an asset may become critical due to the entity conditions.
- Workforce temporary conditions: it considers aspects related to the psychological resilience of employees, and how the change in conditions affect them and thus affect the risk exposure of the entity:
  - Ability to perform their work.
  - Availability: absenteeism, lockdowns, travel restrictions.
  - Behavioural: motivation, compliance with policies.
  - Team's configurations: affected by health-related issues.
- Organization model attributes: parameters which are organization or business sector specific:
  - Asset model.
  - Working conditions adaptation (access control, lockdown).
  - Sector and Critical Infrastructure priorities.
  - Collaboration (authorities, law enforcement).
  - Variation in security policies.

The risk assessment input information to assess the temporary situations includes:

- SIEM (Wazuh) alarms based on the information coming from the different logs of the Insiel and CAFC use cases.
- Workforce questionnaire where the information for the four categories (ability, availability, behavioural, team's configuration) is considered.

Some of these situations may be sudden and non-predictable and need to be informed to CERCA without delay. A new view "Temporary Conditions" has been developed for the context of SUNRISE, where all this information such as probability (likelihood) associated to an attack going forward (under CORAS [12], the probability-likelihood is associated to the edges between nodes. A node is a phase or step of an attack, something the attacker achieves toward the attack's final objective, and an edge is a possible path the attacker may takes to move between nodes. An attacker moves from node A to B with a given probability-likelihood), workforce questionnaire temporary modifications, general global/regional conditions, digital asset temporary status/value/priority, etc, can be modified, and an additional risk assessment is performed to adjust the risk exposure to the new conditions, see Annex section I.III.

Other new functionalities added in the context of SUNRISE, affecting risk assessment, are:

- Threat context: TINTED provides enriched threat intelligence with a parameter, the TIE score (please refer to Section I.II.III), which is now used for risk assessment enrichment (if greater than a threshold). If the information at the threat intelligence event is related to the entity (same sector, region), type of asset (attack against routers, databases, etc.) or attack/technique, the TIE score and threat context information are given as a new input to CERCA risk models, with the main effect being the global risk exposure modulation based on this new information.
- Event and alarm persistence: CERCA now stores all events, alarms and inputs that lead to an incident and classifies them based on severity and/or time frame. This information is now included in the risk report sent to AIRE, also available via GUI and API. The analyst can perform detailed analysis and check the events and alarms that modified the risk exposure.
- Mitigations and countermeasures: CERCA now considers the application/execution of mitigations and countermeasures and how they affect the risk status. There are two new features based on this:
  - Mitigation/countermeasure simulation and effect on the residual risk, allowing cost/benefit analysis. An analyst can search for the best cost-effective set of mitigations, the cheapest set of mitigations that returns the risk to an acceptable level or the set of mitigations that reduces the risk to the lowest possible value.
  - First step for compliance with the NIS 2 [7] (Article 23, section 5) Directive (or any related legislation), which states that for a given attack, CSIRTs may send to the affected companies a set of mitigation actions to be implemented. CERCA considers the effect on the risk of these mitigations and informs the analyst that these mitigations are CSIRT-suggested under NIS 2 Directive (or related local legislation). The input for these mitigations can be interfaces with other tools such as AIRE, a Kafka topic where the mitigations are written and CERCA reads them, or mitigations can also be received via a dedicated endpoint at the API.

Another novelty is ingestion of inputs related to physical risks. The AI-based inspection tool developed under WP7 implements image analysis solutions using computer vision, integrating advanced AI models for Visual Question Answering tasks. This functionality leverages significant advances in visual and large language models to adapt to various contexts and includes an open-vocabulary and zero-shot detection module that can also be applied in cybersecurity. This broad range of applicability has allowed for preliminary proof-of-concept tests with images and videos related to events that could indicate potential physical attacks on infrastructure or cyberattacks.

The tool processes video streams or pre-recorded individual images, analyzing them frame by frame using detection and visual question answering modules to identify predefined objects (for example, people, balaclavas, tools, USB drives) and answer questions related to the elements present in the image.

An example is provided below to illustrate the data flow: in a scenario where a "shoulder surfing" attack is occurring (Figure 88), the tool analyzes the situation and responds whether someone is looking over another person's shoulder at a device. The user question and the response, generated by the multimodal visual-language model LLaVA1.6:

> Question: Is someone looking over someone else’s shoulder at a device?
>
> Response: 'vqa': ["Yes, in the image, it appears that one person is looking over the shoulder of another person who is using a device, possibly a smartphone. The person being looked over is not aware of the other person's attention, as they are focused on their device. This is a common scenario when someone is engrossed in their phone or other device, and it can be a source of amusement or concern, depending on the context."].

This response vector can be sent to CERCA through a Kafka topic or sent to the SIEM, where an alarm is generated and sent to CERCA, where an indicator mapping this activity, shoulder surfing, is activated and evaluated within the risk assessment step.

Screenshots for new functionalities can be found the Annex, section I.III.

New and extended existing functionalities mapped to completed requirements from D3.2 – *Requirements and designs V2* [3]

- “The Tool MUST be developed using container technology as it is suitable for cloud-native production environments (FR.WP6.03)”: CERCA is developed in 5 different modules that are deployed using Docker, 4 modules-containers always need to be deployed: “cerca_dashboard” (Django), “cerca_engine” (Python), “cerca_deployment_rabbitmq” (RabbitMQ) and “cerca_database” (PostGreSQL), while a 5th module-container, “cerca_deployment_nginx” can be deployed or not based on whether an external Nginx is used. CERCA can be deployed in a Cloud Environment with minimal configuration (IPs, images names, etc), by providing 5 different Docker images, each corresponding to one module.
- “The Tool MUST process information from physical sensors to protect the external access of the building (FR.WP6.14)”: information from physical sensors goes to the SIEM Wazuh, where appropriate configured rules may trigger an alarm that is sent to a Kafka topic, then CERCA reads that alarm and process the information from physical sensors, that may trigger a new risk assessment evaluation with an update on the risk level.
- “The Tool MUST calculate the probability of an incident to occur and evaluate the impact on the infrastructure (FR.WP6.18)”: CERCA uses R models to evaluate the quantitative impact on the infrastructure for an entity. These R models define, based on the CORAS Risk Assessment methodology [12], a probability of and attack to start, and a probability of occurrence for each possible path the attacker may use to achieve the attack objective.
- “The cybersecurity resilient framework MUST include a Tool that calculates risk linked to entities (NFR.WP6.04)”: CERCA takes as inputs (via configuration or via GUI/user) different entities and its assets, which have a CIA triad value from 0-10 (Confidentiality, Integrity, and Availability). This information, combined with the selected risk models and inputs (monitoring, questionnaire, etc) is fed to the risk assessment module that gives as output diverse levels of granularity for the risk, being one of these levels the global risk for an entity.
- “CERCA's input MUST be the alarms captured by the SIEM (NFR.WP6.15)”: all monitoring inputs (alarms and events) come from the SIEM Wazuh, using a Kafka broker shared by all CPR tools, using specific topics (i.e. "sunrise-alerts") for the communication with each tool.

Finally, after feasibility analysis based on the data provided by user organizations, and internal testing, the risk models selected for Insiel and CAFC use cases and the related MITRE ATT&ACK techniques, tactics and procedures are:

- WRP1: Denial of Service Attack (T1498, T1499) (monitoring data available)
- WRP2: Invalidated Redirects and Forwards (T1583)
- WRP3: Bypass Login (T1548)
- WRP4: Compromise security via Trojan-malware (T1622)
- WRP5: Client-Server Protocol Manipulation (T1189)
- WRP6: Session Fixation (T1563, T1165)
- WRP7: Cross Site Request Forgery (T1550, T1528)

- WRP8: SQL Injection (T1190) (monitoring data available)
- WRP9: Buffer Overflow (T1190) (monitoring data available)
- WRP10: Relative Path Traversal (T1083)
- Phishing and Impersonation Attacks (T1566)
- Man in The Middle Attack (T1557)
- Amplification Attack (T1498)
- Password Brute-Force Attack (T1110)
- Privilege Escalation Attack (T1068, TA0004)

3.4 Incident Reporting (AIRE)

The Incident Reporting Module (AIRE) deals with communication with different actors. Originally, it only reported cyber incidents to the authorities. However, due to new policies and regulations (NIS 2 Directive [7]) that requires incidents to be reported to service beneficiaries and that promote the sharing of incident and vulnerability information with authorities and other entities, AIRE has been enhanced with additional communication capabilities.

Regarding the functionalities that already existed in the past, AIRE considers if the set of events and evidence (alerts, Indicator of Compromise, number of affected users, service downtime…) that form a cyber incident meet the criteria for reporting to competent authorities. The tool provides automated classification and processing to reduce the analysts' workload during the reporting process to the authorities. In addition, it supports existing directives, such as GDPR or NIS.

This section analyses the NIS 2 Directive [7] regarding AIRE and the communication requirements that will be necessary for the tool to be fully compliant with the directive. Furthermore, it outlines the enhancements that have been incorporated, based on feasibility analysis and data provided by users.

3.4.1 NIS 2 Directive analysis

As NIS 2 is currently a directive, EU countries must create their own laws to implement it in national legislation and in this way enable achievement of the objectives proposed in the directive. Therefore, the exact criteria for each country cannot be determined until the laws are published by 17 October 2024 at the latest. It is anticipated that these national legislations will provide a reasonable period for the creation or adaptation of the competent authorities, which will be responsible for coordinating and supervising the implementation of the new rules, as well as of the Computer Security Incident Response Teams (CSIRTs). Meanwhile, the entities affected by the national regulations derived from the NIS 2 Directive will also have to adapt their internal processes to the new rules, which will require a period of adaptation. Furthermore, the list of entities required to comply with the directive will be published on 17 April 2025. In any case, the full implementation of the directive should be completed by 17 October 2027, the latest date for the first review of the functioning of the NIS 2 Directive.

The exact criteria to be met by critical services will not be known until the competent authorities in each country publish their regulations. This analysis of the directive aims to identify the functionalities already introduced in the directive and therefore will be common to all Member States' regulations. The incident notification module will be enhanced with the necessary functionalities for entities covered by the directive to comply with the directive.

3.4.1.1 Scope

The NIS 2 Directive is designed *to achieve a high common level of cybersecurity across the Union, with a view to improving the functioning of the internal market [Article 1, NIS 2]*. To this end, it implements a national cybersecurity strategy that designates for cybersecurity risk management: cybersecurity crisis management and competent authorities, single points of contact, and CSIRTs. The directive requires that critical entities report any cybersecurity incidents or cyber threats. Furthermore, they are required to share pertinent information on cybersecurity incidents with the relevant authorities or

CSIRTs. Finally, it encourages the voluntary exchange of information and the disclosure of vulnerabilities.

3.4.1.2 Entities, Authorities, and ENISA

The NIS 2 Directive distinguishes between two primary categories: essential entities and important entities. **Essential entities** are those belonging to high criticality sectors, namely: Energy, Transport, Banking, Financial market infrastructures, Health, Drinking water, Waste water, Digital infrastructures, ICT service management (business-to-business), Public administration (excluding the judiciary, parliaments and central banks), and Space, and have more than 250 employees, an annual turnover of at least EUR 50 million or an annual balance sheet total of at least EUR 43 million.

This category of essential entities includes, irrespective of their size or turnover: trust service providers, top-level domain name registries, DNS service providers, and single providers of essential services. Additionally, central public administrations, entities providing services in the areas of public security, public safety, public order, or public health, entities providing services whose disruption may pose a significant systematic risk, critical entities regarding Directive 2022/2557 (CER), and entities considered essential operators by Directive 2016/1148 (NIS) are also considered essential entities.

In contrast, **important entities** are those that belong to a high criticality sector (as listed above), but do not meet the criteria to be considered an essential entity. In addition, important entities are those that belong to other important sectors: Postal and courier services; Waste management; Manufacture, production, and distribution of chemicals; Production, processing, and distribution of food; Manufacture of products: medical devices, computers, electronic, optical, electrical equipment, machinery and equipment, motor vehicles and trailers, and transport equipment; Digital providers; and Research. In addition, all entities identified by the state as significant are included.

Each Member State is required to designate one or more competent authorities responsible for cybersecurity in the State and for overseeing the implementation of the NIS 2 Directive in essential and important entities. Additionally, one or more Computer Security Incident Response Teams (CSIRTs) will be established, equivalent to CERTs in the American context. Their functions will include: the response, monitoring, and analysis of cyber threats, vulnerabilities, and incidents; assisting essential and important entities against incidents; supporting entities in the real-time monitoring of their systems; and disseminating early warnings. The CSIRT will disseminate alerts and information on cyber threats, vulnerabilities, and incidents to the affected entities and the competent authorities concerned. It will also collect and analyse forensic evidence for real-time risk assessment of each sector, support the search for vulnerabilities and coordinate incident response at both national and cross-border level. To achieve these objectives, the CSIRT will collaborate with CSIRTs from other sectors or other states by creating a CSIRT Network. CSIRTs should establish collaborative relationships with both private sector stakeholders and other CSIRTs to enhance the objectives of the NIS 2 Directive. This can be achieved by promoting the use of common, standardized practices and sharing relevant information on incidents, cyber threats, risks, vulnerabilities, and technologies.

As the NIS 2 Directive allows for the creation of different competent authorities for different critical sectors, as well as the creation of several CSIRTs, it is necessary to establish a **single point of contact** to ensure cross-border cooperation and liaison between the authorities of one state and the single point of contact of the other states. CSIRTs and competent authorities should inform the single point of contact of significant incidents and detected cyber threats. It is the responsibility of the single point of contact to notify all other authorities, as well as CSIRTs and other single points of contact, of any pertinent information.

The European Union Agency for Cybersecurity (ENISA) *is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe*[3]. About the NIS 2 Directive, the Agency is responsible

[3] https://www.enisa.europa.eu/

for coordinating the activities of the different states by aggregating the information collected by each of them. It provides guidelines and templates, assesses compliance with the NIS 2 Directive, and assists in the setting up of national cybersecurity schemes and CSIRTs. The establishment of national cybersecurity schemes and CSIRTs; maintenance of the list of critical, important entities and domain name registration providers; secretariat management of the CSIRT network; European vulnerability database management; and information exchange mechanism support. In summary, ENISA will oversee all activities resulting from the implementation of the NIS 2 Directive.

3.4.1.3 Incidents and reporting obligations

The NIS 2 Directive defines an incident as any event that compromises the availability, authenticity, integrity, or confidentiality of stored, transmitted, or processed data, or the services offered. It also requires the reporting of **significant incidents**, which are *those that have caused or may cause serious operational disruption of services or monetary loss to the entity concerned, or that have affected or may affect other natural or legal persons by causing significant material or immaterial damage*. This description of a significant incident includes the concept of a **near miss**, which represents *events that could have compromised availability but did not materialize*. This is intrinsic to the need to assess the risk of entities in the field of cybersecurity. The NIS 2 Directive requires the reporting of incidents of this nature.

It is the responsibility of essential and important entities to notify the assigned CSIRT, or failing that the relevant competent authority, of any significant incident or near miss that impacts the services provided. The notification process is composed of several phases with different deadlines, all of which commence from the time the incident has been detected. The notification process comprises the following phases:

1. **Early warning**, within 24 hours, indicating whether it may be caused by malicious action or may have cross-border impact.
2. **Incident notification**, within 72 hours, update of the information provided and an initial assessment of the incident (including severity, impact, and indicators of compromise).
3. **Intermediate report**, upon request of the CSIRT, with updates on the status of the incident.
4. **Final report** is to be submitted within one month of the incident. It should include a detailed description of the incident, the classification of the incident by type of threat, the underlying cause leading to the incident, the measures implemented or in progress, and the cross-border and cross-sectoral impact of the incident (if applicable).
5. **Progress report** should be submitted in place of the final report if the incident is still ongoing at the time of submission. The final report is to be submitted within one month of the incident being closed.

In response to an early warning, the CSIRT or the competent authority shall provide a response on the incident within a maximum of 24 hours, along with operational advice on the implementation of mitigating measures. Furthermore, they will advise the affected entity on how to report the incident to the relevant legal authority.

Furthermore, entities affected by a significant cyber threat must inform the recipients of their services of the cyber threat and the measures they can implement. In addition, the service recipients may be required to report the incident if the cyber threat has a significant impact on the services they offer.

Furthermore, the relevant authorities or CSIRTs are required to inform other states affected by the cyber incident via their designated point of contact about cross-border incidents and cross-sectoral incidents to CSIRTs or authorities in other sectors. In turn, they must provide support for the incident.

3.4.1.4 Voluntary information sharing

In addition to the mandatory reporting of significant incidents, the NIS 2 Directive encourages the voluntary sharing of relevant cybersecurity information and the reporting of newly found vulnerabilities.

Information deemed relevant includes cyber threats, near misses, vulnerabilities, techniques and procedures, indicators of compromise, adversary tactics, risk actor-specific information, cybersecurity alerts and recommendations on tool configurations to detect cyberattacks. The NIS 2 Directive requires states to ensure that such sharing is limited to the set of interrelated critical entities and their suppliers, if necessary. Furthermore, the directive requires entities to notify the relevant authorities of their participation in the information exchange mechanisms. The objective of information sharing is to enhance the prevention, detection, and response to incidents, thereby reducing their impact.

The NIS 2 Directive encourages the creation of a European vulnerability database to facilitate coordinated disclosure of vulnerabilities. It also proposes that one of the states CIRST should act as a coordinator and trusted intermediary between entities or individuals notifying a vulnerability and the manufacturer or provider of ICT services and products. This would assist with notification and negotiate disclosure deadlines between the different entities involved. Furthermore, the Directive calls on ENISA to create and maintain a European vulnerability database, containing descriptive information on vulnerabilities, affected ICT products and services, an estimation of the severity of vulnerabilities, and vulnerability patches or guidelines needed to reduce the risk of vulnerabilities.

3.4.1.5 Cybersecurity risk-management measures

In accordance with the NIS 2 Directive, institutions are required to implement the necessary organizational, operational, and technical measures to effectively manage the risks associated with their information systems and networks. They must ensure a level of systems security commensurate with the risk posed, considering the exposure of the systems, the size of the entity, the likelihood of incidents and their severity (including both social and economic consequences).

Considering the objectives of the incident notification module, which is to automate the notification of incidents to the competent authorities in case of an incident, several measures have been considered with the aim of evolving AIRE to help it comply with future legislation stemming from the NIS 2 Directive:

1. **Risk analysis**: This process is fundamental for the effective management of cyber threats to critical entities, as it will support decision-making in the event of an incident occurring. While there are tools that assist in this process by providing an estimate of the risk of an asset or the economic cost of an incident, such as CERCA, it is the responsibility of the risk analyst to analyse all available information to determine the risk of a potential incident.
   The NIS 2 Directive requires that any incident involving a potential cyber threat be reported to the relevant authorities, even if the incident has not yet materialized. The identification of such cases can only be achieved using automated risk analysis. AIRE facilitates this process by automatically consolidating the data from the risk analysis tool report with the analyst's input.
2. **Supply chain security**: One of the key improvements brought by the NIS 2 Directive, compared to the NIS Directive, is the consideration of supply chain risk. This directive introduces the concept of considering the risk of the services consumed by an institution when calculating the institution's own risk. At the same time, the entities must notify the critical entities that employ them if the services they provide have any associated risk. This enables the second entities to make a more accurate calculation of the risk associated with their services. It therefore follows that not only notifications to and from the competent authorities need to be managed, but also notifications from providers and consumers of critical services need to be sent and received.
3. **Incident management**: is a critical aspect of business continuity planning. If, based on the risk analysis, an incident has occurred or may occur, it is necessary to implement a management strategy. The objective of this task is to gather as much information as possible to implement the most appropriate measures to deal with the incident. It is essential to ensure that the time spent on information acquisition and decision-making is balanced. Furthermore, the NIS 2 Directive stipulates that incidents must be reported to the relevant authorities as part of the

incident management process. In response to this notification, the competent authorities must propose a set of measures based on previous experiences from other incidents, if requested by the affected entity. It will implement the measures to manage or mitigate the incident.

AIRE, with its task manager, can assist in ensuring that the suggested measures are executed and monitored. The information generated will be added to the interim reports and the final report sent to the authorities or CSIRTs.

4. **Evaluation of the efficiency of the means for cybersecurity risk management**: By re-evaluating the impact of measures taken in response to a cyber incident, it is possible to ascertain whether they are effective or whether a different course of action is required. This reassessment must be carried out by an analyst, although their decision can be supported by risk analysis tools, such as CERCA.

   The NIS 2 Directive requires that updates to the incident status be made when required by the competent authority or when there is a meaningful change in the situation. The AIRE system can automatically aggregate the risk reassessment reports generated by the tool and reviewed by the risk analysts, integrating them into the interim reports and the final incident report.
5. **Vulnerability management and disclosure**: This measure is designed to ensure that the technical knowledge generated by an incident is shared and not lost. Although not a mandatory requirement for organizations, the Directive does require the creation of a European vulnerability database.

   The management of this notification can be done from AIRE, integrating the task as a final task of the incident notifications, after the final report has been sent when all the information is already collected and processed. This task is optional, and it should be noted that a new vulnerability is not always discovered.

In addition to the measures listed above, entities under the NIS 2 Directive are obliged to deploy other measures that have been excluded from the scope of the incident reporting module (AIRE) deployed in SUNRISE. These measures are not related to the core functionality of SUNRISE. The list of measures is as follows:

- **IT system security policies**: These include basic security policies, such as the use of strong passwords and their regular renewal, the systematic updating of deployed software, or policies on the use of USB ports. While these measures can help to reduce the risk of a cybersecurity incident, it is advisable to implement them in a preventive manner, even before the incident occurs.
- **Business continuity**: These are measures that are implemented after an incident, but do not prevent or reduce the risk of an incident. These measures reduce the impact of an incident by enabling the rapid recovery of services or by preventing data loss. Examples of such measures include backup management policies, service recovery measures in case of failure or catastrophe, and crisis management policies.
- **Cybersecurity training**: It enables employees to be better prepared for a cybersecurity incident. The objective is to reduce the likelihood of an incident occurring and to provide employees with the knowledge and skills to identify and manage it effectively. One of the most crucial aspects of this measure is employee training. One example is the use of fake phishing campaigns by companies against their employees. This allows us to assess the awareness of the workforce and, at the same time, to provide them with training.
- **Use of cryptography and encryption**: Procedures that ensure the authenticity, integrity, and confidentiality of data, both stored and transmitted. This protection reduces the risk of data being stolen or manipulated. An example of this type of procedure is the use of public-private keys for the confidential transmission of information, which authenticates the sender and guarantees its integrity.

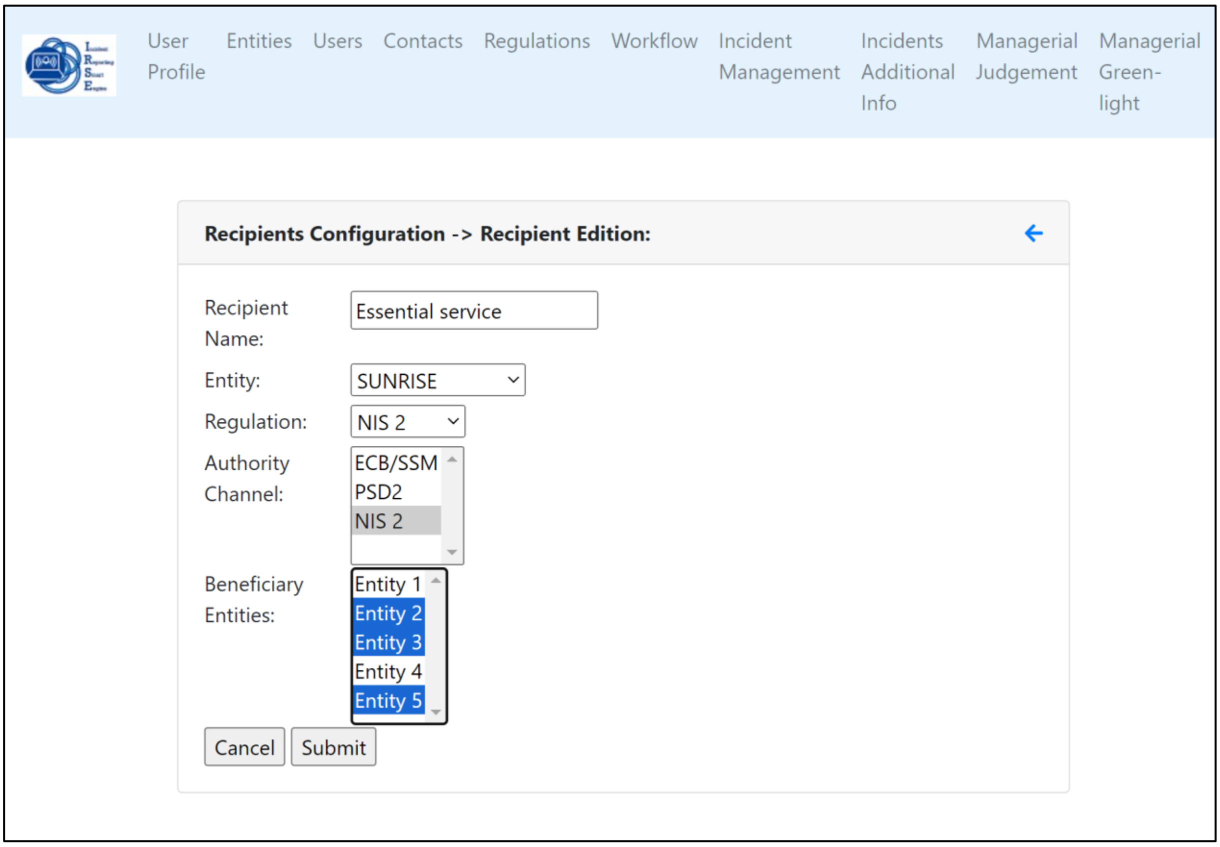
In summary, all these measures must be taken before a cyber incident and must reduce the risk of a cyber incident, either by preventing or hindering the incident or by reducing its effect, enabling rapid service recovery, and avoiding data loss. However, none of these are related to the main function of the AIRE module, as they are not related to incident reporting.

3.4.2 Improvements

Following the analysis of the NIS 2 Directive presented in the previous section, four functionalities have been identified as necessary to comply with the directive and will be implemented to enhance the incident reporting module, AIRE. As Member States have not yet published their respective legislation and designated their CSIRTs, the concrete criteria, procedures, and formats are not available . Consequently, the implemented functionalities may be subject to modification considering future more specific or detailed requirements resulting from the publication of national laws or regulations by Member States.

3.4.2.1 Communication of Supply Chain Risk

The NIS 2 Directive requires entities to report on the risk of their services to the beneficiaries of those services. This requirement has been met by enhancing the incident notification process. To this end, a list of beneficiary entities has been added to the configuration of recipients, as illustrated in Figure 9 Recipient Configuration.



Recipients Configuration -> Recipient Edition:

Recipient Name: Essential service

Entity: SUNRISE

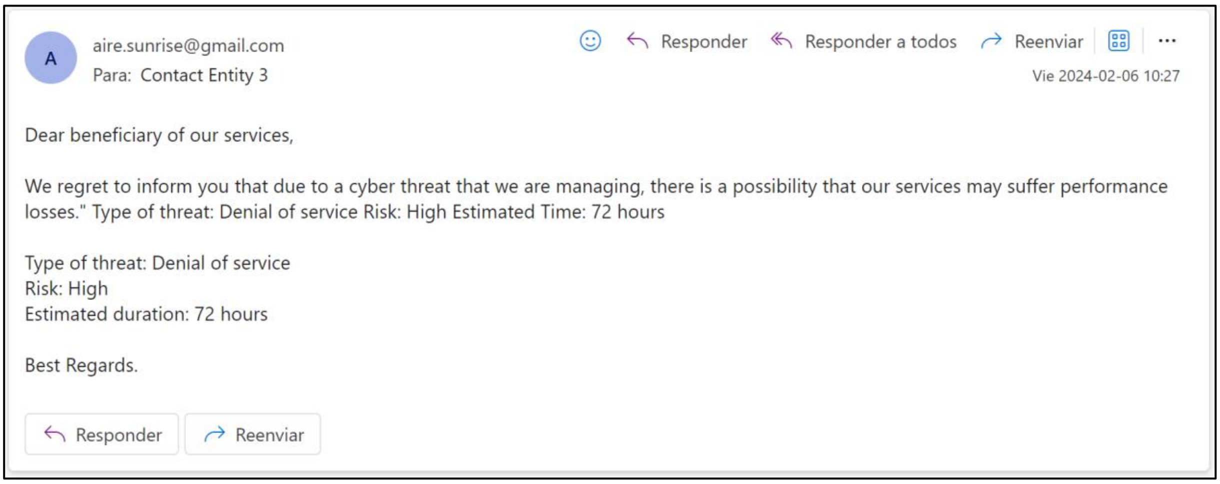
Regulation: NIS 2

Authority Channel: ECB/SSM, PSD2, NIS 2 (selected: NIS 2)

Beneficiary Entities: Entity 1, Entity 2, Entity 3, Entity 4, Entity 5 (selected: Entity 2, Entity 3, Entity 5)

Figure 9 Recipient Configuration.

This process ensures that, upon the transmission of a notification to the relevant authority (Early warning, Incident notification, Intermediate report, or Final report), an email is automatically sent to the entities that benefit from the service, alerting them to any incidents or cyber threats within the service. Furthermore, if there are any significant changes, the email will be used to provide updates on the risk. Please refer to Figure 10 for an illustration of this process.



aire.sunrise@gmail.com
Para: Contact Entity 3

Vie 2024-02-06 10:27

Dear beneficiary of our services,

We regret to inform you that due to a cyber threat that we are managing, there is a possibility that our services may suffer performance losses." Type of threat: Denial of service Risk: High Estimated Time: 72 hours

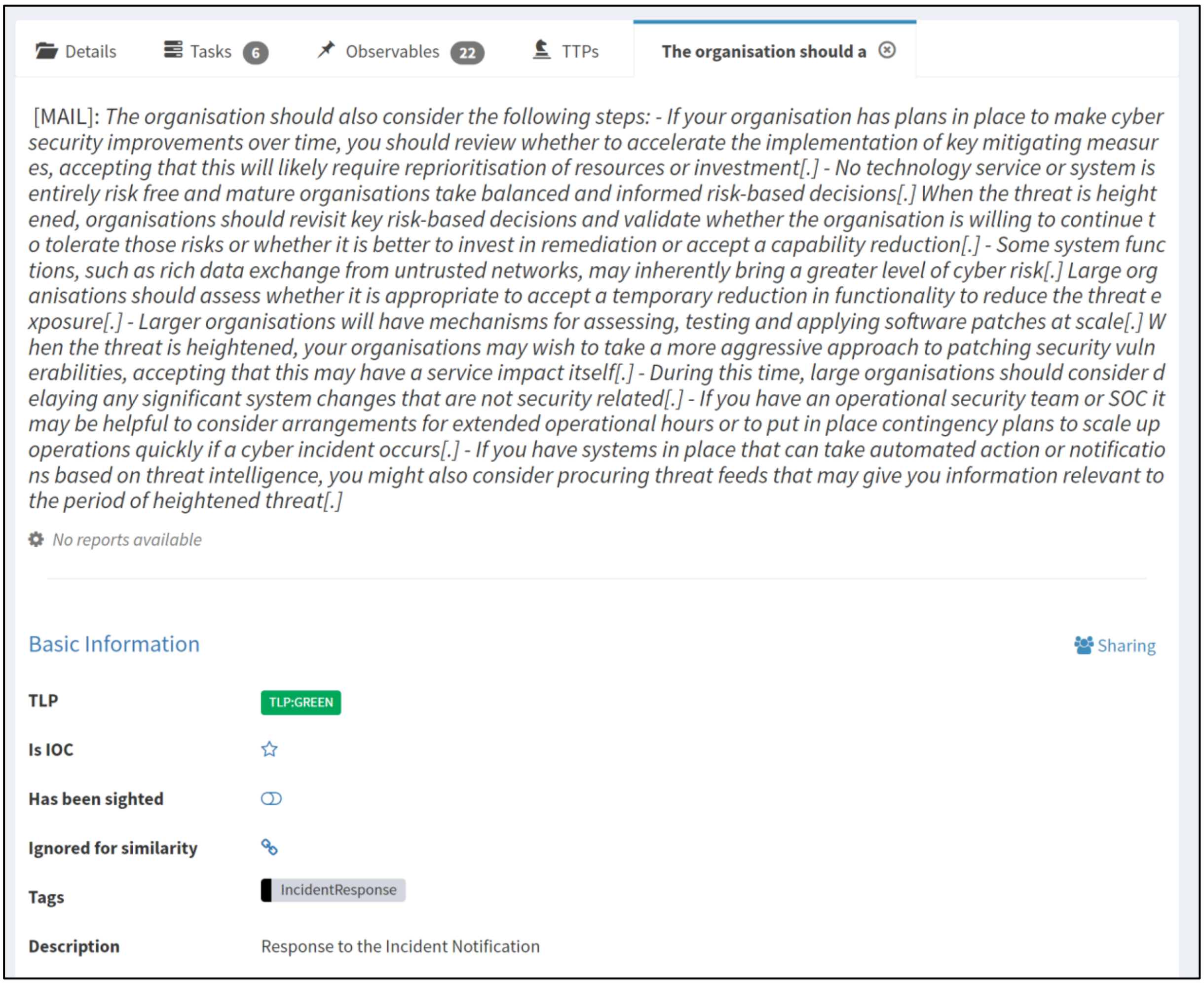
Type of threat: Denial of service
Risk: High
Estimated duration: 72 hours

Best Regards.

Figure 10 E-mail to beneficiaries.

3.4.2.2 Receive the Response to an Incident Notification

In the event of an incident notification, the NIS 2 Directive requires CSIRTs to respond within 24 hours with a set of measures that the affected entity can implement to mitigate and manage the incident. Given the absence of a communication protocol, it has been assumed that this response will be via email. This response is added to AIRE with the tag IncidentResponse, as shown in Figure 11. This provides access to all information in a single application, which is accessible from any location.



[MAIL]: *The organisation should also consider the following steps: - If your organisation has plans in place to make cyber security improvements over time, you should review whether to accelerate the implementation of key mitigating measures, accepting that this will likely require reprioritisation of resources or investment[.] - No technology service or system is entirely risk free and mature organisations take balanced and informed risk-based decisions[.] When the threat is heightened, organisations should revisit key risk-based decisions and validate whether the organisation is willing to continue to tolerate those risks or whether it is better to invest in remediation or accept a capability reduction[.] - Some system functions, such as rich data exchange from untrusted networks, may inherently bring a greater level of cyber risk[.] Large organisations should assess whether it is appropriate to accept a temporary reduction in functionality to reduce the threat exposure[.] - Larger organisations will have mechanisms for assessing, testing and applying software patches at scale[.] When the threat is heightened, your organisations may wish to take a more aggressive approach to patching security vulnerabilities, accepting that this may have a service impact itself[.] - During this time, large organisations should consider delaying any significant system changes that are not security related[.] - If you have an operational security team or SOC it may be helpful to consider arrangements for extended operational hours or to put in place contingency plans to scale up operations quickly if a cyber incident occurs[.] - If you have systems in place that can take automated action or notifications based on threat intelligence, you might also consider procuring threat feeds that may give you information relevant to the period of heightened threat[.]*

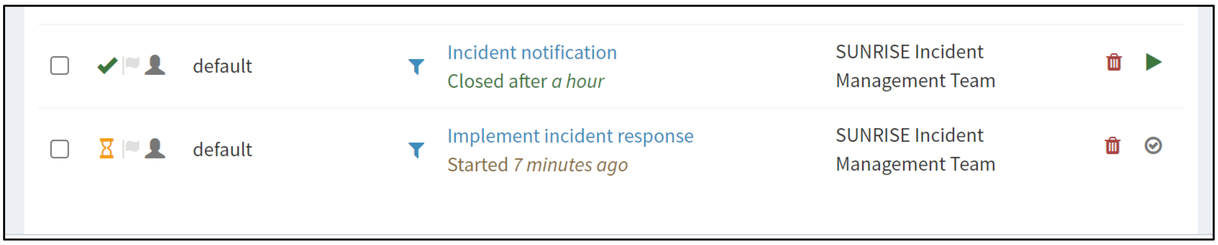
No reports available

Basic Information

TLP	TLP:GREEN
Is IOC	☆
Has been sighted	⬭
Ignored for similarity	
Tags	IncidentResponse
Description	Response to the Incident Notification

Figure 11 Response to an Incident Notification, example of measures obtained from UK's National Cyber Security Centre.[4]

Categorizing an email as an *IncidentResponse* automatically generates a task for the analysis and implementation of the measures proposed by the CSIRT, as illustrated in Figure 12. This task allows for the logging of the measures implemented and the justification for those not implemented.



□	✓	default	Incident notification Closed after *a hour*	SUNRISE Incident Management Team	▶
□	⧗	default	Implement incident response Started *7 minutes ago*	SUNRISE Incident Management Team	✓

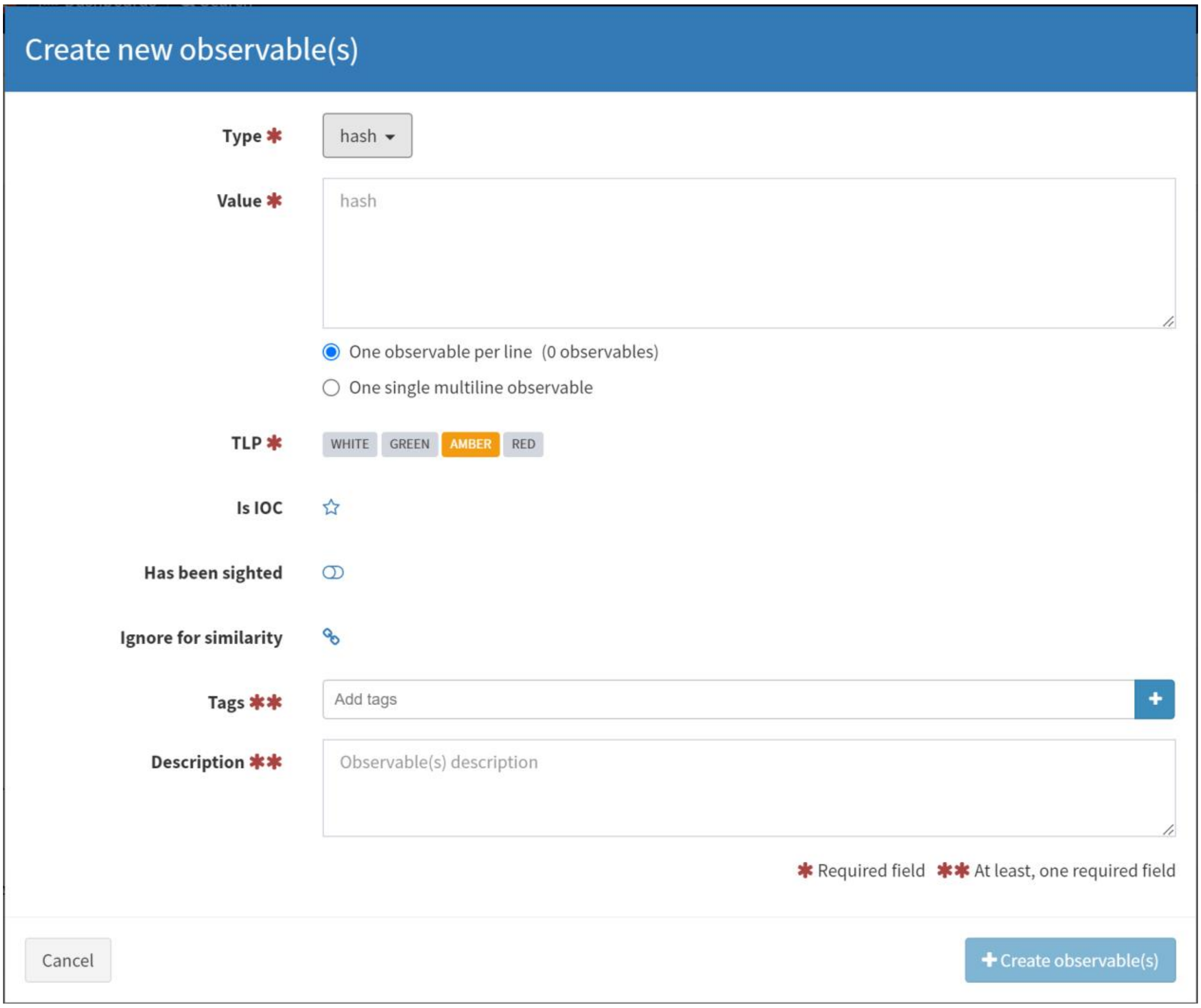
Figure 12 *Implement incident response*: task for applying the measures proposed by CSIRT.

[4] https://www.ncsc.gov.uk/guidance/actions-to-take-when-the-cyber-threat-is-heightened

3.4.2.3 Attaching Indicators of Compromise to Incident Reports

During an investigation, several observations are generated that may or may not be related to the incident in question. These observations must be recorded for further analysis. If these observables are evidence of an attack or an attempt, they are designated as Indicators of Compromise (IOCs). The NIS 2 Directive stipulates that incident notifications and final reports must include the IOCs obtained during the incident investigation. AIRE addresses this requirement by automating the aggregation of IOCs in the reporting process.

Observables can be registered in AIRE via a web form on the tool's management page, as shown in Figure 13. In this form, users must identify the type of observable. There is a predefined list of observable types that can be easily extended or modified from within the application. The observable values can be provided as a list, with one value per line. This approach assumes that all observables have the same attributes and descriptions. Alternatively, the observable values can be provided as a single multi-line item. It is possible to mark observables as IOCs from the outset, although this option can be modified if the evolution of the investigation so determines.



Create new observable(s)

Type * hash ▾

Value * hash

● One observable per line (0 observables)

○ One single multiline observable

TLP * WHITE GREEN AMBER RED

Is IOC ☆

Has been sighted

Ignore for similarity

Tags ** Add tags +

Description ** Observable(s) description

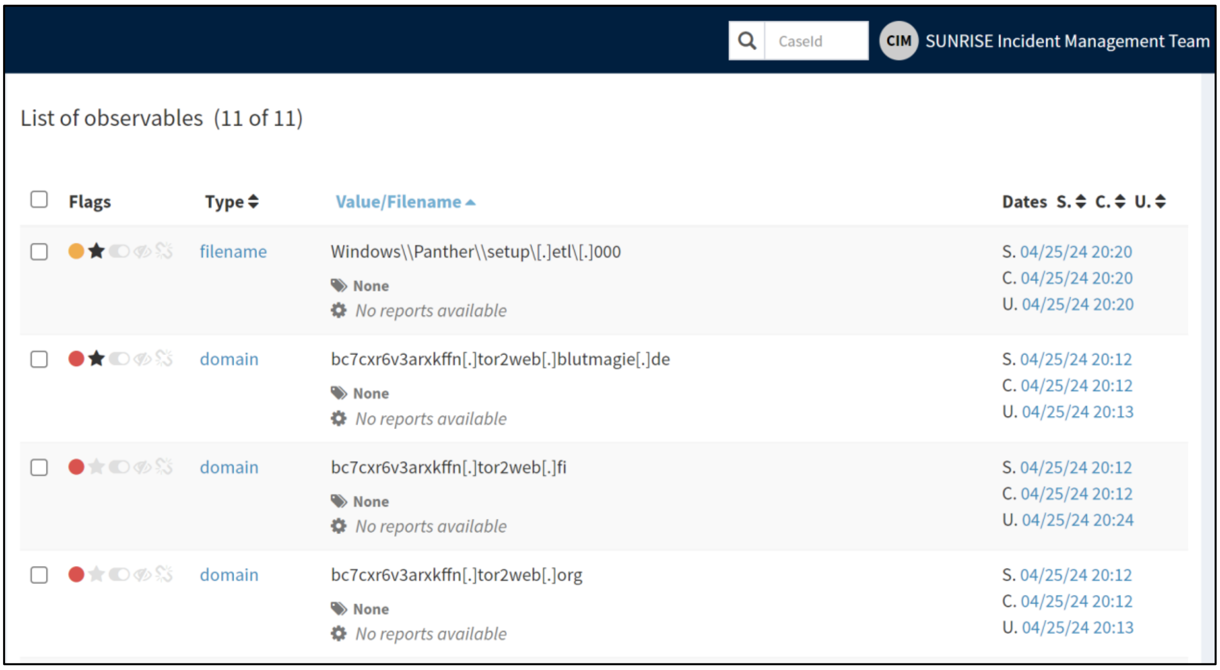
* Required field ** At least, one required field

Cancel

+ Create observable(s)

Figure 13 Form to create new observables.

Each incident contains a list of observables, as shown in Figure 14, which provides an overall view of the information collected on the incident. IOCs are marked with a second symbol, the star, to indicate that they have been classified as such.



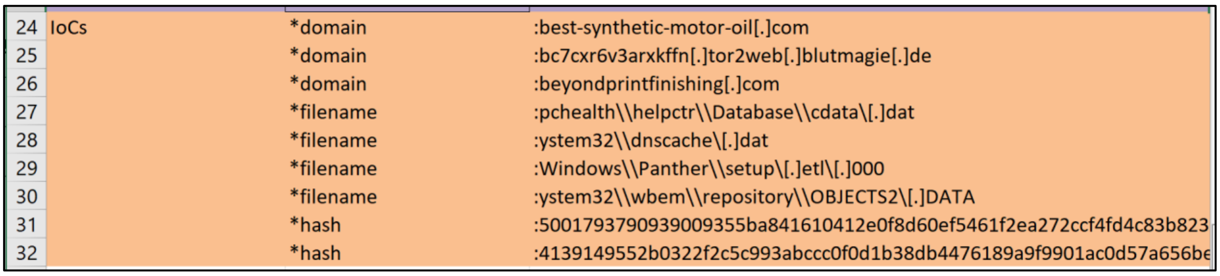
CaseId CIM SUNRISE Incident Management Team

List of observables (11 of 11)

□	Flags	Type	Value/Filename	Dates S. C. U.
□	●★	filename	Windows\\Panther\\setup\[.]etl\[.]000 None *No reports available*	S. 04/25/24 20:20 C. 04/25/24 20:20 U. 04/25/24 20:20
□	●★	domain	bc7cxr6v3arxkffn[.]tor2web[.]blutmagie[.]de None *No reports available*	S. 04/25/24 20:12 C. 04/25/24 20:12 U. 04/25/24 20:13
□	●	domain	bc7cxr6v3arxkffn[.]tor2web[.]fi None *No reports available*	S. 04/25/24 20:12 C. 04/25/24 20:12 U. 04/25/24 20:24
□	●	domain	bc7cxr6v3arxkffn[.]tor2web[.]org None *No reports available*	S. 04/25/24 20:12 C. 04/25/24 20:12 U. 04/25/24 20:13

Figure 14 List of observables, IOCs, and non-IOCs (star flag).

Once a report has been generated, the list of observables that have been marked as IOCs is added. Figure 15 illustrates some example IOCs added to the NIS incident notification report in Excel format, for which there are published report templates.



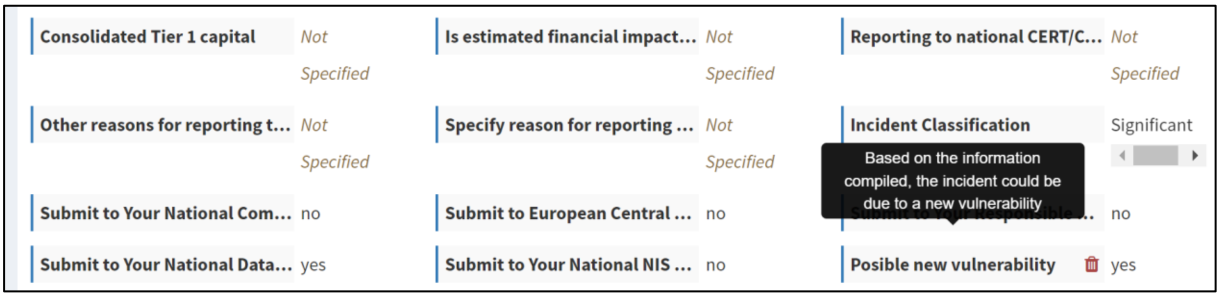
24	IoCs	*domain	:best-synthetic-motor-oil[.]com
25		*domain	:bc7cxr6v3arxkffn[.]tor2web[.]blutmagie[.]de
26		*domain	:beyondprintfinishing[.]com
27		*filename	:pchealth\\helpctr\\Database\\cdata\[.]dat
28		*filename	:ystem32\\dnscache\[.]dat
29		*filename	:Windows\\Panther\\setup\[.]etl\[.]000
30		*filename	:ystem32\\wbem\\repository\\OBJECTS2\[.]DATA
31		*hash	:5001793790939009355ba841610412e0f8d60ef5461f2ea272ccf4fd4c83b823
32		*hash	:4139149552b0322f2c5c993abccc0f0d1b38db4476189a9f9901ac0d57a656be

Figure 15 IOCs aggregated at the end of NIS Directive report.

To provide a proof of concept of this functionality, and in the absence of the final NIS 2 templates, the pilots were asked for the templates of the reports they currently must report to the authorities or internally. The Attach IOC functionality has been incorporated into these templates and feedback on this improvement is currently being collated. The results and validation will be included in the next deliverable D6.4.

3.4.2.4 Vulnerability Disclosure

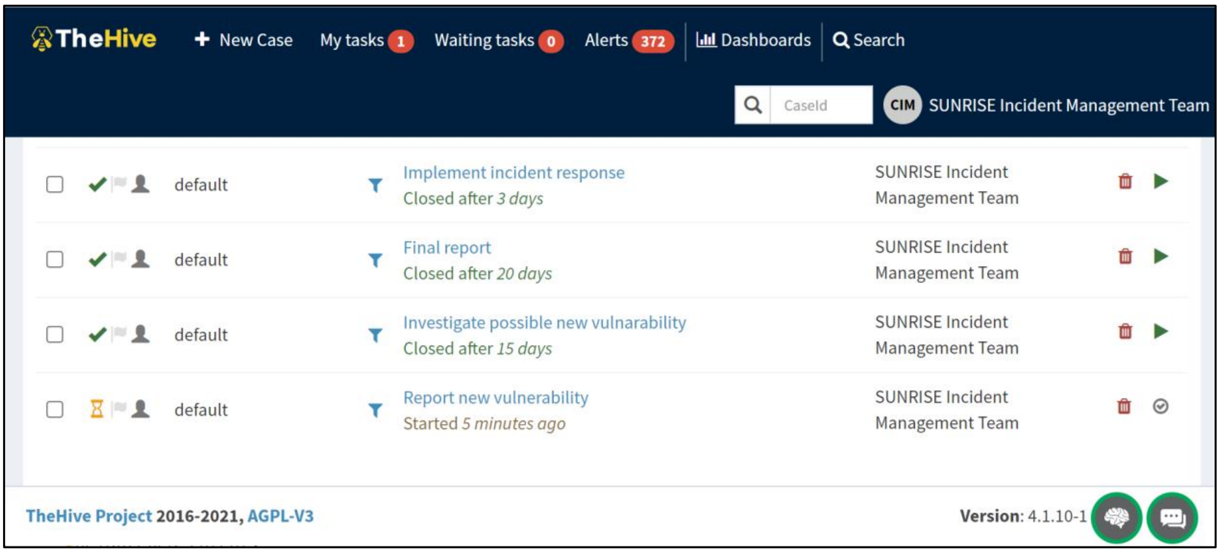
Given that this measure is not mandatory, the associated functionality has been implemented as an optional step at the end of the list of tasks that creates an incident, as illustrated in Figure 17 Vulnerability tasks. It is necessary that during the investigation of the incident it has been identified as a potential unknown vulnerability (Figure 16 Vulnerability field). It is not always necessary to perform this task, and it can be closed if the vulnerability is known. If these conditions are met, the process of reporting the vulnerability to the relevant authorities can then be initiated.



Consolidated Tier 1 capital	*Not Specified*	Is estimated financial impact…	*Not Specified*	Reporting to national CERT/C…	*Not Specified*
Other reasons for reporting t…	*Not Specified*	Specify reason for reporting …	*Not Specified*	Incident Classification	Significant
Submit to Your National Com…	no	Submit to European Central …	no	Submit to Your Responsible …	no
Submit to Your National Data…	yes	Submit to Your National NIS …	no	Posible new vulnerability	yes

Based on the information compiled, the incident could be due to a new vulnerability

Figure 16 Vulnerability field.



□	✓	default	Implement incident response Closed after *3 days*	SUNRISE Incident Management Team
□	✓	default	Final report Closed after *20 days*	SUNRISE Incident Management Team
□	✓	default	Investigate possible new vulnarability Closed after *15 days*	SUNRISE Incident Management Team
□	⌛	default	Report new vulnerability Started *5 minutes ago*	SUNRISE Incident Management Team

TheHive Project 2016-2021, AGPL-V3 **Version:** 4.1.10-1

Figure 17 Vulnerability tasks.

As there is currently no European vulnerability database, the vulnerability reporting process to the CVE Program has been utilized. This program has several CVE Numbering Authorities (CNAs), although none of them are in Italy or Slovenia. Therefore, the Spanish CNA, INCIBE, has been selected as the notification point in this iteration of testing.

The process of notifying a vulnerability to INCIBE begins with the submission of an email containing comprehensive details about the vulnerability. INCIBE will then confirm receipt of the vulnerability and may request additional information to verify its existence and notify the service or application provider of the vulnerability.

4 Legal Compliance and Testing Methodology

Section 4 is designated to outline potential legal concerns, such as data sharing restrictions for CI due to legal regulations or limitations on permissible testing activities. In addition, an outline of piloting activities is presented.

At this stage, no problems have arisen, although they may appear during the testing phase. This section will be revised in the next versions of this document (D6.5) and is closely monitored in WP9 – Management: Project Coordination and Technical Coordination (WP3 in general, specifically T3.4).

On the other hand, and considering WP6 time plan, all CI operators have been notified about the schedule and possible issues, so that the start of piloting activities does not suffer from any delay. The pilot schedule is the following:

- Deployment will be done in the last week of May.
- Testing will be done during the first week of June.
- And collection of feedback is due to second and third week of June.

The testing process will unfold in several meticulous phases. The first two activities will rely on the preparation of a proper environment in terms of hardware and software requirements, which have been detailed in Section 2.4 and considered for the preparation of sandboxes. Initially, deployment will occur within the CI environment, where hardware or virtual machines are prepared, granting access to XLB and ATS to install the CPR tool via VPN. Following installation, XLB and ATS will diligently test CPR tool with mock data to ensure functionality. Subsequently, the CI operators will connect the log source, initiating the processing phase where CI operators, XLB, and ATS collaborate to test functionality. A crucial aspect involves accumulating a sufficient volume of logs, spanning from one hour to a week, to rigorously assess CPR's efficacy with CI operator data. During this period, both CI operators and XLB will undertake the critical tasks of model training and inference. Once an adequate dataset is amassed for real data analysis, typically within a week, CI operators and XLB resume model training and inference to ensure accuracy, together with ATS, as processing of alarms coming from Anomaly Detection Module is done in CERCA and AIRE. Finally, CI operators will conduct periodic testing to uphold continuous performance evaluation and refinement. Each phase reflects a meticulous approach aimed at guaranteeing the reliability and efficacy of the CPR tool within the CI ecosystem.

5 Pilot trials execution

The developed CPR tool needs to provide useful functionality to CI operators and at the same time to reduce CI operator workload required to achieve goals. The pilot trials are planned to show the tool to CI partners, to test deployment in operational environment, to test operational procedures, and to give CI operators an opportunity for early hands-on evaluation.

The main goal of preliminary test on real data is to see if tools are functional and if there are problems that could prevent or make difficult CPR tool installation and subsequent usage in an operational environment. These problems need to be discovered and properly addressed.

The description of the users, their roles within critical infrastructure operators, with their required expertise is given in Section 1.5.

5.1 Pilot Execution Plans

In D6.2[2] was already present initial plan for pilot execution. Those plans are largely unmodified. Here we keep their description to ensure completeness of the document.

5.1.1 Italy: Public Administration

INS plans to test the tools developed in WP6 on a specific part of its regional infrastructure. This subset includes VPN Servers used by INS employees and the SESAMO application, which collects health-related data of citizens in the Region Friuli Venezia Giulia. Access to SESAMO is controlled through federated systems like national SPID and Electronic ID Cards. The testing process will happen in three phases:

Phase 0 (M12): A Proof of Concept will simulate incoming logs from selected applications to identify potential threats to the systems under analysis.

Phase 1 (M23): The tools will be deployed within INS to integrate and aggregate logs with the existing SIEM (Security Information and Event Management) system, which is the Community Edition in the testing environment. Additionally, integrations with the current MISP appliance in the INS infrastructure may be explored to enhance Cyber Threat Intelligence sharing between the Firewall and SIEM. The AIRE functionalities will be integrated to generate incident reports for managing the Incident Response process.

Phase 2 (M34): The tools will be piloted in the operational environment of INS. The tools' output will be monitored using real data from the applications under analysis, as well as simulated data for vulnerability tests. The INS Blue Team might oversee these operations.

In summary, INS aims to test WP6 tools on a specific part of its regional infrastructure, including VPN Servers and the SESAMO application. The testing will progress through phases, beginning with a Proof of Concept, followed by integration with SIEM and MISP, and concluding with operational environment monitoring.

5.1.2 Italy: Water

CAFC intends to test the tools developed by WP6 on its VPN infrastructure to detect and halt suspicious network activities. The VPN system, which has gained crucial importance due to the COVID-19 pandemic, was previously used by a limited group of technical users for a decade. However, it has now become the standard means for employees to remotely access various systems.

For the purpose of training and testing, CAFC will provide logs including network traffic, antispam filter records, antivirus data, and results from ongoing penetration tests.

The testing process will involve these key steps:

Phase 0 (M12): A Proof of Concept will showcase the tools' ability to identify potential threats to the systems being examined through simulated incoming log data.

Phase 1 (M23): The tools will be implemented within CAFC to demonstrate how logs are acquired and analysed.

Phase 2 (M34): CAFC will carry out a trial of the tools in their actual operational environment. This will involve monitoring the tools' output using real data and potentially simulating threats to the VPN infrastructure. The goal is to assess the tools' effectiveness.

To sum up, CAFC plans to test WP6 tools on its VPN system for detecting suspicious network behaviour. The VPN's significance has increased due to the pandemic, and the testing will proceed through phases involving Proof of Concept, deployment, and operational evaluation.

5.1.3 Slovenia: Telecommunication

TS plans to evaluate the WP6-developed tools on a specific segment of its infrastructure associated with the VALU mobile application's accesses and activities. The testing process will follow an iterative approach, involving the following phases:

Phase 0 (M12): The initial Proof of Concept will showcase the tools' ability to detect potential threats within the analysed systems. This will be done by simulating incoming log data from the selected application.

Phase 1 (M23): The tools will be implemented within TS's environment to demonstrate how logs can be integrated and aggregated between the new tools and the existing SIEM monitoring system (Community Edition) that's already in operation within TS.

Phase 2 (M34): In this phase, TS will put the tools to the test within its operational setup. The tools' performance will be monitored using both real data from the applications under analysis and simulated data. For instance, simulated vulnerability tests using known patterns might be conducted. These activities could be supervised by TS's advanced payment and cybersecurity teams.

In summary, TS will assess WP6 tools on a specific infrastructure section linked to the VALU mobile app. The evaluation will occur in iterative stages, comprising Proof of Concept, deployment with log integration, and operational assessment with real and simulated data under the watch of specialized teams.

5.1.4 Slovenia: Transport

As Slovenian transport operators (SZ-SZI), the organization plans to evaluate WP6-developed tools on a specific component of the railway infrastructure referred to as PRI. This component is the railway traffic monitoring system, known as ISSŽP. The system encompasses numerous services and applications designed to monitor real-time events occurring along the railway infrastructure. These events pertain to both freight and passenger transportation. Certain applications facilitate bidirectional data exchange and communication with external carriers, enabling comprehensive real-time management and monitoring of the railway infrastructure.

The testing process will adhere to an iterative approach with the following stages:

Phase 0 (M12): The initial Proof of Concept will illustrate the tools' capability to identify potential threats within the analysed system. This will involve simulating incoming log data from the chosen system.

Phase 1 (M23): The tools will be implemented within SZ-SZI's environment to showcase the integration and aggregation of logs between the proposed tools and the existing railway monitoring system (ISSŽP).

Phase 2 (M34): SZ-SZI will undertake a pilot of the tools within its operational setup. The tools' performance will be observed using both actual data sourced from the applications under examination and simulated data. This could encompass attempts to conduct vulnerability tests on the applications using recognized patterns. These activities may be overseen by SZ-SZI's technical department.

In summary, SZ-SZI, acting as Slovenian transport operators, intends to assess WP6 tools on a specific railway infrastructure asset known as PRI. This asset encompasses the ISSŽP railway traffic monitoring system with various applications. The assessment process will involve iterative stages of Proof of Concept, deployment with log integration, and operational evaluation under the potential supervision of SZ-SZI's technical department.

5.2 Description of End-Users' Roles

User Organization / ROLE	Profile	Skills	CPR tools interaction Description
Authorities			
Government - institutional level decision maker	Strategic	knowledge of policies, competences	May use reports from CPR dashboard to promote policies or strategies that give authority to CI operators or other institutions to define temporary measures (e.g. increase level of access control, introduce remote working)
CI high level decision maker / operator	Strategic	Knowledge of CI and sector business, knowledge of IT infrastructure and services that support CI	May use reports from CPR dashboard to analyse cyber-physical risks related to regions, sectors, and specific CI. They might also decide on how to generate and share risk indicators, and information about threats, techniques, tactics, and procedures, as well as incident reporting protocols.
CI operator			
CI legal and compliance team			
Legal Manager	Tactical	knowledge of policies, knowledge of laws, strategies	Creates reporting directives and procedures based on the strategies and compliance needs of the CI operators. Adapts reporting templates to the case of the CI, deciding which fields are necessary and relevant or which information should be anonymized before sharing.
Legal User	Operational	knowledge of GDPR/NIS 2 reporting protocols	Analyses whether the incident meets the criteria to be reported. Anonymizes the information shared. Ensures that all necessary information is available.
CI risk management team			

Business Risk Manager	Tactical	general risk management skills	Creates cyber risk management procedures based on strategic directives. Defines the cyber infrastructure risk model to assess the effects of a cyber-physical incident and to be able to evaluate the risk/impact. If business or strategic priority is changed during pandemics, adapts data on estimated impact. Provides feedback about tactical level threat information (e.g. observed tactics and techniques of an attacker)
Risk Operator	Operational	Cyber risk analysis	Operates CyberRisk assessment Calculator (CERCA) tool e.g. configuration, manual data inputs where needed, etc. Provides feedback about operational level indicators (e.g. completeness, timeliness etc)
CI Incident Response and security operation team			
IRM/SOC/CERT Manager	Tactical	knowledge of cyber-attacks, knowledge of internal architecture	Defines rules to monitor and detect different threats and decides about response actions, also considering the inputs and priorities received from the Business Risk Manager. It also decides on cyberthreat intelligence (CTI) sharing policies and makes analysis (in collaboration with the other CIs) about adversary tactics, techniques, and procedures (TTP)
IRM/SOC/CERT operator	Operational	knowledge of infrastructure and normal behaviour patterns, knowledge of security countermeasures	Monitors CI cyber assets/services, detecting unusual behaviour. Applies some countermeasures (e.g. fast response such as blocking access) against threats and obtains evidence of incidents for reporting. Shares operational level CTI (indicators of compromise)
IT department			
Administrator	Operational	configuration of CPR tools, access control	Administers CPR tools (LOMOS, CERCA, AIRE…), creating and administrating users

6 Conclusions

Cyber-physical resilience tool design and testing corresponds to the fact that critical infrastructures have evolved during the last years, bringing a wider exposure to attacks, while the pandemic experience revealed new interconnected risk inputs and indicators that must be considered in risk models.

To address the existing, as well as new challenges and gaps related to the operation of CIs and cyber-physical security in temporary conditions such as pandemics, we combine several tools, including anomaly detection, incident reporting, tailored threat intelligence management and semi-automated risk assessment, enhanced by the so-called OODA loop (Observe, Orient, Decide, Act) approach.

This deliverable presents this SUNRISE Cyber-Physical Resilience Tool (CPR Tool) and its modules. It extends and updates description of the tool, given in the previous D6.1[1] and D6.2[2] deliverables. While in former deliverables architecture, piloting and initial tests on the publicly available data are presented, this deliverable also extends this information with validation of the tool on real data provided by the end users and describes additionally the main innovations, as well as the infrastructure needs, such as capturing live log data.

Use of the real data from CI operators showed that we can find anomalies in multiple layers - ranging from resource (e.g. virtual infrastructure) to application layer. This demonstrates the usefulness of the approach in detecting the anomalies, which are subsequently used as an input to risk module (CERCA) next to the other inputs, including the external threat intelligence received from the open sources (e.g. health related information) or other CI operators (e.g. IoC or TTP). We describe approach that combines sensing (“observation”) of internal and external environment (incidents, anomalies, threats…), with a cognitive process of “orientation”, to make an optimal decision. Observation works with outside- in sensory information, while orientation works with inside-out created cyber-physical risk landscape, in order to model what could be suspicious behaviour and a possible threat. In this way, we aim to address not only known risks, but also “unknown unknowns”.

The updates also include risk values re-assessment based on input data, such as Indicators of compromise (IoC) received from TINTED or change of values during temporary conditions such as pandemics. Inputs received from threat intelligence platforms (Indicators of compromise – IoC) are now enriched with assignation of different probabilities (likelihood that indicator could be evidence of an attack), based on threat score. In addition, there is a mapping to tactics, techniques and procedures (TTP) that improves strategic decision making.

Each critical infrastructure (CI) has a different risk context. Type of assets are different, and impacts can be different. Demand of critical goods or essential services or uncertain availability of skilled workers are examples of pandemic specific temporary conditions to be considered. Another novelty is inclusion of physical risk indicators, for example related to unauthorized access to hardware, or so called “shoulder surfing”. Furthermore, training and awareness, psychological or behavioural risks, trust, or workforce availability, are all considered in risk model. By combining many of these risk inputs, indicators and observations, each one with different probability (likelihood), we hope to reveal additional insights for optimized risk assessment, mitigation actions, as well as improved incident reporting that is aligned with the forthcoming NIS 2 Directive. Here, focus is on legal aspects required by different directives and extension of the AIRE component. We enhanced this module with additional communication capabilities, providing in-depth description of the new functionalities.

Finally, we describe the schedule of the future piloting activities. To demonstrate the system in the operational environment, we will install the CPR tool at the CIs premises: the four CI pilots from Italy and Slovenia, including public administration, water, telecommunication, and transport use cases.

An iterative, phased approach will be maintained throughout the lifetime of the project, ensuring proper integration, and testing of all the related tools.

When it comes to reporting and further documentation, Deliverable D6.3 will be followed by the final version, D6.5 and in between, reporting about the piloting activities execution will be provided (D6.4).

7 References

[1] **SUNRISE. D6.1** - Cyber-physical resilience conceptualization. Pablo de Juan. 2023.

[2] **SUNRISE. D6.2** - Cyber-physical resilience tool and training guide V1. Tomaž Martinčič. 2023.

[3] **SUNRISE. D3.2** - Requirements and designs, V2. George Tsakirakis. 2023.

[4] **P. He, J. Zhu, Z. Zheng and M. R. Lyu**, "Drain: An online log parsing approach with fixed depth tree," 2017 IEEE international conference on web services (ICWS), pp. 33-40, 2017.

[5] **H. Guo, S. Yuan and X. Wu**, "LogBERT: Log Anomaly Detection via BERT," 2021 international joint conference on neural networks (IJCNN), pp. 1-8, 2021.

[6] **J. Devlin, M. W. Chang, K. Lee and K. Toutanova**, "BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding," CoRR, vol. abs/1810.04805, 2018.

[7] **The NIS 2 Directive:** http://data.europa.eu/eli/dir/2022/2555/2022-12-27

[8] **ENSURESEC – D4.5**: Human, cyber & physical business components mapping tool. G. Gonzalez-Granadillo, J. Martinez, J. Torner, R. Diaz, A. Alvarez, J.J. De Vicente. 2021.

[9] **A. Oliner and J. Stearley**, "What Supercomputers Say: A Study of Five System Logs," 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN'07), pp. 575-584, 2007.

[10]**W. Xu, L. Huang, A. Fox, D. Patterson and M. I. Jordan**, "Detecting large-scale system problems by mining console logs," Proceedings of the ACM SIGOPS 22nd symposium on Operating systems principles, pp. 117-132, 2009.

[11]**CyberSec4Europe - D3.21** Framework to design and implement adaptive security systems. L. Pasquale and A. Hassan. 2022.

[12]**CORAS** The CORAS Method (sourceforge.net)

Annex I Training guide and user manual

This Annex covers the training guide and user manual for all CPR tool modules.

I.I Anomaly Detection

In this section, we present a step-by-step user guide for working with LOMOS. The first step is model training. The models are then used in the second step, log-based anomaly detection inference.

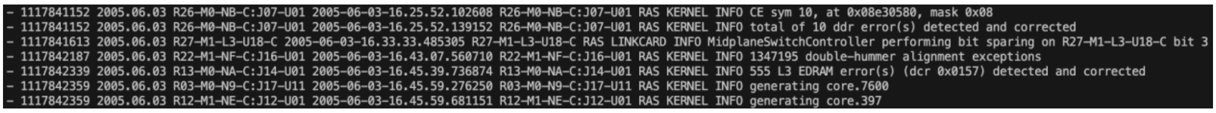
I.I.I Setting up data sources

Elasticsearch is often used as a central database for logs from different components of simple or complex systems. It is highly suitable for handling substantial amounts of data in distributed indices in JSON format, ensuring scalability and availability. Elastic Filebeat is a lightweight agent that can be used to push log data to Elasticsearch. LOMOS is capable of directly interacting with Elasticsearch. It can read data from it, process it, and write the results back.

To set up Filebeat agents, refer to the original and up-to-date documentation by Elastic[5]. Logs from different sources should be stored in separate indices and processed separately by the LOMOS. Elasticsearch has great support for data retention strategies. It is easy to set up the lifecycle policies in Kibana or through the REST endpoint[6].

I.I.II Training a log parser

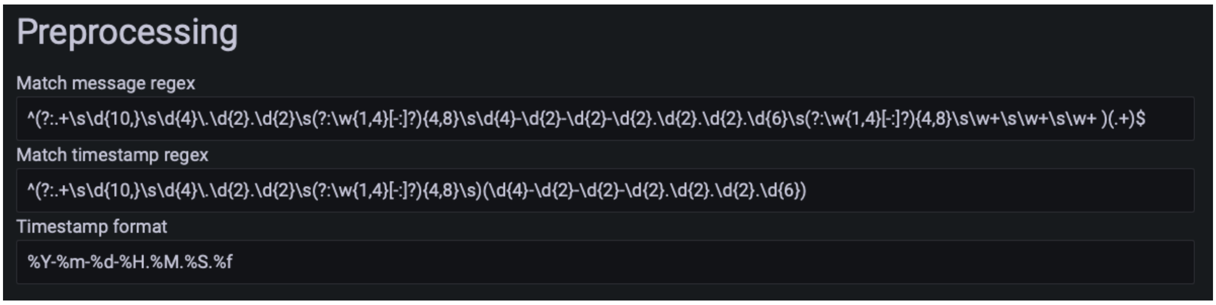
LOMOS can carry out some pre-processing steps on the logs. Logs are sometimes stored in a raw semi-structured format. In such a case, log messages and timestamps must be extracted first.



```
- 1117841152 2005.06.03 R26-M0-NB-C:J07-U01 2005-06-03-16.25.52.102608 R26-M0-NB-C:J07-U01 RAS KERNEL INFO CE sym 10, at 0x08e30580, mask 0x08
- 1117841152 2005.06.03 R26-M0-NB-C:J07-U01 2005-06-03-16.25.52.139152 R26-M0-NB-C:J07-U01 RAS KERNEL INFO total of 10 ddr error(s) detected and corrected
- 1117841613 2005.06.03 R27-M1-L3-U18-C 2005-06-03-16.33.33.485305 R27-M1-L3-U18-C RAS LINKCARD INFO MidplaneSwitchController performing bit sparing on R27-M1-L3-U18-C bit 3
- 1117842187 2005.06.03 R22-M1-NF-C:J16-U01 2005-06-03-16.43.07.560710 R22-M1-NF-C:J16-U01 RAS KERNEL INFO 1347195 double-hummer alignment exceptions
- 1117842339 2005.06.03 R13-M0-NA-C:J14-U01 2005-06-03-16.45.39.736874 R13-M0-NA-C:J14-U01 RAS KERNEL INFO 555 L3 EDRAM error(s) (dcr 0x0157) detected and corrected
- 1117842359 2005.06.03 R03-M0-N9-C:J17-U11 2005-06-03-16.45.59.276250 R03-M0-N9-C:J17-U11 RAS KERNEL INFO generating core.7600
- 1117842359 2005.06.03 R12-M1-NE-C:J12-U01 2005-06-03-16.45.59.681151 R12-M1-NE-C:J12-U01 RAS KERNEL INFO generating core.397
```

Figure 18. A sample of raw BGL logs.

The extraction of the relevant data can be performed by setting the regular expressions in the pre-processing step, as in Figure 19.



Preprocessing

Match message regex

```
^(?:.+\s\d{10,}\s\d{4}\.\d{2}.\d{2}\s(?:\w{1,4}[-:]?){4,8}\s\d{4}-\d{2}-\d{2}-\d{2}.\d{2}.\d{2}.\d{6}\s(?:\w{1,4}[-:]?){4,8}\s\w+\s\w+\s\w+ )(.+)$
```

Match timestamp regex

```
^(?:.+\s\d{10,}\s\d{4}\.\d{2}.\d{2}\s(?:\w{1,4}[-:]?){4,8}\s)(\d{4}-\d{2}-\d{2}-\d{2}.\d{2}.\d{2}.\d{6})
```

Timestamp format

```
%Y-%m-%d-%H.%M.%S.%f
```

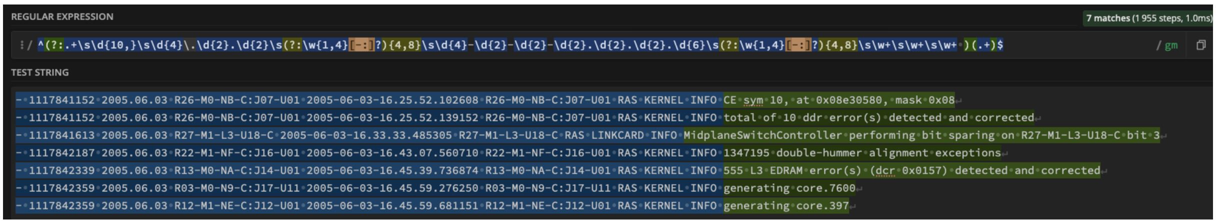
Figure 19. Regular expressions for extracting messages and timestamps from raw logs and the timestamp format.

We generated the regular expressions with the help of the regex101[7] tool (Figure 20 and Figure 21). Based only on the sample of the logs, regular expressions could be simpler; however, this would raise the risk of falsely identifying the components of the logs. In the case that the data is already structured in the Elasticsearch index, we can put a regular expression that matches the whole line “^(.+)$” and leave the other two fields empty.

[5] https://www.elastic.co/guide/en/beats/filebeat/7.17/index.html

[6]https://www.elastic.co/guide/en/elasticsearch/reference/current/getting-started-index-lifecycle-management.html

[7] https://regex101.com



REGULAR EXPRESSION

7 matches (1 955 steps, 1.0ms)

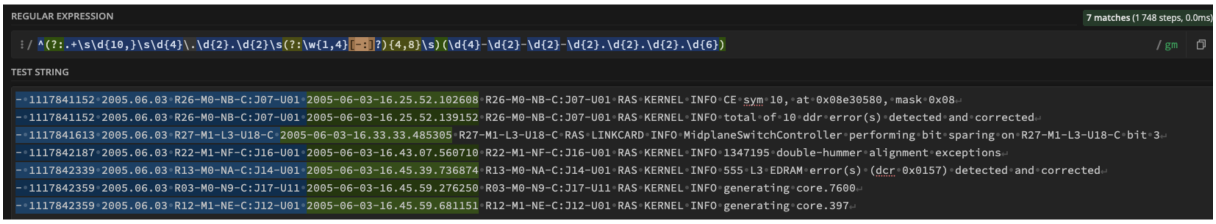
```
^(?:.+\s\d{10,}\s\d{4}\.\d{2}.\d{2}\s(?:\w{1,4}[-:]?){4,8}\s\d{4}-\d{2}-\d{2}-\d{2}.\d{2}.\d{2}.\d{6}\s(?:\w{1,4}[-:]?){4,8}\s\w+\s\w+\s\w+ )(.+)$
```

/ gm

TEST STRING

```
- 1117841152 2005.06.03 R26-M0-NB-C:J07-U01 2005-06-03-16.25.52.102608 R26-M0-NB-C:J07-U01 RAS KERNEL INFO CE sym 10, at 0x08e30580, mask 0x08
- 1117841152 2005.06.03 R26-M0-NB-C:J07-U01 2005-06-03-16.25.52.139152 R26-M0-NB-C:J07-U01 RAS KERNEL INFO total of 10 ddr error(s) detected and corrected
- 1117841613 2005.06.03 R27-M1-L3-U18-C 2005-06-03-16.33.33.485305 R27-M1-L3-U18-C RAS LINKCARD INFO MidplaneSwitchController performing bit sparing on R27-M1-L3-U18-C bit 3
- 1117842187 2005.06.03 R22-M1-NF-C:J16-U01 2005-06-03-16.43.07.560710 R22-M1-NF-C:J16-U01 RAS KERNEL INFO 1347195 double-hummer alignment exceptions
- 1117842339 2005.06.03 R13-M0-NA-C:J14-U01 2005-06-03-16.45.39.736874 R13-M0-NA-C:J14-U01 RAS KERNEL INFO 555 L3 EDRAM error(s) (dcr 0x0157) detected and corrected
- 1117842359 2005.06.03 R03-M0-N9-C:J17-U11 2005-06-03-16.45.59.276250 R03-M0-N9-C:J17-U11 RAS KERNEL INFO generating core.7600
- 1117842359 2005.06.03 R12-M1-NE-C:J12-U01 2005-06-03-16.45.59.681151 R12-M1-NE-C:J12-U01 RAS KERNEL INFO generating core.397
```

Figure 20. Regular expression for extracting log message from a raw log.



REGULAR EXPRESSION

7 matches (1 748 steps, 0.0ms)

```
^(?:.+\s\d{10,}\s\d{4}\.\d{2}.\d{2}\s(?:\w{1,4}[-:]?){4,8}\s)(\d{4}-\d{2}-\d{2}-\d{2}.\d{2}.\d{2}.\d{6})
```

/ gm

TEST STRING

```
- 1117841152 2005.06.03 R26-M0-NB-C:J07-U01 2005-06-03-16.25.52.102608 R26-M0-NB-C:J07-U01 RAS KERNEL INFO CE sym 10, at 0x08e30580, mask 0x08
- 1117841152 2005.06.03 R26-M0-NB-C:J07-U01 2005-06-03-16.25.52.139152 R26-M0-NB-C:J07-U01 RAS KERNEL INFO total of 10 ddr error(s) detected and corrected
- 1117841613 2005.06.03 R27-M1-L3-U18-C 2005-06-03-16.33.33.485305 R27-M1-L3-U18-C RAS LINKCARD INFO MidplaneSwitchController performing bit sparing on R27-M1-L3-U18-C bit 3
- 1117842187 2005.06.03 R22-M1-NF-C:J16-U01 2005-06-03-16.43.07.560710 R22-M1-NF-C:J16-U01 RAS KERNEL INFO 1347195 double-hummer alignment exceptions
- 1117842339 2005.06.03 R13-M0-NA-C:J14-U01 2005-06-03-16.45.39.736874 R13-M0-NA-C:J14-U01 RAS KERNEL INFO 555 L3 EDRAM error(s) (dcr 0x0157) detected and corrected
- 1117842359 2005.06.03 R03-M0-N9-C:J17-U11 2005-06-03-16.45.59.276250 R03-M0-N9-C:J17-U11 RAS KERNEL INFO generating core.7600
- 1117842359 2005.06.03 R12-M1-NE-C:J12-U01 2005-06-03-16.45.59.681151 R12-M1-NE-C:J12-U01 RAS KERNEL INFO generating core.397
```

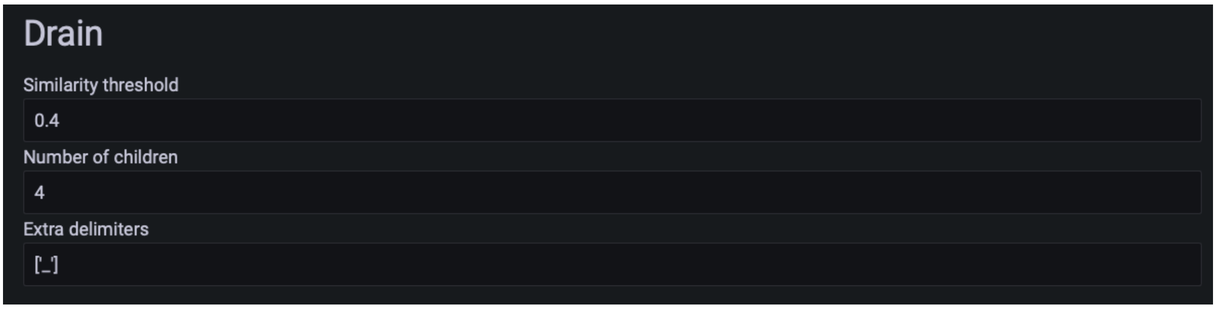
Figure 21. Regular expression for extracting timestamp from a raw log.

The next set of parameters is related to the Drain method which extracts log templates from log messages (Figure 22):

Similarity threshold sets the minimal Jaccard index of log message words for them to match into the same log template.

The number of children sets the depth of the Drain search tree. It specifies how many initial words in a log must be an exact match for a log template. Increasing this number generally accelerates the Drain process. Nevertheless, a too-high value could lead to the incorrect identification of potential parameters located at the beginning of a log.

Extra delimiters can add more characters for splitting the message string into words. For example, we can add an underscore, which will be used beside the default space character.



Drain

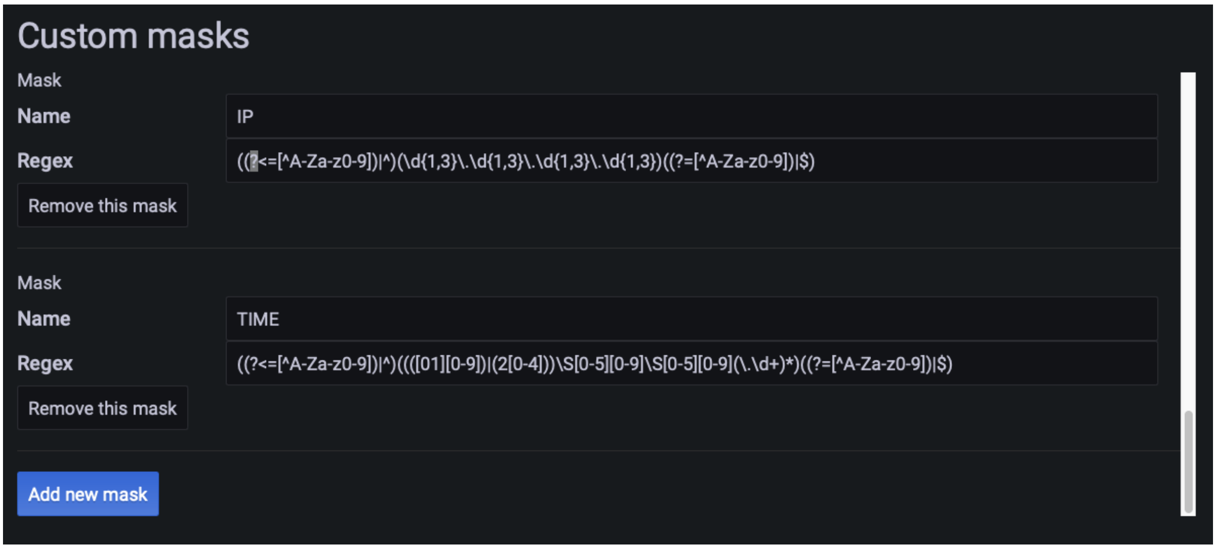
Similarity threshold: 0.4

Number of children: 4

Extra delimiters: [_]

Figure 22. Drain parameters.

Next, we add custom regular expressions for masking complex patterns, such as IP addresses or timestamps. Drain is used for automatic parameter extraction; however, it works better if we add some general or tailored regular expressions, like in Figure 23.



Custom masks

Mask

Name IP

Regex `((?<=[^A-Za-z0-9])|^)(\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})((?=[^A-Za-z0-9])|$)`

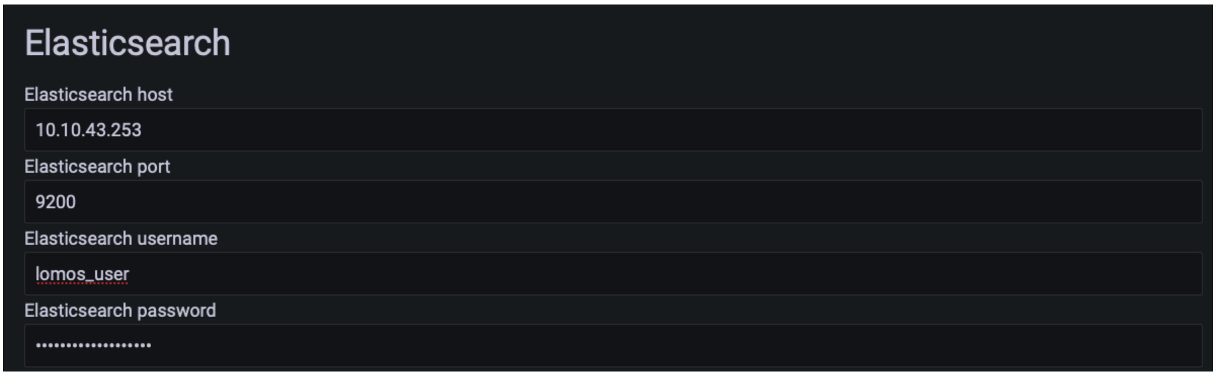
Mask

Name TIME

Regex `((?<=[^A-Za-z0-9])|^)((([01][0-9])|(2[0-4]))\S[0-5][0-9]\S[0-5][0-9](\.\d+)*)((?=[^A-Za-z0-9])|$)`

Figure 23. Custom masks for complex parameters.

The next section is used for setting the connection to Elasticsearch. We must define the IP address, port, and credentials (Figure 24). Leave the credentials empty if they are not required by the selected Elasticsearch deployment.



Elasticsearch

Elasticsearch host
10.10.43.253

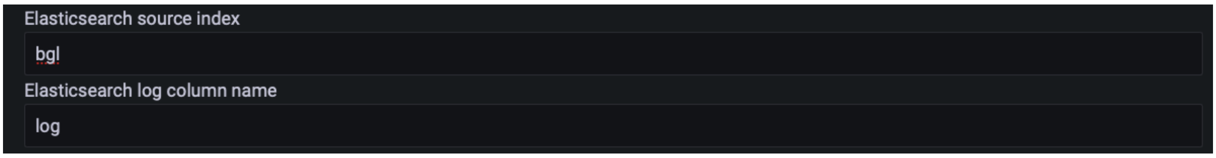
Elasticsearch port
9200

Elasticsearch username
lomos_user

Elasticsearch password
•••••••••••••••••••

Figure 24. Log parser training Elasticsearch connection details and credentials.

Next, we set the source index and message column names (Figure 25).

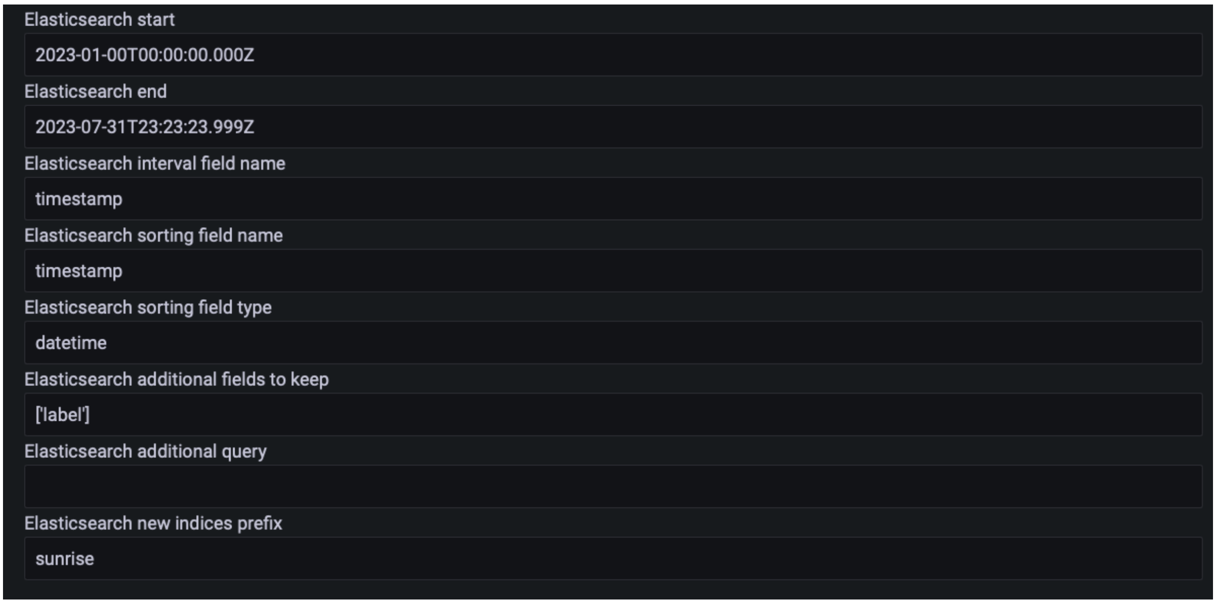


Elasticsearch source index
bgl

Elasticsearch log column name
log

Figure 25. Log parser training source index.

Thereafter, we must select the data with the next set of parameters, as seen in Figure 26. First, select the period we will use for training and the field that will be used for filtering (timestamp or id). Additional Elasticsearch filters can be used to select only the relevant data. The prefix is used to set the name of new indices and is required later in the model training step to reference the parsed data. To start the training, click on the run parser button.



Elasticsearch start

2023-01-00T00:00:00.000Z

Elasticsearch end

2023-07-31T23:23:23.999Z

Elasticsearch interval field name

timestamp

Elasticsearch sorting field name

timestamp

Elasticsearch sorting field type

datetime

Elasticsearch additional fields to keep

['label']

Elasticsearch additional query

Elasticsearch new indices prefix

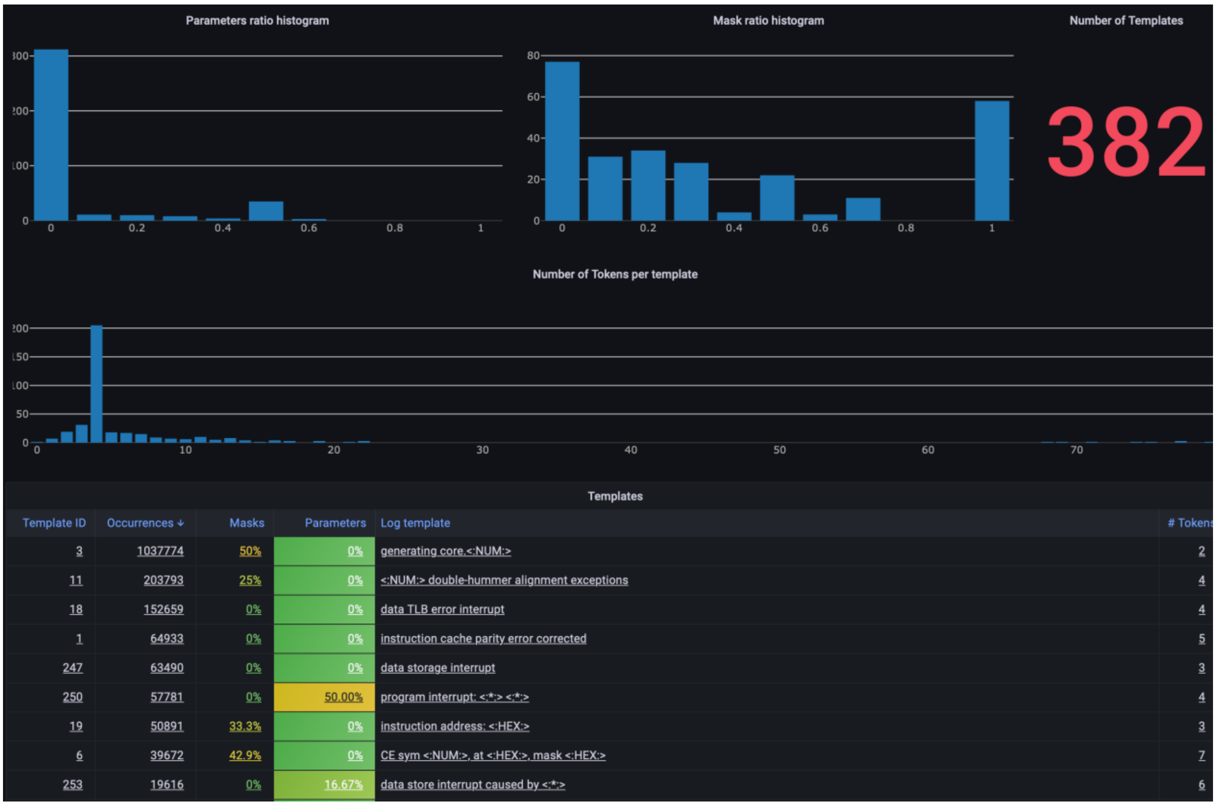
sunrise

Figure 26. Log parser training period selection and addition filters.

I.I.III Inspecting the log parsing results

Once the log parser is trained it is used on the training data to parse the log templates and push them to a new index in Elasticsearch where the name of the index is generated based on the prefix set by the user in the previous step, source index name, and "_logs structured" suffix. Another index is created which stores the unique log templates and relevant statistics describing their frequency and number of detected parameters. The suffix for this index is "_events". The example from the previous step generates "sunrise_bgl_logs_structured" and "sunrise_bgl_events" indices. The data is automatically accessible from the Grafana dashboard, where it can be explored through interactive visualizations. The user can evaluate if the log templates are parsed correctly and proceed with training the model or return to the previous step to adapt the parameters of the log parser and rerun the log parser training.

The first dashboard offers users an overview of the parsed log templates (Figure 27). There are two histograms in the upper row, showing the distributions of the ratio between automatically extracted parameters to the number of words and masked parameters by the regular expressions to the number of words. The number on the right side shows the number of the unique extracted log templates. The histogram below shows the distribution of log message length (number of words). Finally, there is a table of extracted log templates at the bottom, together with relevant statistics. Users can check the statistics from the charts above for each of the log templates.

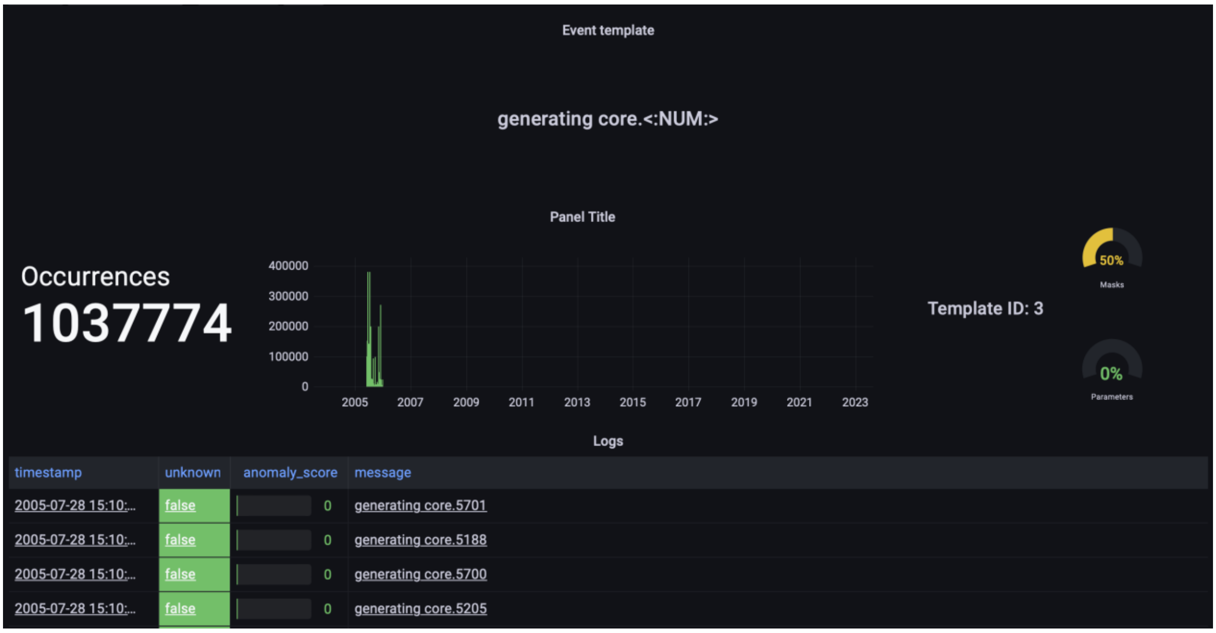


Templates

Template ID	Occurrences ↓	Masks	Parameters	Log template	# Tokens
3	1037774	50%	0%	generating core.<:NUM:>	2
11	203793	25%	0%	<:NUM:> double-hummer alignment exceptions	4
18	152659	0%	0%	data TLB error interrupt	4
1	64933	0%	0%	instruction cache parity error corrected	5
247	63490	0%	0%	data storage interrupt	3
250	57781	0%	50.00%	program interrupt: <:*:> <:*:>	4
19	50891	33.3%	0%	instruction address: <:HEX:>	3
6	39672	42.9%	0%	CE sym <:NUM:>, at <:HEX:>, mask <:HEX:>	7
253	19616	0%	16.67%	data store interrupt caused by <:*:>	6

Figure 27. Extracted log templates overview.

Users can click on the extracted log template, to view its details, as seen in Figure 28. Besides the statistics already mentioned above, user can see actual log messages and their occurrences through time.



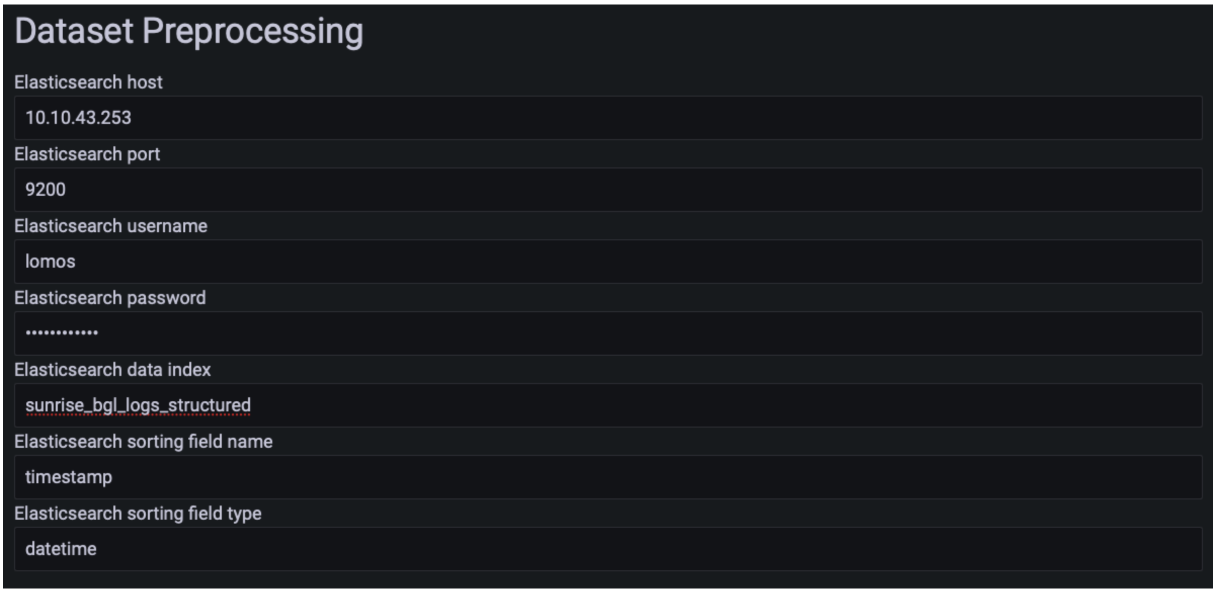
Logs

timestamp	unknown	anomaly_score	message
2005-07-28 15:10:...	false	0	generating core.5701
2005-07-28 15:10:...	false	0	generating core.5188
2005-07-28 15:10:...	false	0	generating core.5700
2005-07-28 15:10:...	false	0	generating core.5205

Figure 28. Log template details.

I.I.IV Training an anomaly detection model

When the log templates are properly parsed, we can proceed to train an anomaly detection model. The first part, shown in Figure 29, is dedicated to the Elasticsearch connection settings and the name of the structured logs index, which was explained in the previous step. The next two fields are used for the proper sorting of the logs.



Dataset Preprocessing

Elasticsearch host: 10.10.43.253

Elasticsearch port: 9200

Elasticsearch username: lomos

Elasticsearch password: ••••••••••••

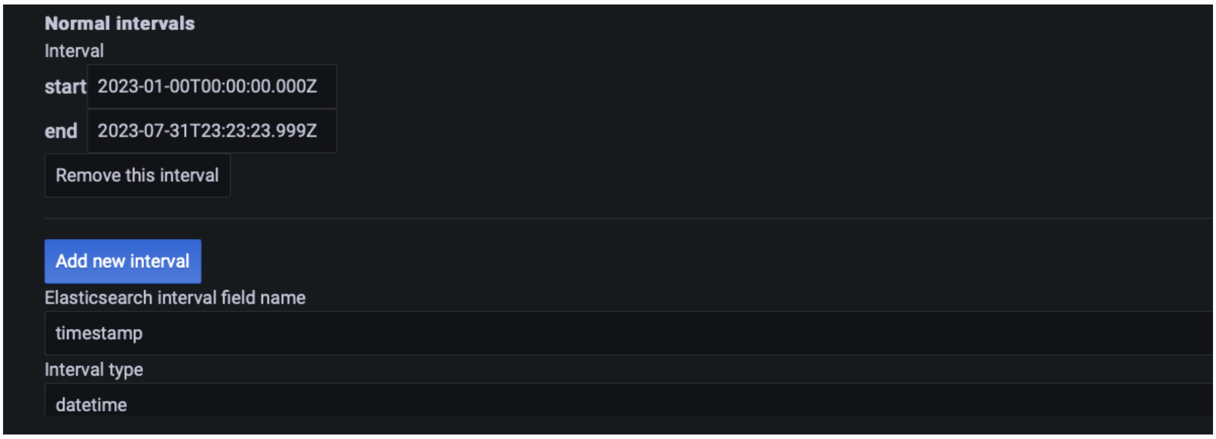
Elasticsearch data index: sunrise_bgl_logs_structured

Elasticsearch sorting field name: timestamp

Elasticsearch sorting field type: datetime

Figure 29. Model training Elasticsearch connection details, credentials, and filters.

To conclude the section related to data, we must select the periods that will be used for training the model, as shown in Figure 30. At least one period is mandatory, but multiple can be set. Such a feature becomes useful when we want to skip (potentially) anomalous data. If we are aware of an anomaly that influenced the logs, we should exclude it from the training set.



Normal intervals

Interval

start 2023-01-00T00:00:00.000Z

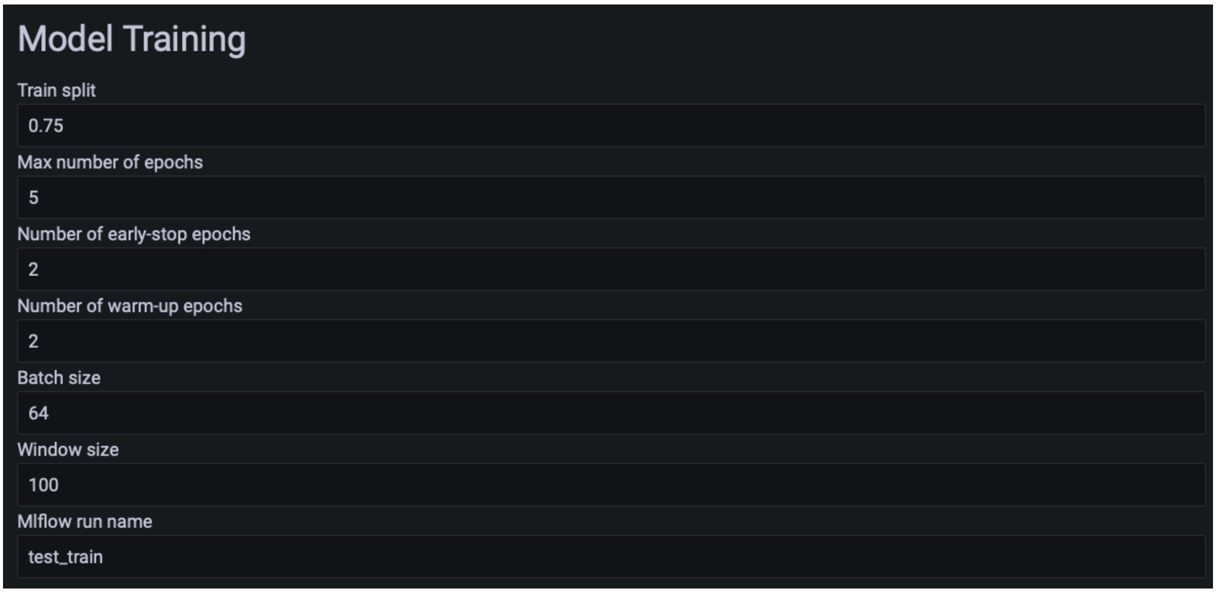
end 2023-07-31T23:23:23.999Z

Elasticsearch interval field name: timestamp

Interval type: datetime

Figure 30. Training data intervals.

The next set of parameters are machine learning hyperparameters (Figure 31). We must set the percentage of data used for training, where the left-out data is used for validation during the training. Next, we set the maximum number of epochs and early stop conditions. Thereafter, we set the number of warm-up epochs, batch size, and window size. The last parameter is the name of the experiment for MLflow tracking. The correct values depend on the amount and complexity of data.



Model Training

Train split

0.75

Max number of epochs

5

Number of early-stop epochs

2

Number of warm-up epochs

2

Batch size

64

Window size

100

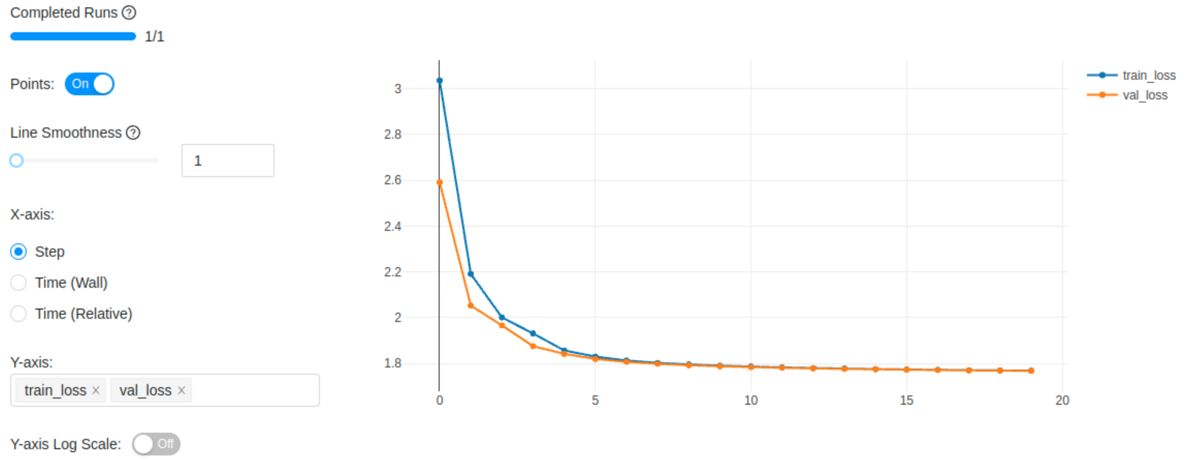
Mlflow run name

test_train

Figure 31. Anomaly detection model training hyperparameters.

I.I.V Inspecting the training results

The training process can be monitored through the MLflow web dashboard. One of the more important indicators is train and validation losses. MLflow enables users to explore those metrics in an interactive chart. Both train and validation losses should decay similarly, as seen in Figure 32.



Completed Runs ⓘ 1/1

Points: On

Line Smoothness ⓘ 1

X-axis:

● Step

○ Time (Wall)

○ Time (Relative)

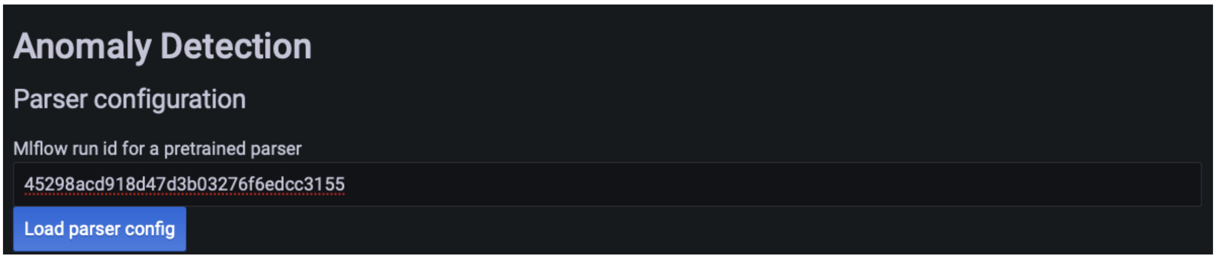
Y-axis: train_loss × val_loss ×

Y-axis Log Scale: Off

Figure 32. Training anomaly detection loss chart displayed in MLflow.

I.I.VI Setting up live inference

Once the log template extraction and anomaly detection training phase are concluded, we can use the model for inference on new data. First, we load the parser configuration (Figure 33) by the MLflow experiment ID. The ID can be found in the MLflow web dashboard.



Anomaly Detection

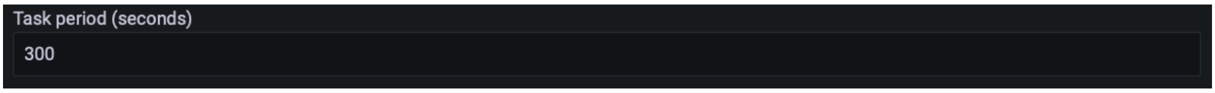
Parser configuration

Mlflow run id for a pretrained parser

45298acd918d47d3b03276f6edcc3155

Figure 33. Pretrained parser MLflow experiment id.

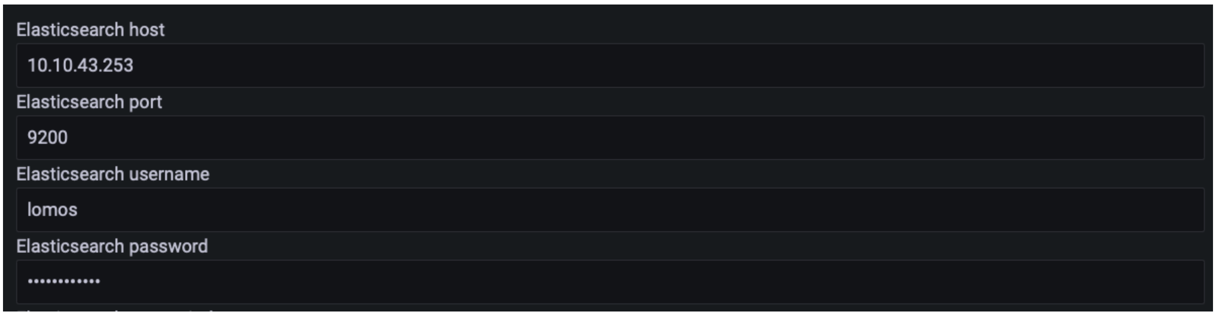
Next, we set the inference task period in seconds. If we want to execute the job only once, we leave the field empty. In Figure 34 we set the job to execute every five minutes.



Task period (seconds)
300

Figure 34. Set the inference schedule period.

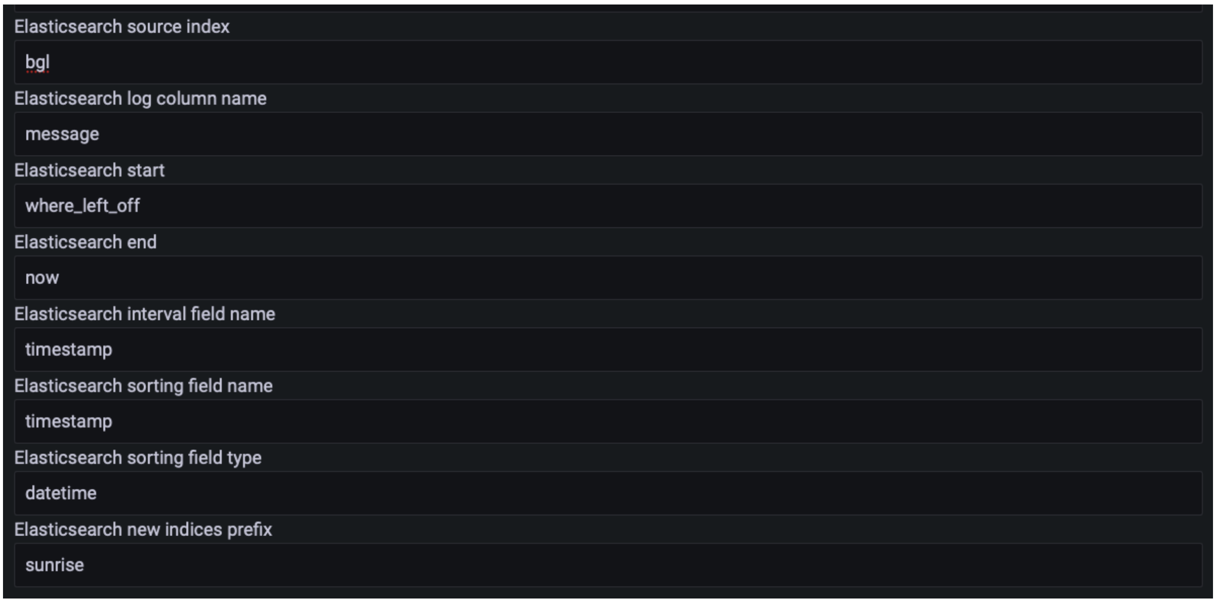
Thereafter, we again set the Elasticsearch endpoint details and credentials as seen in Figure 35.



Elasticsearch host
10.10.43.253
Elasticsearch port
9200
Elasticsearch username
lomos
Elasticsearch password
••••••••••••

Figure 35. Anomaly detection inference ElasticSearch endpoint details and credentials.

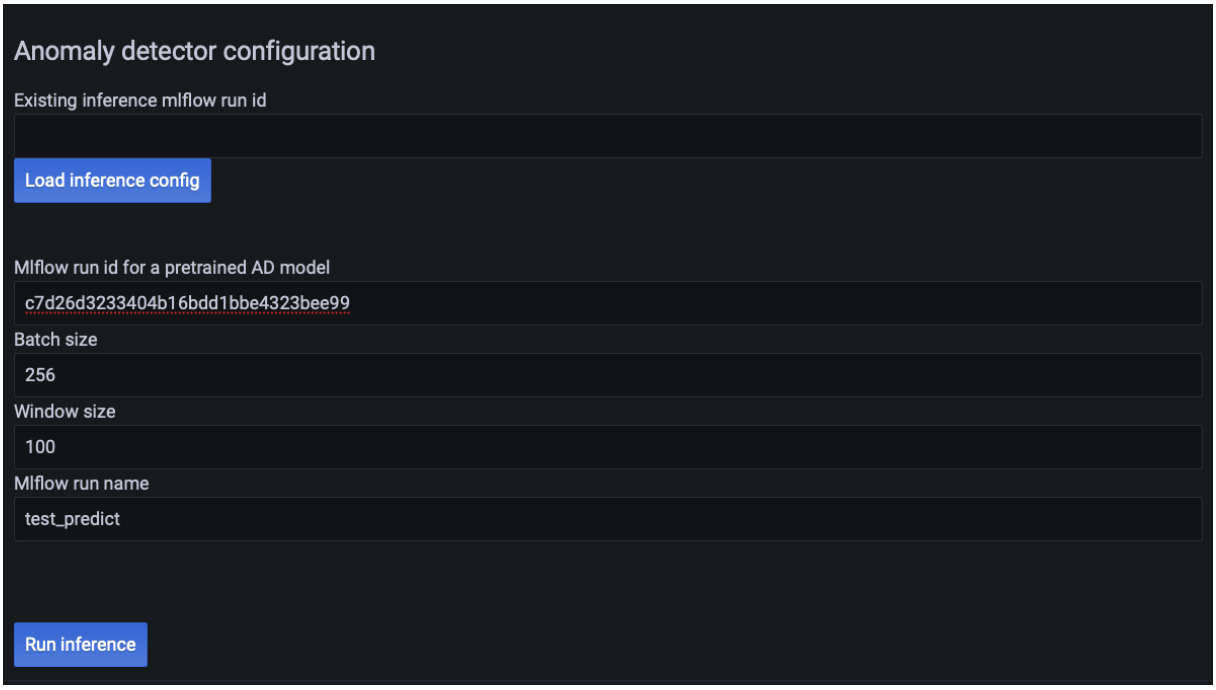
Next, we set the name of the index with logs and the name of the log message column. Thereafter, we must select the period of data that we will pass through the anomaly detector. We can again use timestamps, numerical index, or special keywords: “where_left_off” and “now”. Those two keywords are useful for periodical jobs and will ensure the processing of new data at each execution. The configuration example is shown in Figure 36.



Elasticsearch source index
bgl
Elasticsearch log column name
message
Elasticsearch start
where_left_off
Elasticsearch end
now
Elasticsearch interval field name
timestamp
Elasticsearch sorting field name
timestamp
Elasticsearch sorting field type
datetime
Elasticsearch new indices prefix
sunrise

Figure 36. Elasticsearch index configuration and data filters.

Finally, we set the MLflow run ID of the trained model, batch size, window size, and MLflow run name as seen in Figure 37. To run the inference, click on the “Run inference” button.



Anomaly detector configuration

Existing inference mlflow run id

Load inference config

Mlflow run id for a pretrained AD model

c7d26d3233404b16bdd1bbe4323bee99

Batch size

256

Window size

100

Mlflow run name

test_predict

Run inference

Figure 37. Inference model configuration.

I.I.VII Inspecting live inference results

We finally get to inspect the live results. The default dashboard is presented below, but it is highly customizable since it is based on Grafana. In the first chart (Figure 38), we show log count through time.

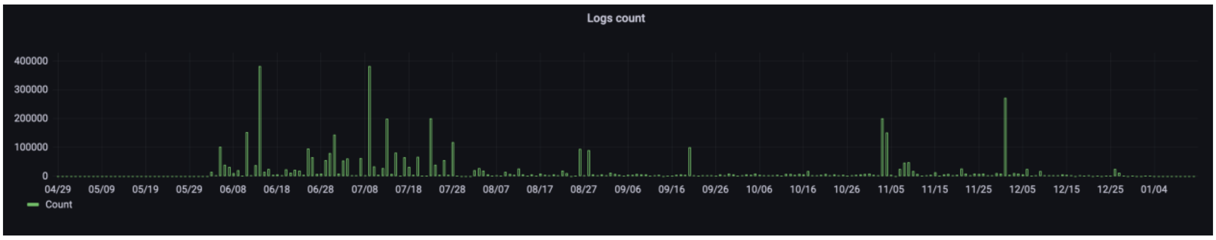


Figure 38. Histogram of logs through time (e.g., per day).

Next, we show the average anomaly score as seen in Figure 39.

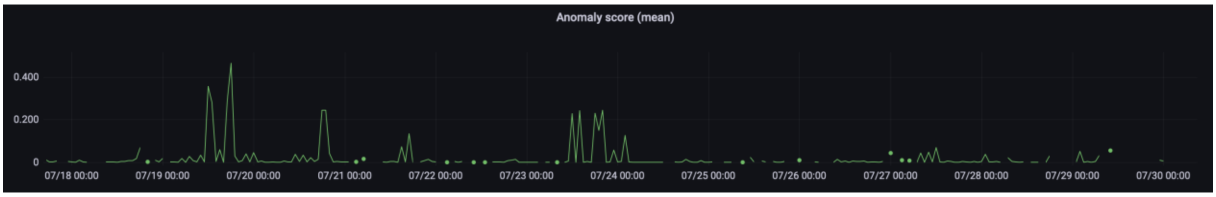


Figure 39. Average anomaly score.

For a better overview of the number of anomalies, charts like those in Figure 40 are useful. This chart shows the count of logs with high anomaly scores. The threshold is customizable and set to 0.7 as a default value.

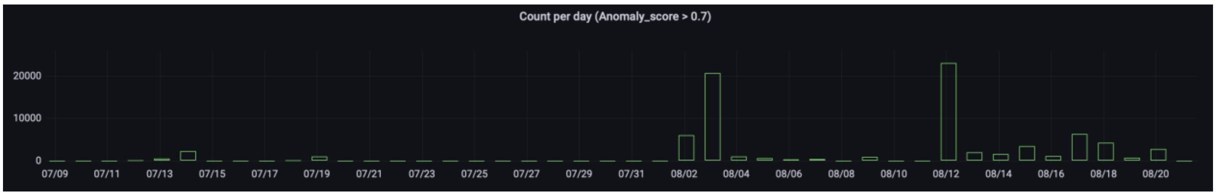
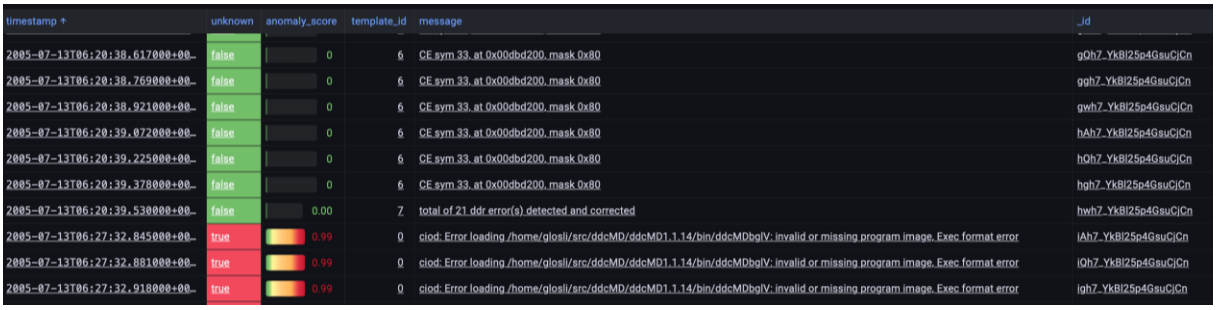


Figure 40. Number of logs with high anomaly score (e.g., above 0.7).

The table at the bottom of the dashboard (Figure 41) shows information about timestamps, log messages, log templates, anomaly scores, and whether the log template was recognized or not.



timestamp ↑	unknown	anomaly_score	template_id	message	_id
2005-07-13T06:20:38.617000+00…	false	0	6	CE sym 33, at 0x00dbd200, mask 0x80	gQh7_YkBI25p4GsuCjCn
2005-07-13T06:20:38.769000+00…	false	0	6	CE sym 33, at 0x00dbd200, mask 0x80	ggh7_YkBI25p4GsuCjCn
2005-07-13T06:20:38.921000+00…	false	0	6	CE sym 33, at 0x00dbd200, mask 0x80	gwh7_YkBI25p4GsuCjCn
2005-07-13T06:20:39.072000+00…	false	0	6	CE sym 33, at 0x00dbd200, mask 0x80	hAh7_YkBI25p4GsuCjCn
2005-07-13T06:20:39.225000+00…	false	0	6	CE sym 33, at 0x00dbd200, mask 0x80	hQh7_YkBI25p4GsuCjCn
2005-07-13T06:20:39.378000+00…	false	0	6	CE sym 33, at 0x00dbd200, mask 0x80	hgh7_YkBI25p4GsuCjCn
2005-07-13T06:20:39.530000+00…	false	0.00	7	total of 21 ddr error(s) detected and corrected	hwh7_YkBI25p4GsuCjCn
2005-07-13T06:27:32.845000+00…	true	0.99	0	ciod: Error loading /home/glosli/src/ddcMD/ddcMD1.1.14/bin/ddcMDbglV: invalid or missing program image, Exec format error	iAh7_YkBI25p4GsuCjCn
2005-07-13T06:27:32.881000+00…	true	0.99	0	ciod: Error loading /home/glosli/src/ddcMD/ddcMD1.1.14/bin/ddcMDbglV: invalid or missing program image, Exec format error	iQh7_YkBI25p4GsuCjCn
2005-07-13T06:27:32.918000+00…	true	0.99	0	ciod: Error loading /home/glosli/src/ddcMD/ddcMD1.1.14/bin/ddcMDbglV: invalid or missing program image, Exec format error	igh7_YkBI25p4GsuCjCn

Figure 41. Table of logs with anomaly scores.

Grafana enables users to focus on the periods of interest (e.g., periods with high anomaly scores) by simply selecting the period in any of the charts. This creates a time-based filter. Furthermore, filters based on any other field are supported. For example, users can select to show only logs with anomaly scores above 0.7. Users can then inspect the logs in the table, can react appropriately to address the issues found by the system.

I.I.VIII CLI interaction with LOMOS

The lomos-cli is a CLI tool intended for frequent log parsing, training in inference. It is written in Python and is packaged in a Python package (.whl). It can be installed using standard "pip install". It is not published on the public pypy.com repository, so the .whl file needs to be downloaded separately.

The needed parameters have 1-to-1 correspondence to GUI dashboard. They are saved in a json file. Example json files are included with the .whl file. An example for log parsing is shown below:

File sunrise-insiel-sesamo-backend_parse.json

```
{
  "PREPROCESSING": {
    "match_message": "^(?:[\\d\\- \\:\\.\\+]{19,32}) (?:[\\w\\-\\.]+) (.*)$",
    "match_timestamp": "^([\\d\\- \\:\\.\\+]{19,32}) (?:.*)$",
    "timestamp_fmt": "%Y-%m-%d %H:%M:%S.%f",
    "match_log_level": null,
    "match_label": null
  },
  "SNAPSHOT": {
    "snapshot_interval_minutes": 10,
    "compress_state": true
  },
  "MASKING": {
    "mask_prefix": "<:",
    "mask_suffix": ":>",
    "masking": [
      OMMITED-FOR-BREVITY
    ]
  },
  "DRAIN": {
    "max_children": 100,
    "max_clusters": 3000,
    "warning_special_wildcards_ratio_threshold": 0.95,
    "warning_auto_wildcards_ratio_threshold": 0.5,
    "sim_th": 0.4,
    "depth": 4,
    "extra_delimiters": "",
    "parametrize_numeric_tokens": false
  },
  "PROFILING": {
    "enabled": true,
    "report_sec": 30
  },
  "elasticsearch_id_field_name": "_id",
  "export_events_format": "elasticsearch",
  "export_logs_format": "elasticsearch",
  "mode": "training",
  "elasticsearch_host": "PROVIDED-VIA-DEPLOY-ENV",
  "elasticsearch_port": PROVIDED-VIA-DEPLOY-ENV,
  "elasticsearch_source_index": "PROVIDED-VIA-CLI",
  "elasticsearch_log_col_name": "logs_full",
  "elasticsearch_start": "2024-01-17T00:00:00",
  "elasticsearch_end": "2024-02-01T00:00:00",
  "elasticsearch_interval_field_name": "timestamp",
  "elasticsearch_sorting_field_name": "timestamp",
  "elasticsearch_sorting_field_type": "datetime",
  "elasticsearch_additional_query_field": null,
  "elasticsearch_fields_to_keep": ["label", "level"],
  "export_name_prefix": "test",
  "mlflow_run_id_pretrained_drain": null,
  "mlflow_tracking_uri": "",
  "mlflow_run_name": "test_parser",
  "task_name": "train_log_parser"
}
```

In similar fashion we need to provide three files:

- sunrise-insiel-sesamo-backend_parse.json (shown above)

- sunrise-insiel-sesamo-backend_train.json

- sunrise-insiel-sesamo-backend_infer.json

With log data stored in Elasticsearch index named sesamo_logs, the parsing, training in inference tasks are run as:

```
lomos-cli sunrise-insiel-sesamo-backend parse sesamo_logs
# in mlfow was created mlflow experiment with id=parse_id
lomos-cli sunrise-insiel-sesamo-backend train sesamo_logs
# in mlfow was created mlflow experiment with id=train_id
lomos-cli sunrise-insiel-sesamo-backend infer sesamo_logs parse_id train_id
```

I.I.IX Access LOMOS results via API

Lomos2-api provides REST API access to LOMOS results. It is implemented as a REST API. It isolates the consuming application from the LOMOS internal working. The consuming application also does not need direct access to LOMOS internal database to find anomalies.

Example REST request:

```
curl http://127.0.0.1:5000/api/top_anomaly?min_anomaly_score=0.7&from_timestamp=2024-01-08T00:00:01.200000Z&to_timestamp=2024-01-18T00:00:01.200000Z"
```

Example REST response:

```
{
 "aggregate": {
  "count": 1,
  "max_anomaly_score": 0.7692307978868484,
  "min_anomaly_score": 0.7692307978868484
 },
 "messages": [
  {
   "_index": "some_app_backend",
   "_type": "_doc",
   "_id": "D01aa40BjZ7m1DvJ_-y0",
   "_score": 1,
   "_source": {
    "timestamp": "2024-01-17T10:06:03.000014",
    "logs_full": "2024-01-17 10:06:03.000014 DEBUG BaseJdbcLogger:159 - <==    Updates: 1",
    "anomaly_score": 0.7692307978868484
   }
  }
 ]
}
```

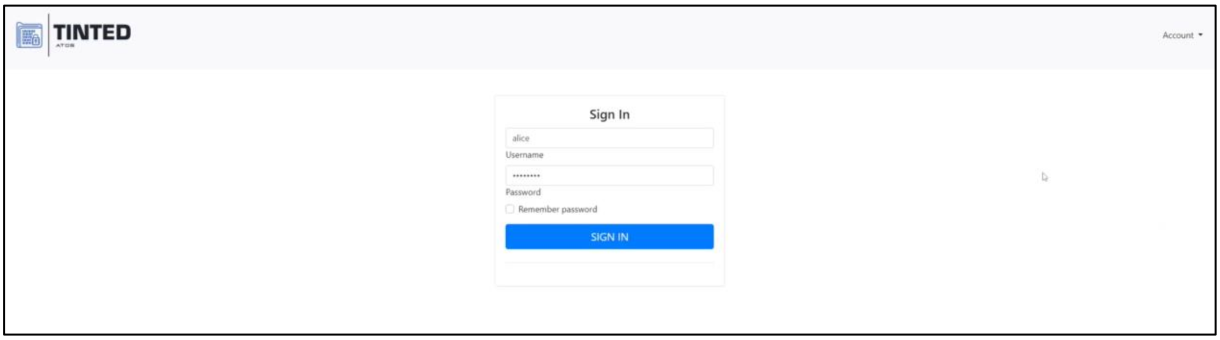
I.II Threat Intelligence

The interaction within the threat intelligence module can be done through two paths: the graphical user interface and the API.

Next paragraphs show and describe the sharing capabilities.

I.II.I WEB-GUI

The WEB-GUI shows a login form (Figure 42) that verifies the credentials against the ones stored in Keycloak.



Sign In

alice

Username

••••••••

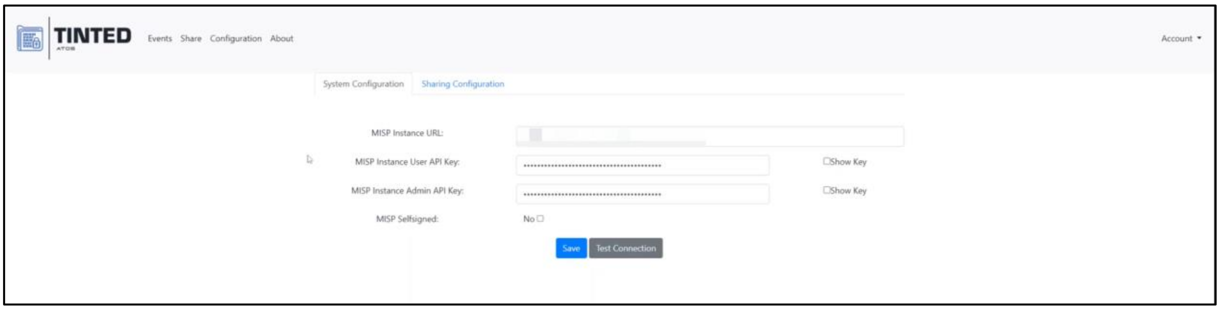
Password

☐ Remember password

SIGN IN

Figure 42. TINTED Login.

Supposing that we have logged in as *Alice* for the first time, then we must configure the platform. We have to indicate different parameters related to the MISP instance such as the URL and the API key (Figure 43), apart from the passphrase for encryption and other information about the events shared within MISP (Figure 44).



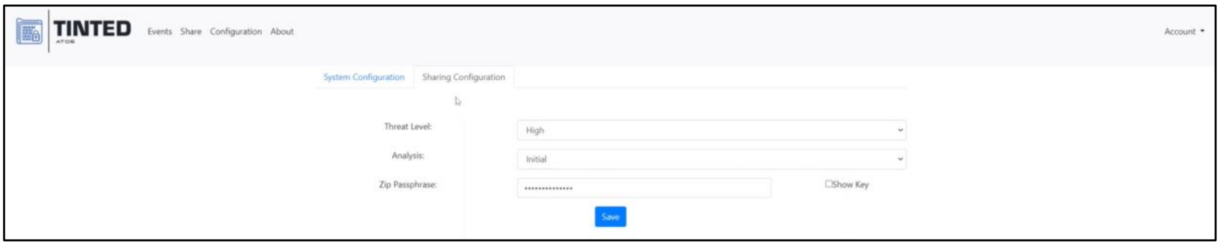
MISP Instance URL:

MISP Instance User API Key: •• ☐Show Key

MISP Instance Admin API Key: •• ☐Show Key

MISP Selfsigned: No ☐

Figure 43. System Configuration.



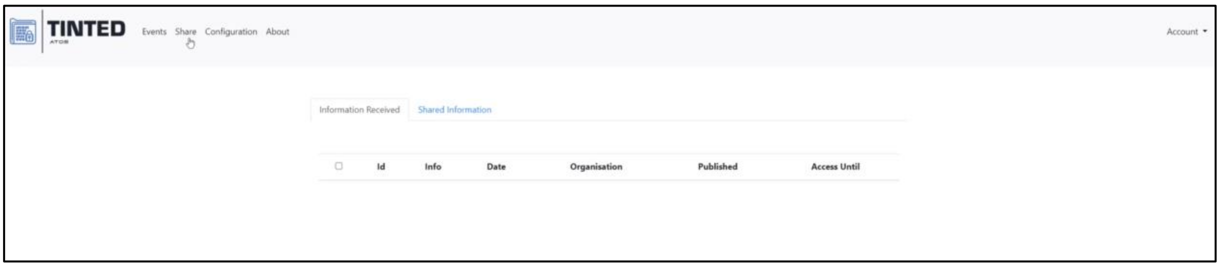
Threat Level: High

Analysis: Initial

Zip Passphrase: ••••••••••••••• ☐Show Key

Figure 44. Sharing Configuration.

After configuring the required parameters, we will be redirected to the main page. In this case, as it is the first time that we access the platform we will observe the absence of events (Figure 45).



Information Received | Shared Information

□	Id	Info	Date	Organisation	Published	Access Until

Figure 45. Events on the main page (currently empty).

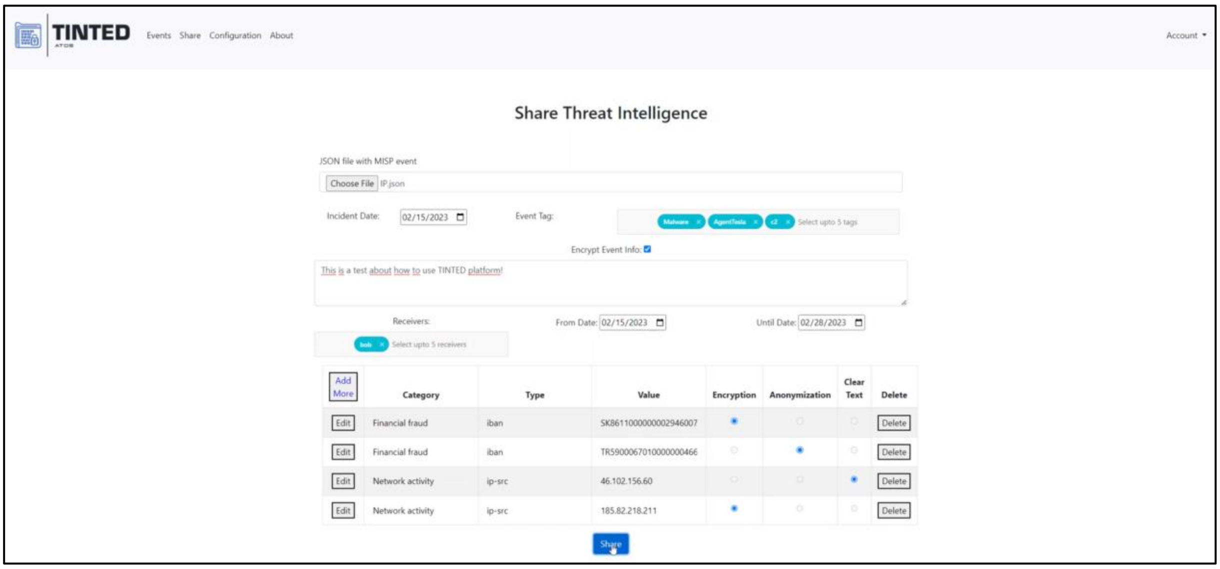
Moving onto the Share webpage, we can see the fields that are available, illustrated in Figure 46.

For the purpose of this guideline, we are going to show how it looks like the process of sending an event from *Alice* to *Bob*.

To initiate the process, a JSON file that follows the MISP event structure is submitted. This file serves to extract the attributes within it, allowing for the selection of desired privacy treatments, which include encryption, anonymization, or maintaining data in cleartext form. Subsequent steps involve populating information fields such as Incident Date (optional, formatted as 'YYYY-MM-DD'), Event Tags (optional keywords describing the event), and Event Info (mandatory event description).

Further actions involve choosing recipients from a Keycloak-loaded list, encompassing various user types like individuals, organizations, sharing groups, or platform roles. Dates are then selected to determine the availability timeframe for the information. Once this period elapses, the event becomes inaccessible on the platform. This information, including start and end dates and the involved users, is stored in the "sharing_agreement" file, attached to the event as depicted in Figure 48.

Lastly, the MISP objects and attributes are contained within a dynamic table. This table is populated with data sourced from the uploaded JSON file. Figure 46 displays a MISP Event with malicious IPs as attributes. Users have the freedom to append or remove attributes while also choosing the desired transformation type. The default choice is "cleartext," which maintains data as is. Alternatively, data protection options of encryption or anonymization can be selected if desired.



Share Threat Intelligence

JSON file with MISP event: IP.json

Incident Date: 02/15/2023

Event Tag: Malware × AgentTesla × c2 × Select upto 5 tags

Encrypt Event Info: ☑

This is a test about how to use TINTED platform!

Receivers: bob × Select upto 5 receivers

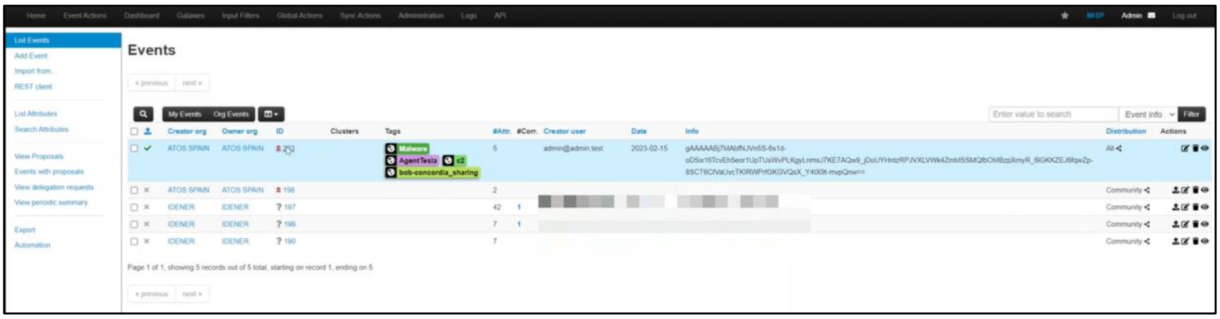
From Date: 02/15/2023

Until Date: 02/28/2023

Add More	Category	Type	Value	Encryption	Anonymization	Clear Text	Delete
Edit	Financial fraud	iban	SK8611000000002946007	●	○	○	Delete
Edit	Financial fraud	iban	TR590006701000000466	○	●	○	Delete
Edit	Network activity	ip-src	46.102.156.60	○	○	●	Delete
Edit	Network activity	ip-src	185.82.218.211	●	○	○	Delete

Figure 46. Information Sharing Form.

After sharing the event, we can observe how it has arrived to the MISP instance. Figure 47 shows that the field Event info is encrypted and if we access the event itself (Figure 48) we also see the different privacy transformations that have been carried out.

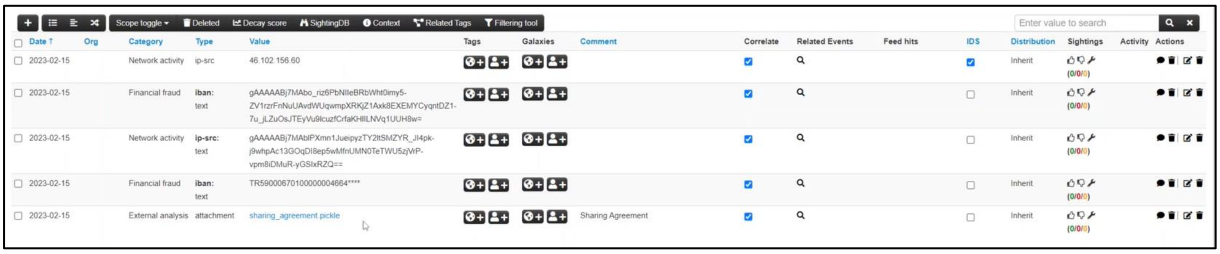


Events

☐		Creator org	Owner org	ID	Clusters	Tags	#Attr.	#Corr.	Creator user	Date	Info	Distribution	Actions
☐	✓	ATOS SPAIN	ATOS SPAIN	263		Malware AgentTesla c2 bob-concordia_sharing	5		admin@admin.test	2023-02-15	gAAAAABj7MAbfNJVn5S-6s1d-oD5ix16TcvEh5eor1UpTUsWvPLKgyLnmsJ7KE7AQw9_jDoUYHntzRPJVXLVWk4ZmMSSMQfbOMBzpXmyR_6lGKKZEJ6fqwZp-8SCT6CfVaUvcTKIRWPrfGKGVQsX_Y4tX9t-mvpQnw==	All	
☐	×	ATOS SPAIN	ATOS SPAIN	198			2		[redacted]			Community	
☐	×	IDENER	IDENER	197			42	1				Community	
☐	×	IDENER	IDENER	196			7	1				Community	
☐	×	IDENER	IDENER	190			7					Community	

Page 1 of 1, showing 5 records out of 5 total, starting on record 1, ending on 5

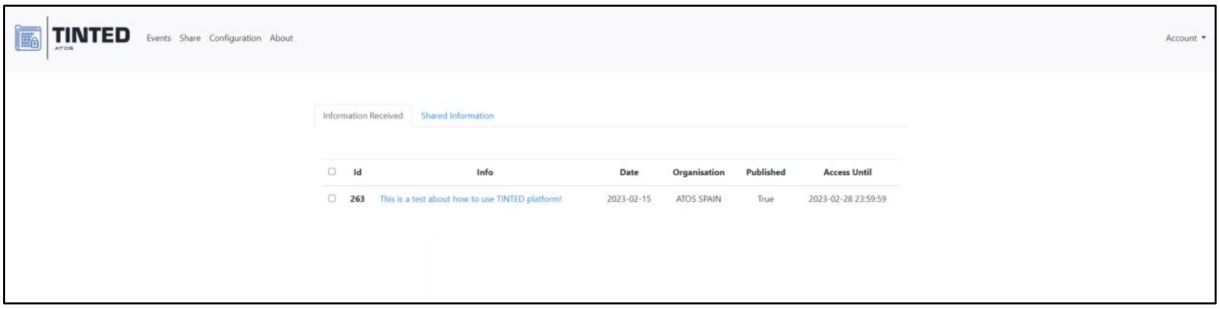
Figure 47. MISP instance.



☐	Date ↑	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings	Activity	Actions
☐	2023-02-15		Network activity	ip-src	46.102.156.60				☑			☑	Inherit	(0/0/0)		
☐	2023-02-15		Financial fraud	iban: text	gAAAAABj7MAbo_riz6PbNIleBRbWht0imy5-ZV1rzrFnNuUAvdWUqwmpXRKjZ1Axk8EXEMYCyqntDZ1-7u_jLZuOsJTEyVu9lcuzfCrfaKHIILNVq1UUH8w=				☑			☐	Inherit	(0/0/0)		
☐	2023-02-15		Network activity	ip-src: text	gAAAAABj7MAbIPXmn1JueipyzTY2ltSMZYR_Jl4pk-j9whpAc13GOqDI8ep5wMfnUMN0TeTWU5zjVrP-vpm8iDMuR-yGSlxRZQ==				☑			☐	Inherit	(0/0/0)		
☐	2023-02-15		Financial fraud	iban: text	TR590006701000000004664****				☑			☐	Inherit	(0/0/0)		
☐	2023-02-15		External analysis	attachment	sharing_agreement.pickle			Sharing Agreement	☑			☐	Inherit	(0/0/0)		

Figure 48. Individual Event details – MISP.

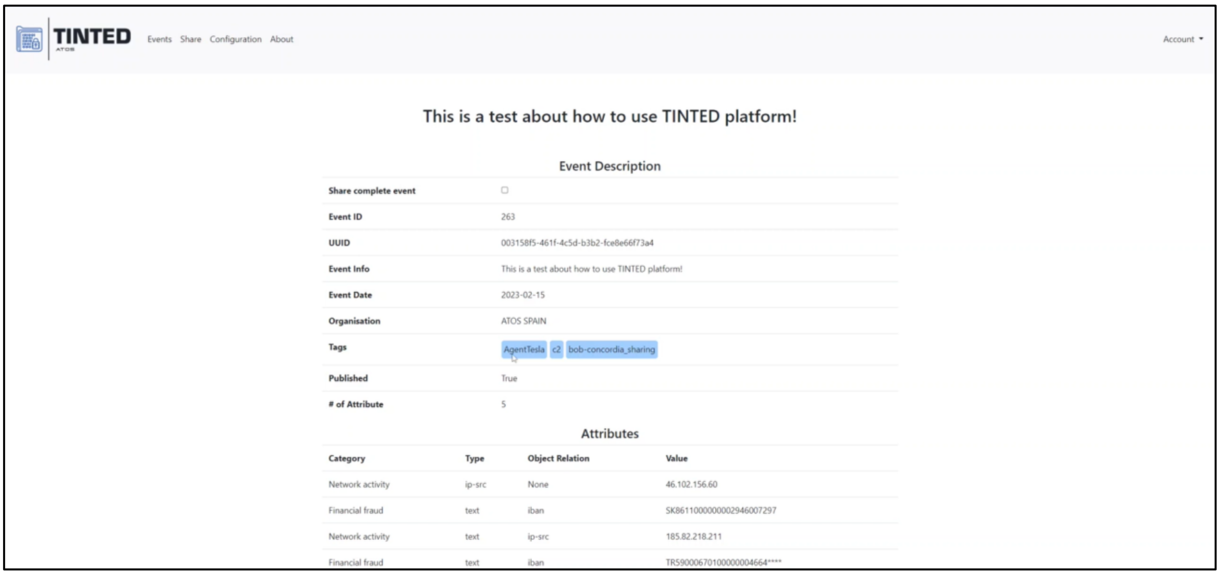
As the MISP instance does not make a distinction between users, it is crucial to protect the information. In this case, if Bob wants to read the specific information that has been shared with him, he just needs to log in into the platform with his credentials (as it was done in Figure 42). Thereafter, he will see that a new event has been received on the dashboard (Figure 49).



☐	Id	Info	Date	Organisation	Published	Access Until
☐	263	This is a test about how to use TINTED platform!	2023-02-15	ATOS SPAIN	True	2023-02-28 23:59:59

Figure 49. TINTED Information Received dashboard.

If we click on the event itself, we can get the information after the decryption process (Figure 50).



This is a test about how to use TINTED platform!

Event Description

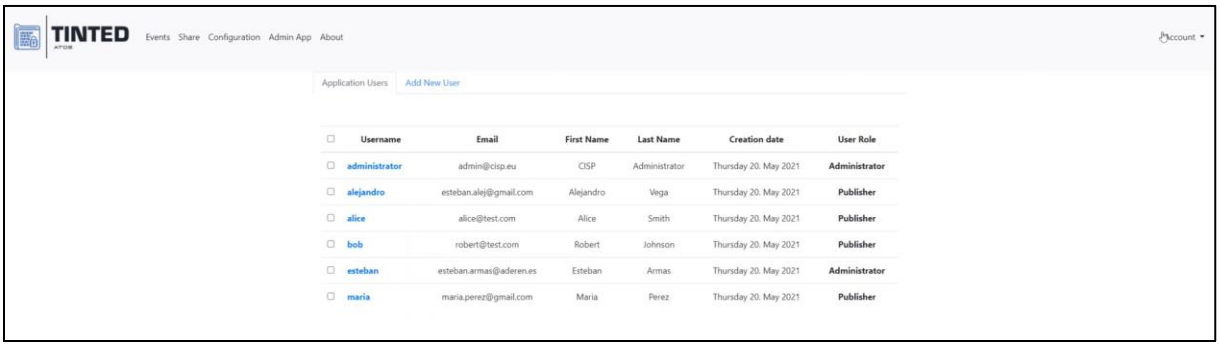
Share complete event	☐
Event ID	263
UUID	003158f5-461f-4c5d-b3b2-fce8e66f73a4
Event Info	This is a test about how to use TINTED platform!
Event Date	2023-02-15
Organisation	ATOS SPAIN
Tags	AgentTesla c2 bob-concordia_sharing
Published	True
# of Attribute	5

Attributes

Category	Type	Object Relation	Value
Network activity	ip-src	None	46.102.156.60
Financial fraud	text	iban	SK8611000000002946007297
Network activity	text	ip-src	185.82.218.211
Financial fraud	text	iban	TR590006701000000004664****

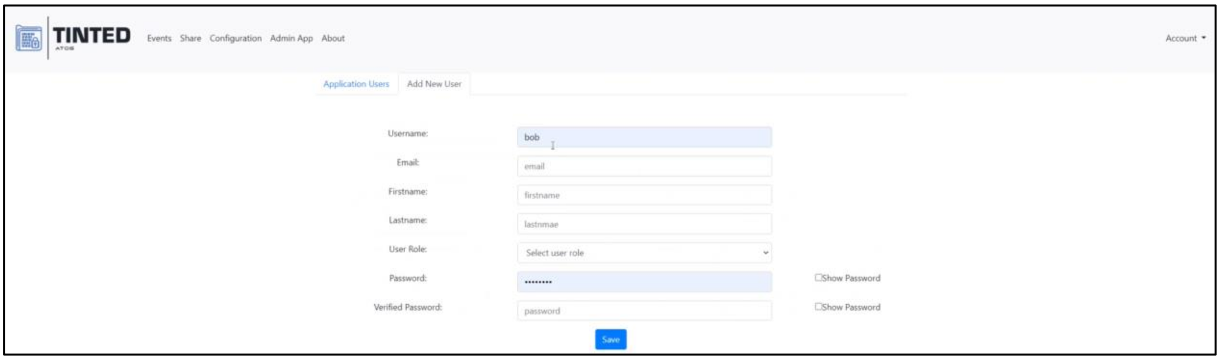
Figure 50. Individual Event details – TINTED.

In case we want to manage the platform with a privileged role we can set up the administrator role. If the user possesses the administrator role within the platform, they will have the capability to oversee other users. Figure 51 and Figure 52 depict the distinct users registered in TINTED and the functionality to sign up a new user, respectively. This dashboard maintains a dynamic link to the data stored in Keycloak.



□	Username	Email	First Name	Last Name	Creation date	User Role
□	administrator	admin@cisp.eu	CISP	Administrator	Thursday 20. May 2021	Administrator
□	alejandro	esteban.alej@gmail.com	Alejandro	Vega	Thursday 20. May 2021	Publisher
□	alice	alice@test.com	Alice	Smith	Thursday 20. May 2021	Publisher
□	bob	robert@test.com	Robert	Johnson	Thursday 20. May 2021	Publisher
□	esteban	esteban.armas@aderen.es	Esteban	Armas	Thursday 20. May 2021	Administrator
□	maria	maria.perez@gmail.com	Maria	Perez	Thursday 20. May 2021	Publisher

Figure 51. Administrator Management Dashboard I.



Username: bob

Email: email

Firstname: firstname

Lastname: lastnmae

User Role: Select user role

Password: •••••••• □Show Password

Verified Password: password □Show Password

Figure 52. Administrator Management Dashboard II.

I.II.II Application Programming Interface

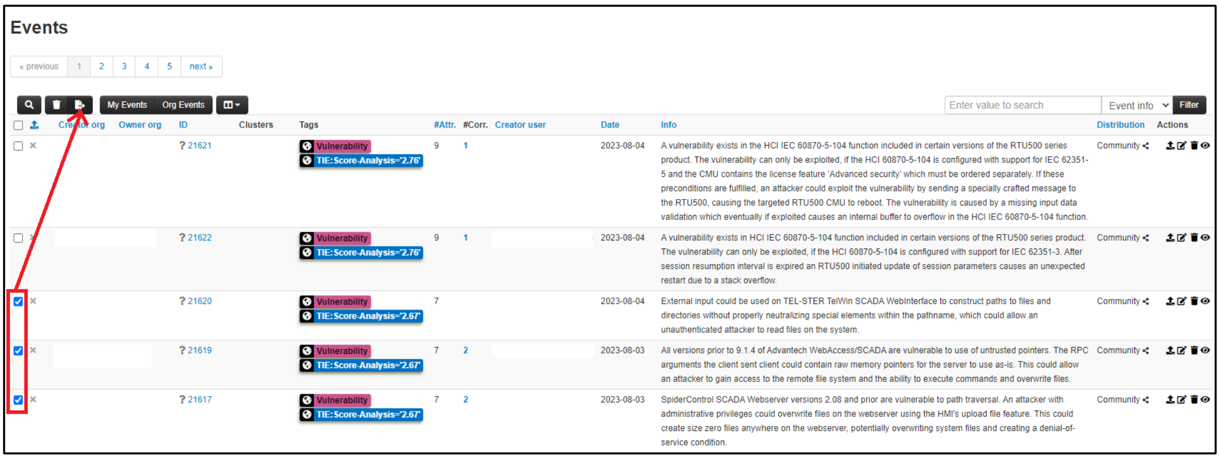
As mentioned earlier, the GUI represents one of the two methods through which we can interact with TINTED. Its purpose is to act as an intermediary layer between the user and the orchestrator API. Nevertheless, there exists a direct means of communicating with the orchestrator API. Presently, the orchestrator API operates as a stateless application, requiring configuration parameters inputted through the GUI to be transmitted with each request to the orchestrator API. These parameters encompass:

Information pertinent to MISP configuration, specifically the URL of the targeted MISP instance for event sharing and its API key.

Sharing Agreement details, outlining the sender of the event and its intended recipient. The sender must match the user authenticated in the parameters.

This approach allows us to replicate the graphical interface's functionalities using the API.

In cases where we retrieve a list of MISP attributes, we can introduce the "transformation" field to these attributes. This empowers us to determine the transformation to be applied: encryption, anonymization, or "clear-text". Additionally, API requests can incorporate an extra parameter, termed "user_policies". This parameter permits the definition of default behaviour for attributes across one or multiple events. Consequently, we can acquire a list of events from MISP and apply a policy defined by the user. To download a list of events, we can do it through the GUI of the instance, like it is shown in Figure 53 and Figure 54, or through an API request to MISP, see Figure 55.



Events

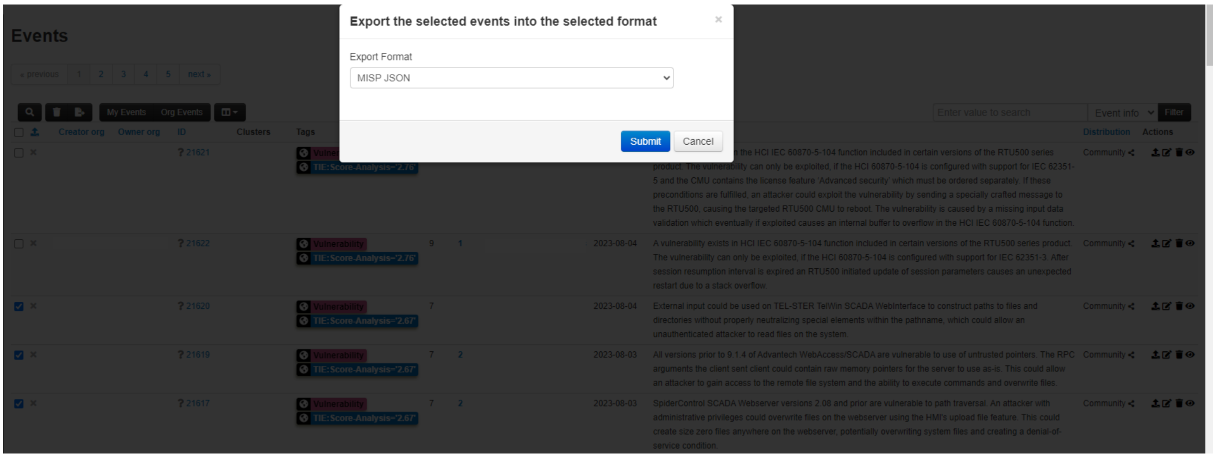
« previous | 1 | 2 | 3 | 4 | 5 | next »

My Events | Org Events

Enter value to search | Event info | Filter

☐		Creator org	Owner org	ID	Clusters	Tags	#Attr.	#Corr.	Creator user	Date	Info	Distribution	Actions
☐	×			? 21621		Vulnerability TIE:Score-Analysis='2.76'	9	1		2023-08-04	A vulnerability exists in the HCI IEC 60870-5-104 function included in certain versions of the RTU500 series product. The vulnerability can only be exploited, if the HCI 60870-5-104 is configured with support for IEC 62351-5 and the CMU contains the license feature 'Advanced security' which must be ordered separately. If these preconditions are fulfilled, an attacker could exploit the vulnerability by sending a specially crafted message to the RTU500, causing the targeted RTU500 CMU to reboot. The vulnerability is caused by a missing input data validation which eventually if exploited causes an internal buffer to overflow in the HCI IEC 60870-5-104 function.	Community	
☐	×			? 21622		Vulnerability TIE:Score-Analysis='2.76'	9	1		2023-08-04	A vulnerability exists in HCI IEC 60870-5-104 function included in certain versions of the RTU500 series product. The vulnerability can only be exploited, if the HCI 60870-5-104 is configured with support for IEC 62351-3. After session resumption interval is expired an RTU500 initiated update of session parameters causes an unexpected restart due to a stack overflow.	Community	
☑	×			? 21620		Vulnerability TIE:Score-Analysis='2.67'	7			2023-08-04	External input could be used on TEL-STER TelWin SCADA WebInterface to construct paths to files and directories without properly neutralizing special elements within the pathname, which could allow an unauthenticated attacker to read files on the system.	Community	
☑	×			? 21619		Vulnerability TIE:Score-Analysis='2.67'	7	2		2023-08-03	All versions prior to 9.1.4 of Advantech WebAccess/SCADA are vulnerable to use of untrusted pointers. The RPC arguments the client sent client could contain raw memory pointers for the server to use as-is. This could allow an attacker to gain access to the remote file system and the ability to execute commands and overwrite files.	Community	
☑	×			? 21617		Vulnerability TIE:Score-Analysis='2.67'	7	2		2023-08-03	SpiderControl SCADA Webserver versions 2.08 and prior are vulnerable to path traversal. An attacker with administrative privileges could overwrite files on the webserver using the HMI's upload file feature. This could create size zero files anywhere on the webserver, potentially overwriting system files and creating a denial-of-service condition.	Community	

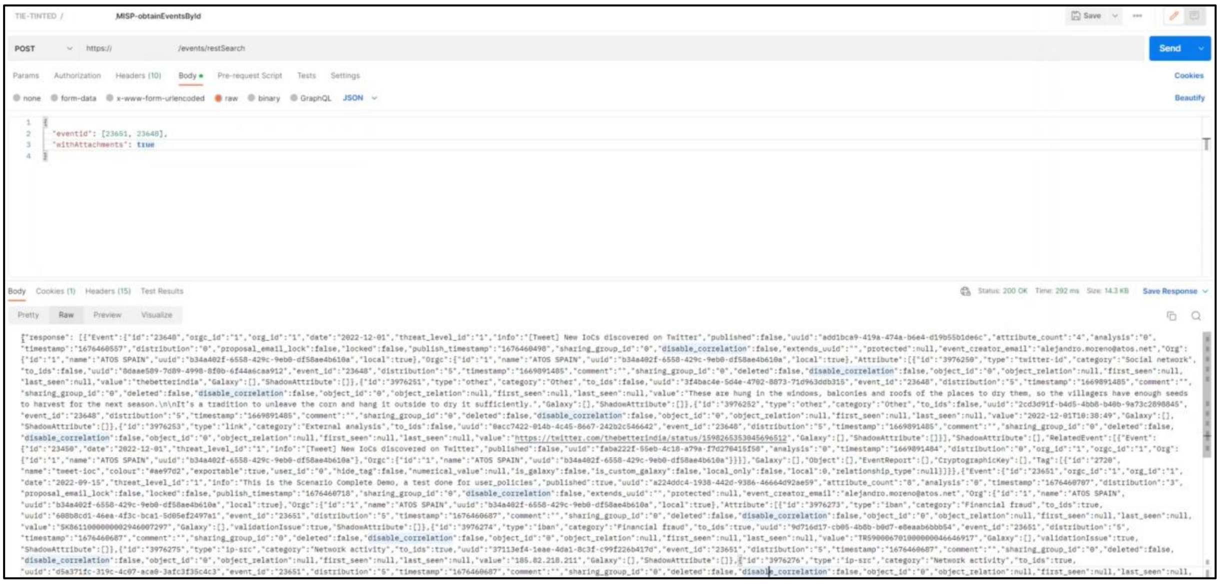
Figure 53. Selection of multiple events in MISP instance.



Export the selected events into the selected format

Export Format: MISP JSON

Figure 54. Download of events in MISP JSON format.



TIE-TINTED / MISP-obtainEventsById

POST https:// /events/restSearch

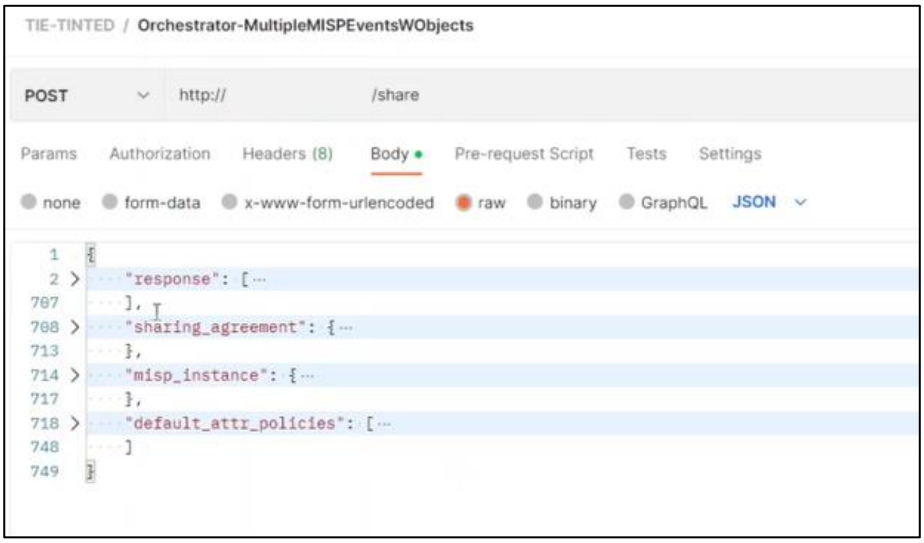
```
{
 "eventid": [23651, 23648],
 "withAttachments": true
}
```

Status: 200 OK Time: 292 ms Size: 14.3 KB

```
{"response": [{"Event":{"id":"23648","orgc_id":"1","org_id":"1","date":"2022-12-01","threat_level_id":"1","info":"[Tweet] New IoCs discovered on Twitter","published":false,"uuid":"add1bca9-419a-474a-b6e4-d19b55b1de6c","attribute_count":"4","analysis":"0",
"timestamp":"1676460557","distribution":"0","proposal_email_lock":false,"locked":false,"publish_timestamp":"1676460498","sharing_group_id":"0","disable_correlation":false,"extends_uuid":"","protected":null,"event_creator_email":"alejandro.moreno@atos.net","Org":
{"id":"1","name":"ATOS SPAIN","uuid":"b34a402f-6558-429c-9eb0-df58ae4b610a","local":true},"Orgc":{"id":"1","name":"ATOS SPAIN","uuid":"b34a402f-6558-429c-9eb0-df58ae4b610a","local":true},"Attribute":[{"id":"3976250","type":"twitter-id","category":"Social network",
"to_ids":false,"uuid":"8daae589-7d89-4998-8f0b-6f44a6caa912","event_id":"23648","distribution":"5","timestamp":"1669891485","comment":"","sharing_group_id":"0","deleted":false,"disable_correlation":false,"object_id":"0","object_relation":null,"first_seen":null,
"last_seen":null,"value":"thebetterindia","Galaxy":[],"ShadowAttribute":[]},{"id":"3976251","type":"other","category":"Other","to_ids":false,"uuid":"3f4bac4e-5d4e-4702-8873-71d963ddb315","event_id":"23648","distribution":"5","timestamp":"1669891485","comment":"",
"sharing_group_id":"0","deleted":false,"disable_correlation":false,"object_id":"0","object_relation":null,"first_seen":null,"last_seen":null,"value":"These are hung in the windows, balconies and roofs of the places to dry them, so the villagers have enough seeds
to harvest for the next season.\n\nIt's a tradition to unleave the corn and hang it outside to dry it sufficiently.","Galaxy":[],"ShadowAttribute":[]},{"id":"3976252","type":"other","category":"Other","to_ids":false,"uuid":"2cd3d91f-b4d5-4bb8-b40b-9a73c2898845",
"event_id":"23648","distribution":"5","timestamp":"1669891485","comment":"","sharing_group_id":"0","deleted":false,"disable_correlation":false,"object_id":"0","object_relation":null,"first_seen":null,"last_seen":null,"value":"2022-12-01T10:38:49","Galaxy":[],
"ShadowAttribute":[]},{"id":"3976253","type":"link","category":"External analysis","to_ids":false,"uuid":"0acc7422-014b-4c45-8667-242b2c546642","event_id":"23648","distribution":"5","timestamp":"1669891485","comment":"","sharing_group_id":"0","deleted":false,
"disable_correlation":false,"object_id":"0","object_relation":null,"first_seen":null,"last_seen":null,"value":"https://twitter.com/thebetterindia/status/1598265353045696512","Galaxy":[],"ShadowAttribute":[]}],"ShadowAttribute":[],"RelatedEvent":[{"Event":
{"id":"23450","date":"2022-12-01","threat_level_id":"1","info":"[Tweet] New IoCs discovered on Twitter","published":false,"uuid":"faba222f-55eb-4c18-a79a-f7d270415f58","analysis":"0","timestamp":"1669891484","distribution":"0","org_id":"1","orgc_id":"1","Org":
{"id":"1","name":"ATOS SPAIN","uuid":"b34a402f-6558-429c-9eb0-df58ae4b610a"},"Orgc":{"id":"1","name":"ATOS SPAIN","uuid":"b34a402f-6558-429c-9eb0-df58ae4b610a"}}}],"Galaxy":[],"Object":[],"EventReport":[],"CryptographicKey":[],"Tag":[{"id":"2720",
"name":"tweet-ioc","colour":"#ae97d2","exportable":true,"user_id":"0","hide_tag":false,"numerical_value":null,"is_galaxy":false,"is_custom_galaxy":false,"local_only":false,"local":0,"relationship_type":null}]}},{"Event":{"id":"23651","orgc_id":"1","org_id":"1",
"date":"2022-09-15","threat_level_id":"1","info":"This is the Scenario Complete Demo, a test done for user_policies","published":true,"uuid":"a224ddc4-1938-442d-9386-46664d92ae59","attribute_count":"8","analysis":"0","timestamp":"1676460707","distribution":"3",
"proposal_email_lock":false,"locked":false,"publish_timestamp":"1676460718","sharing_group_id":"0","disable_correlation":false,"extends_uuid":"","protected":null,"event_creator_email":"alejandro.moreno@atos.net","Org":{"id":"1","name":"ATOS SPAIN",
"uuid":"b34a402f-6558-429c-9eb0-df58ae4b610a","local":true},"Orgc":{"id":"1","name":"ATOS SPAIN","uuid":"b34a402f-6558-429c-9eb0-df58ae4b610a","local":true},"Attribute":[{"id":"3976273","type":"iban","category":"Financial fraud","to_ids":true,
"uuid":"608b8cd1-46ea-4f3c-bca1-5d05ef2497a1","event_id":"23651","distribution":"5","timestamp":"1676460687","comment":"","sharing_group_id":"0","deleted":false,"disable_correlation":false,"object_id":"0","object_relation":null,"first_seen":null,"last_seen":null,
"value":"SK8611000000002946007297","Galaxy":[],"validationIssue":true,"ShadowAttribute":[]},{"id":"3976274","type":"iban","category":"Financial fraud","to_ids":true,"uuid":"9d716d17-cb05-4b6b-b0d7-e8eaab6bbb54","event_id":"23651","distribution":"5",
"timestamp":"1676460687","comment":"","sharing_group_id":"0","deleted":false,"disable_correlation":false,"object_id":"0","object_relation":null,"first_seen":null,"last_seen":null,"value":"TR590006701000000046646917","Galaxy":[],"validationIssue":true,
"ShadowAttribute":[]},{"id":"3976275","type":"ip-src","category":"Network activity","to_ids":true,"uuid":"37113ef4-1eae-4da1-8c3f-c99f226b417d","event_id":"23651","distribution":"5","timestamp":"1676460687","comment":"","sharing_group_id":"0","deleted":false,
"disable_correlation":false,"object_id":"0","object_relation":null,"first_seen":null,"last_seen":null,"value":"185.82.218.211","Galaxy":[],"ShadowAttribute":[]},{"id":"3976276","type":"ip-src","category":"Network activity","to_ids":true,
"uuid":"d5a371fc-319c-4c07-aca0-3afc3f35c4c3","event_id":"23651","distribution":"5","timestamp":"1676460687","comment":"","sharing_group_id":"0","deleted":false,"disable_correlation":false,"object_id":"0","object_relation":null,"first_seen":null,"last_seen":null,
```

Figure 55. HTTP request to download MISP events.

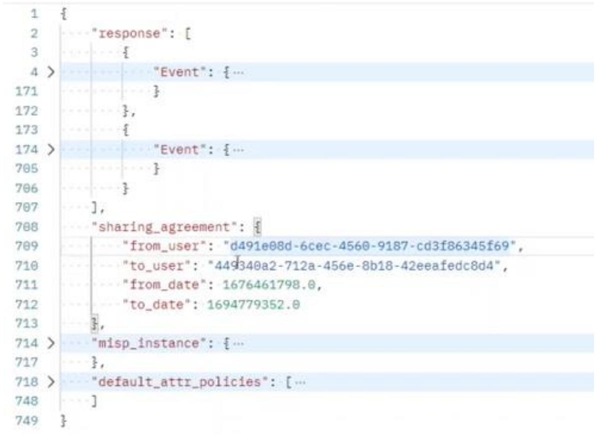
Once we got the desired events, we must insert them in the HTTP request that is sent to the orchestrator. The format of the request is shown in Figure 56.



```
{
    "response": [···
    ],
    "sharing_agreement": {···
    },
    "misp_instance": {···
    },
    "default_attr_policies": [···
    ]
}
```

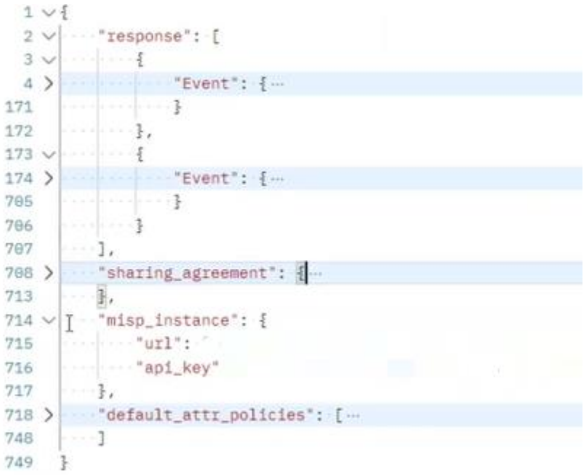
Figure 56. Orchestrator HTTP request format.

The response field is populated with the events that we have previously downloaded meanwhile the format of the *sharing_agreement* and *misp_instance* fields are shown in Figure 57 and Figure 58, respectively.



```
{
    "response": [
        {
            "Event": {···
            }
        },
        {
            "Event": {···
            }
        }
    ],
    "sharing_agreement": {
        "from_user": "d491e08d-6cec-4560-9187-cd3f86345f69",
        "to_user": "449340a2-712a-456e-8b18-42eeafedc8d4",
        "from_date": 1676461798.0,
        "to_date": 1694779352.0
    },
    "misp_instance": {···
    },
    "default_attr_policies": [···
    ]
}
```

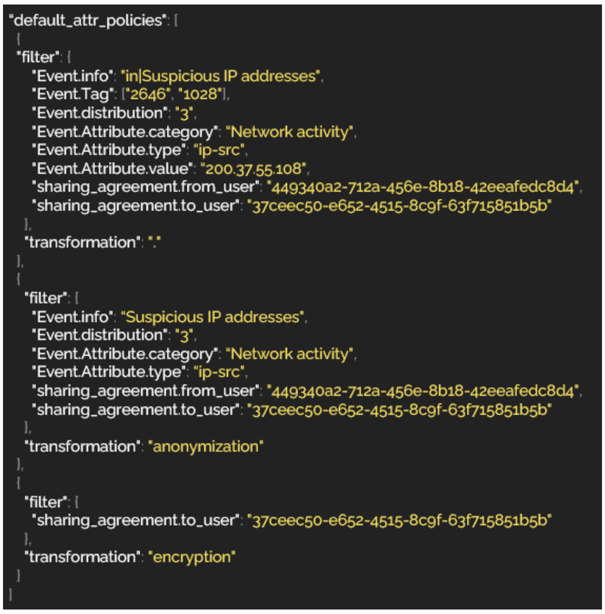
Figure 57. Sharing Agreement field.



```
{
    "response": [
        {
            "Event": {···
            }
        },
        {
            "Event": {···
            }
        }
    ],
    "sharing_agreement": {···
    },
    "misp_instance": {
        "url": 
        "api_key"
    },
    "default_attr_policies": [···
    ]
}
```

Figure 58. MISP instance field.

Concerning the user policies, Figure 59 provides an illustration of them.



```
"default_attr_policies": [
 {
 "filter": {
   "Event.info": "in|Suspicious IP addresses",
   "Event.Tag": ["2646", "1028"],
   "Event.distribution": "3",
   "Event.Attribute.category": "Network activity",
   "Event.Attribute.type": "ip-src",
   "Event.Attribute.value": "200.37.55.108",
   "sharing_agreement.from_user": "449340a2-712a-456e-8b18-42eeafedc8d4",
   "sharing_agreement.to_user": "37ceec50-e652-4515-8c9f-63f715851b5b"
  },
  "transformation": "."
 },
 {
  "filter": {
   "Event.info": "Suspicious IP addresses",
   "Event.distribution": "3",
   "Event.Attribute.category": "Network activity",
   "Event.Attribute.type": "ip-src",
   "sharing_agreement.from_user": "449340a2-712a-456e-8b18-42eeafedc8d4",
   "sharing_agreement.to_user": "37ceec50-e652-4515-8c9f-63f715851b5b"
  },
  "transformation": "anonymization"
 },
 {
  "filter": {
   "sharing_agreement.to_user": "37ceec50-e652-4515-8c9f-63f715851b5b"
  },
  "transformation": "encryption"
 }
]
```

Figure 59. User policies for privacy sharing.

As observed, the "user_policies" parameter consists of a collection of distinct policies. Each policy comprises a combination of a filter and a transformation. The filter establishes a condition that must be met, while the transformation determines whether the attribute is to be encrypted, anonymized, or kept in its original form ("clear-text"). These policies are executed sequentially. When a policy's filter matches the attribute, the corresponding transformation is applied, and subsequent policies are no longer assessed. To fulfil a filter's requirements, all the specific conditions within it must align. The filter can encompass criteria related to the event, attributes, objects, or sharing agreement fields.

Within the first policy filter's "Event.info" field, the "|" operator is employed to signify an "in" condition type. This indicates that the event's "info" field should contain the substring "Suspicious IP addresses". Alternatively, using "=" followed by the "|" operator would indicate an equality condition, requiring the "info" field of the event to precisely match "Suspicious IP addresses". Additionally, it's noteworthy that transformation values can be set as ".", aside from the options of encryption, anonymization, and "clear-text". This specific transformation denotes that the attribute remains unaltered. This feature accommodates instances when received events have already predetermined transformations, offering the capability to introduce exceptions to established rules. In the given example, it serves as an exception for the value "200.37.55.108" concerning the subsequent policy.

I.II.III Scoring capabilities

Finally, the last module that TINTED has is the Threat Intelligence Engine (TIE). It acquires events from the MISP instance and generates a threat score. This score can be divided into two parts: the initial segment is public, as it is founded on open-source data, and it gauges the threat based on diverse metrics like timeliness, trending, and completeness. The second segment, which is private, encompasses these metrics along with the relevance heuristic that factors in CI infrastructure data. To shield against potential information leaks, this segment is encrypted, particularly due to the criticality of its assessment of the infrastructure's vulnerability against threats. Exposure of this information could have severe consequences, enabling attackers to exploit vulnerabilities and target the entity. By partitioning the score, we adhere to the principle of sharing data through the public metrics while simultaneously safeguarding the organization's vital data by encrypting it. Concurrently, we augment the received event's contextual information, a highly valuable enhancement. This entire procedure is referred to as CTI enrichment, described in Figure 60.

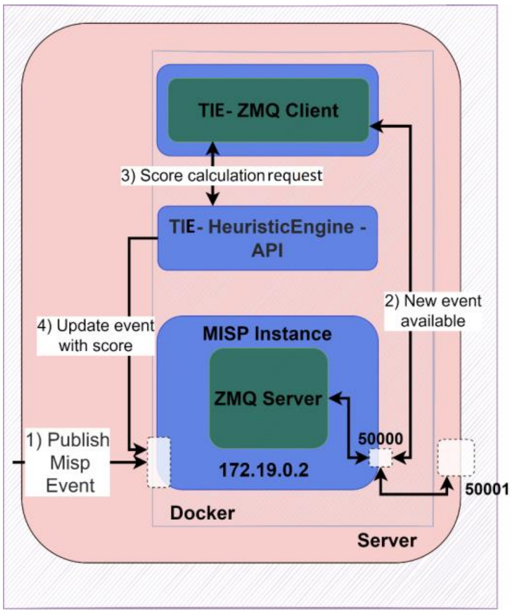


Figure 60. TIE architecture.

The central part of TIE is the HeuristicEngine. It processes API requests containing MISP Events and computes the score by considering the following factors:

Static data: information about the infrastructure.

Dynamic data: events, alerts, and vulnerability assessments.

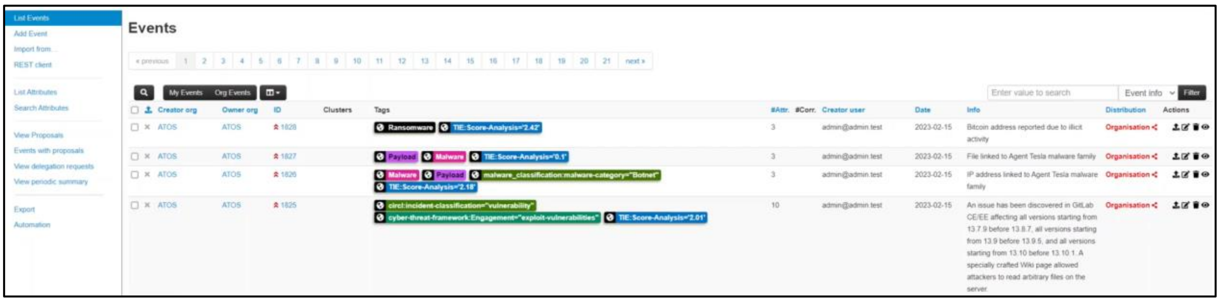
CTI (Cyber Threat Intelligence): the received event itself.

Subsequently, this score is integrated as an Attribute, updating the MISP Event within the MISP Instance.

The second element in TIE's architecture is the ZeroMQ client. A MISP Instance can be configured with a ZeroMQ Server, which the TIE system capitalizes on. The ZMQ Client is established as part of TIE and subscribes to the MISP Instance's ZMQ queue. When a fresh event arrives, the client sends a request to the HeuristicEngine component. This action triggers the execution of heuristic functions that ultimately lead to the score computation.

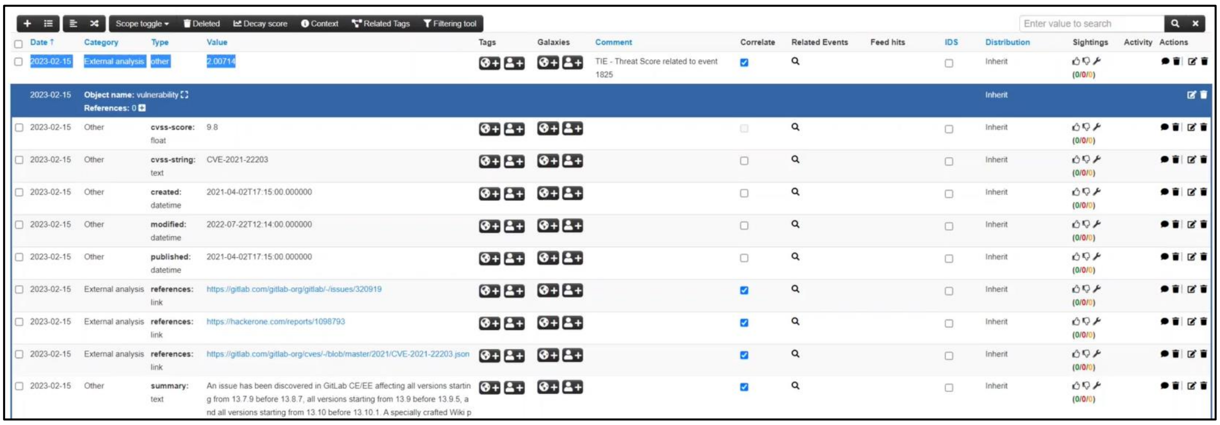
TIE does not encompass all MISP objects; instead, it concentrates on four specific objects considered highly valuable in the realm of threat intelligence: **Vulnerability**, **Domain-IP**, **BTC-Address**, and **File**. These four objects comprise various attributes, including required and optional ones, which later contribute to the heuristics' calculations.

Figure 61 shows different MISP events that have arrived at the instance, and they have been processed for threat score calculation. In Figure 62 we can observe one individual event that contains a vulnerability object.



□	Creator org	Owner org	ID	Clusters	Tags	#Attr.	#Corr.	Creator user	Date	Info	Distribution	Actions
□ ✕	ATOS	ATOS	1828		Ransomware TIE:Score-Analysis='2.42'	3		admin@admin.test	2023-02-15	Bitcoin address reported due to illicit activity	Organisation	
□ ✕	ATOS	ATOS	1827		Payload Malware TIE:Score-Analysis='0.1'	3		admin@admin.test	2023-02-15	File linked to Agent Tesla malware family	Organisation	
□ ✕	ATOS	ATOS	1826		Malware Payload malware_classification:malware-category="Botnet" TIE:Score-Analysis='2.18'	3		admin@admin.test	2023-02-15	IP address linked to Agent Tesla malware family	Organisation	
□ ✕	ATOS	ATOS	1825		circl:incident-classification="vulnerability" cyber-threat-framework:Engagement="exploit-vulnerabilities" TIE:Score-Analysis='2.01'	10		admin@admin.test	2023-02-15	An issue has been discovered in GitLab CE/EE affecting all versions starting from 13.7.9 before 13.8.7, all versions starting from 13.9 before 13.9.5, and all versions starting from 13.10 before 13.10.1. A specially crafted Wiki page allowed attackers to read arbitrary files on the server.	Organisation	

Figure 61. MISP events enriched with TIE’s threat score.



☐	Date ↑	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings	Activity	Actions
☐	2023-02-15	External analysis	other	2.00714			TIE - Threat Score related to event 1825	☑			☐	Inherit	(0/0/0)		
	2023-02-15	Object name: vulnerability References: 0										Inherit			
☐	2023-02-15	Other	cvss-score: float	9.8				☐			☐	Inherit	(0/0/0)		
☐	2023-02-15	Other	cvss-string: text	CVE-2021-22203				☐			☐	Inherit	(0/0/0)		
☐	2023-02-15	Other	created: datetime	2021-04-02T17:15:00.000000				☐			☐	Inherit	(0/0/0)		
☐	2023-02-15	Other	modified: datetime	2022-07-22T12:14:00.000000				☐			☐	Inherit	(0/0/0)		
☐	2023-02-15	Other	published: datetime	2021-04-02T17:15:00.000000				☐			☐	Inherit	(0/0/0)		
☐	2023-02-15	External analysis	references: link	https://gitlab.com/gitlab-org/gitlab/-/issues/320919				☑			☐	Inherit	(0/0/0)		
☐	2023-02-15	External analysis	references: link	https://hackerone.com/reports/1098793				☑			☐	Inherit	(0/0/0)		
☐	2023-02-15	External analysis	references: link	https://gitlab.com/gitlab-org/cves/-/blob/master/2021/CVE-2021-22203.json				☑			☐	Inherit	(0/0/0)		
☐	2023-02-15	Other	summary: text	An issue has been discovered in GitLab CE/EE affecting all versions startin g from 13.7.9 before 13.8.7, all versions starting from 13.9 before 13.9.5, a nd all versions starting from 13.10 before 13.10.1. A specially crafted Wiki p				☑			☐	Inherit	(0/0/0)		

Figure 62. Vulnerability object.

I.II.III.I Source Confidence Score

The new functionality "Source Confidence Calculation" has been implemented in TINTED, introducing several capabilities to enhance existing functionalities:

Dynamic Adjustment of Source Confidence: Allows dynamic updates to the confidence level of intelligence sources, ensuring users have access to the most up-to-date data reliability assessment.

NATO Admiralty Tag Assignment: Assigns a specific "admiralty" tag to each intelligence source, facilitating identification and categorization within the system.

Scoring Model Integration/Adjustment: Integrates TINTED's existing scoring model with state-of-the-art methodology to provide a comprehensive and accurate evaluation of source reliability.

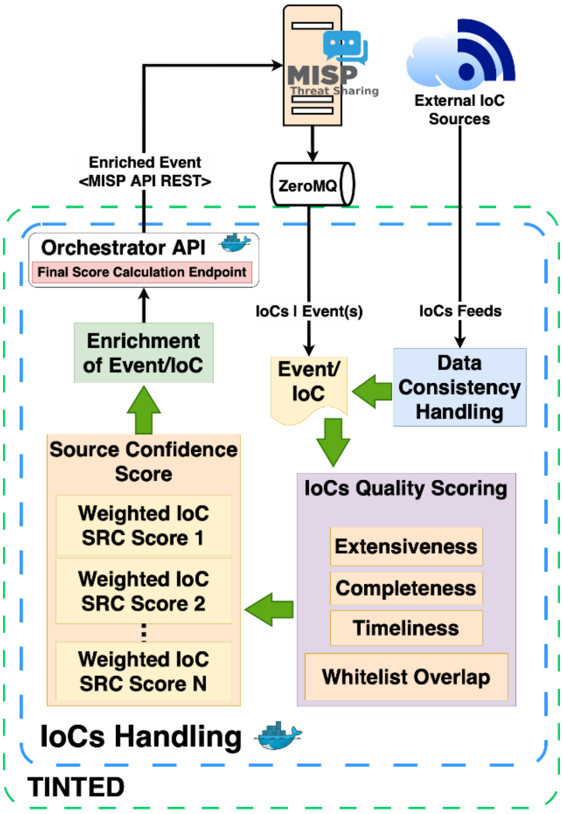


Figure 63: Source Confidence Score Architecture.

This functionality operates in three modes, configured via the "FEEDING_MODE" environment variable:

- MISP: Intelligence feeds received from MISP through ZeroMQ Client.

- API: Intelligence feeds received by invoking APIs provided by the sources.
- ANY: Both modes of data collection are enabled.

The list of intelligence feeds considered for source confidence calculation is defined in the "intelligence_feeds.json" file. Each source is defined by a JSON structure including fields such as Name, Description, URL, Apikey, Periodicity, Interval, Options, Format, Categories, Service, Context_properties, Enabled, and Private. These fields provide essential information for retrieving IoCs (Indicators of Compromise) and determining source confidence.

Concerning the heuristics that are involved in the source confidence score, we have the following ones:

Extensiveness. Measures how much additional information an intelligence feed provides with each Indicator of Compromise (IoC), assigning higher confidence to feeds with more context. Context properties include timestamps, country, service, threat descriptions, etc. The system assumes all IoCs within a feed have the same context properties.

Timeliness. Determines how quickly intelligence feed shares IoCs compared to others, using timestamps to assess recentness.

Completeness. Evaluates the quantity of IoCs contributed by an intelligence feed, prioritizing quantity over quality.

Whitelist Overlap Score. Calculates the extent to which IoCs in an intelligence feed overlap with trusted whitelists, adjusting for known sources like Cisco Umbrella domains and cloud provider IP ranges.

Finally, the Source Confidence score combines these factors into a weighted average to determine the confidence level of intelligence feeds. Each feed's confidence is reflected in the "TINTED:Source-Score" tag in associated MISP events.

Furthermore, Admiralty taxonomy is integrated into IoC decay calculation, adjusting IoC significance based on taxonomy classification. The mapping between TINTED source scoring and the admiralty tag is done according to the following table:

Table 2: Mapping between TINTED Score & Admiralty tag

TINTED Score	Admiralty Tag	Numeric Value
>= 87,5	admiralty-scale:information-credibility="1"	100
>= 62,5	admiralty-scale:information-credibility="2"	75
>= 37,5	admiralty-scale:information-credibility="3"	50
< 12,5	admiralty-scale:information-credibility="4"	25

To leverage this functionality, we must go through the already mentioned .env file. Apart from setting up the correct values for the MISP instance and the ZMQ queue, we need to consider these other variables:

FEEDING_MODE. This setting configures how the process receives intelligence feeds. Options include fetching feeds from MISP (set to “MISP”), directly invoking the API provided by the intelligence feed sources (set to “API”) or utilizing both methods (set to “ANY”). It's important to note that if external access is not available, this variable should be configured to “MISP”.

INTELLIGENCE_FEEDS_FILE. This file is used to configure the intelligence feeds enabled for scoring. During deployment, this file is mounted as a volume for easier modification.

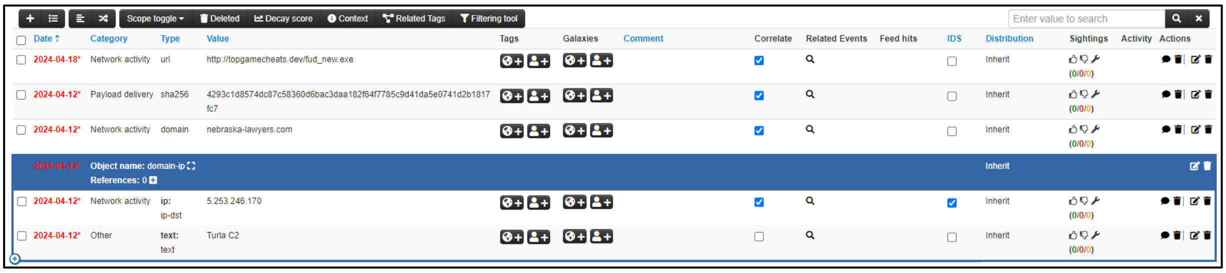
ENABLE_WHITELIST. Set this to “true” if you wish to activate the whitelist overlap score feature. Keep in mind that this score requires external access to download IP and domain whitelists. The URLs for these whitelists are configured in WHITELIST_IP_URL and WHITELIST_DOMAIN_URL. By default, these lists are downloaded upon image deployment and then at 07:00h. To adjust the download time, configure WHITELIST_DOWNLOAD_TIME (without double quotes).

I.II.III.II IoC enrichment with MITRE ATT&CK techniques

Another important feature that has been integrated in TINTED is the ability to enrich IoC with techniques from the MITRE ATT&CK matrix.

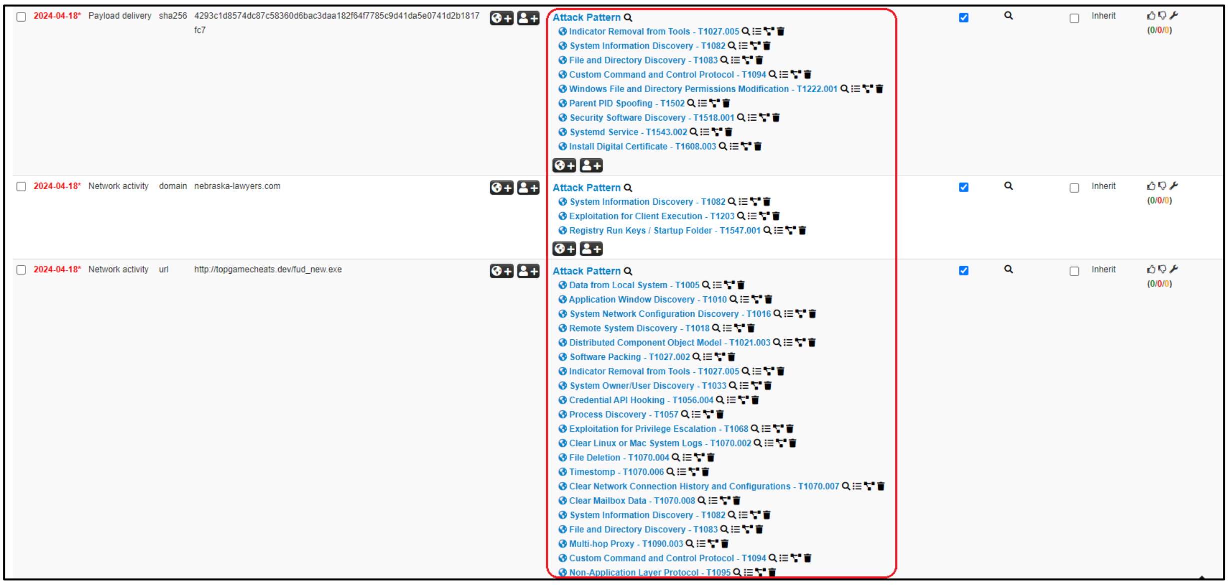
The feature uses the same logic as the scoring. For each new event that is received in the MISP instance, the HeuristicEngine, leveraging VirusTotal API endpoints, introduces the techniques associated to those attributes.

This way, CI operators whenever they pull information from intelligence feeds, which is not very rich (Figure 64), can get more insights about the IoC that arrive to their instance, as it can be observed in Figure 65.



□	Date	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings	Activity	Actions
□	2024-04-18*	Network activity	url	http://topgamecheats.dev/fud_new.exe				☑			□	Inherit	(0/0/0)		
□	2024-04-12*	Payload delivery	sha256	4293c1d8574dc87c58360d6bac3daa182f64f7785c9d41da5e0741d2b1817fc7				☑			□	Inherit	(0/0/0)		
□	2024-04-12*	Network activity	domain	nebraska-lawyers.com				☑			□	Inherit	(0/0/0)		
	2024-04-12*	Object name: domain-ip References: 0										Inherit			
□	2024-04-12*	Network activity	ip: ip-dst	5.253.246.170				☑			☑	Inherit	(0/0/0)		
□	2024-04-12*	Other	text: text	Turla C2				□			□	Inherit	(0/0/0)		

Figure 64. IoCs before enrichment with MITRE ATT&CK techniques.



□	2024-04-18*	Payload delivery	sha256	4293c1d8574dc87c58360d6bac3daa182f64f7785c9d41da5e0741d2b1817fc7	Attack Pattern Indicator Removal from Tools - T1027.005 System Information Discovery - T1082 File and Directory Discovery - T1083 Custom Command and Control Protocol - T1094 Windows File and Directory Permissions Modification - T1222.001 Parent PID Spoofing - T1502 Security Software Discovery - T1518.001 Systemd Service - T1543.002 Install Digital Certificate - T1608.003	☑	□	Inherit	(0/0/0)
□	2024-04-18*	Network activity	domain	nebraska-lawyers.com	Attack Pattern System Information Discovery - T1082 Exploitation for Client Execution - T1203 Registry Run Keys / Startup Folder - T1547.001	☑	□	Inherit	(0/0/0)
□	2024-04-18*	Network activity	url	http://topgamecheats.dev/fud_new.exe	Attack Pattern Data from Local System - T1005 Application Window Discovery - T1010 System Network Configuration Discovery - T1016 Remote System Discovery - T1018 Distributed Component Object Model - T1021.003 Software Packing - T1027.002 Indicator Removal from Tools - T1027.005 System Owner/User Discovery - T1033 Credential API Hooking - T1056.004 Process Discovery - T1057 Exploitation for Privilege Escalation - T1068 Clear Linux or Mac System Logs - T1070.002 File Deletion - T1070.004 Timestomp - T1070.006 Clear Network Connection History and Configurations - T1070.007 Clear Mailbox Data - T1070.008 System Information Discovery - T1082 File and Directory Discovery - T1083 Multi-hop Proxy - T1090.003 Custom Command and Control Protocol - T1094 Non-Application Layer Protocol - T1095	☑	□	Inherit	(0/0/0)

Figure 65. IoCs after enrichment with MITRE ATT&CK techniques.

To enable this functionality, the user must set the environment variable "ENABLE_MITRE_ENRICHMENT" in the .env file to True.

I.II.III.III Contextualization of health trends for threat score

One of the key SUNRISE's strategy points, developed under WP2, is workforce absenteeism.

This feature tries to leverage the nature of the threat intelligence module and monitors cyber and *physical* events which may have an impact on CI. Figure 66 shows a graph of searches for some keywords (influenza, fever, and sick leave) that have a peak around Christmas time (24th-25th December).

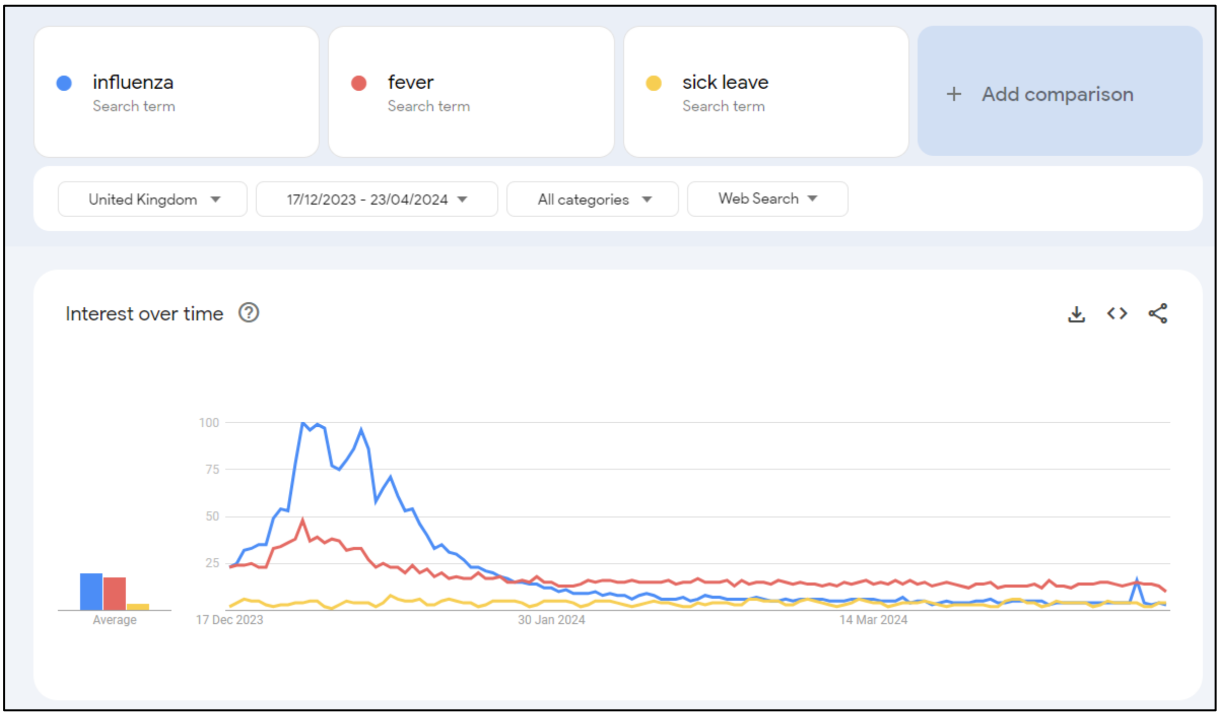


Figure 66. Interest over time for health-related keywords in Google Trends.

This is a good example that shows that special events during the year, especially in a pandemic scenario, can produce an increase in infections. If we can detect anomalies in the number of searches for health topics, we may be able to predict whether our workforce can be unavailable to attend to their workplace due to illness.

The feature can be enabled in the .env file under the variable ENABLE_GOOGLE_TRENDS_MONITORING and requires a minimum set of configurations:

```
[search_query]

physical_events_keywords = influenza, fever, sick leave

[location]

# https://serpapi.com/google-trends-locations

geo = UK
```

First, we need a list of keywords that we want to monitor and then the country where we want to check the number of searches. It is worth noting that the keywords should be written in the same language as the country is selected to avoid bias as most of the population search for content in their mother-tongue language.

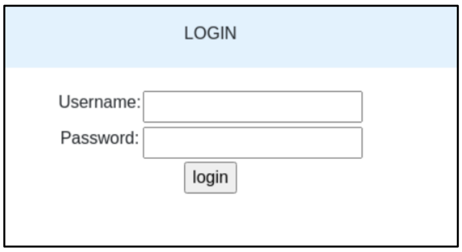
By default, the timespan of the search covers the last 30 days, as it is enough for retrieving a sample of the trend.

If the script detects a high increase in the graph, the Heuristic Engine module will send an alarm to the risk assessment module so that indicators are triggered with their respective risk models.

I.III Risk Assessment

I.III.I WEB-GUI

The first step to access the risk assessment module is to enter valid credentials to log in, as shown in Figure 67.



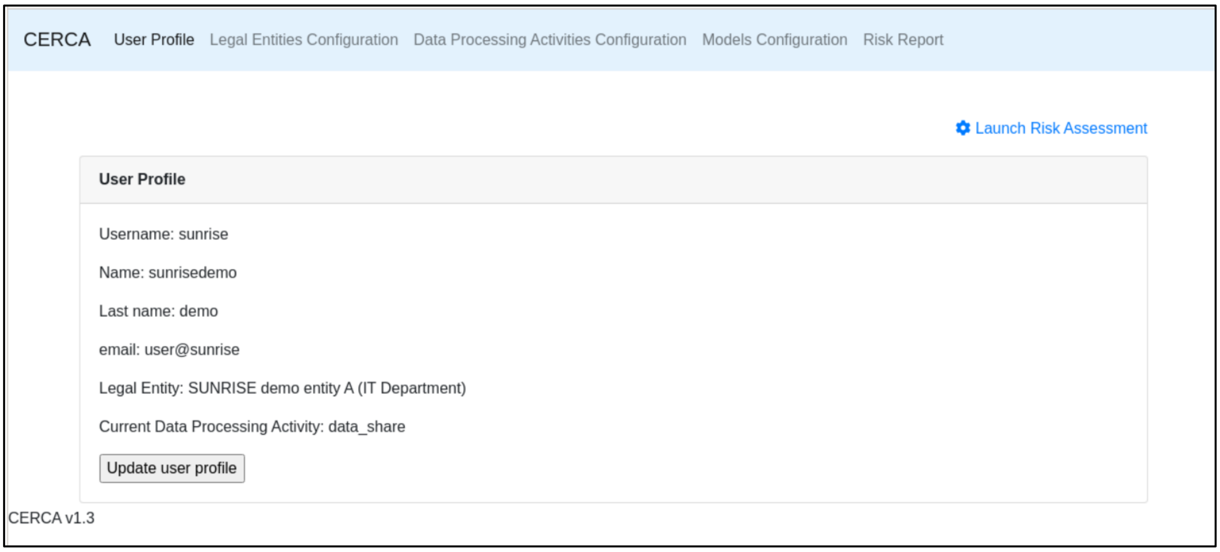
LOGIN

Username:

Password:

Figure 67. Login form.

Once we have logged in, the user will see a dashboard (Figure 68) with his personal information and a button to update any of the fields.



User Profile

Username: sunrise

Name: sunrisedemo

Last name: demo

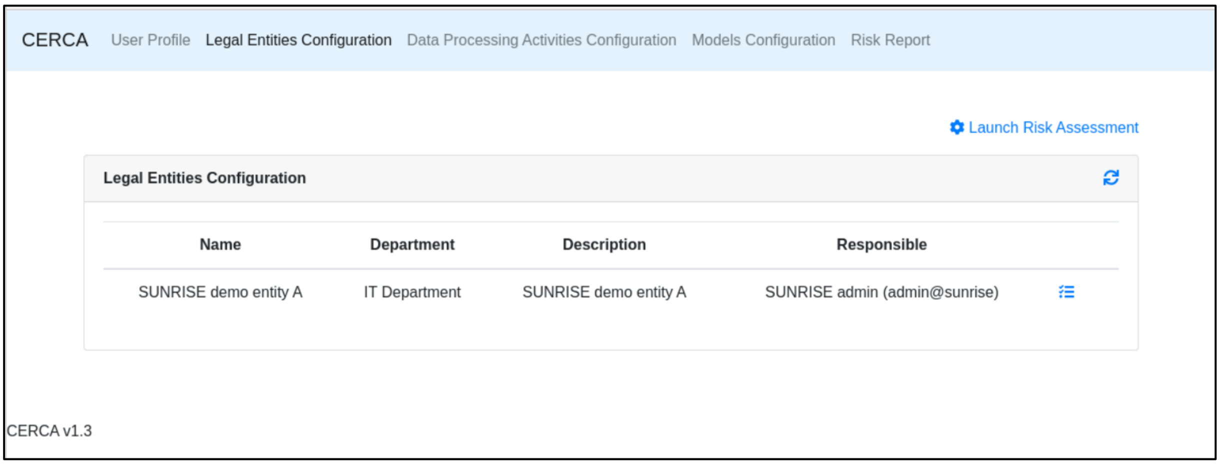
email: user@sunrise

Legal Entity: SUNRISE demo entity A (IT Department)

Current Data Processing Activity: data_share

Figure 68. User profile menu.

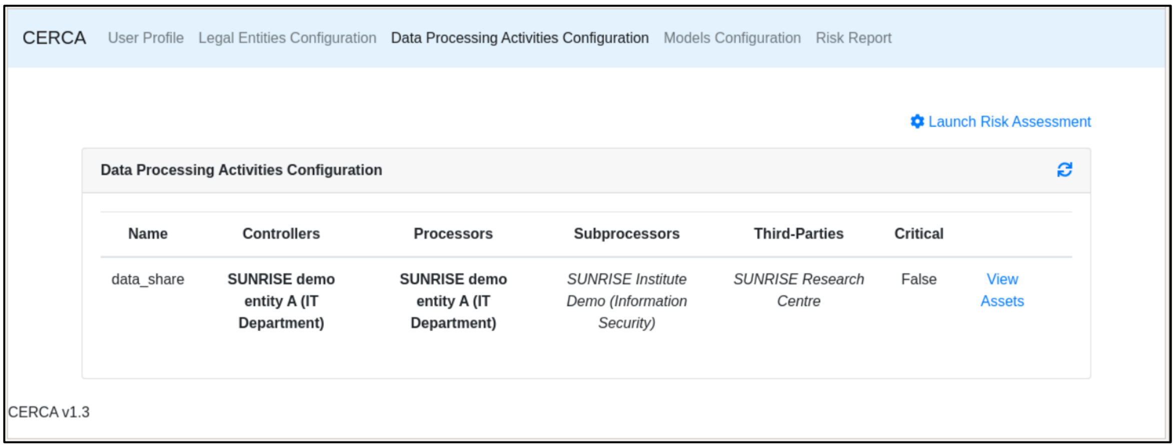
The following two screenshots, Figure 69 and Figure 70, show information from the user profile with more depth. Regarding Figure 70 we can also analyse the assets that we have served as input for the risk assessment module.



Legal Entities Configuration

Name	Department	Description	Responsible	
SUNRISE demo entity A	IT Department	SUNRISE demo entity A	SUNRISE admin (admin@sunrise)	☰

Figure 69. Legal entities configuration menu.

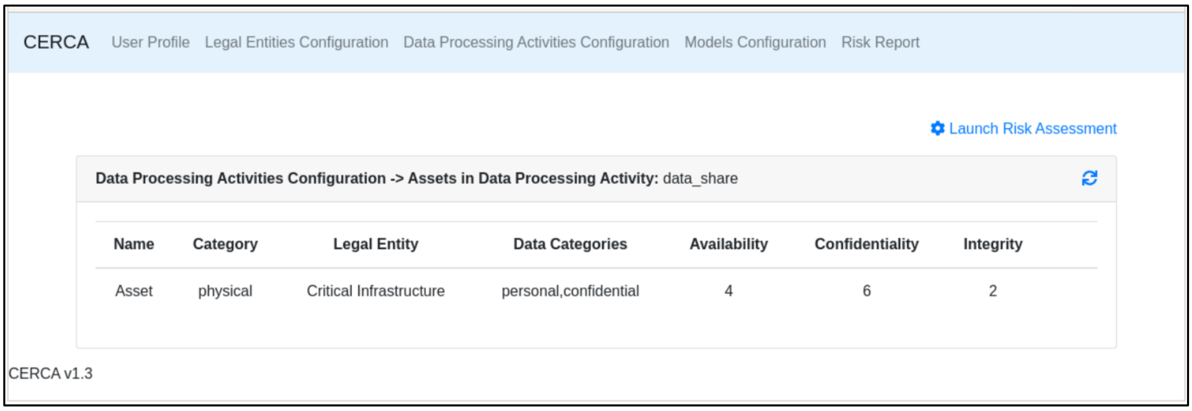


Data Processing Activities Configuration

Name	Controllers	Processors	Subprocessors	Third-Parties	Critical	
data_share	**SUNRISE demo entity A (IT Department)**	**SUNRISE demo entity A (IT Department)**	*SUNRISE Institute Demo (Information Security)*	*SUNRISE Research Centre*	False	View Assets

Figure 70. Data processing activities configuration

Figure 71 shows the menu where all the assets are displayed following the CIA triad (confidentiality, integrity, and availability).

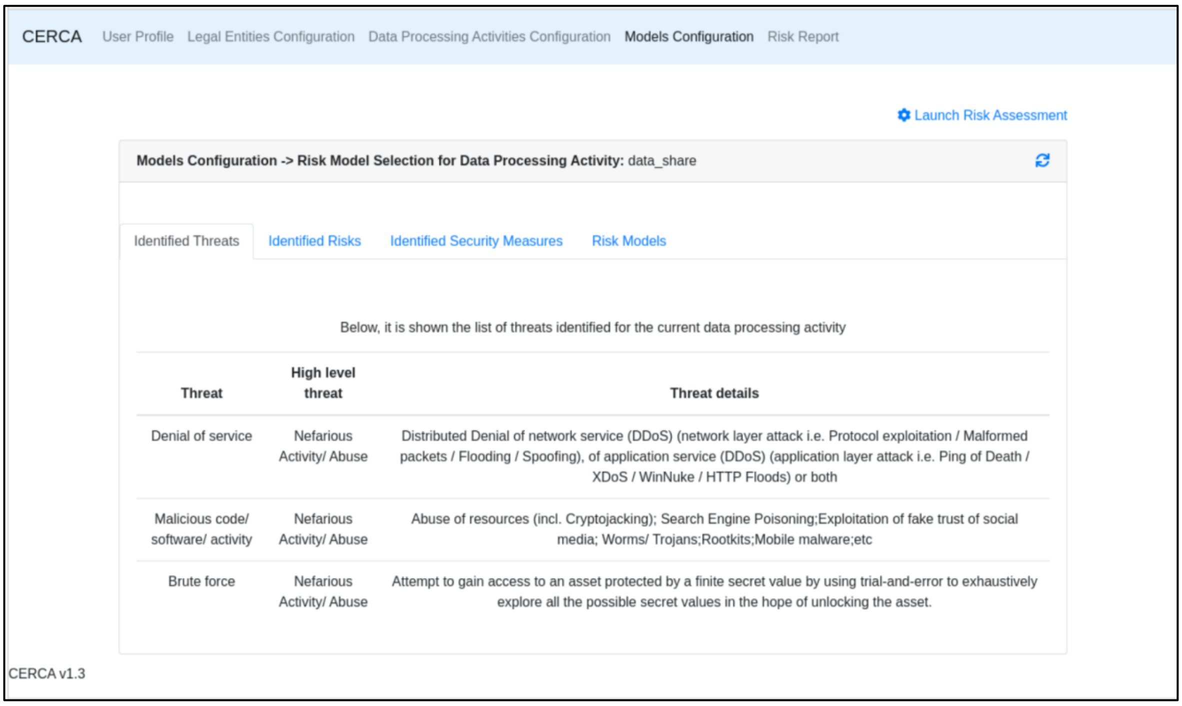


Data Processing Activities Configuration -> Assets in Data Processing Activity: data_share

Name	Category	Legal Entity	Data Categories	Availability	Confidentiality	Integrity
Asset	physical	Critical Infrastructure	personal,confidential	4	6	2

Figure 71. Asset view dashboard.

In Figure 72, a list of threats, risks, and security measures is displayed. We can also select a risk model or clear the current selection.



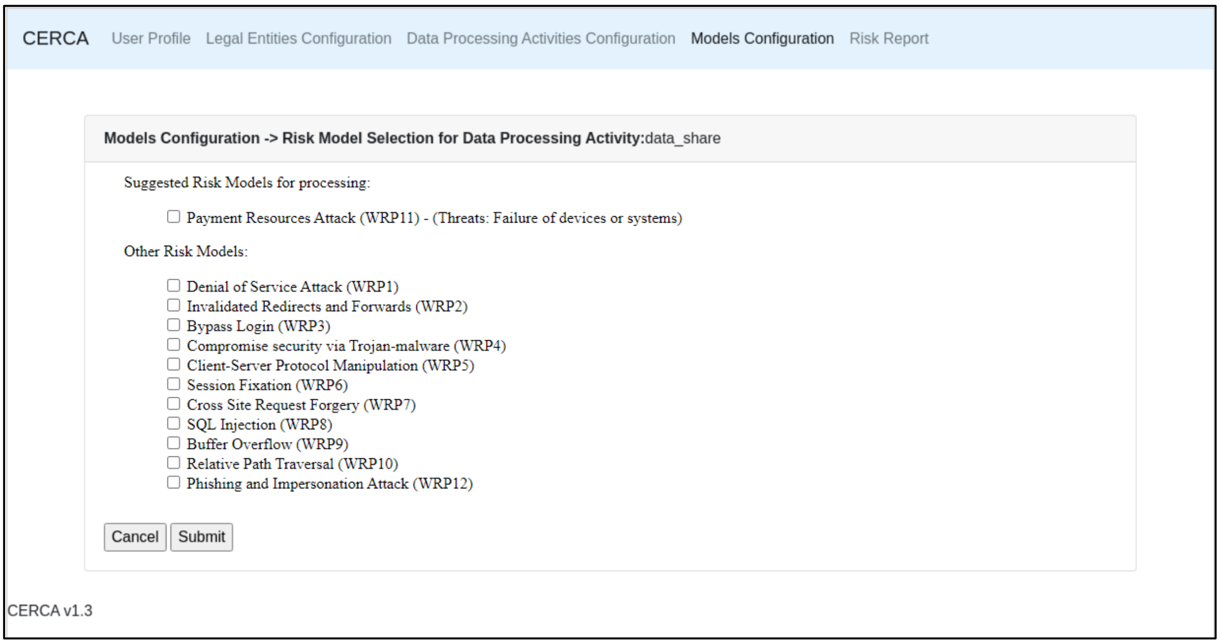
Models Configuration -> Risk Model Selection for Data Processing Activity: data_share

Below, it is shown the list of threats identified for the current data processing activity

Threat	High level threat	Threat details
Denial of service	Nefarious Activity/ Abuse	Distributed Denial of network service (DDoS) (network layer attack i.e. Protocol exploitation / Malformed packets / Flooding / Spoofing), of application service (DDoS) (application layer attack i.e. Ping of Death / XDoS / WinNuke / HTTP Floods) or both
Malicious code/ software/ activity	Nefarious Activity/ Abuse	Abuse of resources (incl. Cryptojacking); Search Engine Poisoning;Exploitation of fake trust of social media; Worms/ Trojans;Rootkits;Mobile malware;etc
Brute force	Nefarious Activity/ Abuse	Attempt to gain access to an asset protected by a finite secret value by using trial-and-error to exhaustively explore all the possible secret values in the hope of unlocking the asset.

Figure 72. Model configuration dashboard.

After clicking the "Select risk models" hyperlink, we are redirected to another menu, which is shown in Figure 73. The tool can suggest a risk model, but the user is free to choose whatever risk model he thinks that might suit better to his infrastructure.


CERCA
User Profile
Legal Entities Configuration
Data Processing Activities Configuration
Models Configuration
Risk Report

Models Configuration -> Risk Model Selection for Data Processing Activity:data_share

Suggested Risk Models for processing:

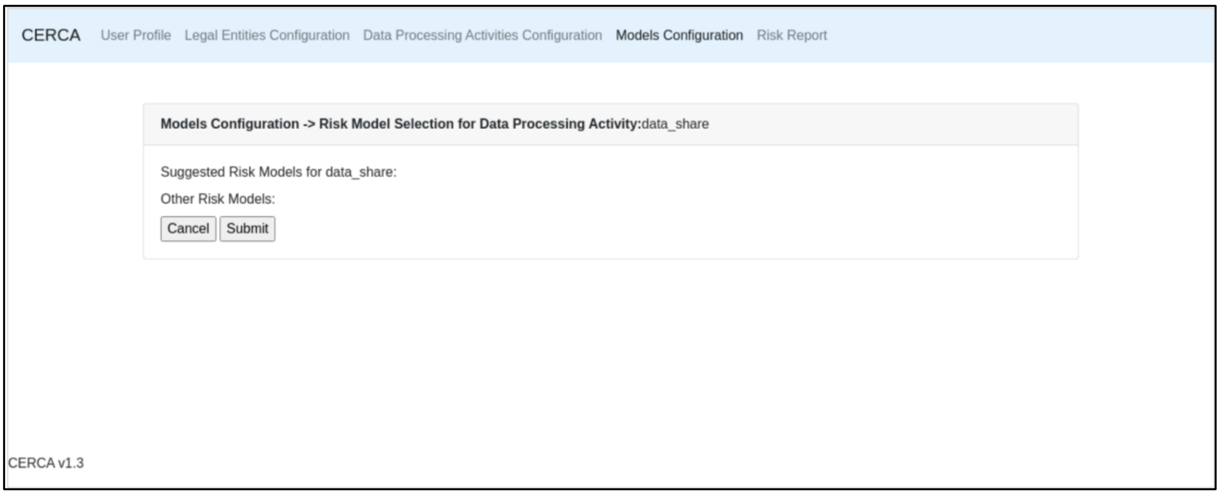
☐ Payment Resources Attack (WRP11) - (Threats: Failure of devices or systems)

Other Risk Models:

☐ Denial of Service Attack (WRP1)
☐ Invalidated Redirects and Forwards (WRP2)
☐ Bypass Login (WRP3)
☐ Compromise security via Trojan-malware (WRP4)
☐ Client-Server Protocol Manipulation (WRP5)
☐ Session Fixation (WRP6)
☐ Cross Site Request Forgery (WRP7)
☐ SQL Injection (WRP8)
☐ Buffer Overflow (WRP9)
☐ Relative Path Traversal (WRP10)
☐ Phishing and Impersonation Attack (WRP12)

Figure 73. Risk model selection dashboard.

After selecting one of the risk models, we can observe that the models' configuration menu (Figure 74) is updated with the new information.


CERCA
User Profile
Legal Entities Configuration
Data Processing Activities Configuration
Models Configuration
Risk Report

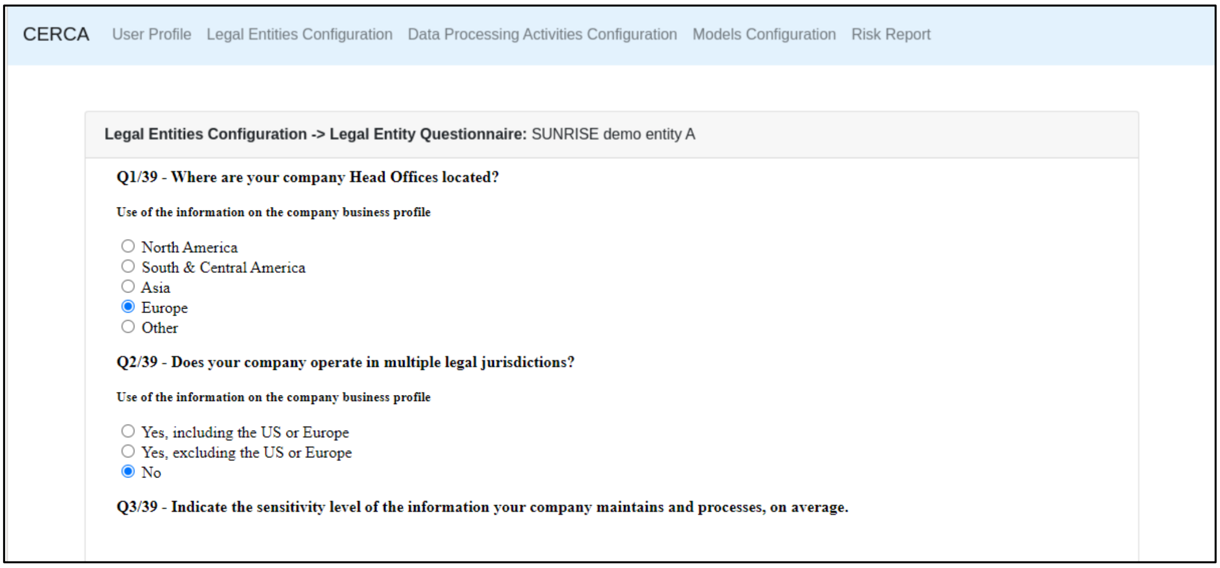
Models Configuration -> Risk Model Selection for Data Processing Activity:data_share

Suggested Risk Models for data_share:

Other Risk Models:

Figure 74. Model configuration dashboard updated with risk model.

One of the most important inputs that CERCA needs to process the cyber risk calculation is the questionnaire. In Figure 75 we can observe an example of it.


CERCA
User Profile
Legal Entities Configuration
Data Processing Activities Configuration
Models Configuration
Risk Report

Legal Entities Configuration -> Legal Entity Questionnaire: SUNRISE demo entity A

Q1/39 - Where are your company Head Offices located?

Use of the information on the company business profile

○ North America
○ South & Central America
○ Asia
● Europe
○ Other

Q2/39 - Does your company operate in multiple legal jurisdictions?

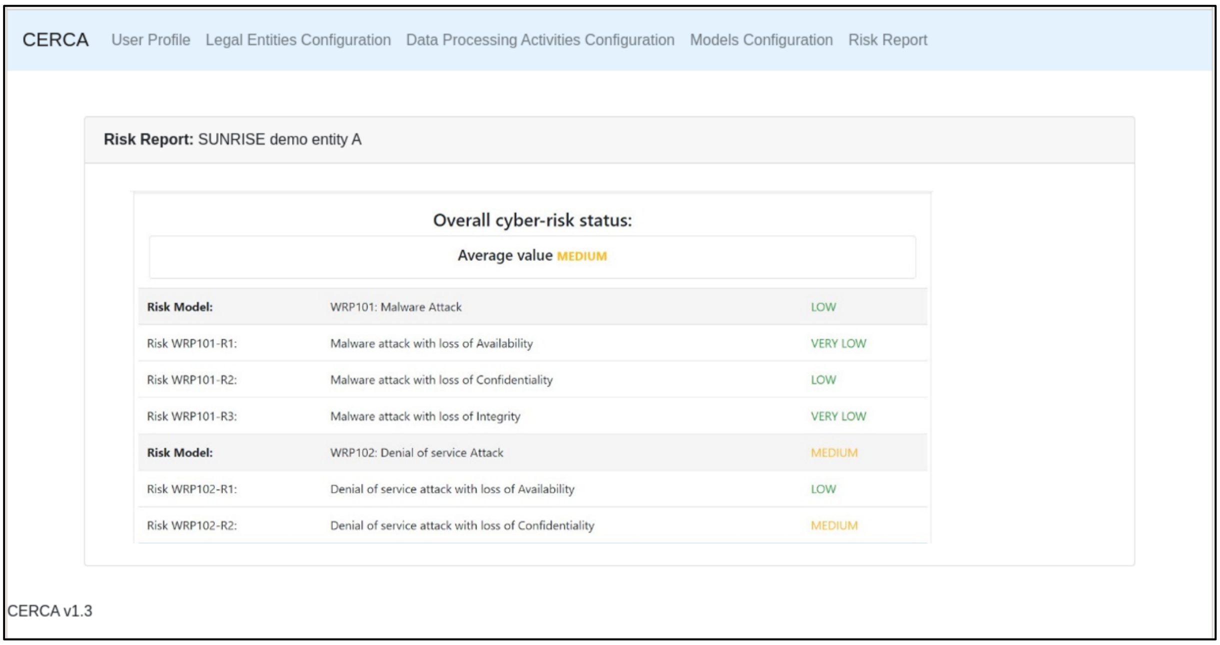
Use of the information on the company business profile

○ Yes, including the US or Europe
○ Yes, excluding the US or Europe
● No

Q3/39 - Indicate the sensitivity level of the information your company maintains and processes, on average.

Figure 75. Questionnaire for risk model.

Finally, after filling the necessary information, we would be able to get the analysis performed by the tool. Figure 76 shows that the risk report works either in a qualitative and quantitative way.


CERCA
User Profile
Legal Entities Configuration
Data Processing Activities Configuration
Models Configuration
Risk Report

Risk Report: SUNRISE demo entity A

Overall cyber-risk status:

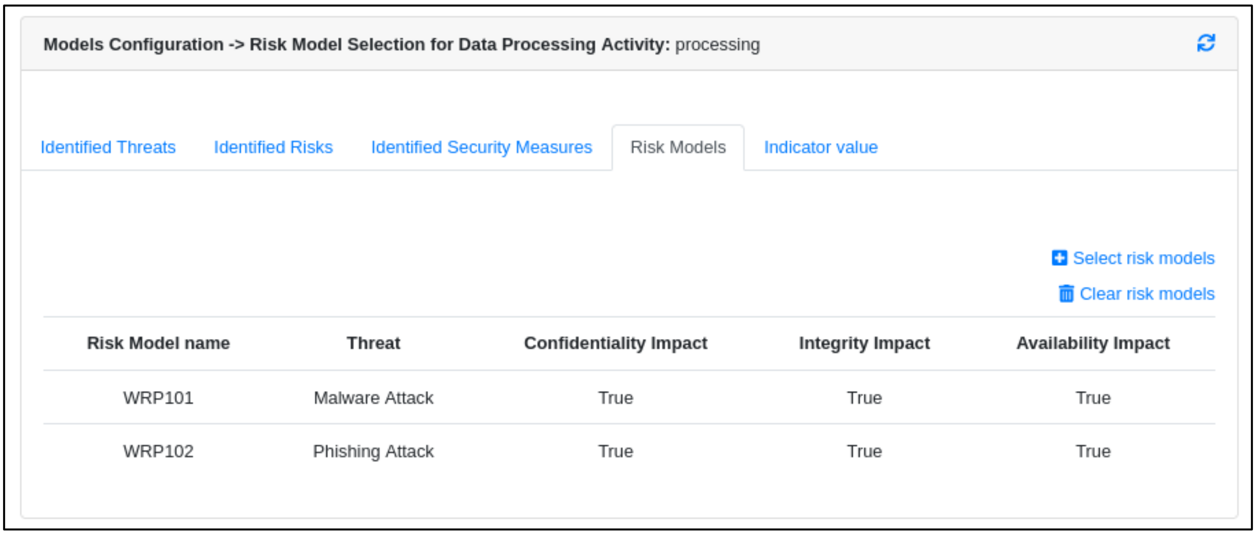
Average value MEDIUM

Risk Model:	WRP101: Malware Attack	LOW
Risk WRP101-R1:	Malware attack with loss of Availability	VERY LOW
Risk WRP101-R2:	Malware attack with loss of Confidentiality	LOW
Risk WRP101-R3:	Malware attack with loss of Integrity	VERY LOW
Risk Model:	WRP102: Denial of service Attack	MEDIUM
Risk WRP102-R1:	Denial of service attack with loss of Availability	LOW
Risk WRP102-R2:	Denial of service attack with loss of Confidentiality	MEDIUM

CERCA v1.3

Figure 76. Risk Report summary.

Indicator view and reset to default value functionality. This view shows the current value of the indicators for the selected risk models:

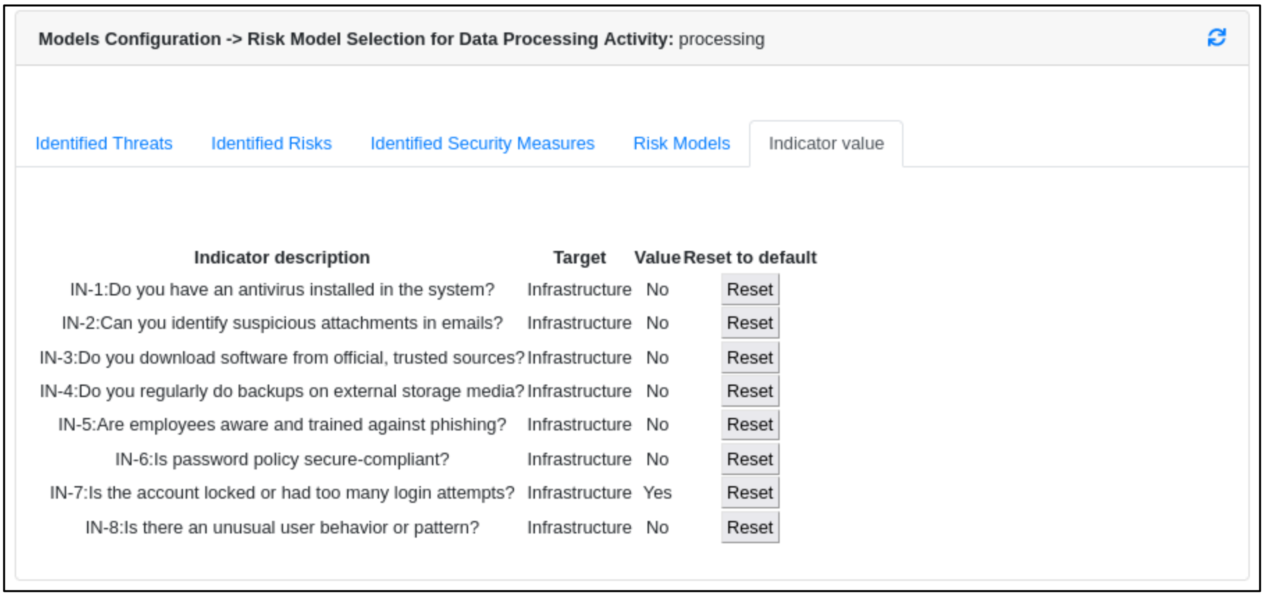


Models Configuration -> Risk Model Selection for Data Processing Activity: processing

Risk Model name	Threat	Confidentiality Impact	Integrity Impact	Availability Impact
WRP101	Malware Attack	True	True	True
WRP102	Phishing Attack	True	True	True

Figure 77: CERCA Selected risk models.

I.III.II NEW FUNCTIONALITIES, GUI, ADMINISTRATION

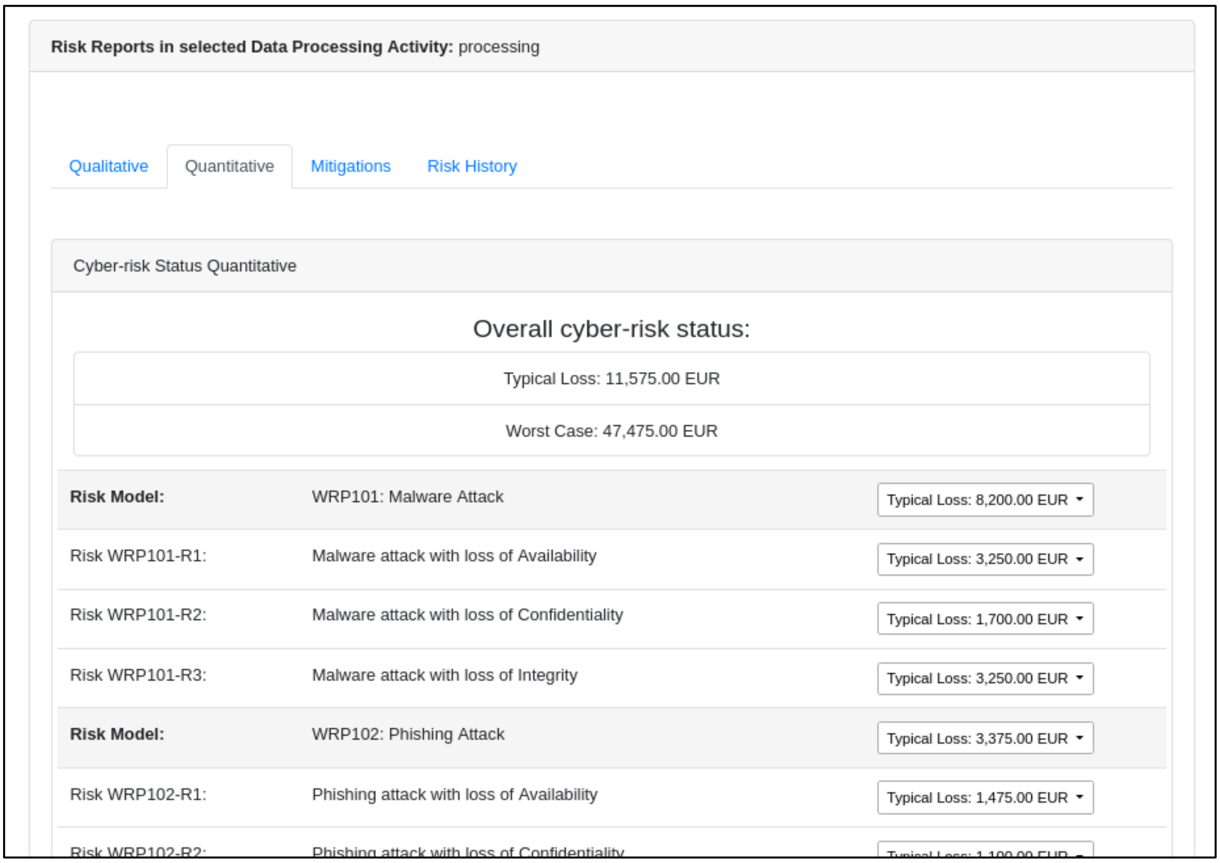


Models Configuration -> Risk Model Selection for Data Processing Activity: processing

Indicator description	Target	Value	Reset to default
IN-1:Do you have an antivirus installed in the system?	Infrastructure	No	Reset
IN-2:Can you identify suspicious attachments in emails?	Infrastructure	No	Reset
IN-3:Do you download software from official, trusted sources?	Infrastructure	No	Reset
IN-4:Do you regularly do backups on external storage media?	Infrastructure	No	Reset
IN-5:Are employees aware and trained against phishing?	Infrastructure	No	Reset
IN-6:Is password policy secure-compliant?	Infrastructure	No	Reset
IN-7:Is the account locked or had too many login attempts?	Infrastructure	Yes	Reset
IN-8:Is there an unusual user behavior or pattern?	Infrastructure	No	Reset

Figure 78: CERCA Indicators current values and reset.

An indicator may need to be reset to its default value to observe the effect on the risk assessment. In this example "IN-7 Is the account locked or had too many login attempts?" has a value of "Yes" (default value is "No") making the risk higher than it would be for the default value:



Risk Reports in selected Data Processing Activity: processing

Cyber-risk Status Quantitative

Overall cyber-risk status:

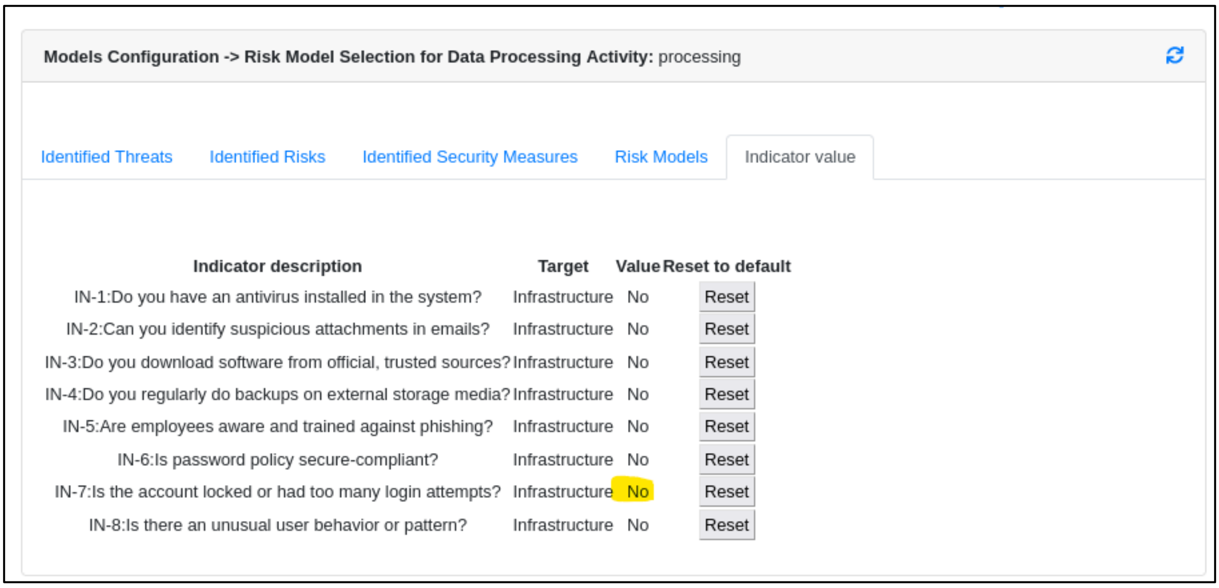
Typical Loss: 11,575.00 EUR

Worst Case: 47,475.00 EUR

Risk Model:	WRP101: Malware Attack	Typical Loss: 8,200.00 EUR
Risk WRP101-R1:	Malware attack with loss of Availability	Typical Loss: 3,250.00 EUR
Risk WRP101-R2:	Malware attack with loss of Confidentiality	Typical Loss: 1,700.00 EUR
Risk WRP101-R3:	Malware attack with loss of Integrity	Typical Loss: 3,250.00 EUR
Risk Model:	WRP102: Phishing Attack	Typical Loss: 3,375.00 EUR
Risk WRP102-R1:	Phishing attack with loss of Availability	Typical Loss: 1,475.00 EUR
Risk WRP102-R2:	Phishing attack with loss of Confidentiality	Typical Loss: 1,100.00 EUR

Figure 79: CERCA risk report before reset.

The value of any indicator can be reset:

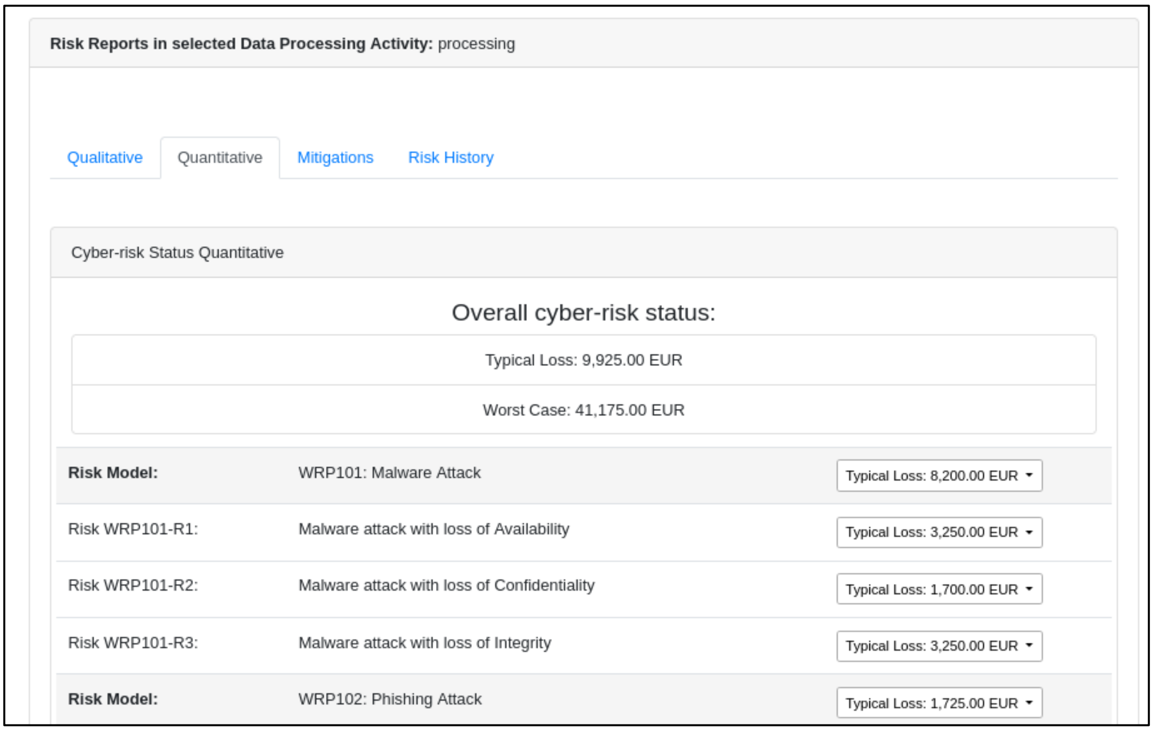


Models Configuration -> Risk Model Selection for Data Processing Activity: processing

Indicator description	Target	Value	Reset to default
IN-1:Do you have an antivirus installed in the system?	Infrastructure	No	Reset
IN-2:Can you identify suspicious attachments in emails?	Infrastructure	No	Reset
IN-3:Do you download software from official, trusted sources?	Infrastructure	No	Reset
IN-4:Do you regularly do backups on external storage media?	Infrastructure	No	Reset
IN-5:Are employees aware and trained against phishing?	Infrastructure	No	Reset
IN-6:Is password policy secure-compliant?	Infrastructure	No	Reset
IN-7:Is the account locked or had too many login attempts?	Infrastructure	No	Reset
IN-8:Is there an unusual user behavior or pattern?	Infrastructure	No	Reset

Figure 80: CERCA indicator reset.

The indicator update is automatically detected, and a new risk report is automatically generated:



Risk Reports in selected Data Processing Activity: processing

Cyber-risk Status Quantitative

Overall cyber-risk status:

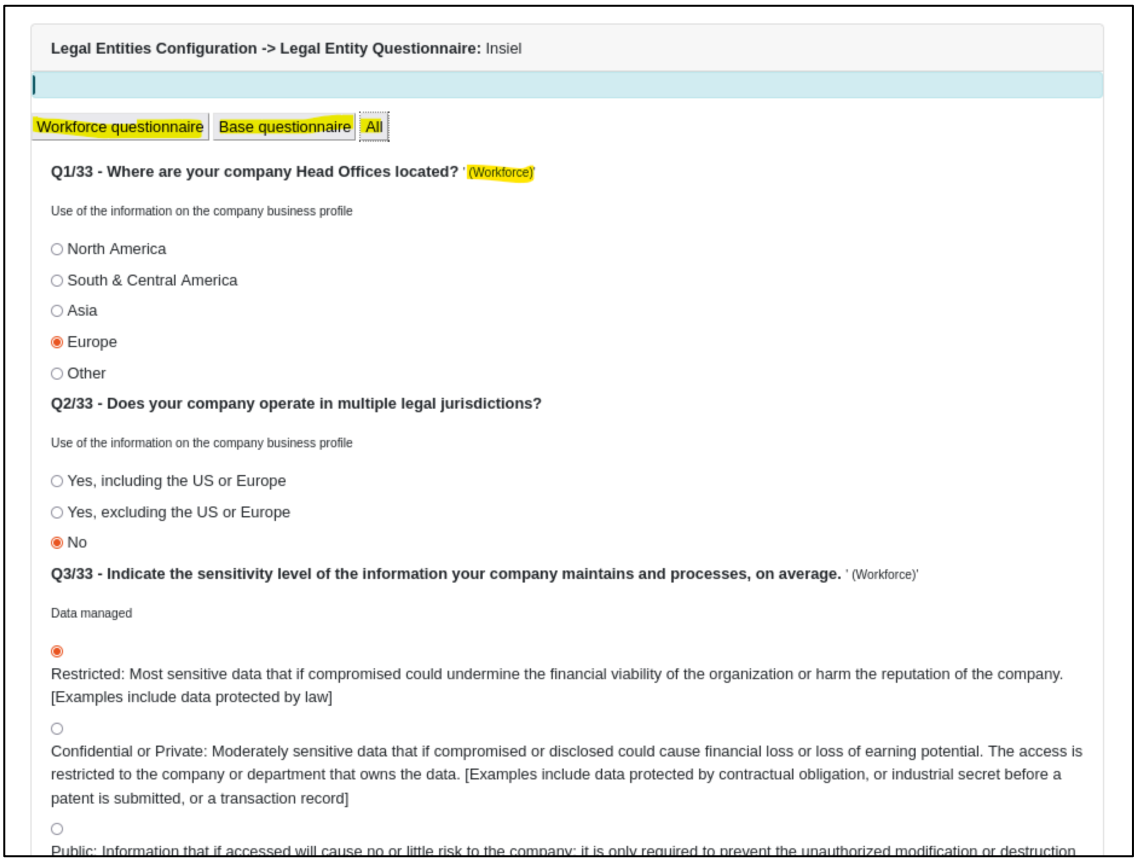
Typical Loss: 9,925.00 EUR

Worst Case: 41,175.00 EUR

Risk Model:	WRP101: Malware Attack	Typical Loss: 8,200.00 EUR ▾
Risk WRP101-R1:	Malware attack with loss of Availability	Typical Loss: 3,250.00 EUR ▾
Risk WRP101-R2:	Malware attack with loss of Confidentiality	Typical Loss: 1,700.00 EUR ▾
Risk WRP101-R3:	Malware attack with loss of Integrity	Typical Loss: 3,250.00 EUR ▾
Risk Model:	WRP102: Phishing Attack	Typical Loss: 1,725.00 EUR ▾

Figure 81: CERCA risk report after reset.

The workforce questionnaire contains:



Legal Entities Configuration -> Legal Entity Questionnaire: Insiel

Q1/33 - Where are your company Head Offices located? '(Workforce)'

Use of the information on the company business profile

○ North America

○ South & Central America

○ Asia

● Europe

○ Other

Q2/33 - Does your company operate in multiple legal jurisdictions?

Use of the information on the company business profile

○ Yes, including the US or Europe

○ Yes, excluding the US or Europe

● No

Q3/33 - Indicate the sensitivity level of the information your company maintains and processes, on average. '(Workforce)'

Data managed

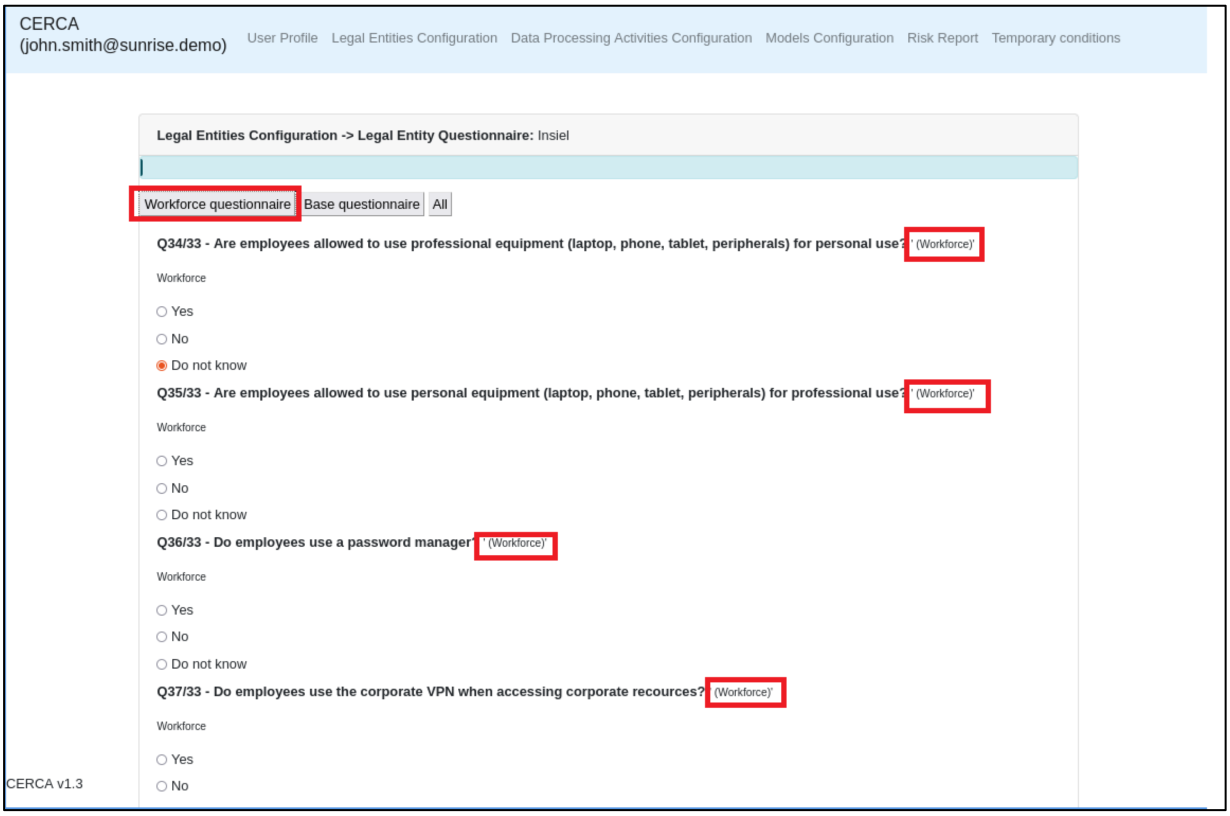
●
Restricted: Most sensitive data that if compromised could undermine the financial viability of the organization or harm the reputation of the company. [Examples include data protected by law]

○
Confidential or Private: Moderately sensitive data that if compromised or disclosed could cause financial loss or loss of earning potential. The access is restricted to the company or department that owns the data. [Examples include data protected by contractual obligation, or industrial secret before a patent is submitted, or a transaction record]

○
Public: Information that if accessed will cause no or little risk to the company; it is only required to prevent the unauthorized modification or destruction

Figure 82: CERCA questionnaire options.

After clicking the “Workforce questionnaire” button, questions are filtered to “Workforce” questions:



CERCA
(john.smith@sunrise.demo)
User Profile
Legal Entities Configuration
Data Processing Activities Configuration
Models Configuration
Risk Report
Temporary conditions

Legal Entities Configuration -> Legal Entity Questionnaire: Insiel

Q34/33 - Are employees allowed to use professional equipment (laptop, phone, tablet, peripherals) for personal use? ' (Workforce)'

Workforce

○ Yes
○ No
● Do not know

Q35/33 - Are employees allowed to use personal equipment (laptop, phone, tablet, peripherals) for professional use? ' (Workforce)'

Workforce

○ Yes
○ No
○ Do not know

Q36/33 - Do employees use a password manager? ' (Workforce)'

Workforce

○ Yes
○ No
○ Do not know

Q37/33 - Do employees use the corporate VPN when accessing corporate recources? ' (Workforce)'

Workforce

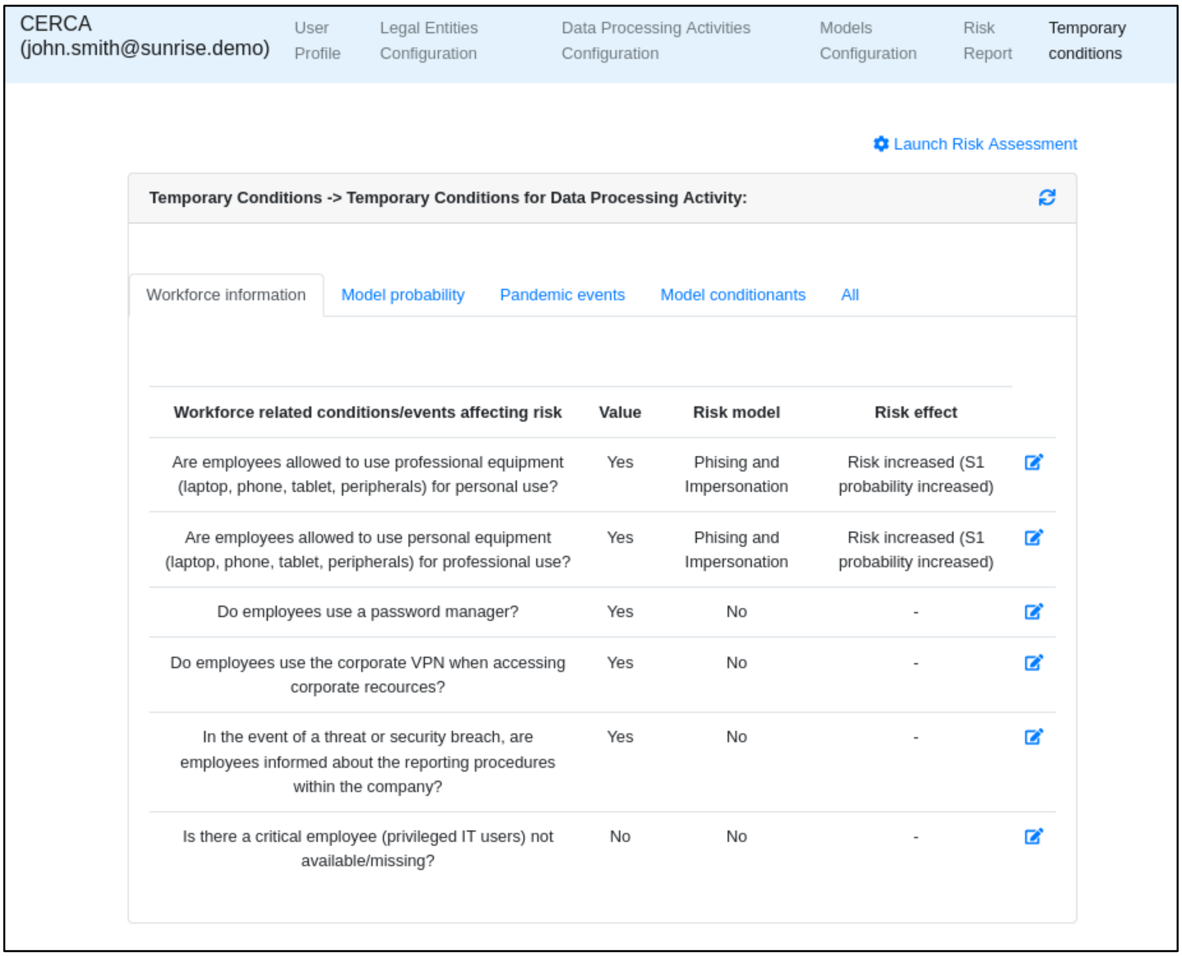
○ Yes
○ No

Figure 83: CERCA Workforce questionnaire.

Questions tagged as “Workforce questionnaire” can be treated and configured separately and affect the risk within the context of workforce conditions.

The temporary conditions view contains configurations and information regarding the workforce.

The “workforce information” tab shows the answers to the workforce questionnaire, its effects on the risk models and the possibility to edit the answers.



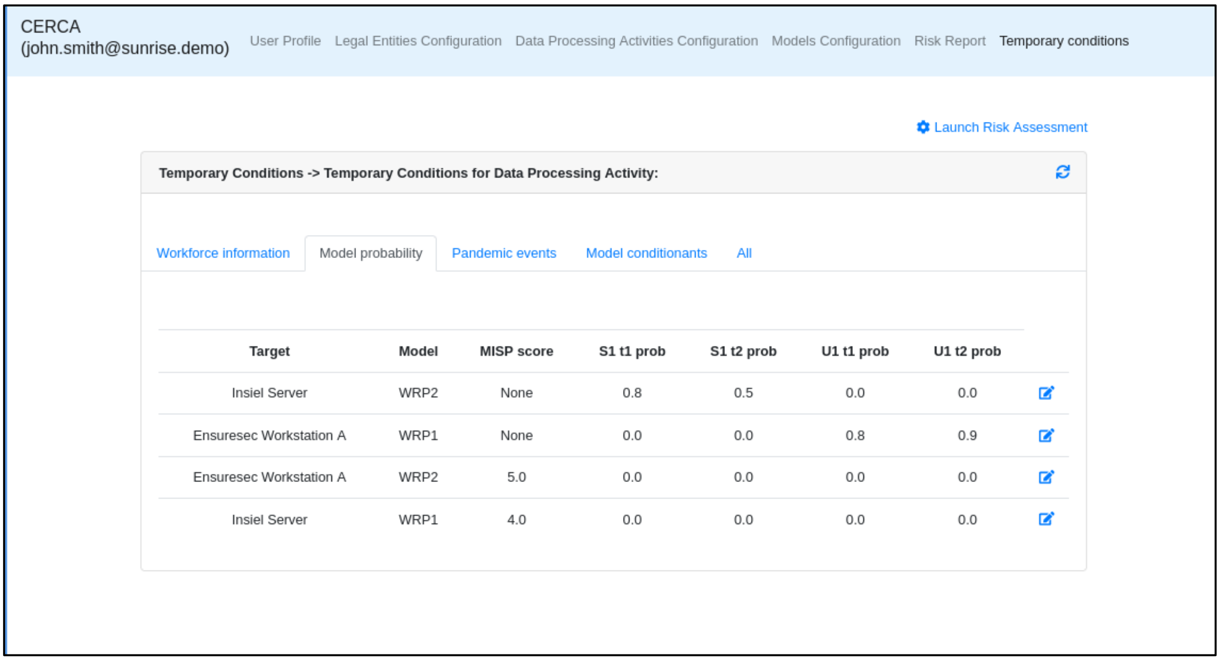
CERCA (john.smith@sunrise.demo)

Temporary Conditions -> Temporary Conditions for Data Processing Activity:

Workforce related conditions/events affecting risk	Value	Risk model	Risk effect	
Are employees allowed to use professional equipment (laptop, phone, tablet, peripherals) for personal use?	Yes	Phising and Impersonation	Risk increased (S1 probability increased)	✎
Are employees allowed to use personal equipment (laptop, phone, tablet, peripherals) for professional use?	Yes	Phising and Impersonation	Risk increased (S1 probability increased)	✎
Do employees use a password manager?	Yes	No	-	✎
Do employees use the corporate VPN when accessing corporate recources?	Yes	No	-	✎
In the event of a threat or security breach, are employees informed about the reporting procedures within the company?	Yes	No	-	✎
Is there a critical employee (privileged IT users) not available/missing?	No	No	-	✎

Figure 84: Workforce information tab.

Probabilities of an attack initiating “Start-1” or S1 and of an attack being successful “Unwanted incident 1” or U1 (the number after S and U indicates a possible path from “Start” to “Unwanted incident”, N:N relation) are available under the “Model probability” tab and can be edited.

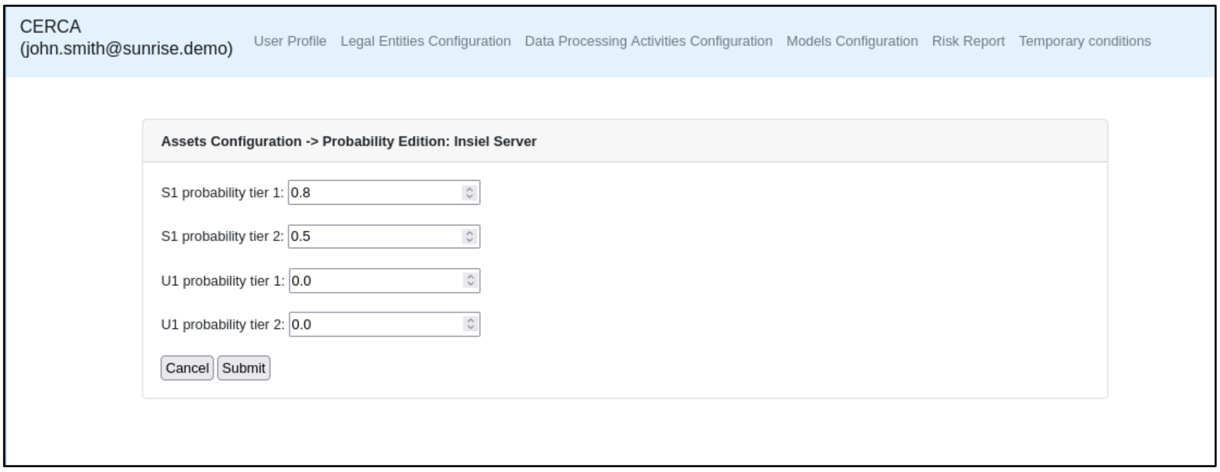


CERCA (john.smith@sunrise.demo)

Temporary Conditions -> Temporary Conditions for Data Processing Activity:

Target	Model	MISP score	S1 t1 prob	S1 t2 prob	U1 t1 prob	U1 t2 prob	
Insiel Server	WRP2	None	0.8	0.5	0.0	0.0	✎
Ensuresec Workstation A	WRP1	None	0.0	0.0	0.8	0.9	✎
Ensuresec Workstation A	WRP2	5.0	0.0	0.0	0.0	0.0	✎
Insiel Server	WRP1	4.0	0.0	0.0	0.0	0.0	✎

Figure 85: Model probability tab: information per asset.



CERCA
(john.smith@sunrise.demo)

User Profile
Legal Entities Configuration
Data Processing Activities Configuration
Models Configuration
Risk Report
Temporary conditions

Assets Configuration -> Probability Edition: Insiel Server

S1 probability tier 1: 0.8

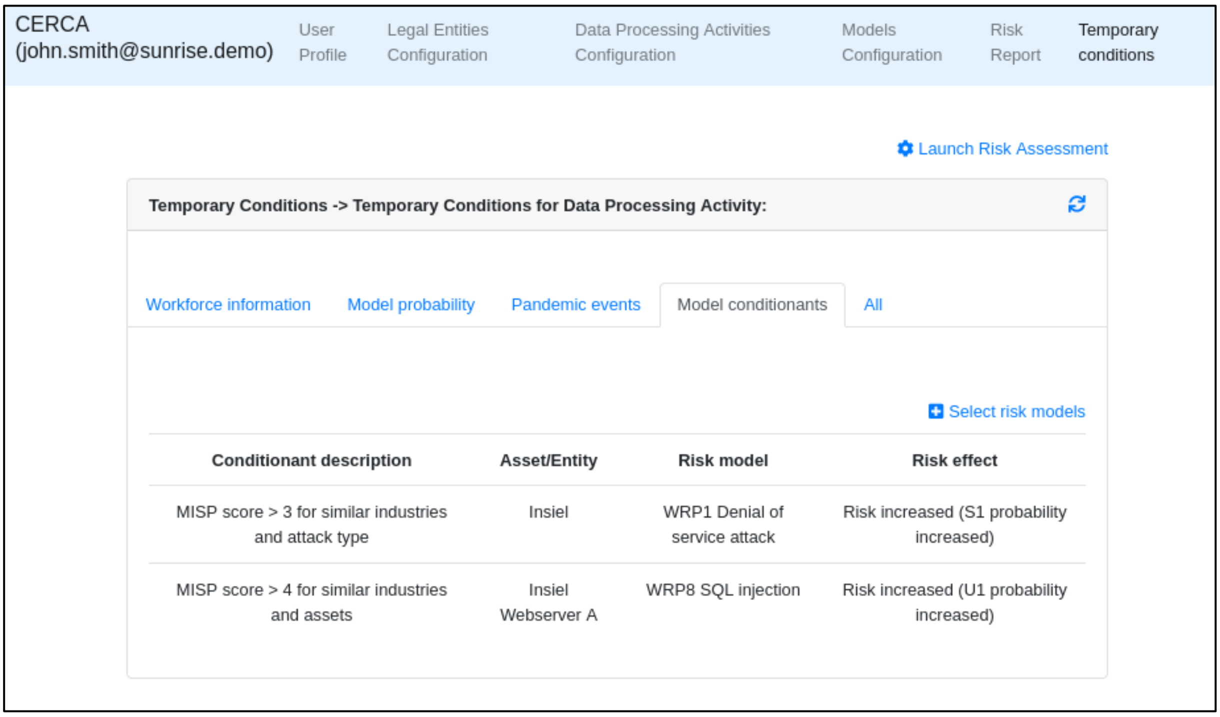
S1 probability tier 2: 0.5

U1 probability tier 1: 0.0

U1 probability tier 2: 0.0

Figure 86: Probability edition for an asset and model.

Model conditionings tab shows conditionings like MISP events affecting a specific target or entity:



CERCA
(john.smith@sunrise.demo)

Temporary Conditions -> Temporary Conditions for Data Processing Activity:

Conditionant description	Asset/Entity	Risk model	Risk effect
MISP score > 3 for similar industries and attack type	Insiel	WRP1 Denial of service attack	Risk increased (S1 probability increased)
MISP score > 4 for similar industries and assets	Insiel Webserver A	WRP8 SQL injection	Risk increased (U1 probability increased)

Figure 87: Model conditionings tab.

Image used by the AI-based inspection tool to generate the output vector that triggers an indicator update at CERCA and a new risk assessment.

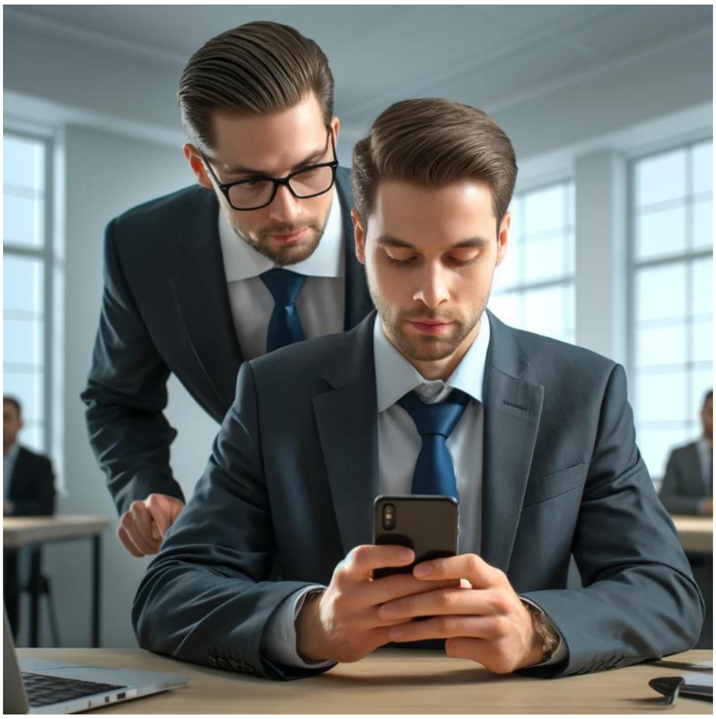


Figure 88: Shoulder surfing example.

The image displayed has been generated using artificial intelligence (AI) technology, specifically through the use of Dally3 from OpenAI. This choice was made due to the lack of freely licensable images that adequately represent this concept. During the proof of concept (PoC) phase, real images were used that cannot be included in this document due to copyright restrictions, though these images represent scenarios and results similar to those presented here.

I.IV Incident Reporting

This manual is an initial version based on the previous manual of the CyberSec4Europe project [11]. Field names and screenshots are for financial entities and bank regulations because the behaviour and functionalities of the module is equal for both cases, and we have not addressed the changes in the graphical interfaces. However, the interfaces and guides will be updated in future releases of the modules and deliverables.

The Incident Reporting module (AIRE) has two main interaction modes. The first is a graphical interface where users can create new incidents or transform the alarms into new incidents, follow the evolution of the incidents, and create and manage reports for authorities. The second is an API that allows the unattended ingestion of the output from other assets. In addition, AIRE has an integrated connection with MISP, which allows it to receive threat alarms from other similar infrastructures.

I.IV.I WEB-GUI

The AIRE web allows creating report templates, mapping incident fields with report forms and setting timers, and managing the reports of the incidents; showing the preview, checking that all fields are fulfilled, and finally generating and sending the report.

I.IV.I.I AIRE GUI – ADMINISTRATOR

Before starting to work normally with AIRE, it is necessary to register an organization, users, contact addresses, regulations, etc. To do so, it is necessary to login as admin, then there is the list of tabs for the different configurations, Figure 89:

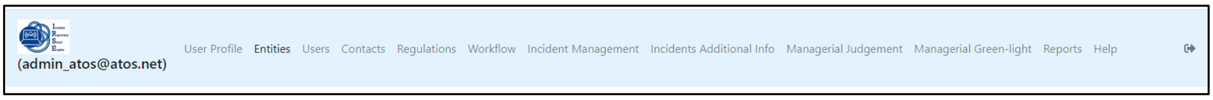
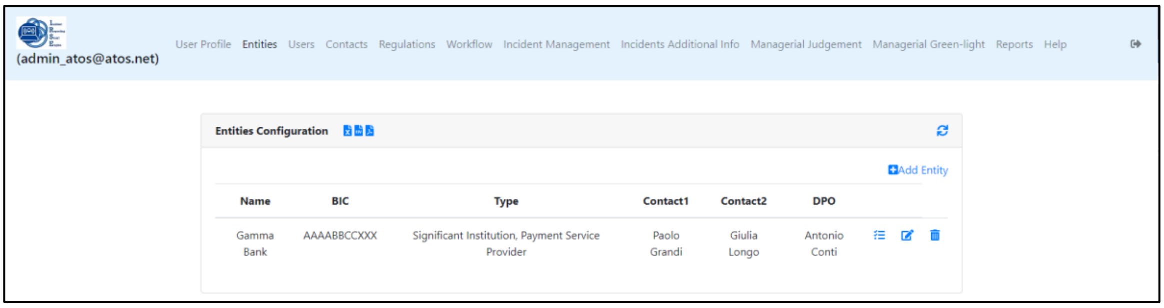


Figure 89. AIRE navigation bar.

1. **Entities:** Show the list of organizations that are registered on AIRE, Figure 90:

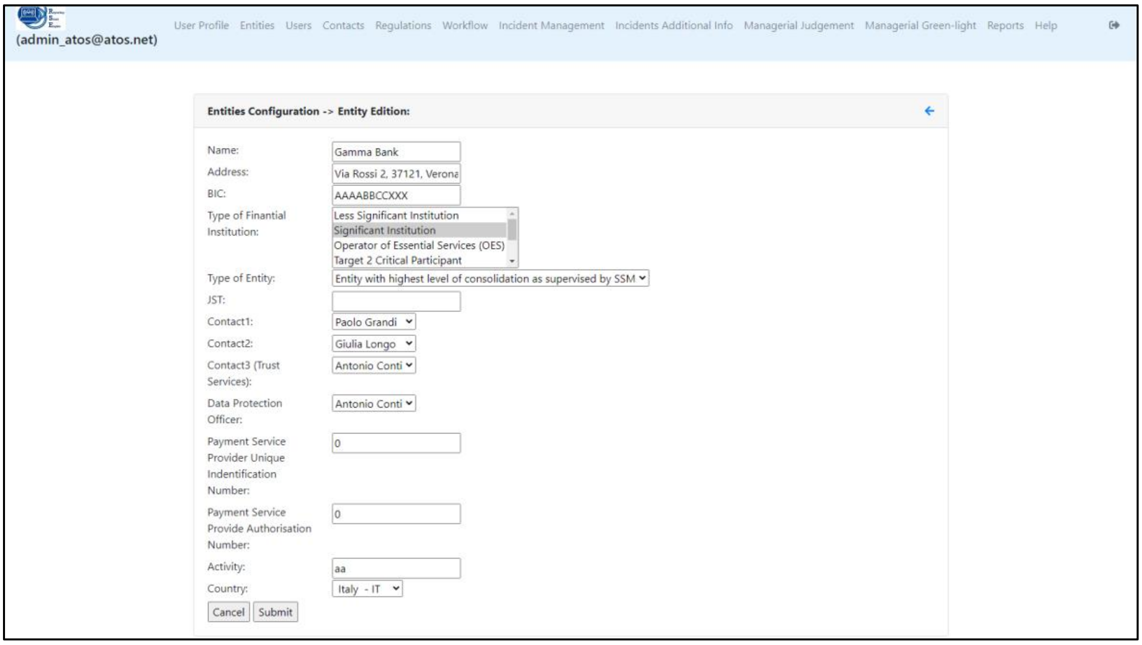


Entities Configuration

Name	BIC	Type	Contact1	Contact2	DPO
Gamma Bank	AAAABBCCXXX	Significant Institution, Payment Service Provider	Paolo Grandi	Giulia Longo	Antonio Conti

Figure 90. Entities Configuration List.

Add Entity or the edit button open a form that allows to create or modify a new organization, Figure 91:

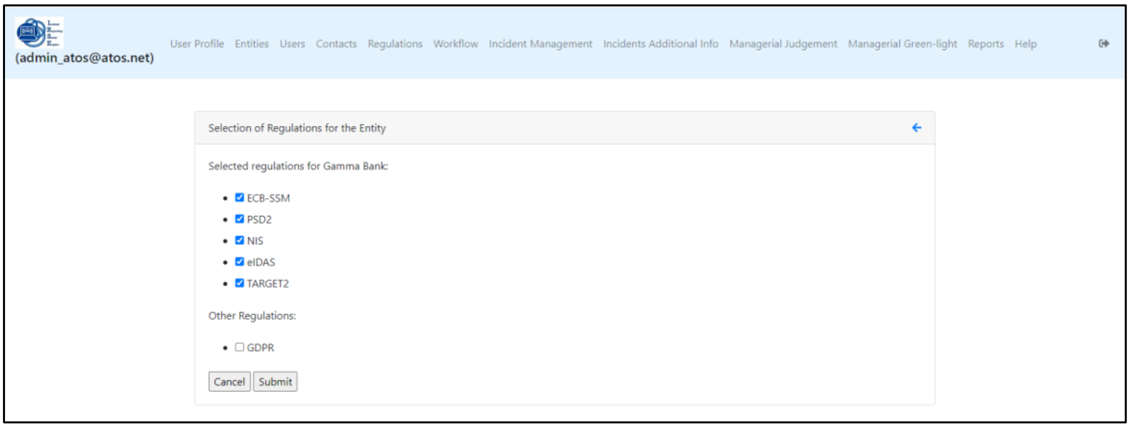


Entities Configuration -> Entity Edition:

Name:	Gamma Bank
Address:	Via Rossi 2, 37121, Verona
BIC:	AAAABBCCXXX
Type of Finantial Institution:	Less Significant Institution Significant Institution Operator of Essential Services (OES) Target 2 Critical Participant
Type of Entity:	Entity with highest level of consolidation as supervised by SSM
JST:	
Contact1:	Paolo Grandi
Contact2:	Giulia Longo
Contact3 (Trust Services):	Antonio Conti
Data Protection Officer:	Antonio Conti
Payment Service Provider Unique Indentification Number:	0
Payment Service Provide Authorisation Number:	0
Activity:	aa
Country:	Italy - IT

Figure 91. New entity form.

Then it is necessary to choose the regulation that the entity must meet, only reports associated to enabled regulations will be generated by the platform, Figure 92.



Selection of Regulations for the Entity

Selected regulations for Gamma Bank:

- ☑ ECB-SSM
- ☑ PSD2
- ☑ NIS
- ☑ eIDAS
- ☑ TARGET2

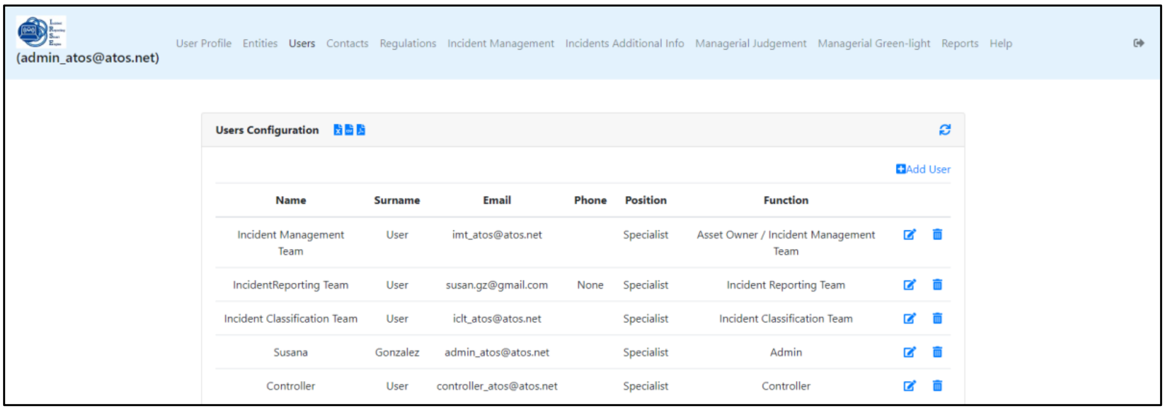
Other Regulations:

- ☐ GDPR

Cancel | Submit

Figure 92. Regulation for entities.

2. **Users:** Show the list of registered users with their information: contact information, position, or function. This page allows creating new users, *Add User*, or edit the information on the created users, Figure 93.



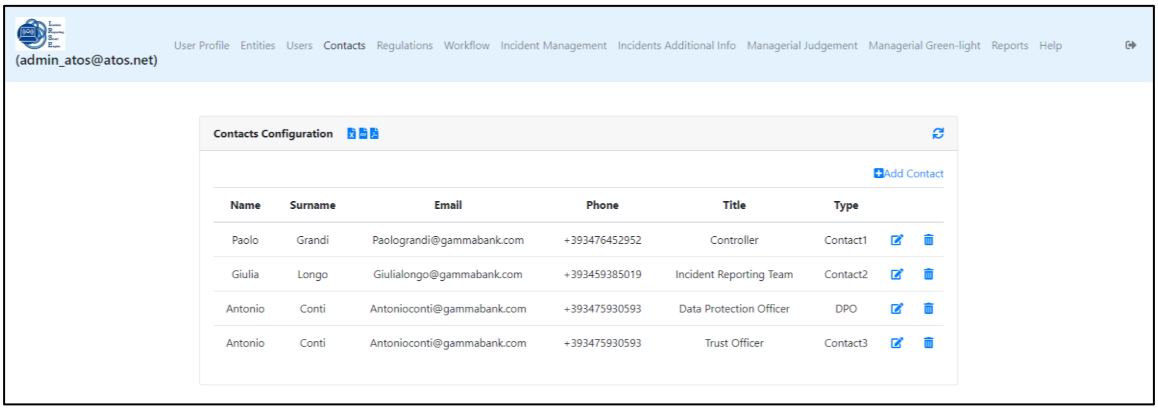
Users Configuration

Add User

Name	Surname	Email	Phone	Position	Function
Incident Management Team	User	imt_atos@atos.net		Specialist	Asset Owner / Incident Management Team
IncidentReporting Team	User	susan.gz@gmail.com	None	Specialist	Incident Reporting Team
Incident Classification Team	User	iclt_atos@atos.net		Specialist	Incident Classification Team
Susana	Gonzalez	admin_atos@atos.net		Specialist	Admin
Controller	User	controller_atos@atos.net		Specialist	Controller

Figure 93. List of registered users.

3. **Contacts:** List of all contacts registered in AIRE, Figure 94. There are the following contact types:
   - Contact1: primary contact
   - Contact2: secondary contact
   - Contact3: associated to the trust officer
   - DPO: Data Protection Officer



Contacts Configuration

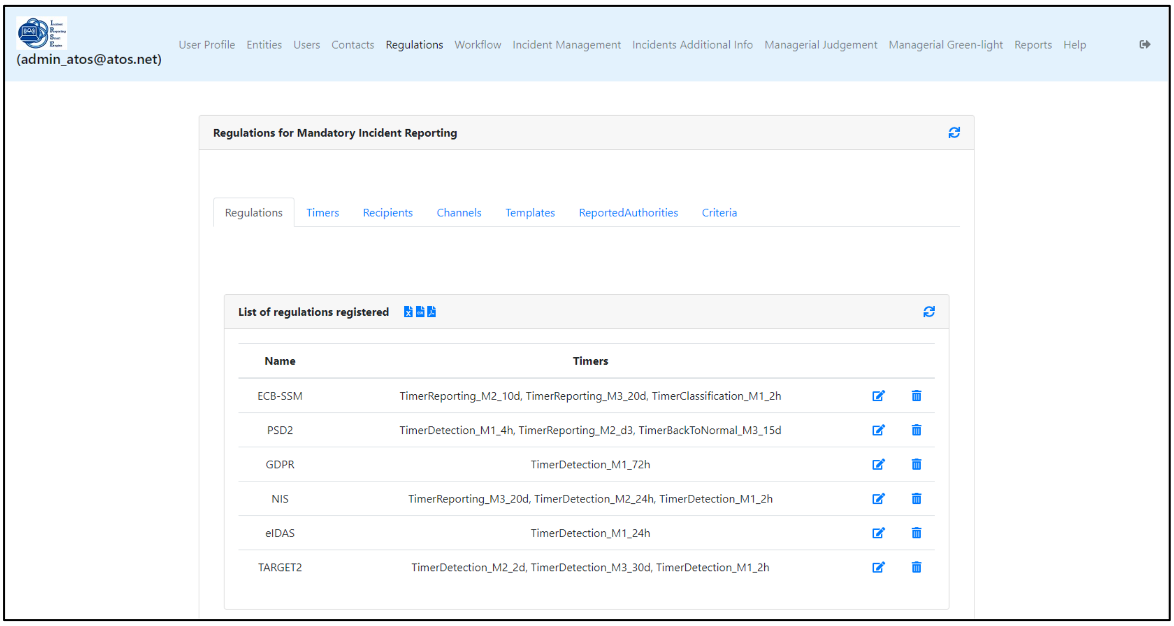
Add Contact

Name	Surname	Email	Phone	Title	Type
Paolo	Grandi	Paolograndi@gammabank.com	+393476452952	Controller	Contact1
Giulia	Longo	Giulialongo@gammabank.com	+393459385019	Incident Reporting Team	Contact2
Antonio	Conti	Antonioconti@gammabank.com	+393475930593	Data Protection Officer	DPO
Antonio	Conti	Antonioconti@gammabank.com	+393475930593	Trust Officer	Contact3

Figure 94. List of configured contacts.

4. **Regulations:** Regulations for Mandatory Incident Reporting. This section manages the different regulations and has several subsections:

   4.1. **Regulations:** List of registered regulations, Figure 95.


(admin_atos@atos.net)
User Profile Entities Users Contacts Regulations Workflow Incident Management Incidents Additional Info Managerial Judgement Managerial Green-light Reports Help

Regulations for Mandatory Incident Reporting

Regulations Timers Recipients Channels Templates ReportedAuthorities Criteria

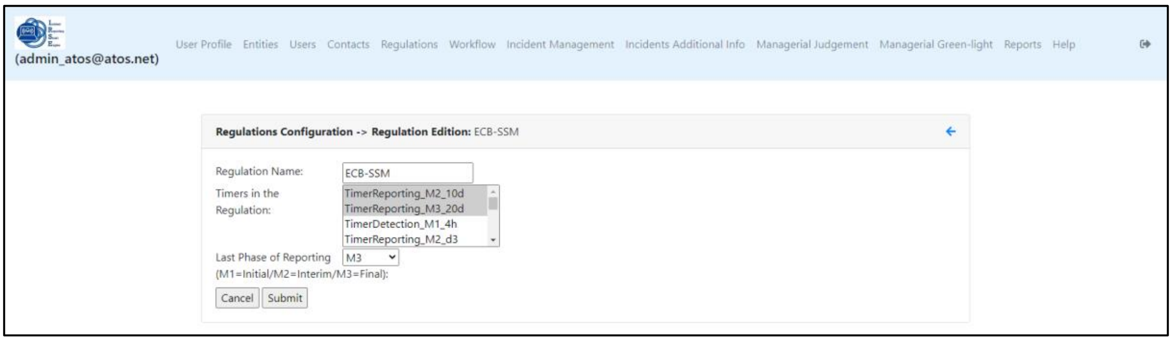
List of regulations registered

Name	Timers
ECB-SSM	TimerReporting_M2_10d, TimerReporting_M3_20d, TimerClassification_M1_2h
PSD2	TimerDetection_M1_4h, TimerReporting_M2_d3, TimerBackToNormal_M3_15d
GDPR	TimerDetection_M1_72h
NIS	TimerReporting_M3_20d, TimerDetection_M2_24h, TimerDetection_M1_2h
eIDAS	TimerDetection_M1_24h
TARGET2	TimerDetection_M2_2d, TimerDetection_M3_30d, TimerDetection_M1_2h

Figure 95. List of regulations registered.

For each regulation registered in the platform, Figure 95, it is necessary to indicate:

- Last phase of reporting: depending on the reports that must be disseminated according to a specific directive or regulation, it will be selected:
  - M1 (Initial) if only one report is required.
  - M2 (interim) in case a first and a second reports are required.
  - M3 (final) in case three mandatory reports (first, interim, and final) are necessary.
- The Timers that will be triggered with the regulations (see next point about Timers)


(admin_atos@atos.net)
User Profile Entities Users Contacts Regulations Workflow Incident Management Incidents Additional Info Managerial Judgement Managerial Green-light Reports Help

Regulations Configuration -> Regulation Edition: ECB-SSM

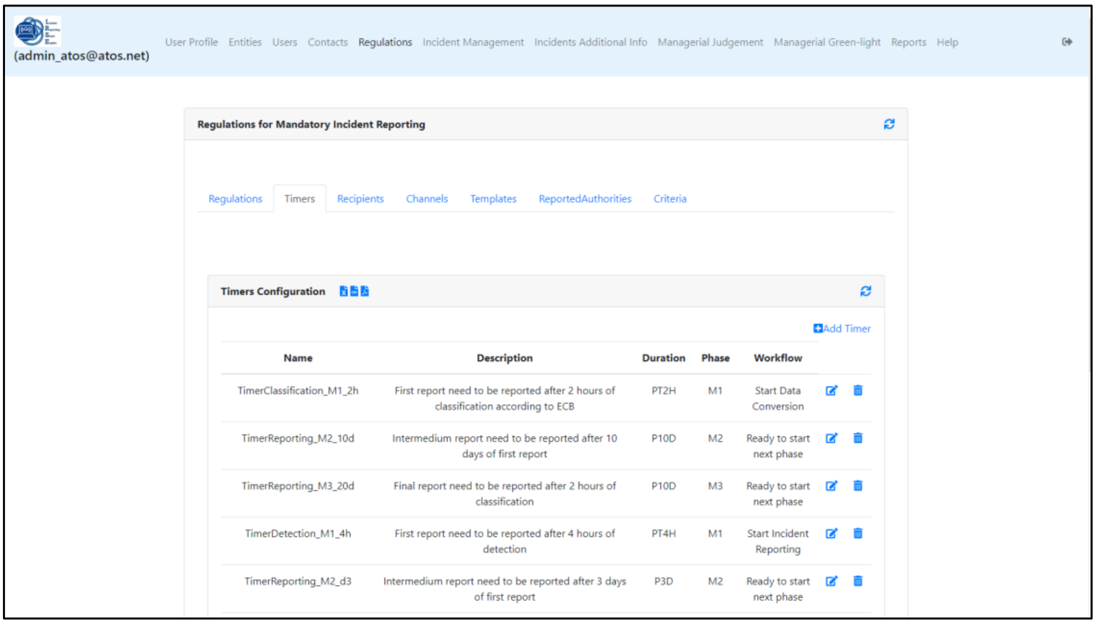
Regulation Name: ECB-SSM

Timers in the Regulation: TimerReporting_M2_10d, TimerReporting_M3_20d, TimerDetection_M1_4h, TimerReporting_M2_d3

Last Phase of Reporting (M1=Initial/M2=Interim/M3=Final): M3

Figure 96. New regulation form.

4.2. **Timers:** Indicate when a notification needs to be sent to the incident contact user (the email configured as Contact User in the TheHive template), Figure 95. In case a mandatory report has not been sent to the corresponding Supervisory Authorities in the deadline defined by a specific regulation.



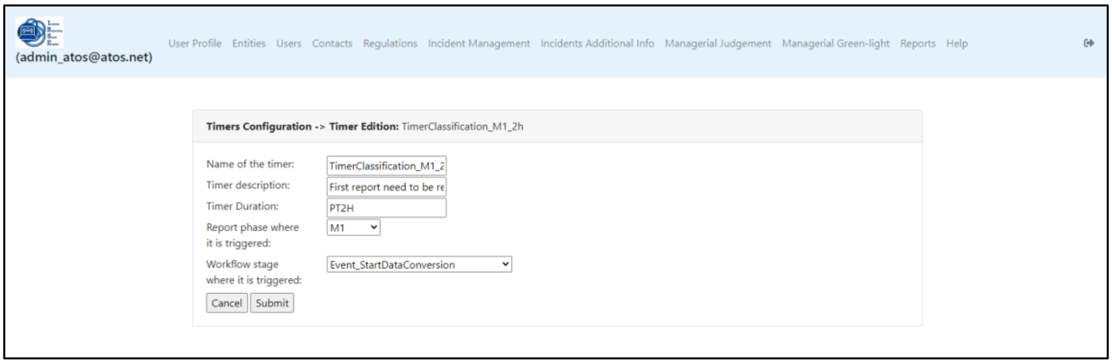
Regulations for Mandatory Incident Reporting

Timers Configuration

Name	Description	Duration	Phase	Workflow
TimerClassification_M1_2h	First report need to be reported after 2 hours of classification according to ECB	PT2H	M1	Start Data Conversion
TimerReporting_M2_10d	Intermedium report need to be reported after 10 days of first report	P10D	M2	Ready to start next phase
TimerReporting_M3_20d	Final report need to be reported after 2 hours of classification	P10D	M3	Ready to start next phase
TimerDetection_M1_4h	First report need to be reported after 4 hours of detection	PT4H	M1	Start Incident Reporting
TimerReporting_M2_d3	Intermedium report need to be reported after 3 days of first report	P3D	M2	Ready to start next phase

Figure 97. List of timers.

Timer Edition, Figure 98, allows creating new timers or modifying existing ones. The *timer duration* field defines the time windows within the report must be sent and uses ISO 8601 durations format[8]. *Report phase* defines the phase in which the report should be sent. And the *Workflow stage* defines the event that triggers the current timer.



Timers Configuration -> Timer Edition: TimerClassification_M1_2h

Name of the timer: TimerClassification_M1_2

Timer description: First report need to be re

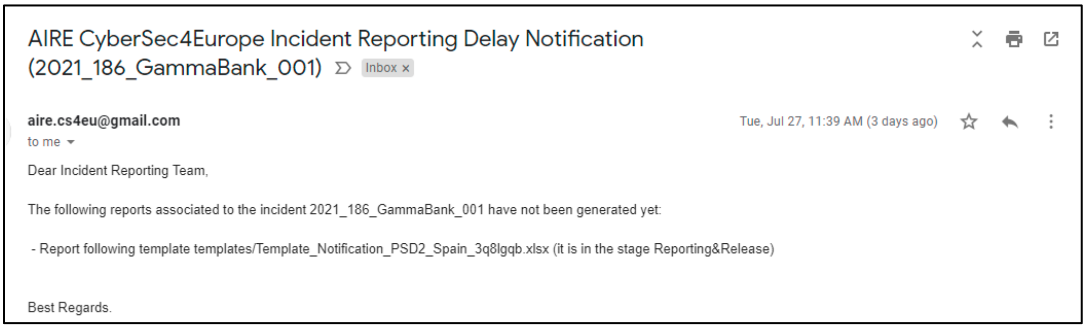
Timer Duration: PT2H

Report phase where it is triggered: M1

Workflow stage where it is triggered: Event_StartDataConversion

Figure 98. Timer edition form.

AIRE sends an email to the responsible party when a report is not sent on time, Figure 99.



AIRE CyberSec4Europe Incident Reporting Delay Notification (2021_186_GammaBank_001)

aire.cs4eu@gmail.com

Tue, Jul 27, 11:39 AM (3 days ago)

Dear Incident Reporting Team,

The following reports associated to the incident 2021_186_GammaBank_001 have not been generated yet:

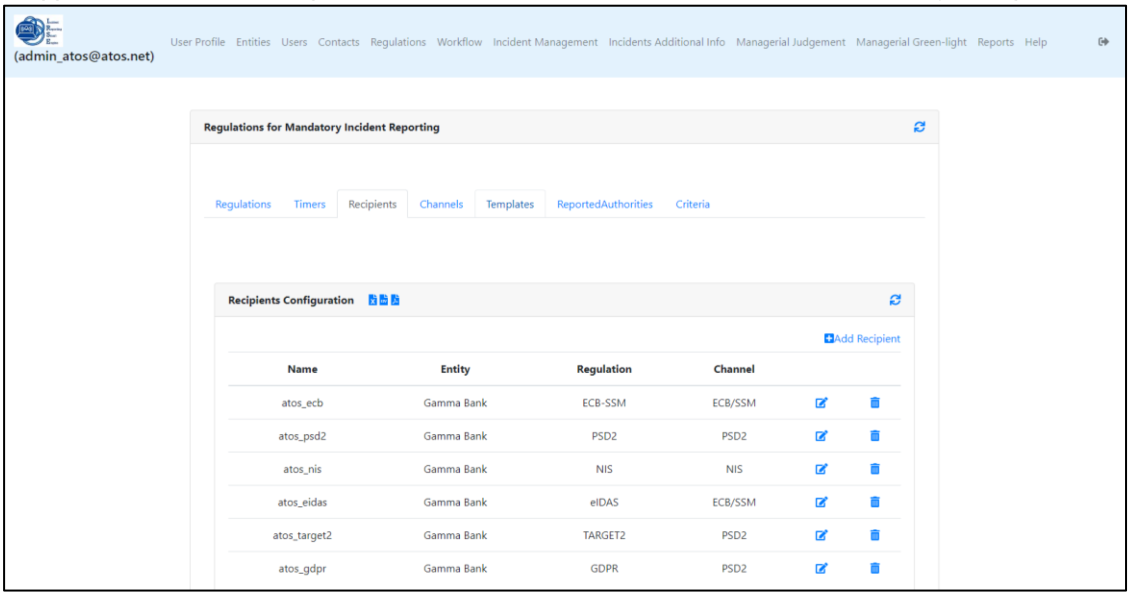
- Report following template templates/Template_Notification_PSD2_Spain_3q8lgqb.xlsx (it is in the stage Reporting&Release)

Best Regards.

Figure 99. Example of email sent by AIRE.

[8] https://en.wikipedia.org/wiki/ISO_8601

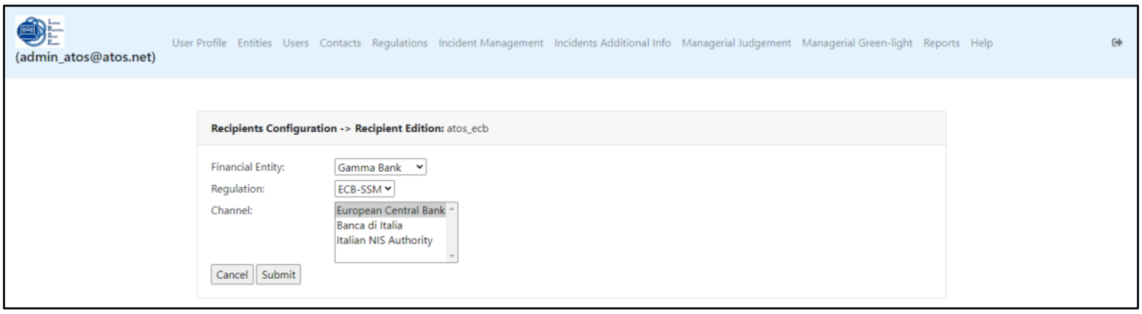
4.3. **Recipients:** Associated to each entity and regulation, Figure 100. It will have also a Channel associated, which will be shown once the report has been generated by the platform as a suggestion of channel (e.g., email address) that need to be followed for the reporting.


(admin_atos@atos.net)
User Profile Entities Users Contacts Regulations Workflow Incident Management Incidents Additional Info Managerial Judgement Managerial Green-light Reports Help
Regulations for Mandatory Incident Reporting
Regulations Timers Recipients Channels Templates ReportedAuthorities Criteria
Add Recipient

Recipients Configuration

Name	Entity	Regulation	Channel
atos_ecb	Gamma Bank	ECB-SSM	ECB/SSM
atos_psd2	Gamma Bank	PSD2	PSD2
atos_nis	Gamma Bank	NIS	NIS
atos_eidas	Gamma Bank	eIDAS	ECB/SSM
atos_target2	Gamma Bank	TARGET2	PSD2
atos_gdpr	Gamma Bank	GDPR	PSD2

Figure 100. List of Recipient Configurations.

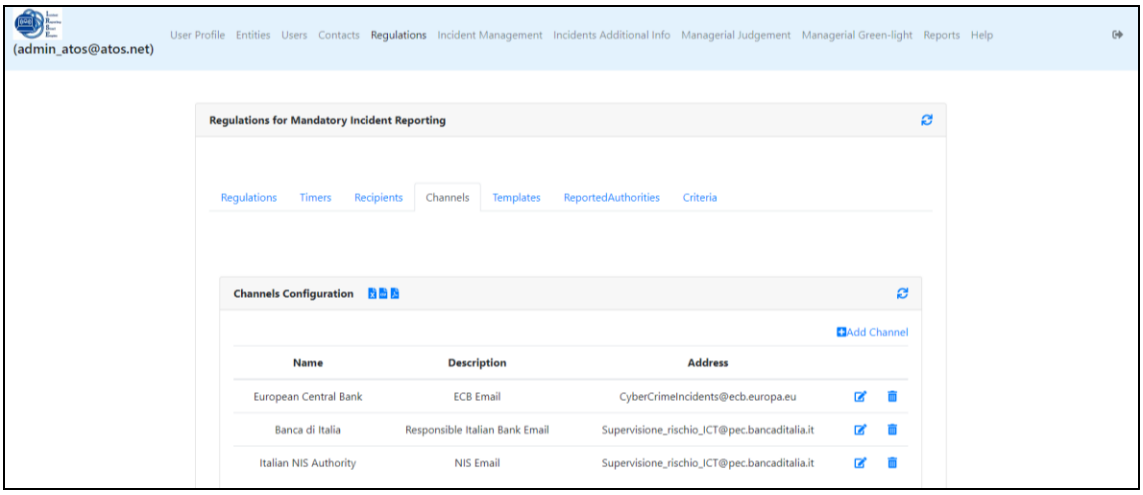

(admin_atos@atos.net)
User Profile Entities Users Contacts Regulations Incident Management Incidents Additional Info Managerial Judgement Managerial Green-light Reports Help
Cancel
Submit

Recipients Configuration -> Recipient Edition: atos_ecb

Financial Entity: Gamma Bank
Regulation: ECB-SSM
Channel: European Central Bank
Banca di Italia
Italian NIS Authority

Figure 101. Recipient Edition Form.

4.4. **Channels:** The information registered here, Figure 102, will be used in the Recipients and shown to the user as a suggestion when the reports are ready for revision and releasing.

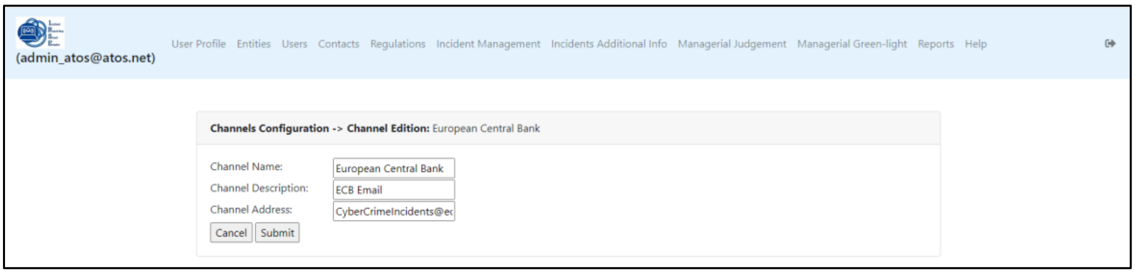

(admin_atos@atos.net)
User Profile Entities Users Contacts Regulations Incident Management Incidents Additional Info Managerial Judgement Managerial Green-light Reports Help
Regulations for Mandatory Incident Reporting
Regulations Timers Recipients Channels Templates ReportedAuthorities Criteria
Add Channel

Channels Configuration

Name	Description	Address
European Central Bank	ECB Email	CyberCrimeIncidents@ecb.europa.eu
Banca di Italia	Responsible Italian Bank Email	Supervisione_rischio_ICT@pec.bancaditalia.it
Italian NIS Authority	NIS Email	Supervisione_rischio_ICT@pec.bancaditalia.it

Figure 102. List of communication channels.

Add Channel button allow adding or modifying channels, Figure 103.



Channels Configuration -> Channel Edition: European Central Bank

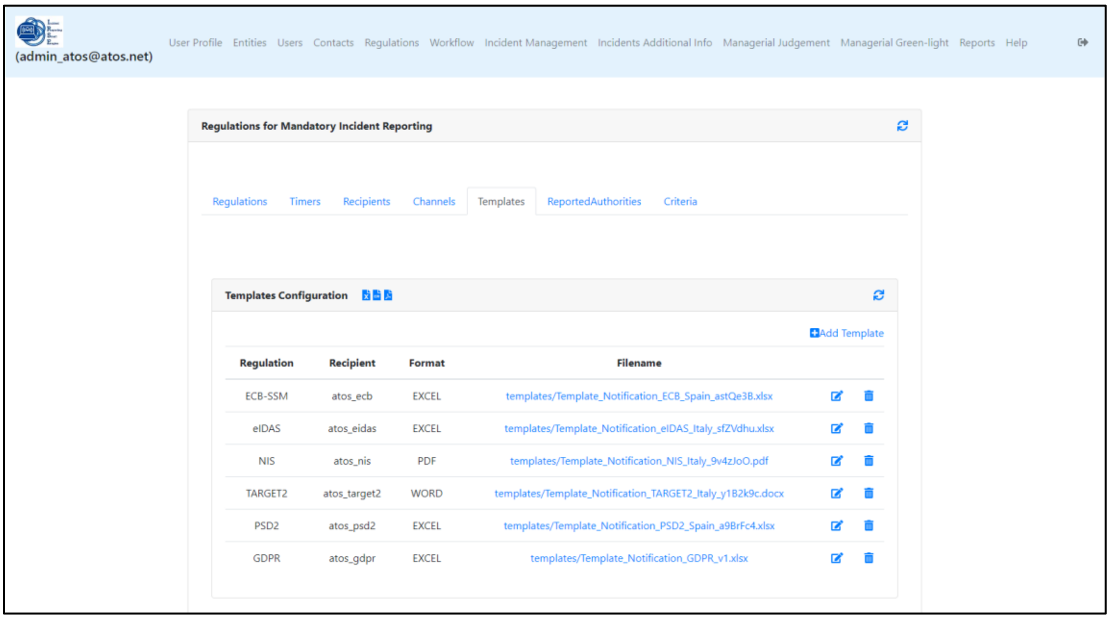
Channel Name: European Central Bank

Channel Description: ECB Email

Channel Address: CyberCrimeIncidents@ec

Figure 103. Channel Edition.

Templates: used by the platform for the generation of the reports will need to be associated to a regulation and a recipient. The formats currently supported are EXCEL, PDF, and WORD. The template data format is the format used by the platform to populate information about times in the reports. Date and time formats used are the ones defined in SimpleDateFormat[9].

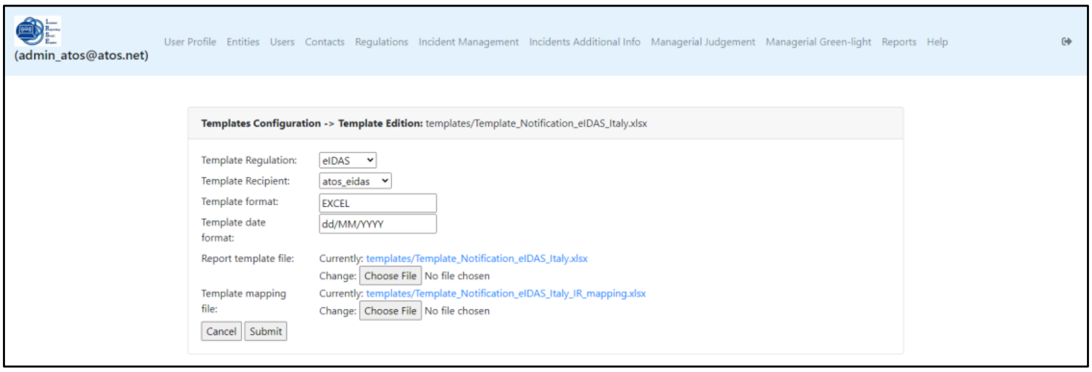


Regulation	Recipient	Format	Filename
ECB-SSM	atos_ecb	EXCEL	templates/Template_Notification_ECB_Spain_astQe3B.xlsx
eIDAS	atos_eidas	EXCEL	templates/Template_Notification_eIDAS_Italy_sfZVdhu.xlsx
NIS	atos_nis	PDF	templates/Template_Notification_NIS_Italy_9v4zJoO.pdf
TARGET2	atos_target2	WORD	templates/Template_Notification_TARGET2_Italy_y1B2k9c.docx
PSD2	atos_psd2	EXCEL	templates/Template_Notification_PSD2_Spain_a9BrFc4.xlsx
GDPR	atos_gdpr	EXCEL	templates/Template_Notification_GDPR_v1.xlsx

Figure 104. List of Templates.

Each *Template* is associated with a *Regulation*, a *Recipient*, a *Report template file*, and a *Template mapping file*. The *Report template file* is the base for the generated report and allows the extensions *pdf*, *doc*, *docx*, *xls*, and *xlsx*; the extension must be specified in the *Template format* field. The *Template mapping file* identifies which information from the Incident Register database need to be used in each field of the report template file, and the *Template date format* specifies what the date format is. Figure 105 shows an example.

[9] https://docs.oracle.com/javase/7/docs/api/java/text/SimpleDateFormat.html



Templates Configuration -> Template Edition: templates/Template_Notification_eIDAS_Italy.xlsx

Template Regulation: eIDAS

Template Recipient: atos_eidas

Template format: EXCEL

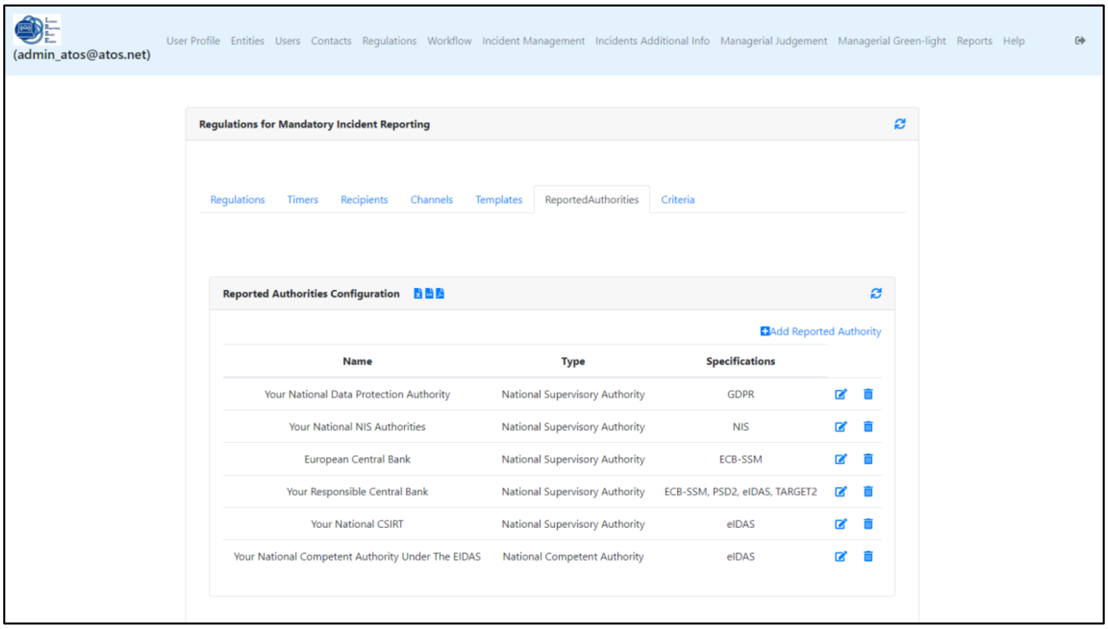
Template date format: dd/MM/YYYY

Report template file: Currently: templates/Template_Notification_eIDAS_Italy.xlsx
Change: Choose File No file chosen

Template mapping file: Currently: templates/Template_Notification_eIDAS_Italy_IR_mapping.xlsx
Change: Choose File No file chosen

Figure 105. Template Edition Form.

4.5. **Reported Authorities:** In this menu, Figure 106, it is necessary to associate each reported authority with the regulations or specifications that require a mandatory report to be sent to it. This information will be used in the Managerial Judgement process to suggest the reported authorities that need to be notified in case the criteria and thresholds associated to those specifications are matched.



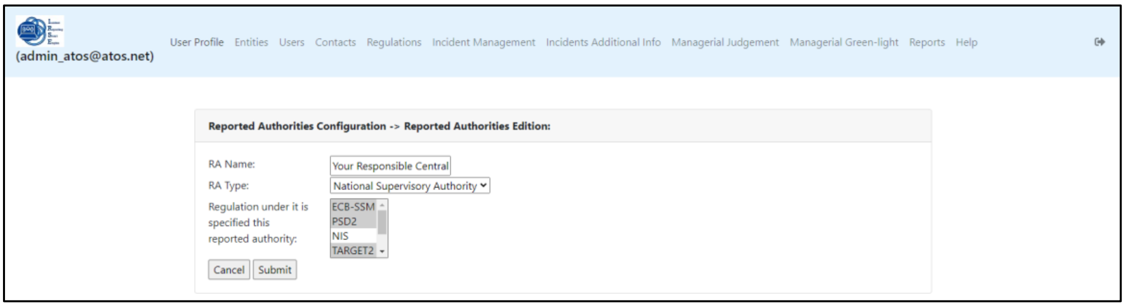
Regulations for Mandatory Incident Reporting

Reported Authorities Configuration

Name	Type	Specifications
Your National Data Protection Authority	National Supervisory Authority	GDPR
Your National NIS Authorities	National Supervisory Authority	NIS
European Central Bank	National Supervisory Authority	ECB-SSM
Your Responsible Central Bank	National Supervisory Authority	ECB-SSM, PSD2, eIDAS, TARGET2
Your National CSIRT	National Supervisory Authority	eIDAS
Your National Competent Authority Under The EIDAS	National Competent Authority	eIDAS

Figure 106. Reported Authorities Configuration.

The Reported Authorities Editor, Figure 107, allows creating or modifying the entries of Reported Authorities.



Reported Authorities Configuration -> Reported Authorities Edition:

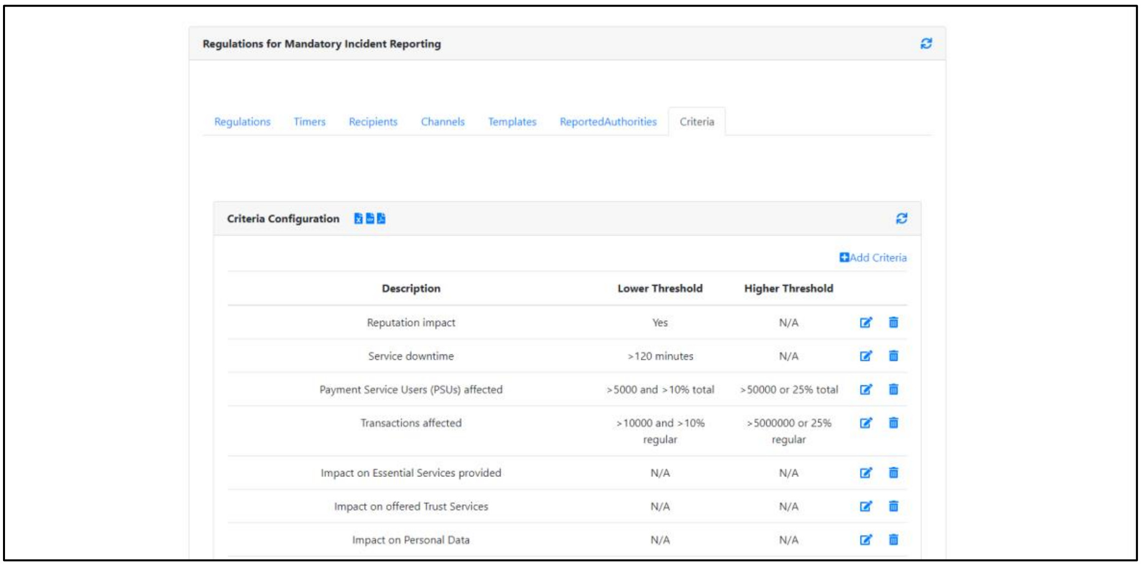
RA Name: Your Responsible Central

RA Type: National Supervisory Authority

Regulation under it is specified this reported authority: ECB-SSM, PSD2, NIS, TARGET2

Figure 107. Reported Authorities Editor.

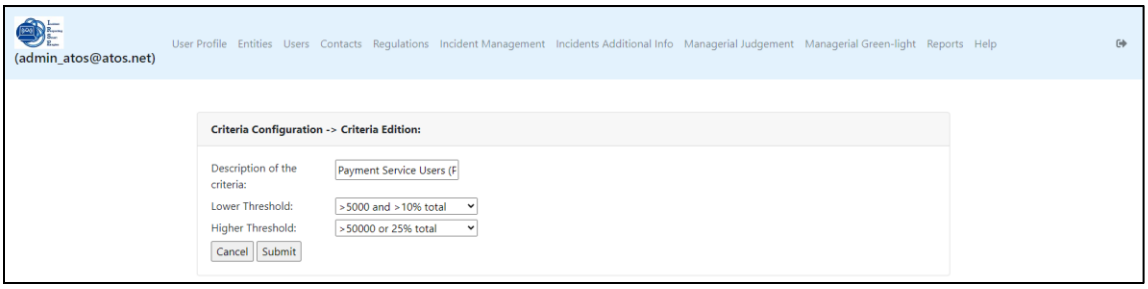
4.6. **Criteria:** Figure 108 shows the criteria supported by the platform for the event classification. The current version of the demonstrator does not support customization of the criteria included in the regulations. These criteria are included here are preloaded and just included for information purposes, but they are not considered in real-time by the responder IR Event Classifier included in the demonstrator. Consequently, if some of them is removed or some is added, the changes will not be considered by the classifier.



Description	Lower Threshold	Higher Threshold
Reputation impact	Yes	N/A
Service downtime	>120 minutes	N/A
Payment Service Users (PSUs) affected	>5000 and >10% total	>50000 or 25% total
Transactions affected	>10000 and >10% regular	>5000000 or 25% regular
Impact on Essential Services provided	N/A	N/A
Impact on offered Trust Services	N/A	N/A
Impact on Personal Data	N/A	N/A

Figure 108. List of Criteria.

Figure 109 displays the *Criteria Edition* View, where the user can set the lower and higher thresholds.



Criteria Configuration -> Criteria Edition:

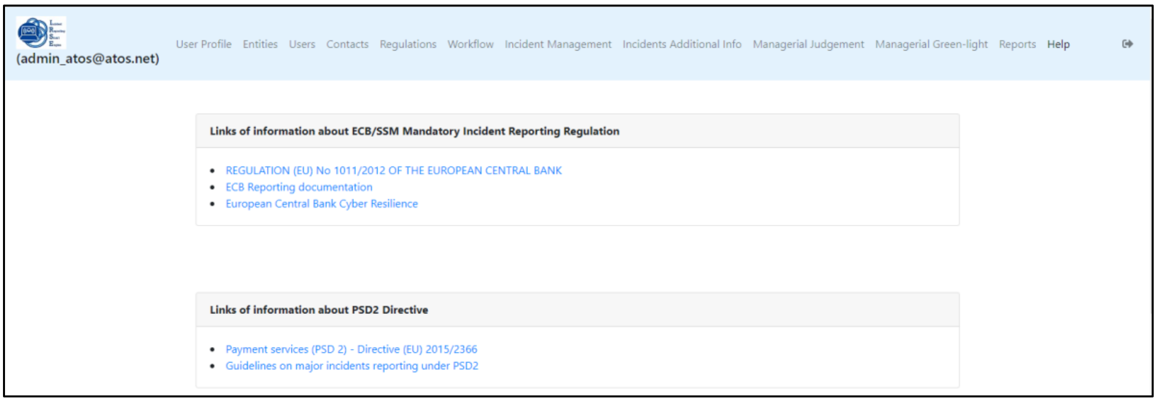
Description of the criteria: Payment Service Users (F

Lower Threshold: >5000 and >10% total

Higher Threshold: >50000 or 25% total

Figure 109. Criteria Edition.

More information about regulations can be found under the menu *Help*, Figure 110:



Links of information about ECB/SSM Mandatory Incident Reporting Regulation

- REGULATION (EU) No 1011/2012 OF THE EUROPEAN CENTRAL BANK
- ECB Reporting documentation
- European Central Bank Cyber Resilience

Links of information about PSD2 Directive

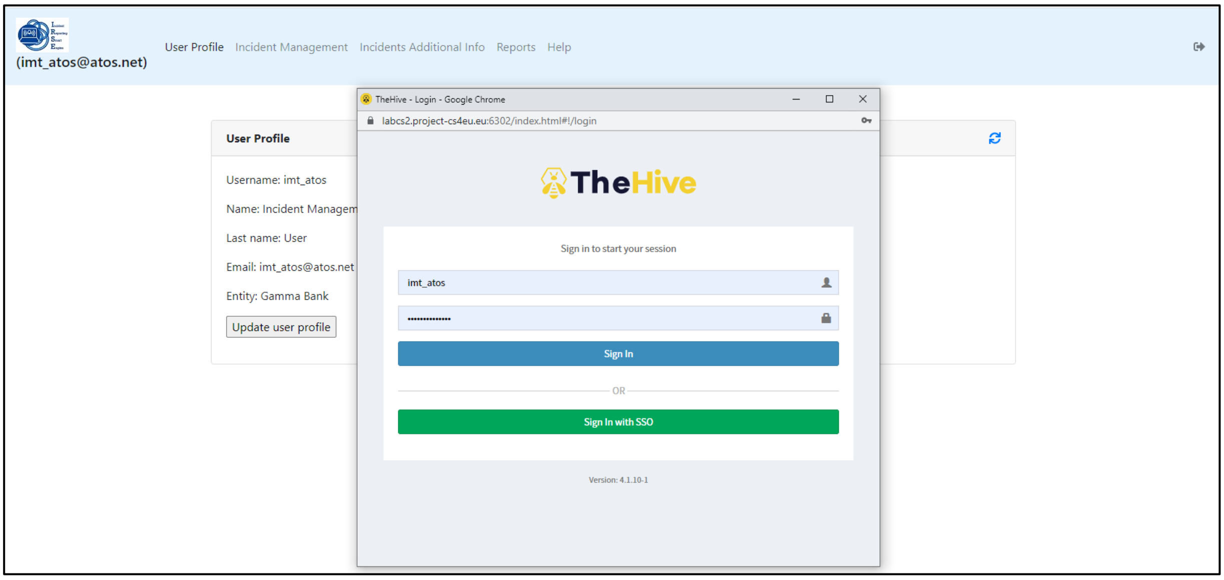
- Payment services (PSD 2) - Directive (EU) 2015/2366
- Guidelines on major incidents reporting under PSD2

Figure 110. Help menu.

I.IV.I.II AIRE GUI – USER

Once AIRE has been configured by the administrator, users can manage incidents and send reports. This section describes the functionalities that the assets offer.

The incidents are managed by the TheHive[10] tool. When "Incident Management" is clicked, a pop-up window will be shown with the graphical interface provided by TheHive, Figure 111.



User Profile

Username: imt_atos

Name: Incident Managem

Last name: User

Email: imt_atos@atos.net

Entity: Gamma Bank

Sign in to start your session

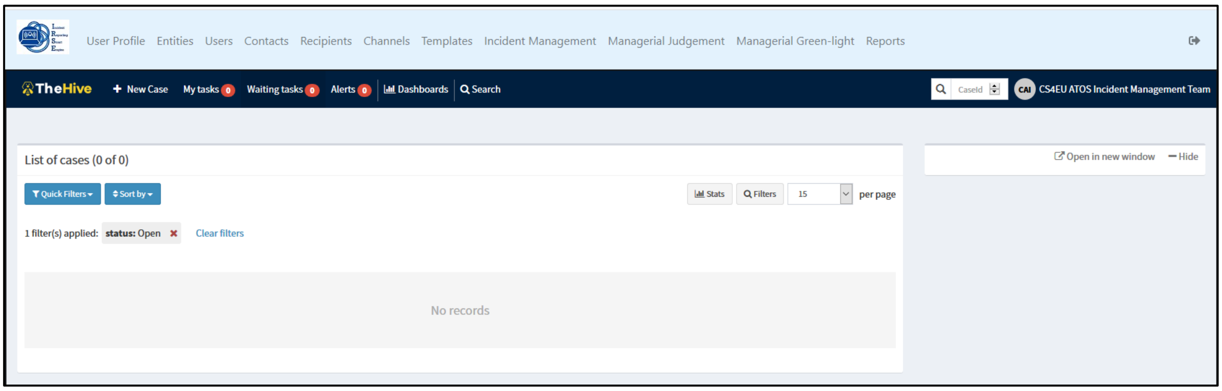
imt_atos

•••••••••••••••

Version: 4.1.10-1

Figure 111. TheHive login interface.

After signing in, the TheHive graphical interface is embedded within the AIRE interface, Figure 112. Where the user can perform several actions related with incident management.



List of cases (0 of 0)

15 per page

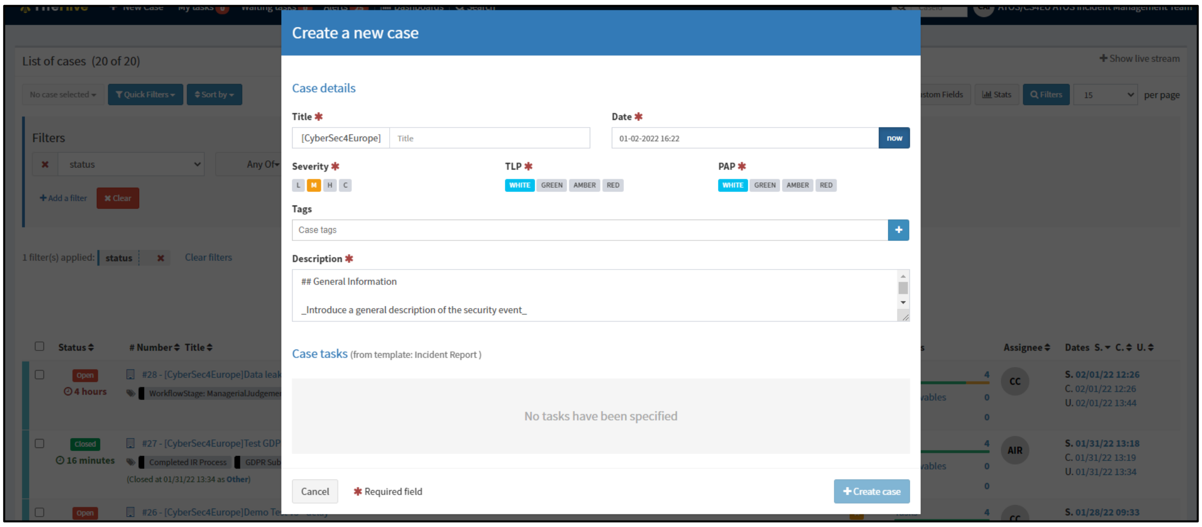
1 filter(s) applied: status: Open

No records

Figure 112. TheHive embedded in AIRE interface.

[10] http://thehive-project.org/

1. **New Case:** Start the process of creating a case for an incident. This may be an empty case or use a predefined template, Figure 104. List of Templates. The template “Incident Report” includes the fields required for the mandatory incident reporting, Figure 114.



Create a new case

Case details

Title ✱ [CyberSec4Europe] Title

Date ✱ 01-02-2022 16:22

Severity ✱ L M H C

TLP ✱ WHITE GREEN AMBER RED

PAP ✱ WHITE GREEN AMBER RED

Tags: Case tags

Description ✱

General Information

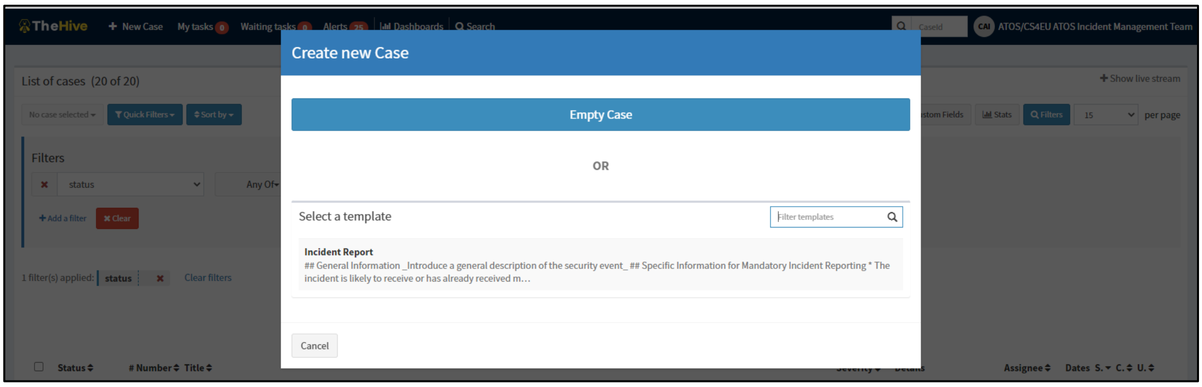
Introduce a general description of the security event

Case tasks (from template: Incident Report)

No tasks have been specified

✱ Required field

Figure 113. Template selection for a new Case.



Create new Case

Empty Case

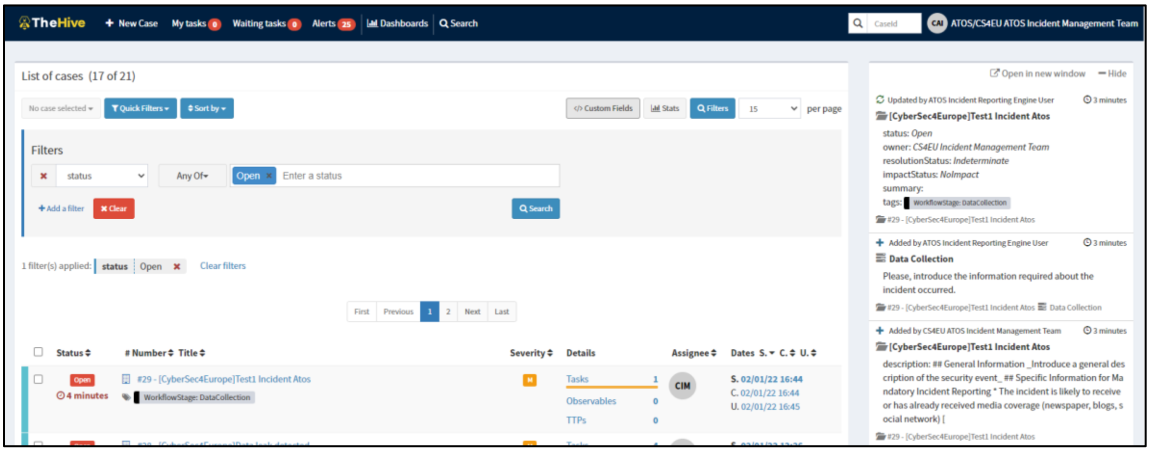
OR

Select a template

Incident Report
General Information _Introduce a general description of the security event_ ## Specific Information for Mandatory Incident Reporting * The incident is likely to receive or has already received m…

Figure 114. New case form with Incident Report template.

This action creates an empty case in TheHive, Figure 115:



List of cases (17 of 21)

1 filter(s) applied: status Open

Status	# Number Title	Severity	Details	Assignee	Dates S. C. U.
Open 4 minutes	#29 - [CyberSec4Europe]Test1 Incident Atos WorkflowStage: DataCollection	M	Tasks 1 Observables 0 TTPs 0	CIM	S. 02/01/22 16:44 C. 02/01/22 16:44 U. 02/01/22 16:45

Updated by ATOS Incident Reporting Engine User — 3 minutes

[CyberSec4Europe]Test1 Incident Atos

status: *Open*
owner: *CS4EU Incident Management Team*
resolutionStatus: *Indeterminate*
impactStatus: *NoImpact*
summary:
tags: WorkflowStage: DataCollection

#29 - [CyberSec4Europe]Test1 Incident Atos

Added by ATOS Incident Reporting Engine User — 3 minutes

Data Collection

Please, introduce the information required about the incident occurred.

#29 - [CyberSec4Europe]Test1 Incident Atos Data Collection

Added by CS4EU ATOS Incident Management Team — 3 minutes

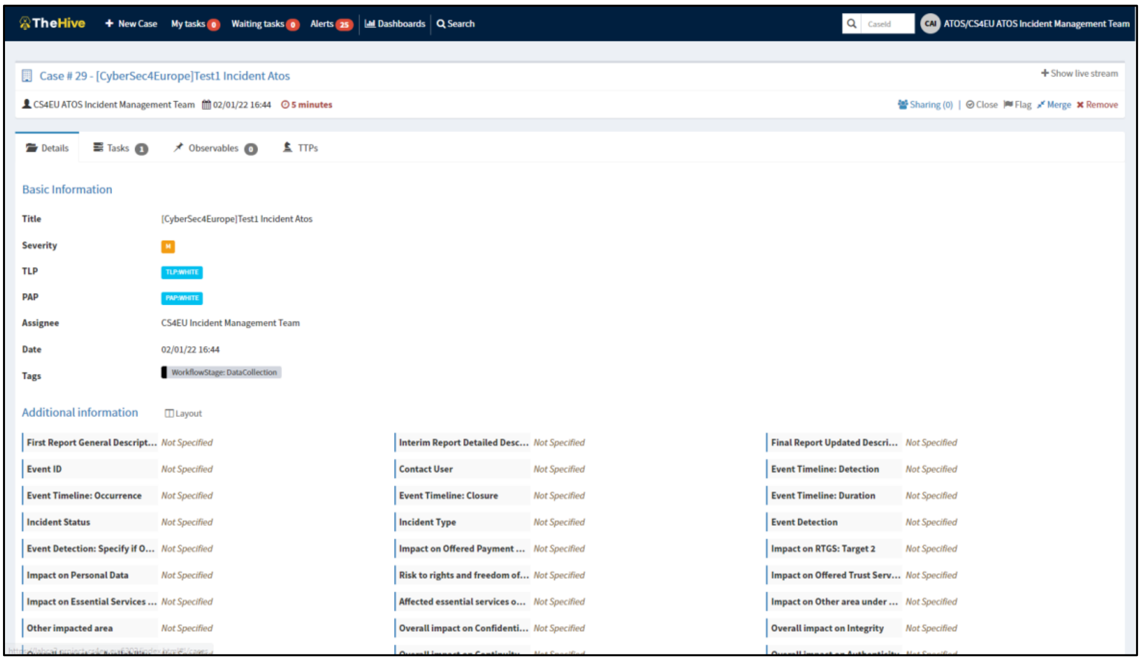
[CyberSec4Europe]Test1 Incident Atos

description: ## General Information _Introduce a general description of the security event_ ## Specific Information for Mandatory Incident Reporting * The incident is likely to receive or has already received media coverage (newspaper, blogs, social network) [

#29 - [CyberSec4Europe]Test1 Incident Atos

Figure 115. New incident in the list of cases.

Figure 116 displays the details of the case.



Case # 29 - [CyberSec4Europe]Test1 Incident Atos

CS4EU ATOS Incident Management Team 02/01/22 16:44 5 minutes

Basic Information

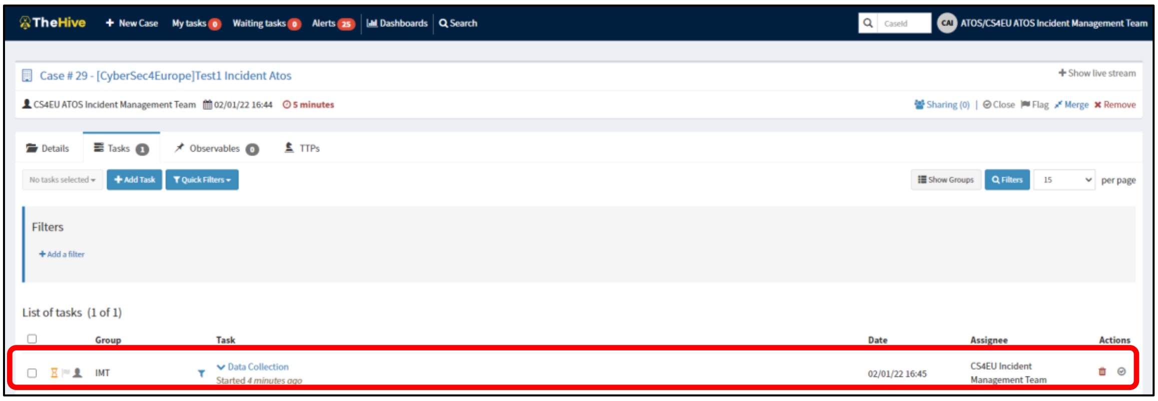
Title	[CyberSec4Europe]Test1 Incident Atos
Severity	M
TLP	TLP:WHITE
PAP	PAP:WHITE
Assignee	CS4EU Incident Management Team
Date	02/01/22 16:44
Tags	WorkflowStage: DataCollection

Additional information

First Report General Descript…	Not Specified	Interim Report Detailed Desc…	Not Specified	Final Report Updated Descri…	Not Specified
Event ID	Not Specified	Contact User	Not Specified	Event Timeline: Detection	Not Specified
Event Timeline: Occurrence	Not Specified	Event Timeline: Closure	Not Specified	Event Timeline: Duration	Not Specified
Incident Status	Not Specified	Incident Type	Not Specified	Event Detection	Not Specified
Event Detection: Specify if O…	Not Specified	Impact on Offered Payment …	Not Specified	Impact on RTGS: Target 2	Not Specified
Impact on Personal Data	Not Specified	Risk to rights and freedom of…	Not Specified	Impact on Offered Trust Serv…	Not Specified
Impact on Essential Services …	Not Specified	Affected essential services o…	Not Specified	Impact on Other area under …	Not Specified
Other impacted area	Not Specified	Overall impact on Confidenti…	Not Specified	Overall impact on Integrity	Not Specified

Figure 116. Details of a case.

In the *Tasks* tab there are the pending tasks for the case, Figure 117. *Data Collection* task is automatically created and assigned to the *IMT* group.



Case # 29 - [CyberSec4Europe]Test1 Incident Atos

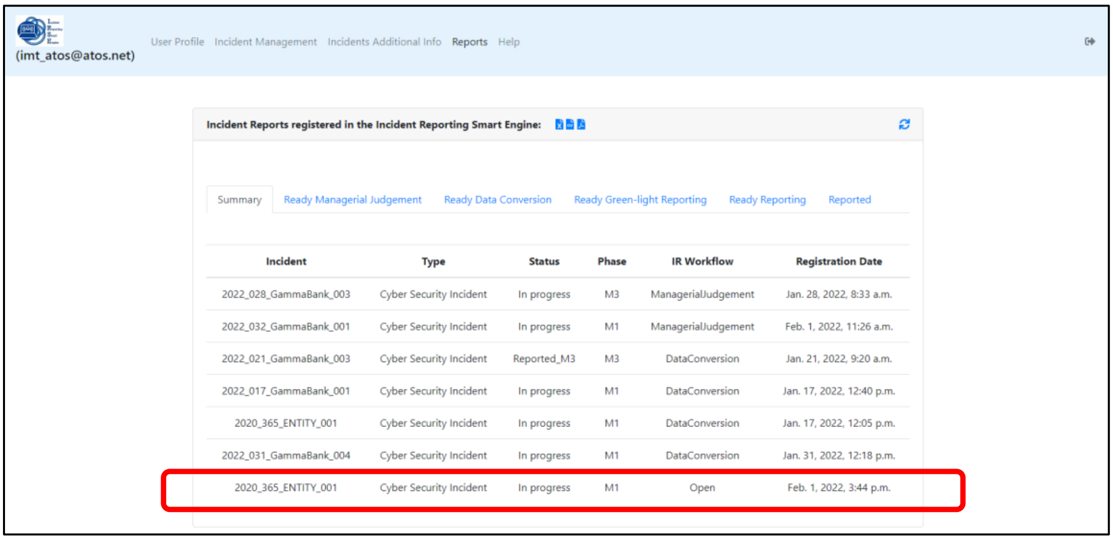
CS4EU ATOS Incident Management Team 02/01/22 16:44 5 minutes

List of tasks (1 of 1)

□	Group	Task	Date	Assignee	Actions
□	IMT	Data Collection Started 4 minutes ago	02/01/22 16:45	CS4EU Incident Management Team	

Figure 117. Tasks associated with a case.

In the tab *Reports* of the general interface, Figure 118, there will be a new report opened:



(imt_atos@atos.net)

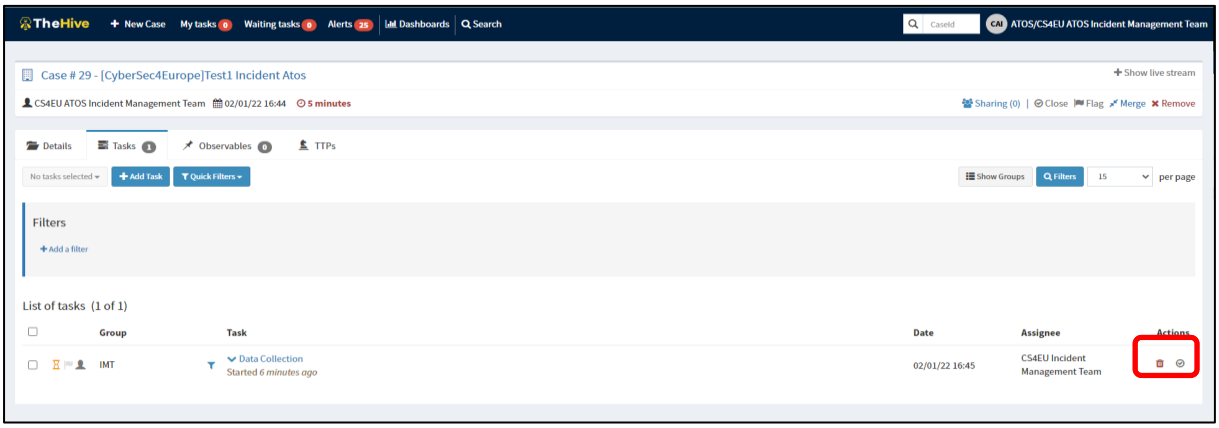
Incident Reports registered in the Incident Reporting Smart Engine:

Incident	Type	Status	Phase	IR Workflow	Registration Date
2022_028_GammaBank_003	Cyber Security Incident	In progress	M3	ManagerialJudgement	Jan. 28, 2022, 8:33 a.m.
2022_032_GammaBank_001	Cyber Security Incident	In progress	M1	ManagerialJudgement	Feb. 1, 2022, 11:26 a.m.
2022_021_GammaBank_003	Cyber Security Incident	Reported_M3	M3	DataConversion	Jan. 21, 2022, 9:20 a.m.
2022_017_GammaBank_001	Cyber Security Incident	In progress	M1	DataConversion	Jan. 17, 2022, 12:40 p.m.
2020_365_ENTITY_001	Cyber Security Incident	In progress	M1	DataConversion	Jan. 17, 2022, 12:05 p.m.
2022_031_GammaBank_004	Cyber Security Incident	In progress	M1	DataConversion	Jan. 31, 2022, 12:18 p.m.
2020_365_ENTITY_001	Cyber Security Incident	In progress	M1	Open	Feb. 1, 2022, 3:44 p.m.

Figure 118. List of Reports.

NOTE: When *New Case* is registered, since no information has been provided yet, the event ID "2020_365_ENTITY_001" will be assigned by default. Once the information is included through TheHive, it will be reflected also in the dashboard.

2. **Task Actions:** allow closing, resume, or delete the task of a case, Figure 119.



Case # 29 - [CyberSec4Europe]Test1 Incident Atos

CS4EU ATOS Incident Management Team 02/01/22 16:44 5 minutes

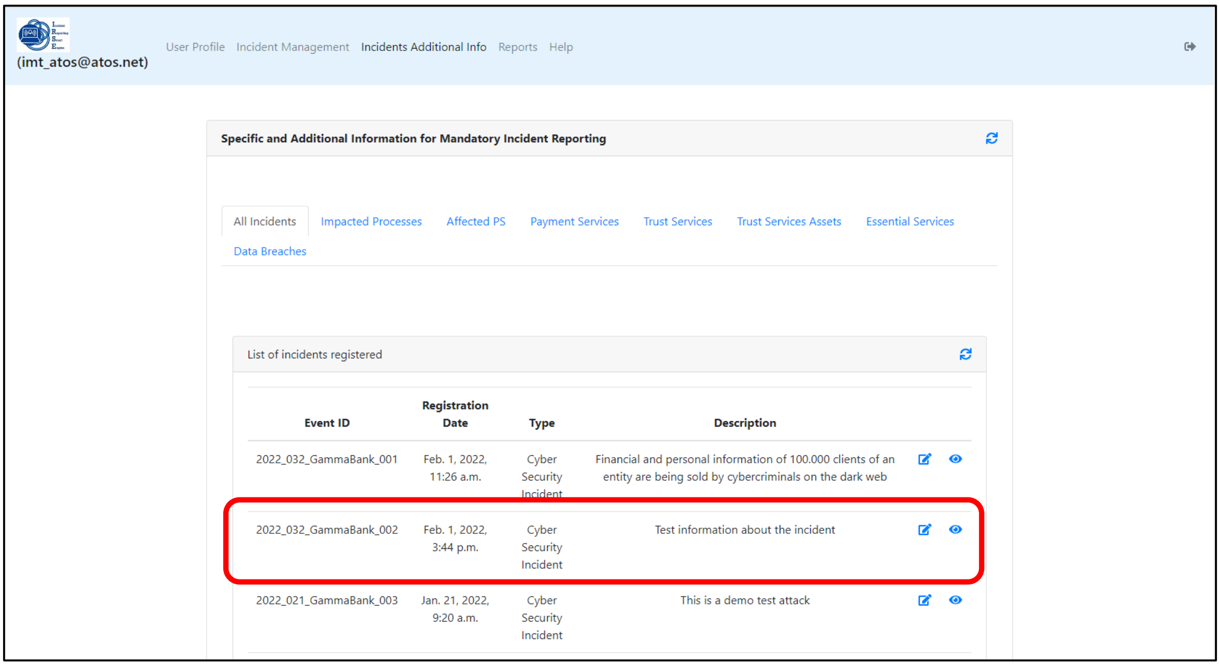
List of tasks (1 of 1)

☐	Group	Task	Date	Assignee	Actions
☐	IMT	Data Collection Started *6 minutes ago*	02/01/22 16:45	CS4EU Incident Management Team	

Figure 119. Task list of a case.

When the *Data Collection* task is closed, the associated report changes to *Enrichment.*

3. **Incident Additional Info:** *All Incidents* tab displays the list of all incidents registered, Figure 120.



(imt_atos@atos.net)

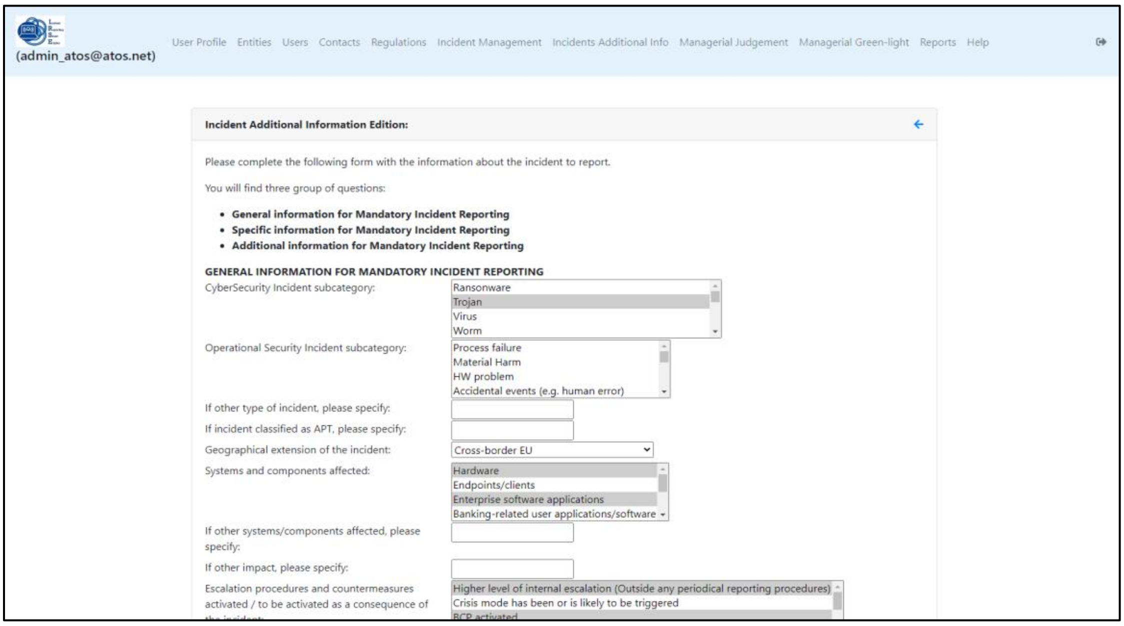
Specific and Additional Information for Mandatory Incident Reporting

List of incidents registered

Event ID	Registration Date	Type	Description
2022_032_GammaBank_001	Feb. 1, 2022, 11:26 a.m.	Cyber Security Incident	Financial and personal information of 100.000 clients of an entity are being sold by cybercriminals on the dark web
2022_032_GammaBank_002	Feb. 1, 2022, 3:44 p.m.	Cyber Security Incident	Test information about the incident
2022_021_GammaBank_003	Jan. 21, 2022, 9:20 a.m.	Cyber Security Incident	This is a demo test attack

Figure 120. List of incidents registered.

In addition, a user can enrich the data editing the information about a registered incident, Figure 121.



(admin_atos@atos.net)

Incident Additional Information Edition:

Please complete the following form with the information about the incident to report.

You will find three group of questions:

- **General information for Mandatory Incident Reporting**
- **Specific information for Mandatory Incident Reporting**
- **Additional information for Mandatory Incident Reporting**

GENERAL INFORMATION FOR MANDATORY INCIDENT REPORTING

CyberSecurity Incident subcategory: Ransonware / Trojan / Virus / Worm

Operational Security Incident subcategory: Process failure / Material Harm / HW problem / Accidental events (e.g. human error)

If other type of incident, please specify:

If incident classified as APT, please specify:

Geographical extension of the incident: Cross-border EU

Systems and components affected: Hardware / Endpoints/clients / Enterprise software applications / Banking-related user applications/software

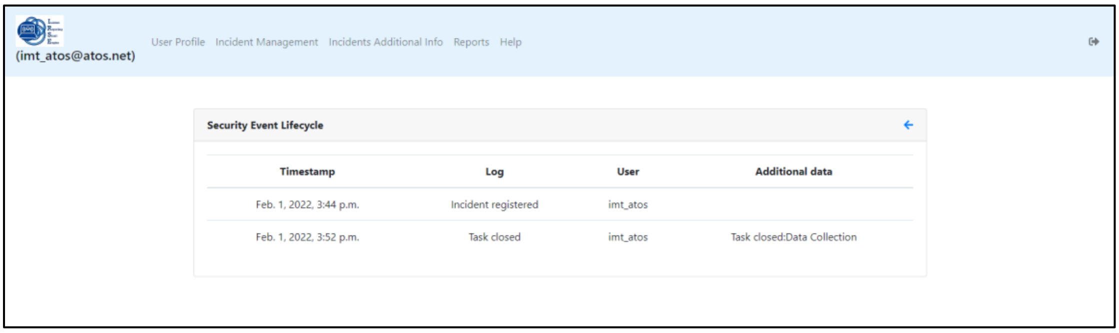
If other systems/components affected, please specify:

If other impact, please specify:

Escalation procedures and countermeasures activated / to be activated as a consequence of the incident: Higher level of internal escalation (Outside any periodical reporting procedures) / Crisis mode has been or is likely to be triggered / BCP activated

Figure 121. Incident Additional Information Edition.

The *eye* icon, Figure 120, shows the logs registered related to the security event lifecycle, Figure 122Figure 121:



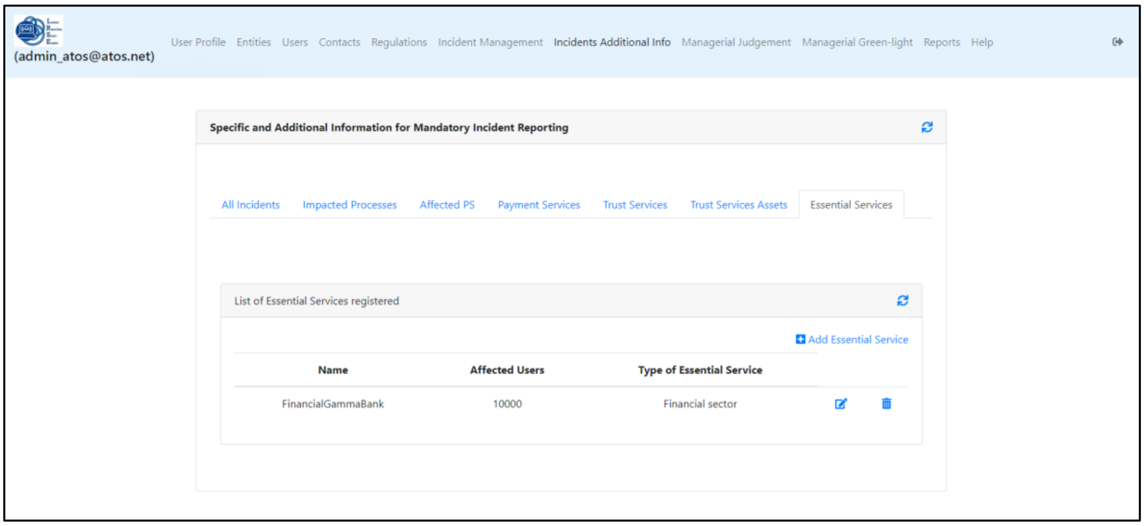
Security Event Lifecycle

Timestamp	Log	User	Additional data
Feb. 1, 2022, 3:44 p.m.	Incident registered	imt_atos	
Feb. 1, 2022, 3:52 p.m.	Task closed	imt_atos	Task closed:Data Collection

Figure 122. Security Event Lifecycle.

The other tabs in the Figure 120 allow managing the elements that are affected by an incident, such as services, assets, processes, or data. These elements are:

- Essential Services: In case the institution is a provider of essential services, they will be defined in this menu. A name needs to be assigned so it can be assigned to the incident.



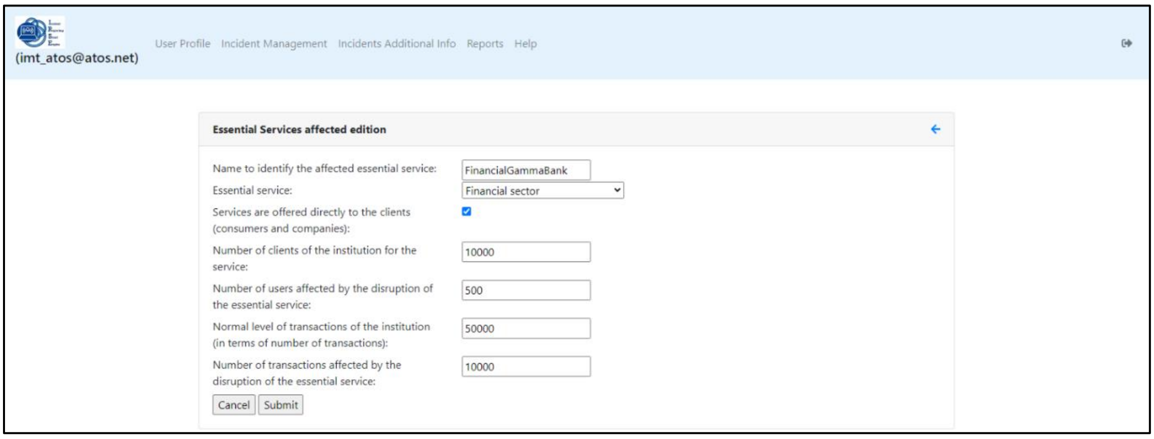
Specific and Additional Information for Mandatory Incident Reporting

List of Essential Services registered

Name	Affected Users	Type of Essential Service
FinancialGammaBank	10000	Financial sector

Figure 123. List of Essential Services.

Figure 124 displays the edition/creation form for this sub-menu.

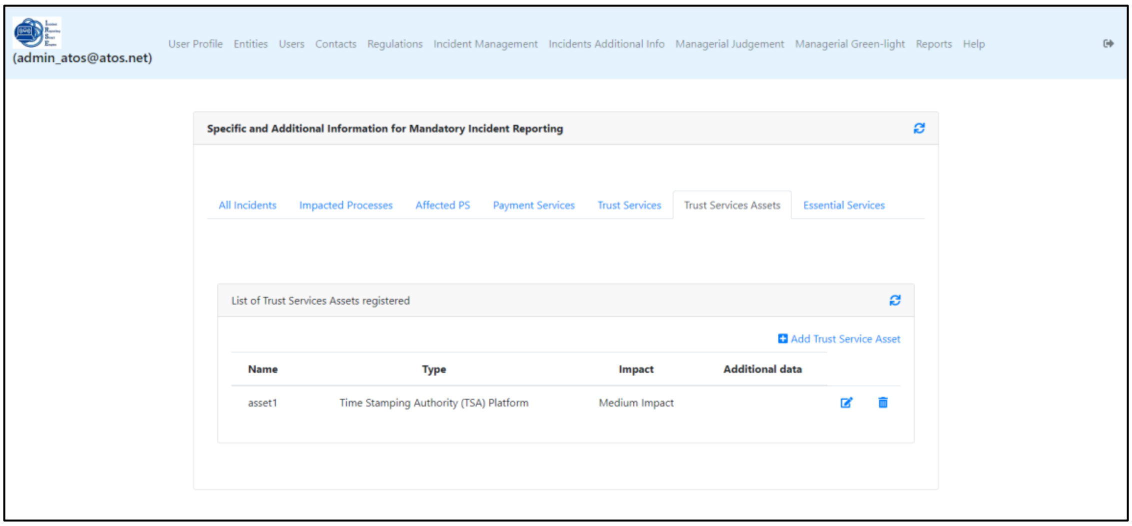


Essential Services affected edition

Name to identify the affected essential service:	FinancialGammaBank
Essential service:	Financial sector
Services are offered directly to the clients (consumers and companies):	☑
Number of clients of the institution for the service:	10000
Number of users affected by the disruption of the essential service:	500
Normal level of transactions of the institution (in terms of number of transactions):	50000
Number of transactions affected by the disruption of the essential service:	10000

Figure 124. Essential Services edition.

- Trust Services Assets: External services that support the trust protocols for Critical Infrastructures. Figure 125 displays the list of Trust Services Assets registered.



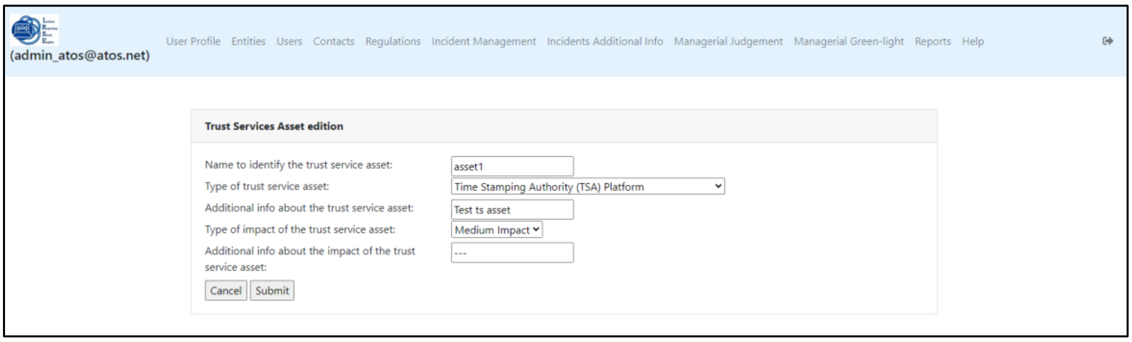
Specific and Additional Information for Mandatory Incident Reporting

List of Trust Services Assets registered

Name	Type	Impact	Additional data
asset1	Time Stamping Authority (TSA) Platform	Medium Impact	

Figure 125. List of Trust Services Assets registered.

Figure 126 shows the edition form of one Trust Service Asset.

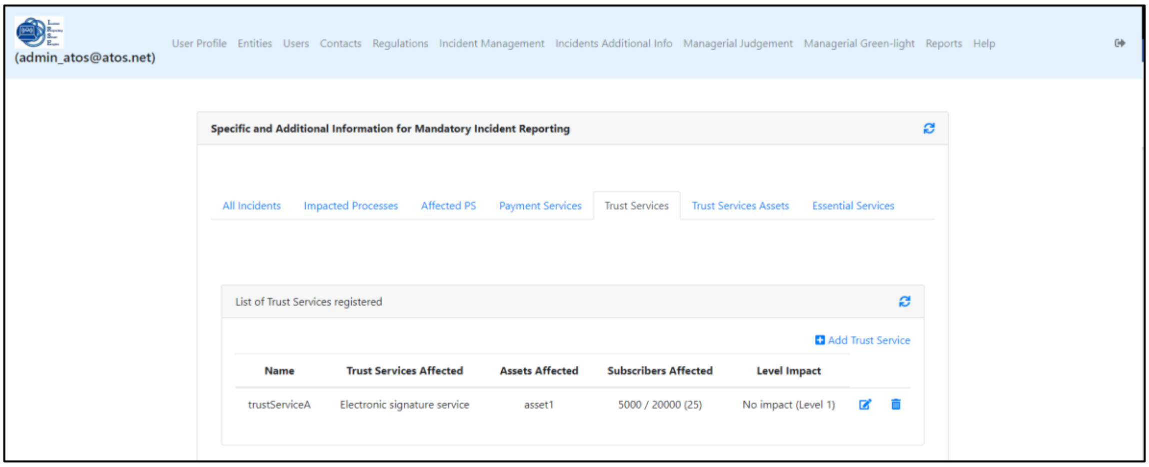


Trust Services Asset edition

Name to identify the trust service asset:	asset1
Type of trust service asset:	Time Stamping Authority (TSA) Platform
Additional info about the trust service asset:	Test ts asset
Type of impact of the trust service asset:	Medium Impact
Additional info about the impact of the trust service asset:	---

Figure 126. Trust Services Asset edition.

- Trust Services: Internal services that support the trust protocols for Critical Infrastructures. Figure 127 displays the list of Trust Services registered.



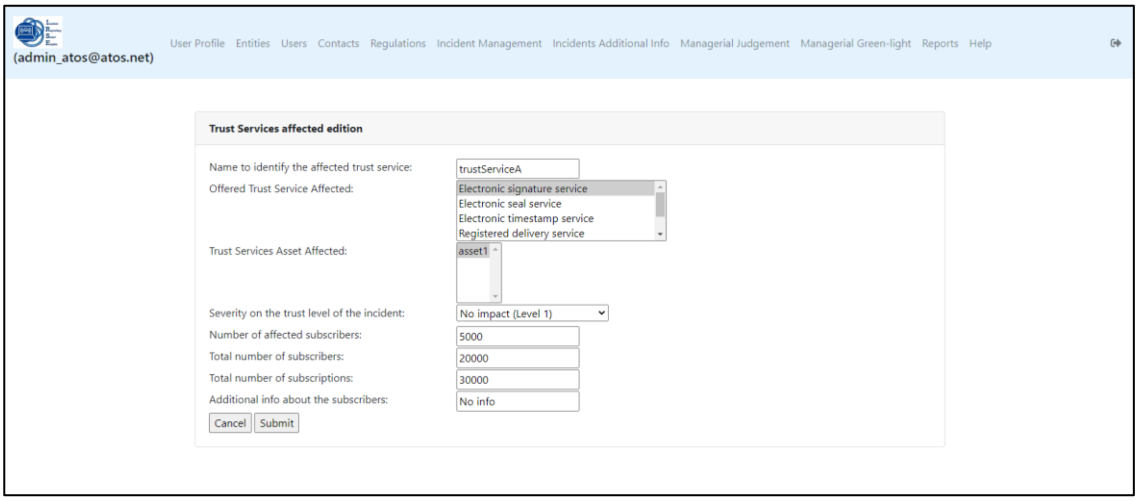
Specific and Additional Information for Mandatory Incident Reporting

List of Trust Services registered

Name	Trust Services Affected	Assets Affected	Subscribers Affected	Level Impact
trustServiceA	Electronic signature service	asset1	5000 / 20000 (25)	No impact (Level 1)

Figure 127. List of Trust Services registered.

Figure 128 shows the edition form of one Trust Service Asset.

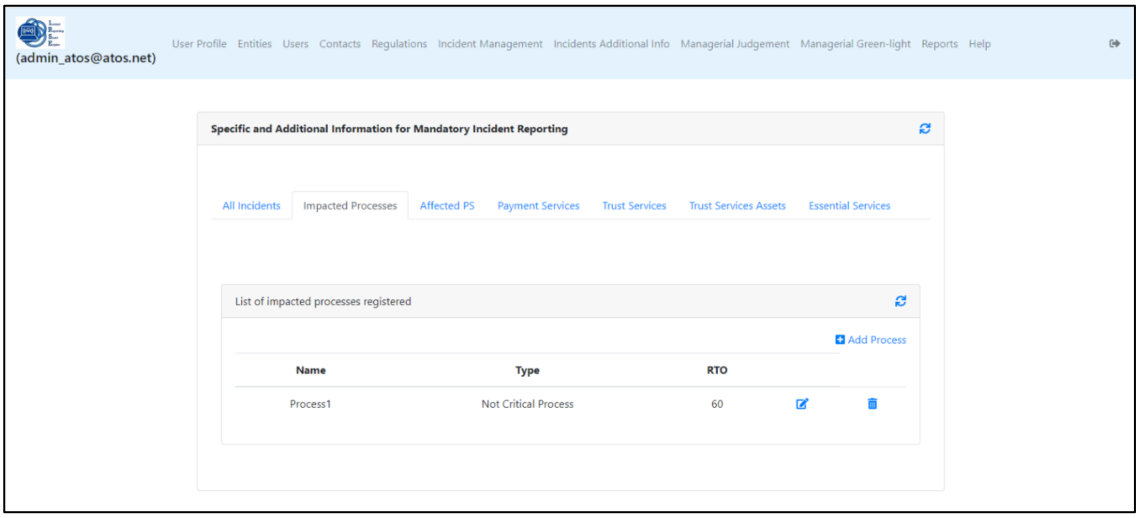


Trust Services affected edition

Name to identify the affected trust service:	trustServiceA
Offered Trust Service Affected:	Electronic signature service Electronic seal service Electronic timestamp service Registered delivery service
Trust Services Asset Affected:	asset1
Severity on the trust level of the incident:	No impact (Level 1)
Number of affected subscribers:	5000
Total number of subscribers:	20000
Total number of subscriptions:	30000
Additional info about the subscribers:	No info

Figure 128. Trust Services affected edition.

- Impacted Processes: Shows the list of processes impacted by an attack, the impact, and the recovery time.



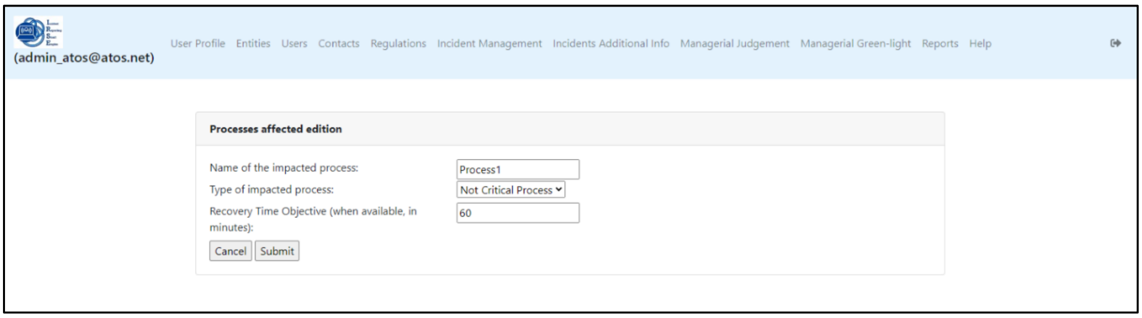
Specific and Additional Information for Mandatory Incident Reporting

List of impacted processes registered

Name	Type	RTO
Process1	Not Critical Process	60

Figure 129. List of Impacted Processes.

Figure 130 shows the form to add or create *Processes Affected*.

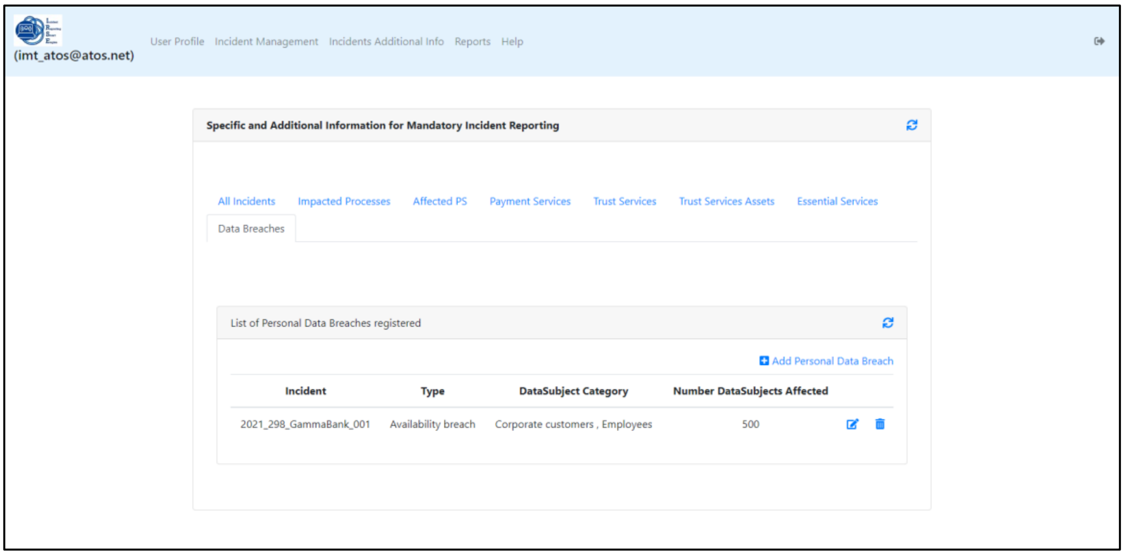


Processes affected edition

Name of the impacted process:	Process1
Type of impacted process:	Not Critical Process
Recovery Time Objective (when available, in minutes):	60

Figure 130. Processes Affected edition.

- Data Breaches: lists the *Personal Data Breaches* with the type, data category and the number of affected subjects, Figure 131.



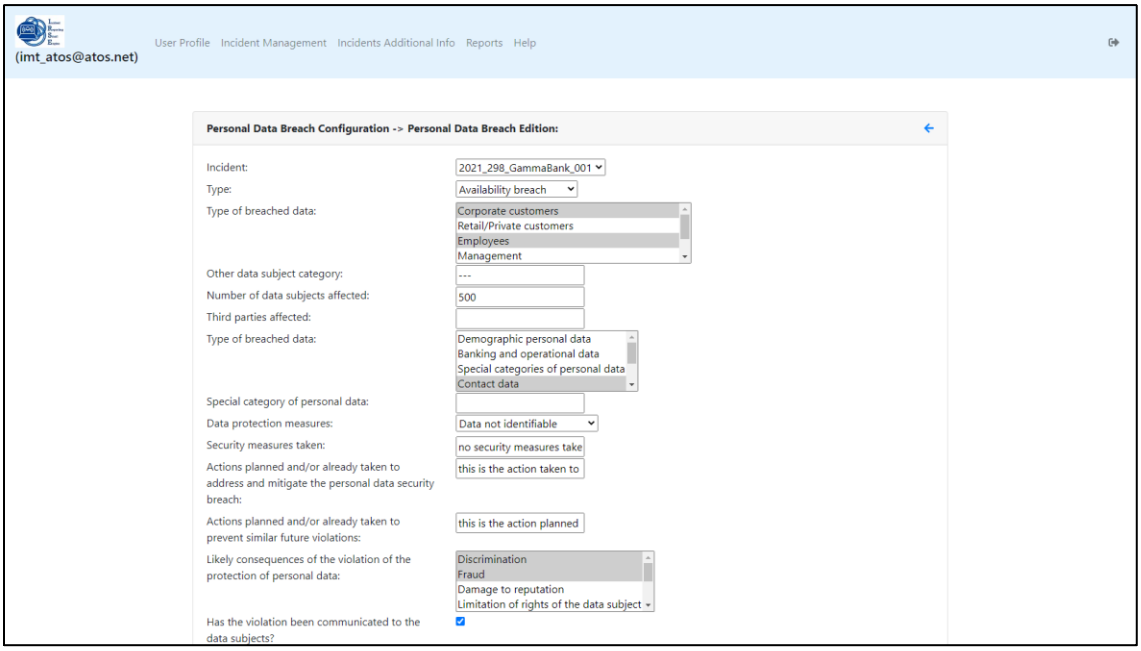
Specific and Additional Information for Mandatory Incident Reporting

List of Personal Data Breaches registered

Incident	Type	DataSubject Category	Number DataSubjects Affected
2021_298_GammaBank_001	Availability breach	Corporate customers , Employees	500

Figure 131. List of Personal Data Breaches registered.

Figure 132 displays the form to add or edit the information about a *Personal Data Breach*.



Personal Data Breach Configuration -> Personal Data Breach Edition:

Incident:	2021_298_GammaBank_001
Type:	Availability breach
Type of breached data:	Corporate customers Retail/Private customers Employees Management
Other data subject category:	---
Number of data subjects affected:	500
Third parties affected:	
Type of breached data:	Demographic personal data Banking and operational data Special categories of personal data Contact data
Special category of personal data:	
Data protection measures:	Data not identifiable
Security measures taken:	no security measures take
Actions planned and/or already taken to address and mitigate the personal data security breach:	this is the action taken to
Actions planned and/or already taken to prevent similar future violations:	this is the action planned
Likely consequences of the violation of the protection of personal data:	Discrimination Fraud Damage to reputation Limitation of rights of the data subject
Has the violation been communicated to the data subjects?	☑

Figure 132. Personal Data Breach Edition.

NOTE: The association of a data breach with an incident is done by selecting from the list of active incidents in that menu.

4. **Add observables:** Include information about the incident and run analysers on them, Figure 133.

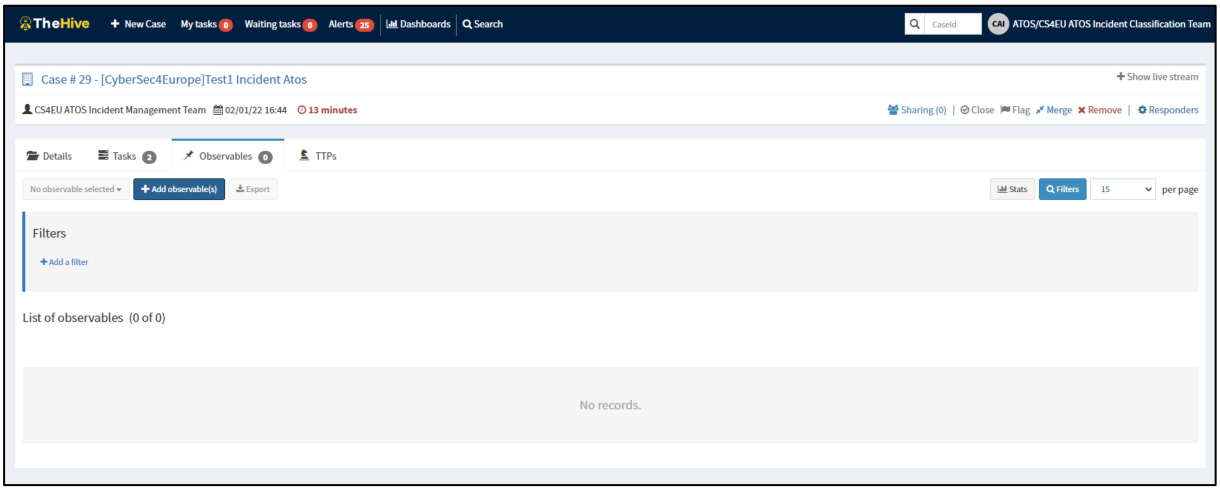
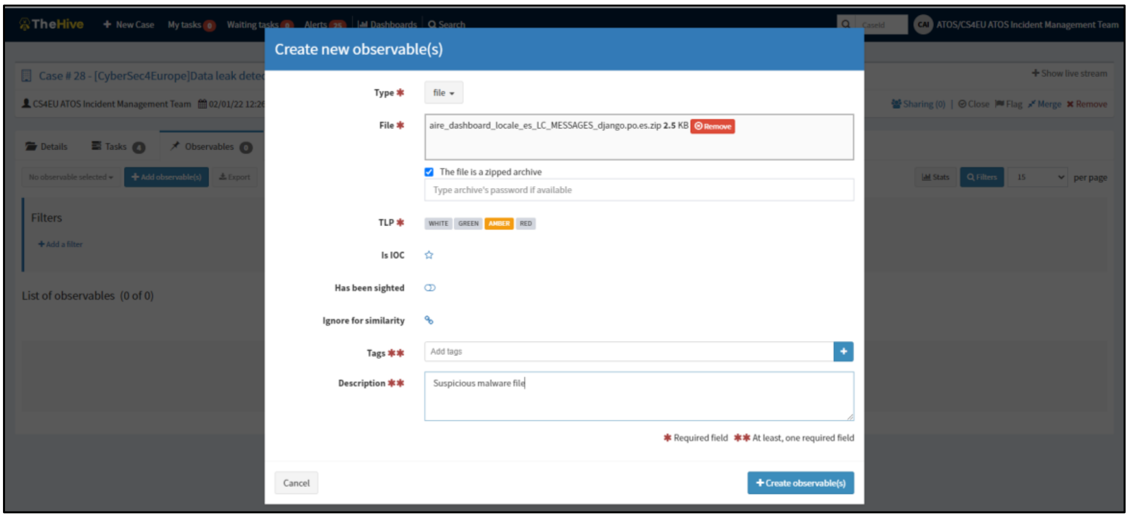


Figure 133. List of observables.

The button *Add observable* open a form to create new observables elements, Figure 134.



Type * file

File * aire_dashboard_locale_es_LC_MESSAGES_django.po.es.zip 2.5 KB

☑ The file is a zipped archive

Type archive's password if available

TLP *

Is IOC

Has been sighted

Ignore for similarity

Tags **

Description ** Suspicious malware file

* Required field ** At least, one required field

Figure 134. Create new observable form.

After selecting some observables, *Run analysers* allow us to run different analysers, Figure 135.

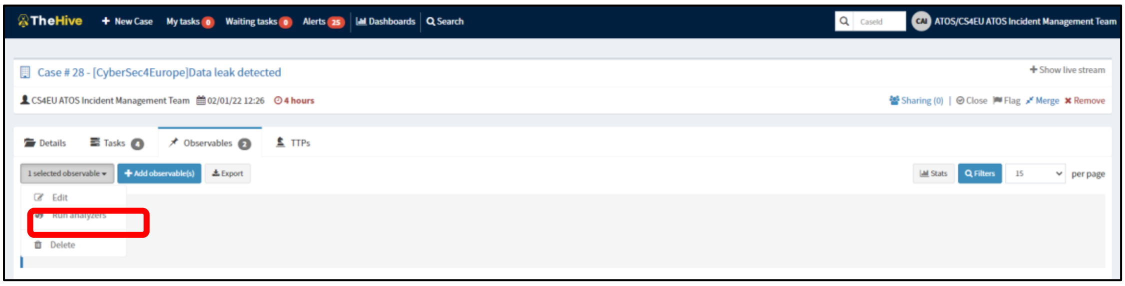
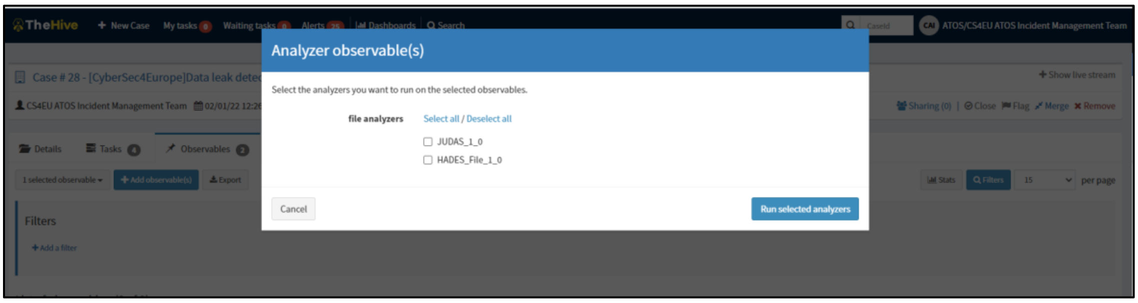


Figure 135. Run analyzers option.

Multiple analysers can be selected to run together, Figure 136.



Analyzer observable(s)

Select the analyzers you want to run on the selected observables.

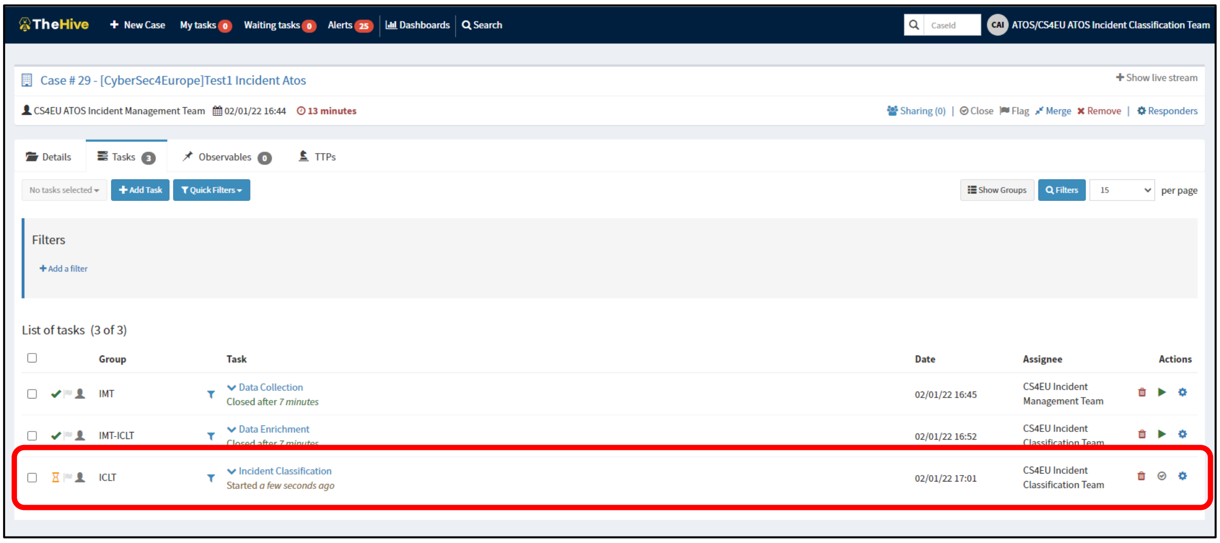
file analyzers — Select all / Deselect all

□ JUDAS_1_0

□ HADES_File_1_0

Figure 136. Selection of the analysers to run.

5. ***Incident Classification* Task:** is automatically created when the *Data Enrichment* Task is completed, Figure 137.



Case # 29 - [CyberSec4Europe]Test1 Incident Atos

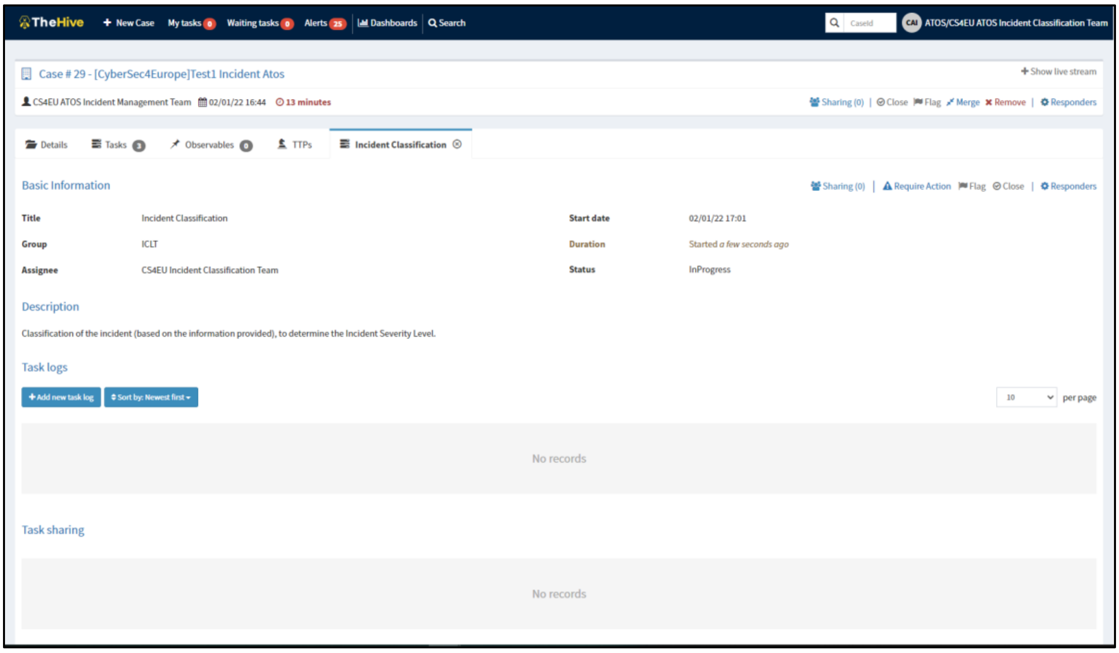
CS4EU ATOS Incident Management Team 02/01/22 16:44 13 minutes

List of tasks (3 of 3)

□	Group	Task	Date	Assignee	Actions
□	IMT	Data Collection Closed after *7 minutes*	02/01/22 16:45	CS4EU Incident Management Team	
□	IMT-ICLT	Data Enrichment Closed after *7 minutes*	02/01/22 16:52	CS4EU Incident Classification Team	
□	ICLT	Incident Classification Started *a few seconds ago*	02/01/22 17:01	CS4EU Incident Classification Team	

Figure 137. Automated creation of Incident Classification task.

Each task has its view where details and actions are shown, Figure 138.



Case # 29 - [CyberSec4Europe]Test1 Incident Atos

CS4EU ATOS Incident Management Team 02/01/22 16:44 13 minutes

Basic Information

Title	Incident Classification	Start date	02/01/22 17:01
Group	ICLT	Duration	Started *a few seconds ago*
Assignee	CS4EU Incident Classification Team	Status	InProgress

Description

Classification of the incident (based on the information provided), to determine the Incident Severity Level.

Task logs

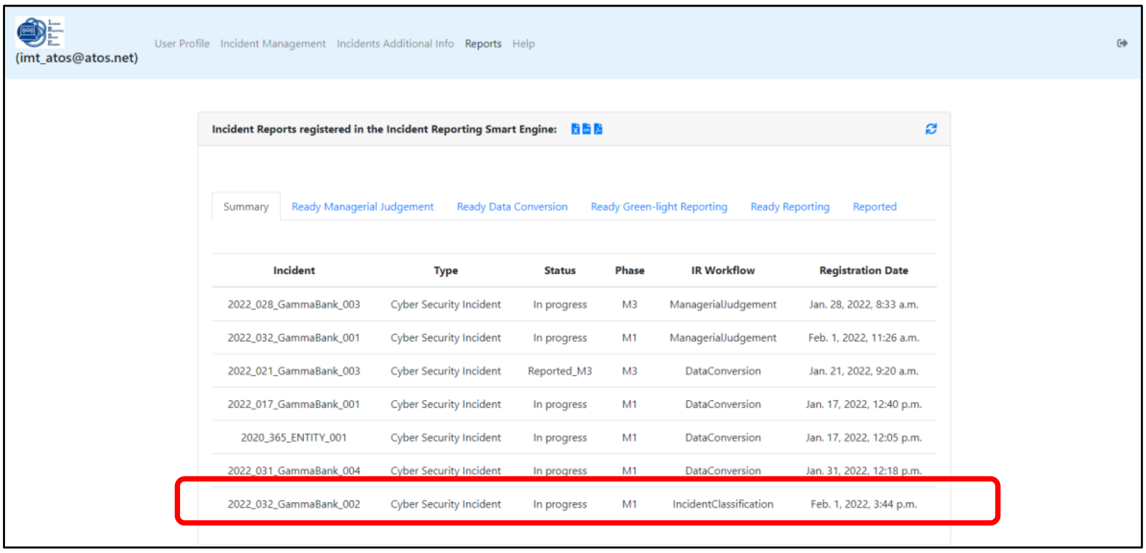
No records

Task sharing

No records

Figure 138. Detail of a task.

The report passes to the next IR workflow, Figure 139.

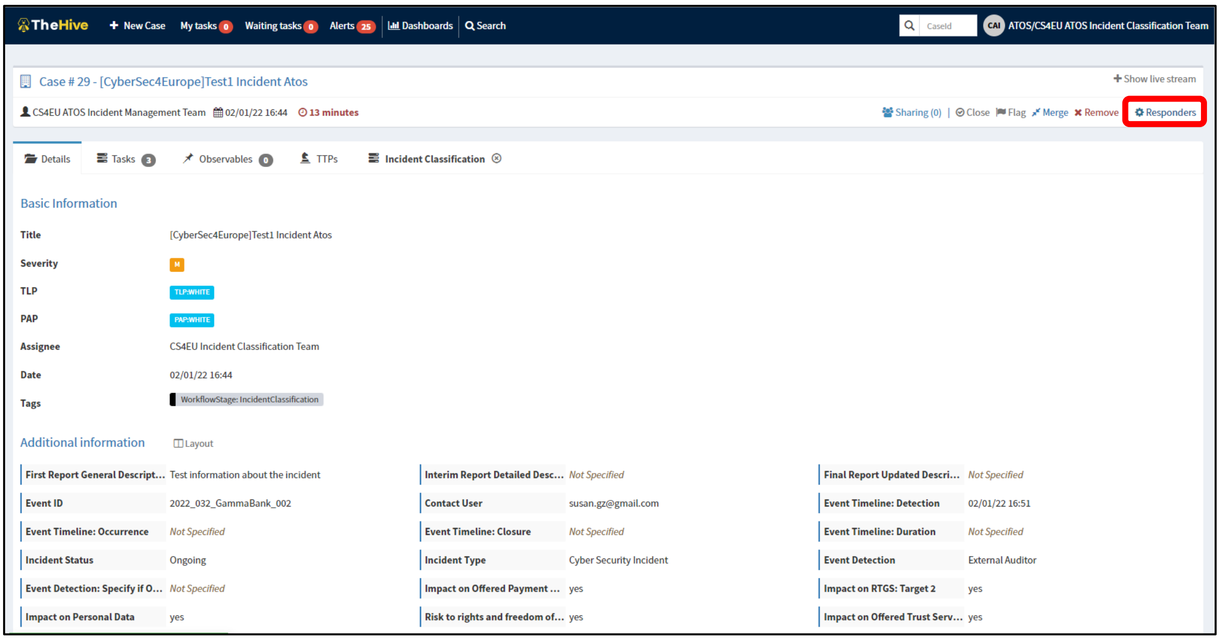


Incident Reports registered in the Incident Reporting Smart Engine:

Incident	Type	Status	Phase	IR Workflow	Registration Date
2022_028_GammaBank_003	Cyber Security Incident	In progress	M3	ManagerialJudgement	Jan. 28, 2022, 8:33 a.m.
2022_032_GammaBank_001	Cyber Security Incident	In progress	M1	ManagerialJudgement	Feb. 1, 2022, 11:26 a.m.
2022_021_GammaBank_003	Cyber Security Incident	Reported_M3	M3	DataConversion	Jan. 21, 2022, 9:20 a.m.
2022_017_GammaBank_001	Cyber Security Incident	In progress	M1	DataConversion	Jan. 17, 2022, 12:40 p.m.
2020_365_ENTITY_001	Cyber Security Incident	In progress	M1	DataConversion	Jan. 17, 2022, 12:05 p.m.
2022_031_GammaBank_004	Cyber Security Incident	In progress	M1	DataConversion	Jan. 31, 2022, 12:18 p.m.
2022_032_GammaBank_002	Cyber Security Incident	In progress	M1	IncidentClassification	Feb. 1, 2022, 3:44 p.m.

Figure 139. List of Incident Reports registered.

6. **Event Classification Task:** Check the information to do the event classification has been introduced in the template and invoke the *Responder* (located in the upper-right corner in TheHive GUI from the page with the Case details), Figure 140.



Case # 29 - [CyberSec4Europe]Test1 Incident Atos

CS4EU ATOS Incident Management Team 02/01/22 16:44 13 minutes

Basic Information

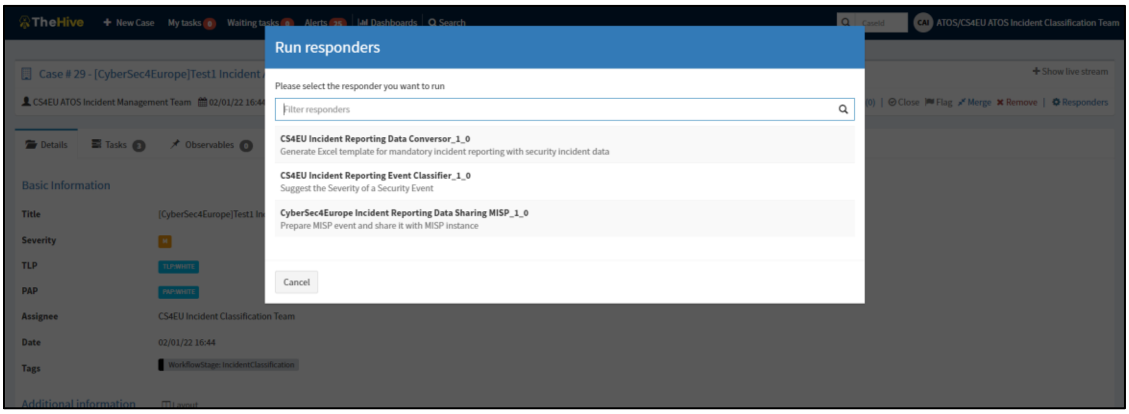
Title	[CyberSec4Europe]Test1 Incident Atos
Severity	M
TLP	TLP:WHITE
PAP	PAP:WHITE
Assignee	CS4EU Incident Classification Team
Date	02/01/22 16:44
Tags	WorkflowStage: IncidentClassification

Additional information

First Report General Descript…	Test information about the incident	Interim Report Detailed Desc…	Not Specified	Final Report Updated Descri…	Not Specified
Event ID	2022_032_GammaBank_002	Contact User	susan.gz@gmail.com	Event Timeline: Detection	02/01/22 16:51
Event Timeline: Occurrence	Not Specified	Event Timeline: Closure	Not Specified	Event Timeline: Duration	Not Specified
Incident Status	Ongoing	Incident Type	Cyber Security Incident	Event Detection	External Auditor
Event Detection: Specify if O…	Not Specified	Impact on Offered Payment …	yes	Impact on RTGS: Target 2	yes
Impact on Personal Data	yes	Risk to rights and freedom of…	yes	Impact on Offered Trust Serv…	yes

Figure 140. Responders in an Incident Detail View.

The Responder is integrated with AIRE asset, Figure 141, so the function of the user who executes it will be checked, and it only will get a result in case it belongs to ICLT (according to the workflow configuration).



Run responders

Please select the responder you want to run

CS4EU Incident Reporting Data Conversor_1_0
Generate Excel template for mandatory incident reporting with security incident data

CS4EU Incident Reporting Event Classifier_1_0
Suggest the Severity of a Security Event

CyberSec4Europe Incident Reporting Data Sharing MISP_1_0
Prepare MISP event and share it with MISP instance

Title: [CyberSec4Europe]Test1 In

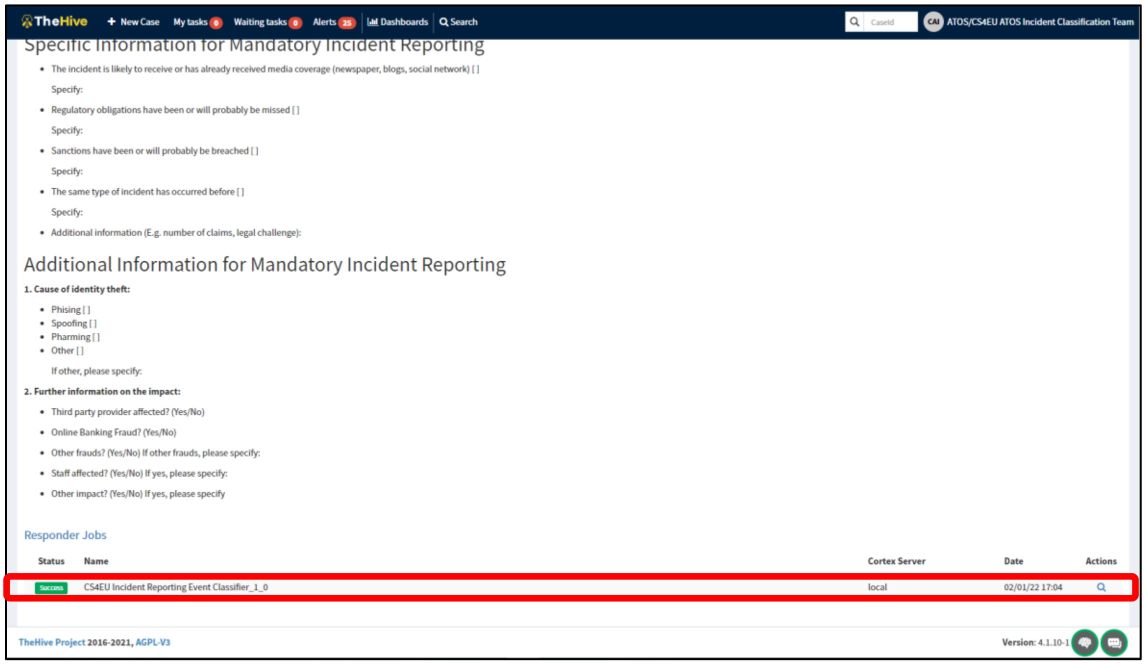
Assignee: CS4EU Incident Classification Team

Date: 02/01/22 16:44

Tags: WorkflowStage: IncidentClassification

Figure 141. Selection of one responder to run for an incident case.

The result of the classification is available at the end of the incident page, Figure 142.



Specific Information for Mandatory Incident Reporting

- The incident is likely to receive or has already received media coverage (newspaper, blogs, social network) [ ]

  Specify:
- Regulatory obligations have been or will probably be missed [ ]

  Specify:
- Sanctions have been or will probably be breached [ ]

  Specify:
- The same type of incident has occurred before [ ]

  Specify:
- Additional information (E.g. number of claims, legal challenge):

Additional Information for Mandatory Incident Reporting

1. Cause of identity theft:

- Phising [ ]
- Spoofing [ ]
- Pharming [ ]
- Other [ ]

  If other, please specify:

2. Further information on the impact:

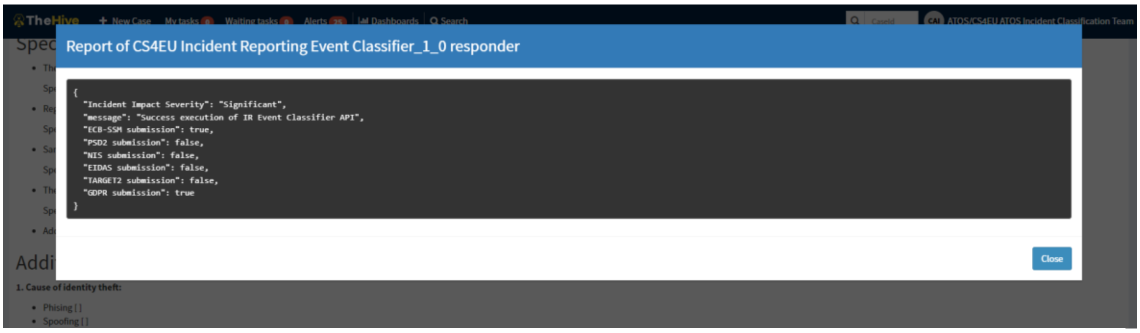
- Third party provider affected? (Yes/No)
- Online Banking Fraud? (Yes/No)
- Other frauds? (Yes/No) If other frauds, please specify:
- Staff affected? (Yes/No) If yes, please specify:
- Other impact? (Yes/No) If yes, please specify

Responder Jobs

Status	Name	Cortex Server	Date	Actions
Success	CS4EU Incident Reporting Event Classifier_1_0	local	02/01/22 17:04	🔍

Figure 142. List of Responder Jobs with status.

The action button shows the output, Figure 143.



Report of CS4EU Incident Reporting Event Classifier_1_0 responder

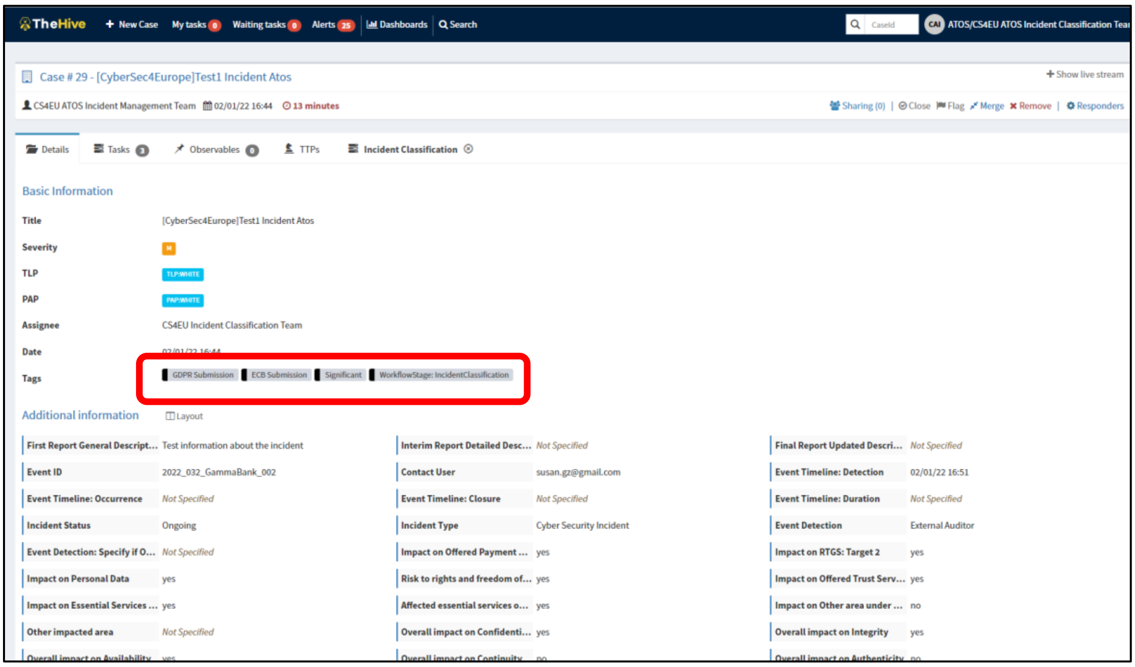
```
{
  "Incident Impact Severity": "Significant",
  "message": "Success execution of IR Event Classifier API",
  "ECB-SSM submission": true,
  "PSD2 submission": false,
  "NIS submission": false,
  "EIDAS submission": false,
  "TARGET2 submission": false,
  "GDPR submission": true
}
```

1. Cause of identity theft:

- Phising [ ]
- Spoofing [ ]

Figure 143. Output example for after run a responder.

This information will also be automatically updated in the tags of the case, Figure 144, and in the fields of the template, so the ICLT user can check the suggestion and modify it if he/she considers it.



Case # 29 - [CyberSec4Europe]Test1 Incident Atos

CS4EU ATOS Incident Management Team 02/01/22 16:44 13 minutes

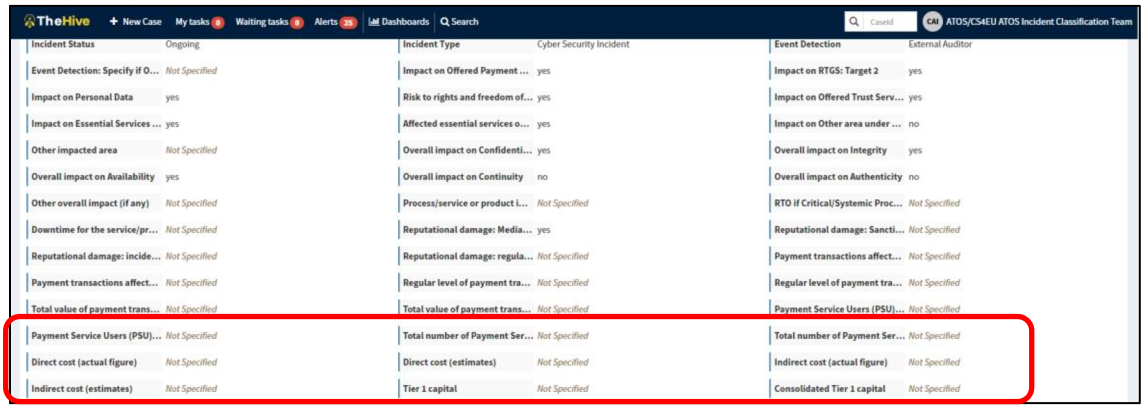
Basic Information

Title	[CyberSec4Europe]Test1 Incident Atos
Severity	M
TLP	TLP:WHITE
PAP	PAP:WHITE
Assignee	CS4EU Incident Classification Team
Date	02/01/22 16:44
Tags	GDPR Submission ECB Submission Significant WorkflowStage: IncidentClassification

Additional information

First Report General Descript...	Test information about the incident	Interim Report Detailed Desc...	Not Specified	Final Report Updated Descri...	Not Specified
Event ID	2022_032_GammaBank_002	Contact User	susan.gz@gmail.com	Event Timeline: Detection	02/01/22 16:51
Event Timeline: Occurrence	Not Specified	Event Timeline: Closure	Not Specified	Event Timeline: Duration	Not Specified
Incident Status	Ongoing	Incident Type	Cyber Security Incident	Event Detection	External Auditor
Event Detection: Specify if O...	Not Specified	Impact on Offered Payment ...	yes	Impact on RTGS: Target 2	yes
Impact on Personal Data	yes	Risk to rights and freedom of...	yes	Impact on Offered Trust Serv...	yes
Impact on Essential Services ...	yes	Affected essential services o...	yes	Impact on Other area under ...	no
Other impacted area	Not Specified	Overall impact on Confidenti...	yes	Overall impact on Integrity	yes
Overall impact on Availability	yes	Overall impact on Continuity	no	Overall impact on Authenticity	no

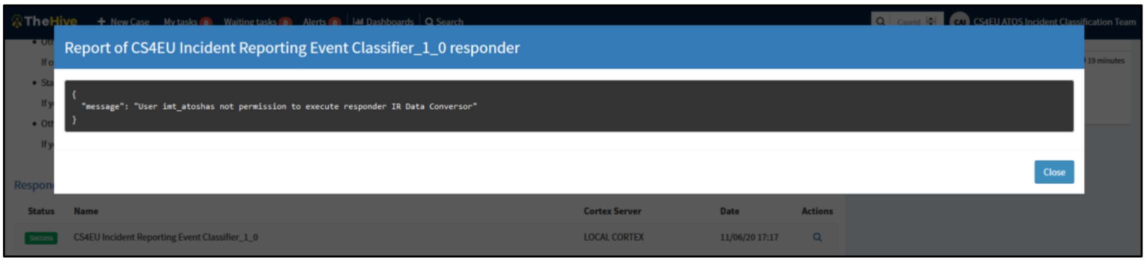
Figure 144. Tags of an Incident Case.



Incident Status	Ongoing	Incident Type	Cyber Security Incident	Event Detection	External Auditor
Event Detection: Specify if O...	Not Specified	Impact on Offered Payment ...	yes	Impact on RTGS: Target 2	yes
Impact on Personal Data	yes	Risk to rights and freedom of...	yes	Impact on Offered Trust Serv...	yes
Impact on Essential Services ...	yes	Affected essential services o...	yes	Impact on Other area under ...	no
Other impacted area	Not Specified	Overall impact on Confidenti...	yes	Overall impact on Integrity	yes
Overall impact on Availability	yes	Overall impact on Continuity	no	Overall impact on Authenticity	no
Other overall impact (if any)	Not Specified	Process/service or product i...	Not Specified	RTO if Critical/Systemic Proc...	Not Specified
Downtime for the service/pr...	Not Specified	Reputational damage: Media...	yes	Reputational damage: Sancti...	Not Specified
Reputational damage: incide...	Not Specified	Reputational damage: regula...	Not Specified	Payment transactions affect...	Not Specified
Payment transactions affect...	Not Specified	Regular level of payment tra...	Not Specified	Regular level of payment tra...	Not Specified
Total value of payment trans...	Not Specified	Total value of payment trans...	Not Specified	Payment Service Users (PSU)...	Not Specified
Payment Service Users (PSU)...	Not Specified	Total number of Payment Ser...	Not Specified	Total number of Payment Ser...	Not Specified
Direct cost (actual figure)	Not Specified	Direct cost (estimates)	Not Specified	Indirect cost (actual figure)	Not Specified
Indirect cost (estimates)	Not Specified	Tier 1 capital	Not Specified	Consolidated Tier 1 capital	Not Specified

Figure 145. Fields of a template.

The execution of the responder will invoke AIRE asset to determine if the user has permissions to execute for this phase of the workflow. If not, it will be shown something like Figure 146.



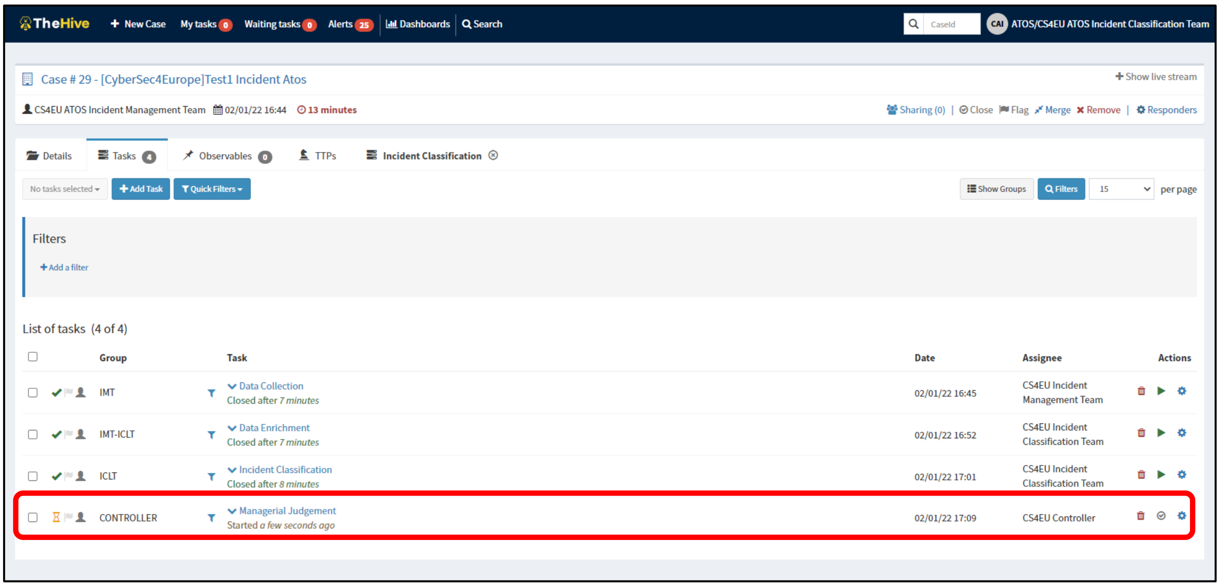
Report of CS4EU Incident Reporting Event Classifier_1_0 responder

```
{
  "message": "User imt_atoshas not permission to execute responder IR Data Conversor"
}
```

Status	Name	Cortex Server	Date	Actions
Success	CS4EU Incident Reporting Event Classifier_1_0	LOCAL CORTEX	11/06/20 17:17	

Figure 146. Output of a responder without permission.

7. **Managerial Judgement Task:** is automatically created and assigned to the Controller when the *Incident Classification* task is closed, Figure 147 and Figure 148.



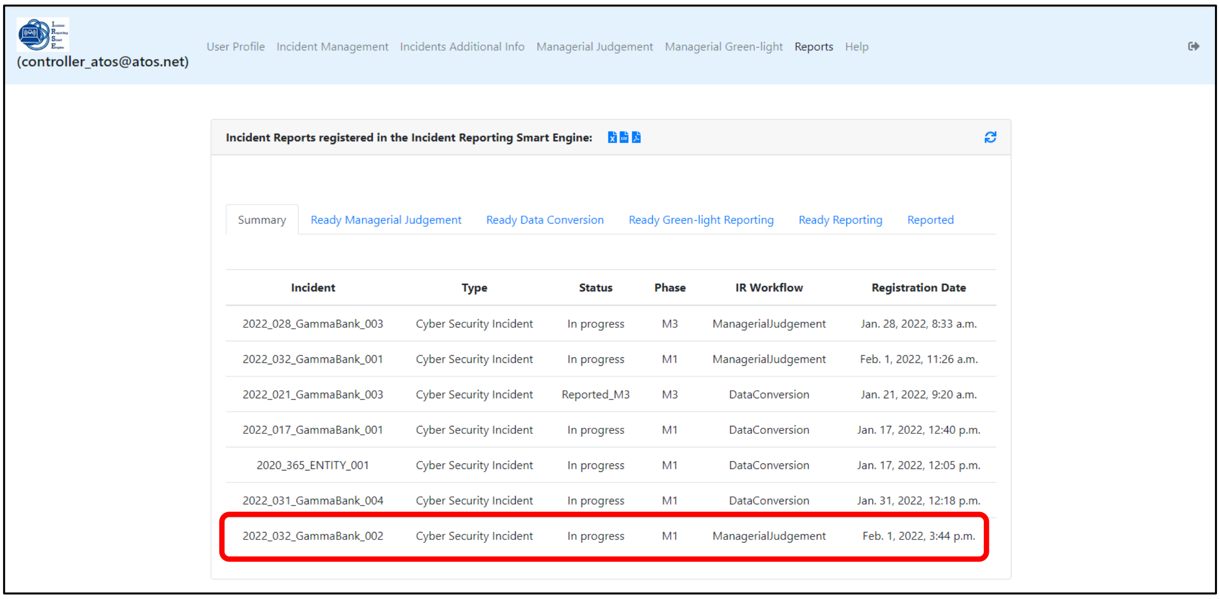
Case # 29 - [CyberSec4Europe]Test1 Incident Atos

CS4EU ATOS Incident Management Team 02/01/22 16:44 13 minutes

List of tasks (4 of 4)

☐	Group	Task	Date	Assignee
☐ ✓	IMT	Data Collection Closed after *7 minutes*	02/01/22 16:45	CS4EU Incident Management Team
☐ ✓	IMT-ICLT	Data Enrichment Closed after *7 minutes*	02/01/22 16:52	CS4EU Incident Classification Team
☐ ✓	ICLT	Incident Classification Closed after *8 minutes*	02/01/22 17:01	CS4EU Incident Classification Team
☐ ⌛	CONTROLLER	Managerial Judgement Started *a few seconds ago*	02/01/22 17:09	CS4EU Controller

Figure 147. Automatic creation of Managerial Judgement Task.

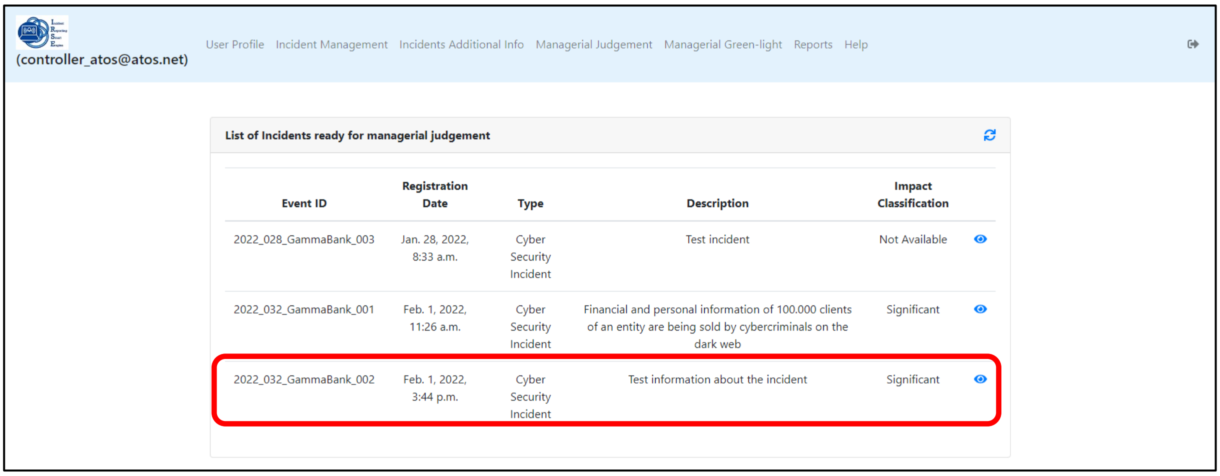

(controller_atos@atos.net)

Incident Reports registered in the Incident Reporting Smart Engine:

Incident	Type	Status	Phase	IR Workflow	Registration Date
2022_028_GammaBank_003	Cyber Security Incident	In progress	M3	ManagerialJudgement	Jan. 28, 2022, 8:33 a.m.
2022_032_GammaBank_001	Cyber Security Incident	In progress	M1	ManagerialJudgement	Feb. 1, 2022, 11:26 a.m.
2022_021_GammaBank_003	Cyber Security Incident	Reported_M3	M3	DataConversion	Jan. 21, 2022, 9:20 a.m.
2022_017_GammaBank_001	Cyber Security Incident	In progress	M1	DataConversion	Jan. 17, 2022, 12:40 p.m.
2020_365_ENTITY_001	Cyber Security Incident	In progress	M1	DataConversion	Jan. 17, 2022, 12:05 p.m.
2022_031_GammaBank_004	Cyber Security Incident	In progress	M1	DataConversion	Jan. 31, 2022, 12:18 p.m.
2022_032_GammaBank_002	Cyber Security Incident	In progress	M1	ManagerialJudgement	Feb. 1, 2022, 3:44 p.m.

Figure 148. Automatic creation of Managerial Judgement IR Workflow.

8. Under the menu *Managerial Judgement*, the controller will see the report with the impact classification, Figure 149.

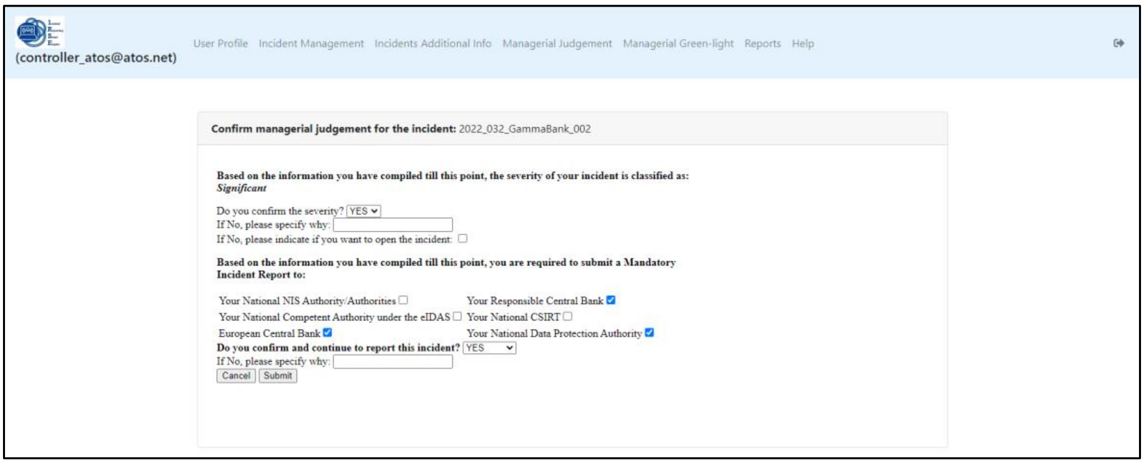


List of Incidents ready for managerial judgement

Event ID	Registration Date	Type	Description	Impact Classification	
2022_028_GammaBank_003	Jan. 28, 2022, 8:33 a.m.	Cyber Security Incident	Test incident	Not Available	👁
2022_032_GammaBank_001	Feb. 1, 2022, 11:26 a.m.	Cyber Security Incident	Financial and personal information of 100.000 clients of an entity are being sold by cybercriminals on the dark web	Significant	👁
2022_032_GammaBank_002	Feb. 1, 2022, 3:44 p.m.	Cyber Security Incident	Test information about the incident	Significant	👁

Figure 149. List of Incident ready for managerial judgement.

The *Detail* button (the “Eye”) shows the event severity classification and the suggested mandatory reporting based on the criteria of the regulations enabled, Figure 150.



Confirm managerial judgement for the incident: 2022_032_GammaBank_002

Based on the information you have compiled till this point, the severity of your incident is classified as:
Significant

Do you confirm the severity? YES
If No, please specify why:
If No, please indicate if you want to open the incident: □

Based on the information you have compiled till this point, you are required to submit a Mandatory Incident Report to:

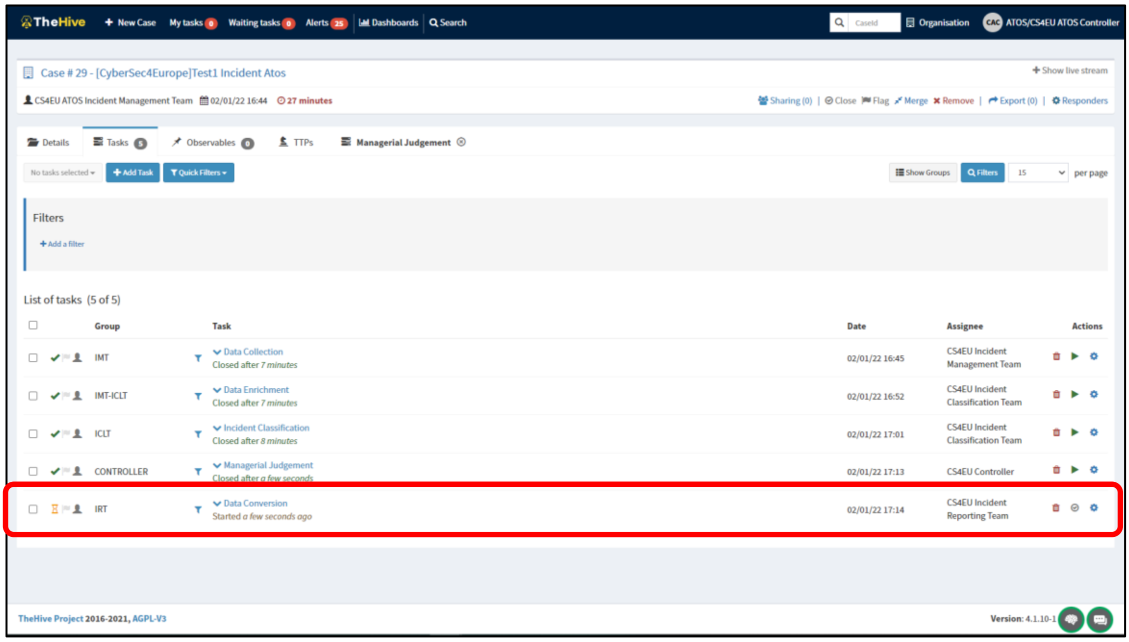
Your National NIS Authority/Authorities □
Your National Competent Authority under the eIDAS □
European Central Bank ☑
Your Responsible Central Bank ☑
Your National CSIRT □
Your National Data Protection Authority ☑

Do you confirm and continue to report this incident? YES
If No, please specify why:

Figure 150. Form for a managerial judgement.

NOTE: In case the Controller does not confirm the classification and select to open the incident, the incident reporting process will come back to the “Data Enrichment” phase. In this case, the controller does not confirm to proceed with the reporting, the incident reporting process will finish, and the reports will be closed.

Once the managerial judgement is done, go to Incident Management tab to close the task. Automatically, the task called "Managerial Judgement" will be closed by AIRE asset and the workflow of the report will be moved to the following step (depending on the managerial judgement). Then, a new task "Data Conversion" will be created assigned to the Incident Reporting Team and the report will be ready for report preparation, Figure 151.



Case # 29 - [CyberSec4Europe]Test1 Incident Atos

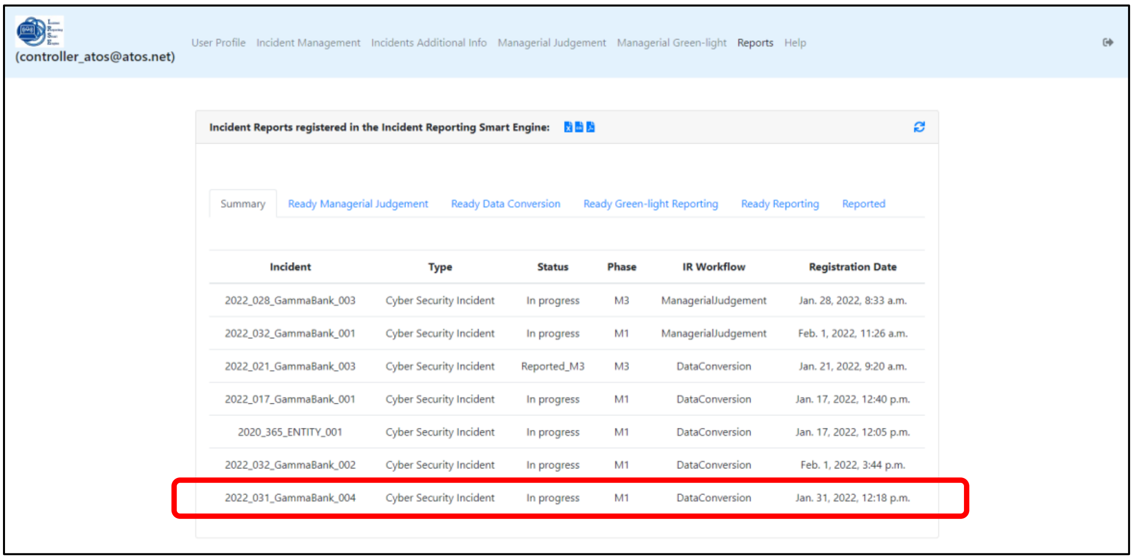
CS4EU ATOS Incident Management Team 02/01/22 16:44 27 minutes

List of tasks (5 of 5)

□	Group	Task	Date	Assignee	Actions
□	IMT	Data Collection Closed after *7 minutes*	02/01/22 16:45	CS4EU Incident Management Team	
□	IMT-ICLT	Data Enrichment Closed after *7 minutes*	02/01/22 16:52	CS4EU Incident Classification Team	
□	ICLT	Incident Classification Closed after *8 minutes*	02/01/22 17:01	CS4EU Incident Classification Team	
□	CONTROLLER	Managerial Judgement Closed after *a few seconds*	02/01/22 17:13	CS4EU Controller	
□	IRT	Data Conversion Started *a few seconds ago*	02/01/22 17:14	CS4EU Incident Reporting Team	

Figure 151. New Data Conversion Task.

This event is registered in the *Summary* of the *Reports* tab, Figure 152.

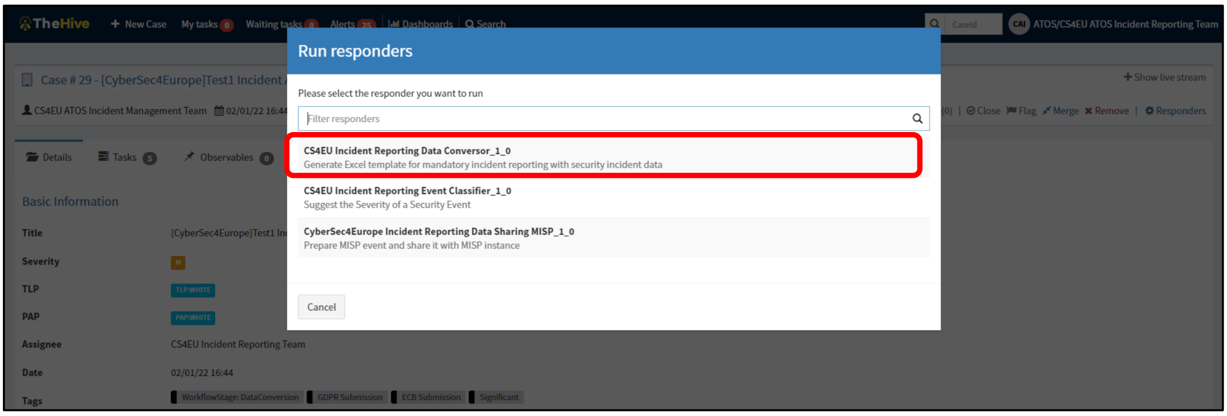


Incident Reports registered in the Incident Reporting Smart Engine:

Incident	Type	Status	Phase	IR Workflow	Registration Date
2022_028_GammaBank_003	Cyber Security Incident	In progress	M3	ManagerialJudgement	Jan. 28, 2022, 8:33 a.m.
2022_032_GammaBank_001	Cyber Security Incident	In progress	M1	ManagerialJudgement	Feb. 1, 2022, 11:26 a.m.
2022_021_GammaBank_003	Cyber Security Incident	Reported_M3	M3	DataConversion	Jan. 21, 2022, 9:20 a.m.
2022_017_GammaBank_001	Cyber Security Incident	In progress	M1	DataConversion	Jan. 17, 2022, 12:40 p.m.
2020_365_ENTITY_001	Cyber Security Incident	In progress	M1	DataConversion	Jan. 17, 2022, 12:05 p.m.
2022_032_GammaBank_002	Cyber Security Incident	In progress	M1	DataConversion	Feb. 1, 2022, 3:44 p.m.
2022_031_GammaBank_004	Cyber Security Incident	In progress	M1	DataConversion	Jan. 31, 2022, 12:18 p.m.

Figure 152. Register of Data Conversion Task.

9. **Run Responder:** the additional information required for reporting needs to be completed by the Incident Reporting Team user for invoking the responder *CS4EU Incident Reporting Data Converter*, which generates the Excel files associated to the regulations enabled and confirmed by the Controller in the managerial judgement, Figure 153.



Case # 29 - [CyberSec4Europe]Test1 Incident

CS4EU ATOS Incident Management Team 02/01/22 16:44

Basic Information

Title [CyberSec4Europe]Test1 In

Severity M

TLP TLP:WHITE

PAP PAP:WHITE

Assignee CS4EU Incident Reporting Team

Date 02/01/22 16:44

Tags WorkflowStage: DataConversion GDPR Submission ECB Submission Significant

Run responders

Please select the responder you want to run

Filter responders

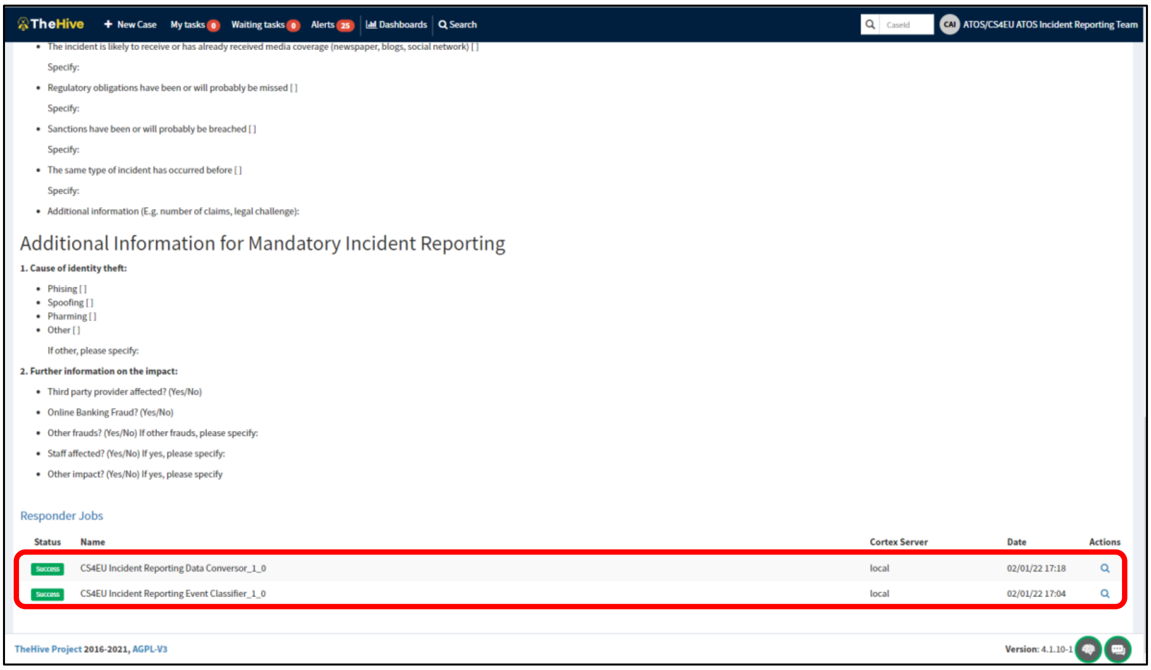
CS4EU Incident Reporting Data Conversor_1_0
Generate Excel template for mandatory incident reporting with security incident data

CS4EU Incident Reporting Event Classifier_1_0
Suggest the Severity of a Security Event

CyberSec4Europe Incident Reporting Data Sharing MISP_1_0
Prepare MISP event and share it with MISP instance

Figure 153. Run responder invocation.

The result of the execution is shown at the end of the page, Figure 154.



- The incident is likely to receive or has already received media coverage (newspaper, blogs, social network) [ ]

  Specify:
- Regulatory obligations have been or will probably be missed [ ]

  Specify:
- Sanctions have been or will probably be breached [ ]

  Specify:
- The same type of incident has occurred before [ ]

  Specify:
- Additional information (E.g. number of claims, legal challenge):

Additional Information for Mandatory Incident Reporting

1. Cause of identity theft:

- Phising [ ]
- Spoofing [ ]
- Pharming [ ]
- Other [ ]

  If other, please specify:

2. Further information on the impact:

- Third party provider affected? (Yes/No)
- Online Banking Fraud? (Yes/No)
- Other frauds? (Yes/No) If other frauds, please specify:
- Staff affected? (Yes/No) If yes, please specify:
- Other impact? (Yes/No) If yes, please specify

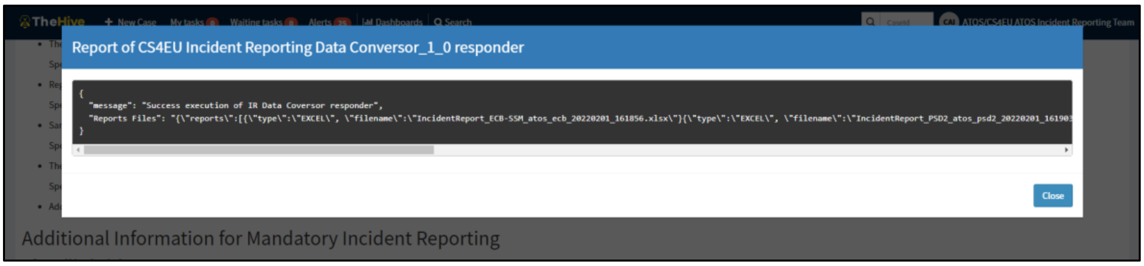
Responder Jobs

Status	Name	Cortex Server	Date	Actions
Success	CS4EU Incident Reporting Data Conversor_1_0	local	02/01/22 17:18	🔍
Success	CS4EU Incident Reporting Event Classifier_1_0	local	02/01/22 17:04	🔍

TheHive Project 2016-2021, AGPL-V3 Version: 4.1.10-1

Figure 154. Status of Responders Jobs.

The action button opens a text box with the result of the responder execution, Figure 155.



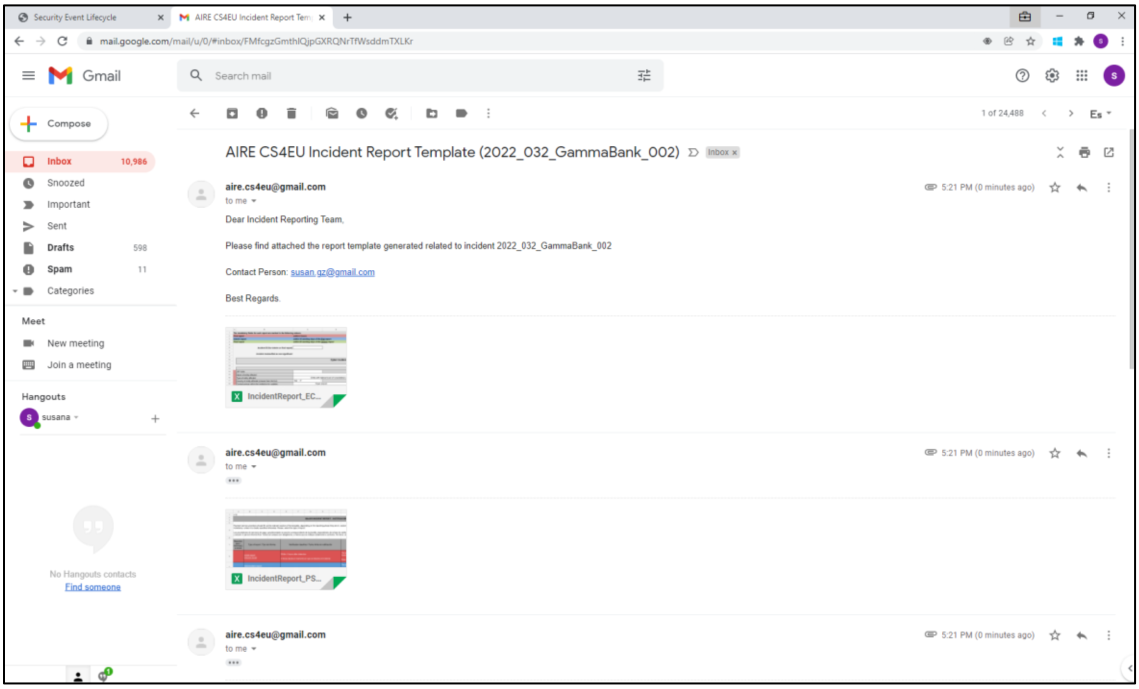
Report of CS4EU Incident Reporting Data Conversor_1_0 responder

```
{
  "message": "Success execution of IR Data Coversor responder",
  "Reports Files": "{\"reports\":[{\"type\":\"EXCEL\", \"filename\":\"IncidentReport_ECB-SSM_atos_ecb_20220201_161856.xlsx\"}{\"type\":\"EXCEL\", \"filename\":\"IncidentReport_PSD2_atos_psd2_20220201_16190
}
```

Additional Information for Mandatory Incident Reporting

Figure 155. Result of a Responder Job.

An email is sent to the Incident Reporting Team user who executed the responder job with the Excel file generated attached, Figure 156.



AIRE CS4EU Incident Report Template (2022_032_GammaBank_002)

aire.cs4eu@gmail.com
to me
5:21 PM (0 minutes ago)

Dear Incident Reporting Team,

Please find attached the report template generated related to incident 2022_032_GammaBank_002

Contact Person: susan.gz@gmail.com

Best Regards.

IncidentReport_EC...

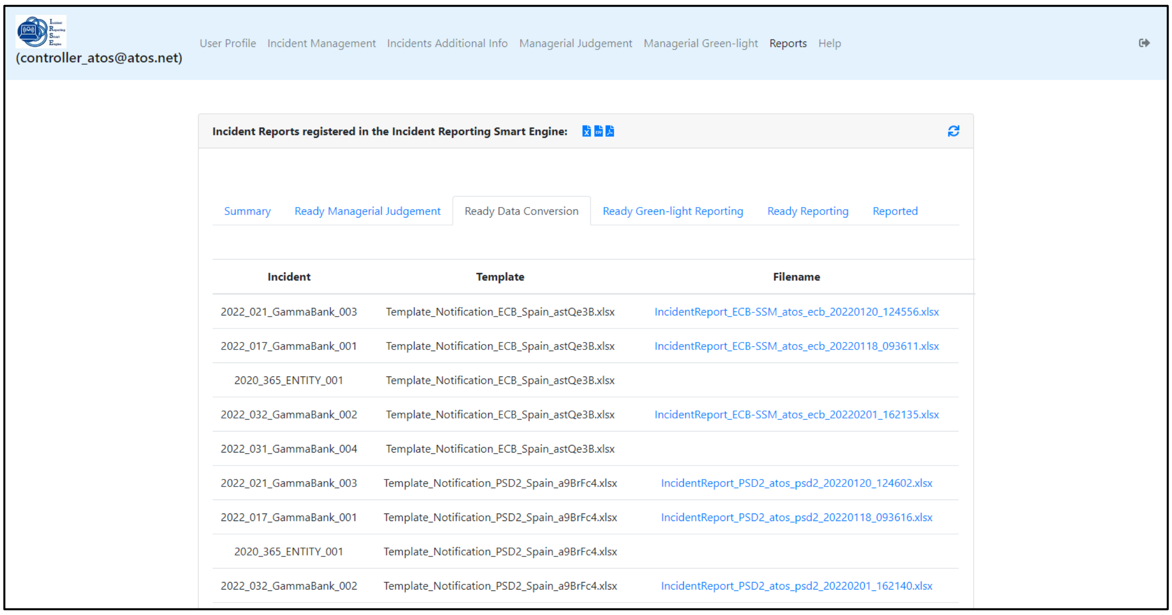
aire.cs4eu@gmail.com
to me
5:21 PM (0 minutes ago)

IncidentReport_PS...

aire.cs4eu@gmail.com
to me
5:21 PM (0 minutes ago)

Figure 156. Email to Incident Reporting Team user.

All the reports are available in the dashboard under *Reports* in *Ready Data Conversion,* Figure 157.

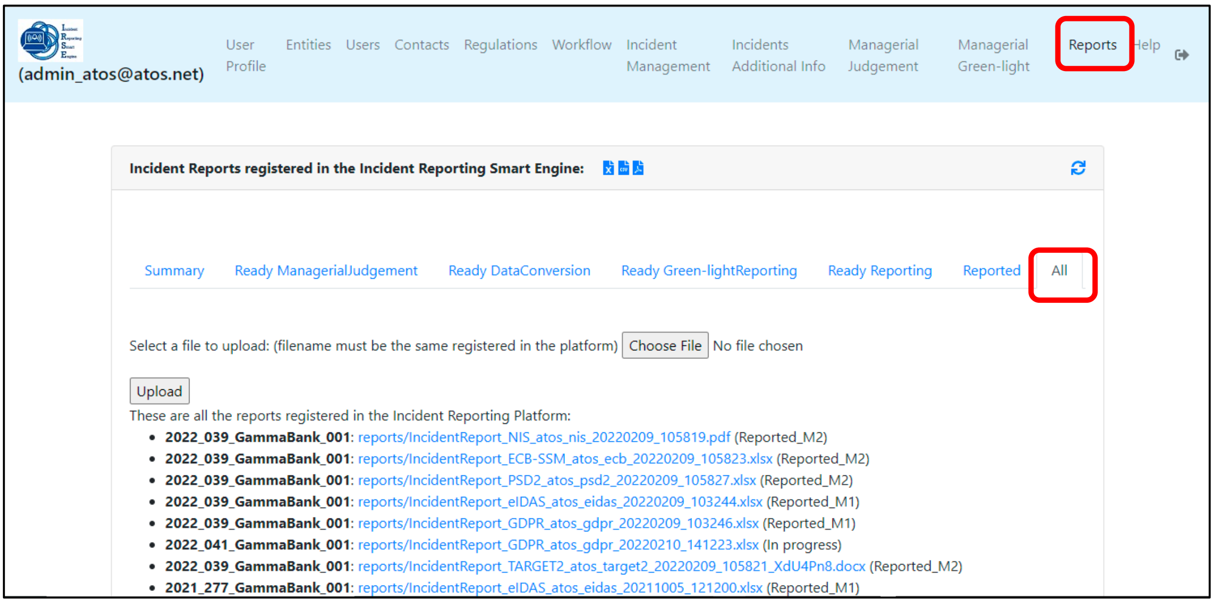


Incident Reports registered in the Incident Reporting Smart Engine:

Incident	Template	Filename
2022_021_GammaBank_003	Template_Notification_ECB_Spain_astQe3B.xlsx	IncidentReport_ECB-SSM_atos_ecb_20220120_124556.xlsx
2022_017_GammaBank_001	Template_Notification_ECB_Spain_astQe3B.xlsx	IncidentReport_ECB-SSM_atos_ecb_20220118_093611.xlsx
2020_365_ENTITY_001	Template_Notification_ECB_Spain_astQe3B.xlsx	
2022_032_GammaBank_002	Template_Notification_ECB_Spain_astQe3B.xlsx	IncidentReport_ECB-SSM_atos_ecb_20220201_162135.xlsx
2022_031_GammaBank_004	Template_Notification_ECB_Spain_astQe3B.xlsx	
2022_021_GammaBank_003	Template_Notification_PSD2_Spain_a9BrFc4.xlsx	IncidentReport_PSD2_atos_psd2_20220120_124602.xlsx
2022_017_GammaBank_001	Template_Notification_PSD2_Spain_a9BrFc4.xlsx	IncidentReport_PSD2_atos_psd2_20220118_093616.xlsx
2020_365_ENTITY_001	Template_Notification_PSD2_Spain_a9BrFc4.xlsx	
2022_032_GammaBank_002	Template_Notification_PSD2_Spain_a9BrFc4.xlsx	IncidentReport_PSD2_atos_psd2_20220201_162140.xlsx

Figure 157. List of available reports.

10. **Upload modified reports:** In case the report is modified, the latest version of the documents can be uploaded to the platform from the Reports section. This upload functionality is available from the menu “All” under “Reports” menu. The name of the file selected to upload to the platform must be the same of one already existent, Figure 158.



Incident Reports registered in the Incident Reporting Smart Engine:

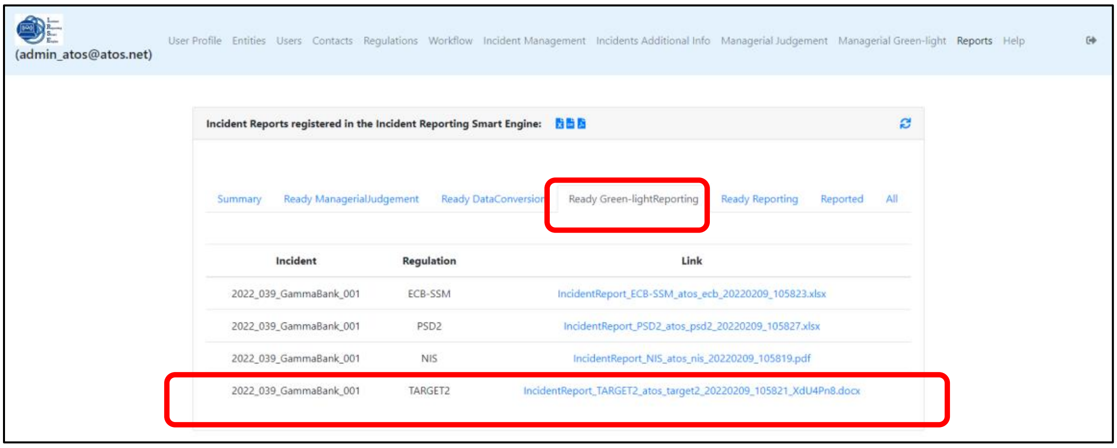
Select a file to upload: (filename must be the same registered in the platform) Choose File No file chosen

These are all the reports registered in the Incident Reporting Platform:

- **2022_039_GammaBank_001**: reports/IncidentReport_NIS_atos_nis_20220209_105819.pdf (Reported_M2)
- **2022_039_GammaBank_001**: reports/IncidentReport_ECB-SSM_atos_ecb_20220209_105823.xlsx (Reported_M2)
- **2022_039_GammaBank_001**: reports/IncidentReport_PSD2_atos_psd2_20220209_105827.xlsx (Reported_M2)
- **2022_039_GammaBank_001**: reports/IncidentReport_eIDAS_atos_eidas_20220209_103244.xlsx (Reported_M1)
- **2022_039_GammaBank_001**: reports/IncidentReport_GDPR_atos_gdpr_20220209_103246.xlsx (Reported_M1)
- **2022_041_GammaBank_001**: reports/IncidentReport_GDPR_atos_gdpr_20220210_141223.xlsx (In progress)
- **2022_039_GammaBank_001**: reports/IncidentReport_TARGET2_atos_target2_20220209_105821_XdU4Pn8.docx (Reported_M2)
- **2021_277_GammaBank_001**: reports/IncidentReport_eIDAS_atos_eidas_20211005_121200.xlsx (Reported_M1)

Figure 158. Upload modified reports menu.

The new file will be registered with the same name but automatically adding a suffix. In this way, the users will always visualize the last version of the reports but can identify which ones are the generated automatically by the platform (they end with the timestamp <yyyymmdd_HHMMSS>) or have been modified (they end with <yyyymmdd_HHMMSS> followed by _<suffix>), Figure 159.

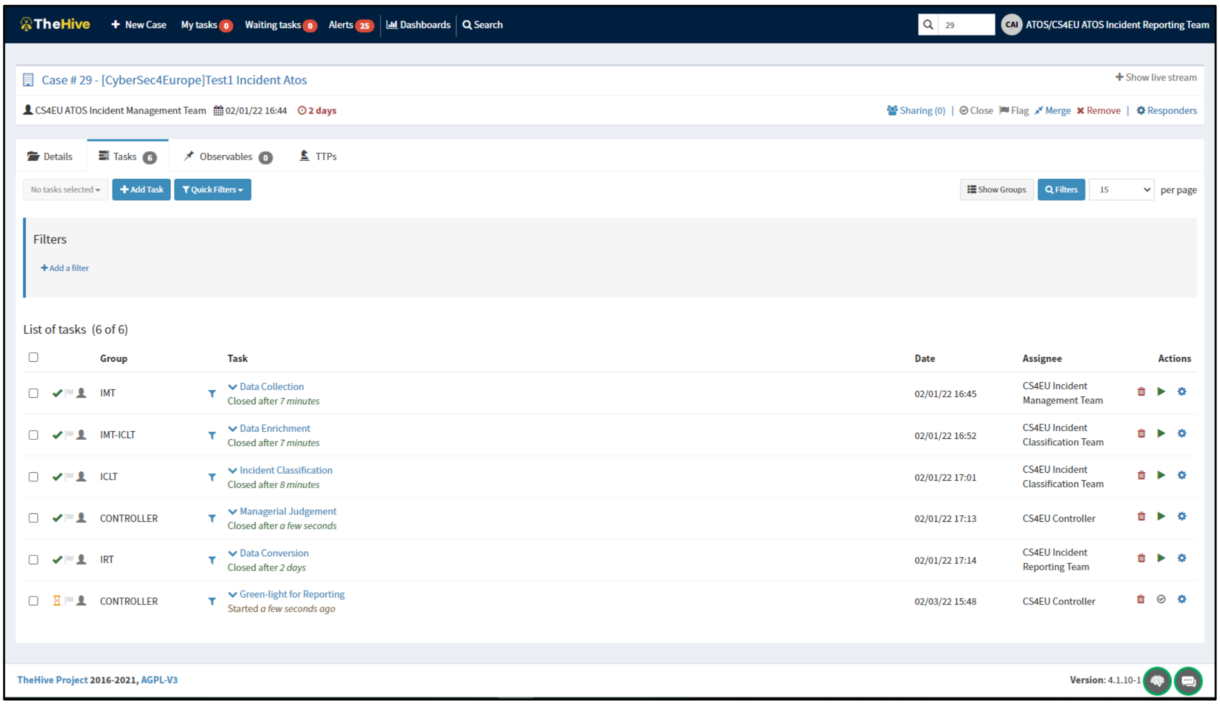


Incident Reports registered in the Incident Reporting Smart Engine:

Incident	Regulation	Link
2022_039_GammaBank_001	ECB-SSM	IncidentReport_ECB-SSM_atos_ecb_20220209_105823.xlsx
2022_039_GammaBank_001	PSD2	IncidentReport_PSD2_atos_psd2_20220209_105827.xlsx
2022_039_GammaBank_001	NIS	IncidentReport_NIS_atos_nis_20220209_105819.pdf
2022_039_GammaBank_001	TARGET2	IncidentReport_TARGET2_atos_target2_20220209_105821_XdU4Pn8.docx

Figure 159. Ready Green-light Reporting list.

11. **Close *Data Conversion* Task:** Once the report has been completed and reviewed by the IRT, the user will close the task *Data Conversion* associated and a new task *Green-light for Reporting* will appear assigned to the CONTROLLER, Figure 160.



Case # 29 - [CyberSec4Europe]Test1 Incident Atos

CS4EU ATOS Incident Management Team 02/01/22 16:44 2 days

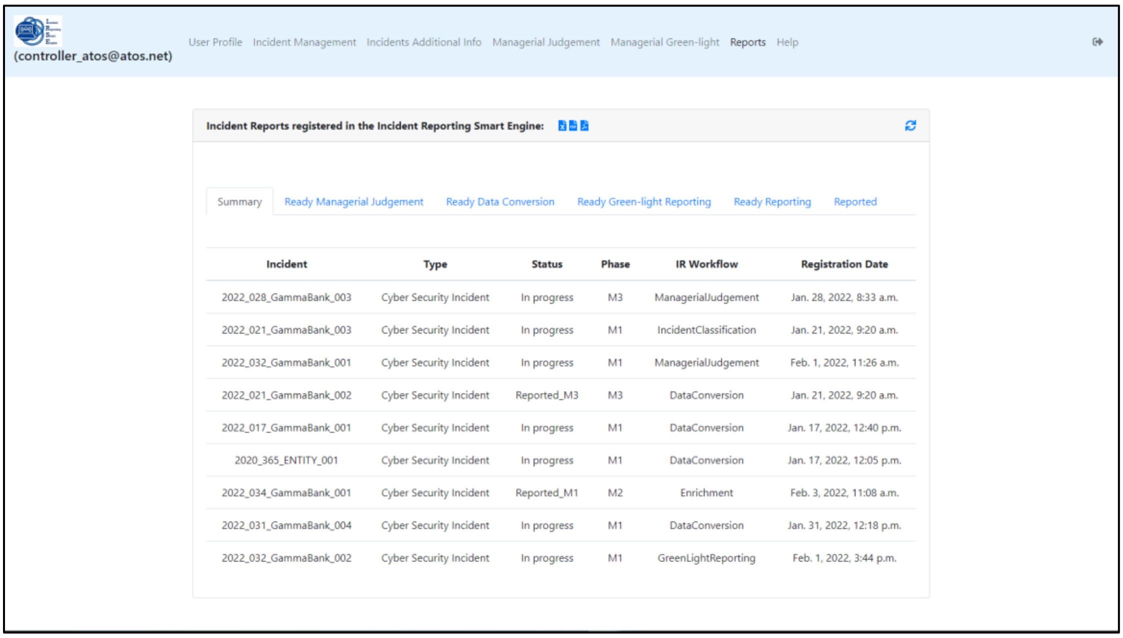
Filters

List of tasks (6 of 6)

□	Group	Task	Date	Assignee	Actions
□ ✓	IMT	Data Collection Closed after *7 minutes*	02/01/22 16:45	CS4EU Incident Management Team	
□ ✓	IMT-ICLT	Data Enrichment Closed after *7 minutes*	02/01/22 16:52	CS4EU Incident Classification Team	
□ ✓	ICLT	Incident Classification Closed after *8 minutes*	02/01/22 17:01	CS4EU Incident Classification Team	
□ ✓	CONTROLLER	Managerial Judgement Closed after *a few seconds*	02/01/22 17:13	CS4EU Controller	
□ ✓	IRT	Data Conversion Closed after *2 days*	02/01/22 17:14	CS4EU Incident Reporting Team	
□ ⌛	CONTROLLER	Green-light for Reporting Started *a few seconds ago*	02/03/22 15:48	CS4EU Controller	

Figure 160. New Green-light for Reporting Task.

A new register is added into the *Summary* of the *Reports*, Figure 161.

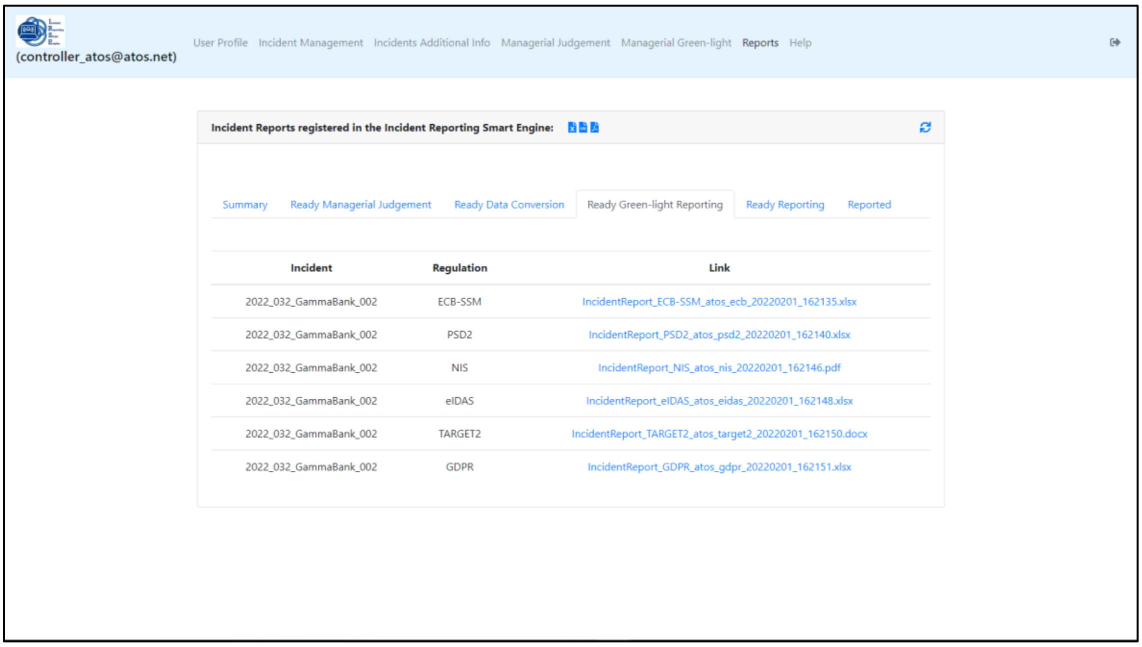


Incident Reports registered in the Incident Reporting Smart Engine:

Incident	Type	Status	Phase	IR Workflow	Registration Date
2022_028_GammaBank_003	Cyber Security Incident	In progress	M3	ManagerialJudgement	Jan. 28, 2022, 8:33 a.m.
2022_021_GammaBank_003	Cyber Security Incident	In progress	M1	IncidentClassification	Jan. 21, 2022, 9:20 a.m.
2022_032_GammaBank_001	Cyber Security Incident	In progress	M1	ManagerialJudgement	Feb. 1, 2022, 11:26 a.m.
2022_021_GammaBank_002	Cyber Security Incident	Reported_M3	M3	DataConversion	Jan. 21, 2022, 9:20 a.m.
2022_017_GammaBank_001	Cyber Security Incident	In progress	M1	DataConversion	Jan. 17, 2022, 12:40 p.m.
2020_365_ENTITY_001	Cyber Security Incident	In progress	M1	DataConversion	Jan. 17, 2022, 12:05 p.m.
2022_034_GammaBank_001	Cyber Security Incident	Reported_M1	M2	Enrichment	Feb. 3, 2022, 11:08 a.m.
2022_031_GammaBank_004	Cyber Security Incident	In progress	M1	DataConversion	Jan. 31, 2022, 12:18 p.m.
2022_032_GammaBank_002	Cyber Security Incident	In progress	M1	GreenLightReporting	Feb. 1, 2022, 3:44 p.m.

Figure 161. Register of Green Light Report.

In the tab *Ready Green-light Reporting* inside *Reports* there is a list of all ready reports, Figure 162.

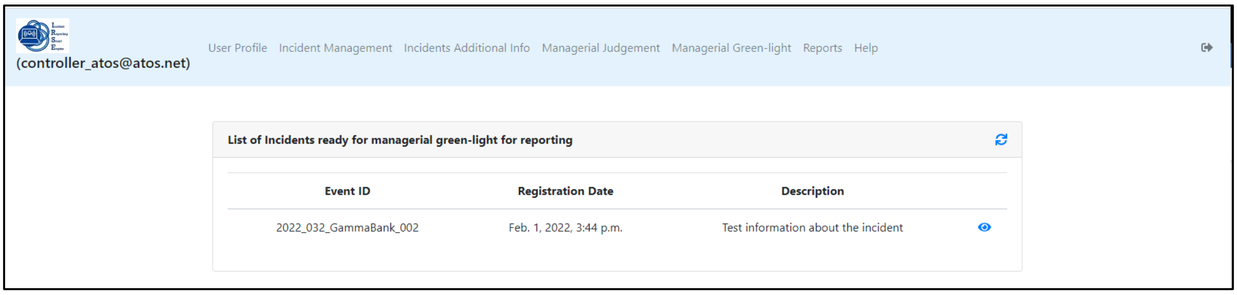


Incident Reports registered in the Incident Reporting Smart Engine:

Incident	Regulation	Link
2022_032_GammaBank_002	ECB-SSM	IncidentReport_ECB-SSM_atos_ecb_20220201_162135.xlsx
2022_032_GammaBank_002	PSD2	IncidentReport_PSD2_atos_psd2_20220201_162140.xlsx
2022_032_GammaBank_002	NIS	IncidentReport_NIS_atos_nis_20220201_162146.pdf
2022_032_GammaBank_002	eIDAS	IncidentReport_eIDAS_atos_eidas_20220201_162148.xlsx
2022_032_GammaBank_002	TARGET2	IncidentReport_TARGET2_atos_target2_20220201_162150.docx
2022_032_GammaBank_002	GDPR	IncidentReport_GDPR_atos_gdpr_20220201_162151.xlsx

Figure 162. List of Ready Green-light Reporting.

12. **Managerial Green-light:** allows performing the managerial judgement. The tab displays the list of ready reports, Figure 163.

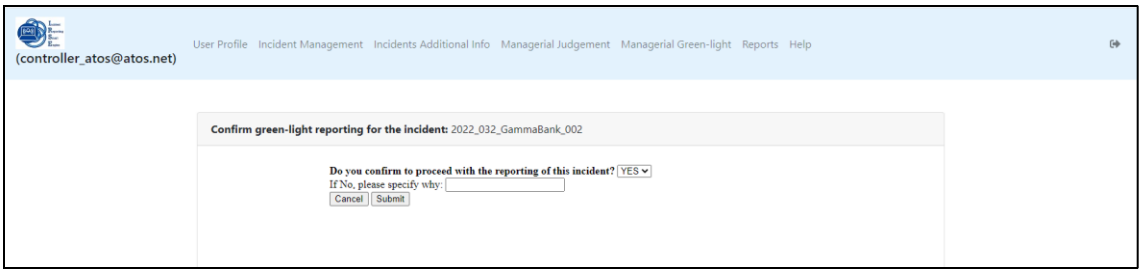


List of Incidents ready for managerial green-light for reporting

Event ID	Registration Date	Description
2022_032_GammaBank_002	Feb. 1, 2022, 3:44 p.m.	Test information about the incident

Figure 163. List of Incident ready for managerial green-light for reporting.

Selecting in the details (eye) the managerial judgement form will appear to confirm if proceeding with the reporting, Figure 164.



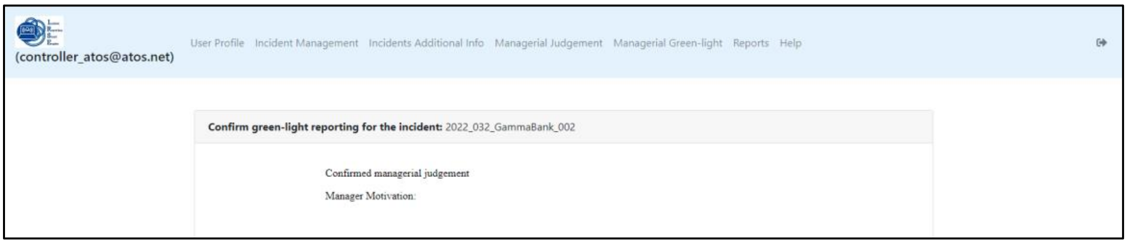
Confirm green-light reporting for the incident: 2022_032_GammaBank_002

Do you confirm to proceed with the reporting of this incident? YES

If No, please specify why:

Figure 164. Configuration of green-light reporting form.

Submit button automatically closes the task *Green-light for Reporting*, showing a confirmation, Figure 165.



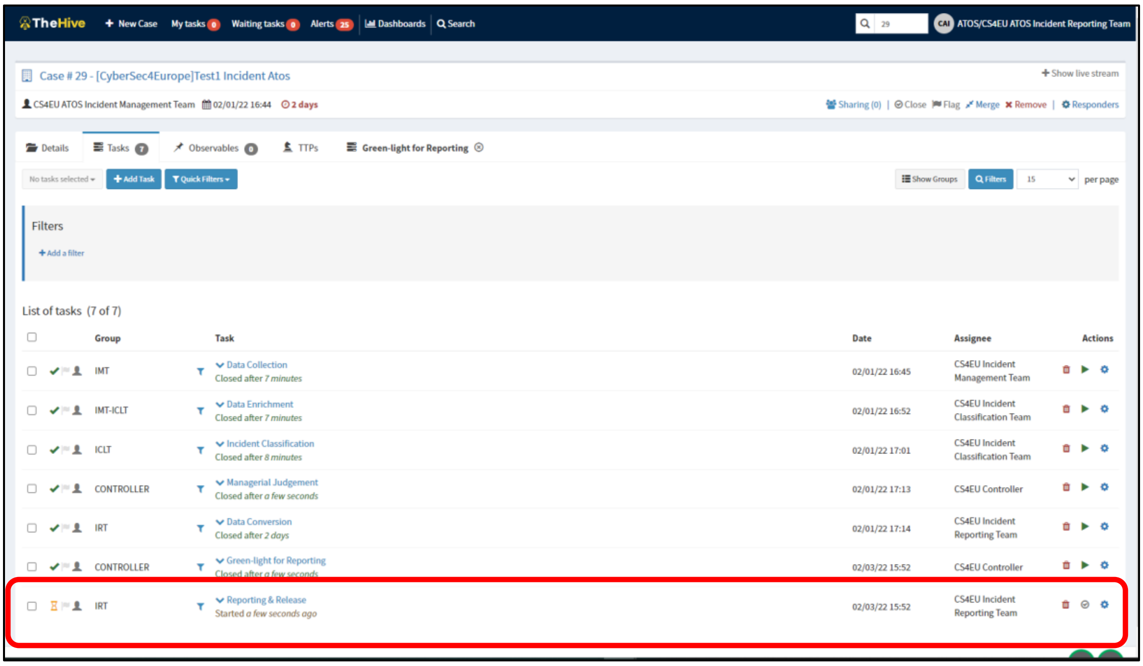
Confirm green-light reporting for the incident: 2022_032_GammaBank_002

Confirmed managerial judgement

Manager Motivation:

Figure 165. Confirmation of task closed.

It also creates new task, *Reporting & Release*, which will be assigned to IRT user, Figure 166.



Case # 29 - [CyberSec4Europe]Test1 Incident Atos

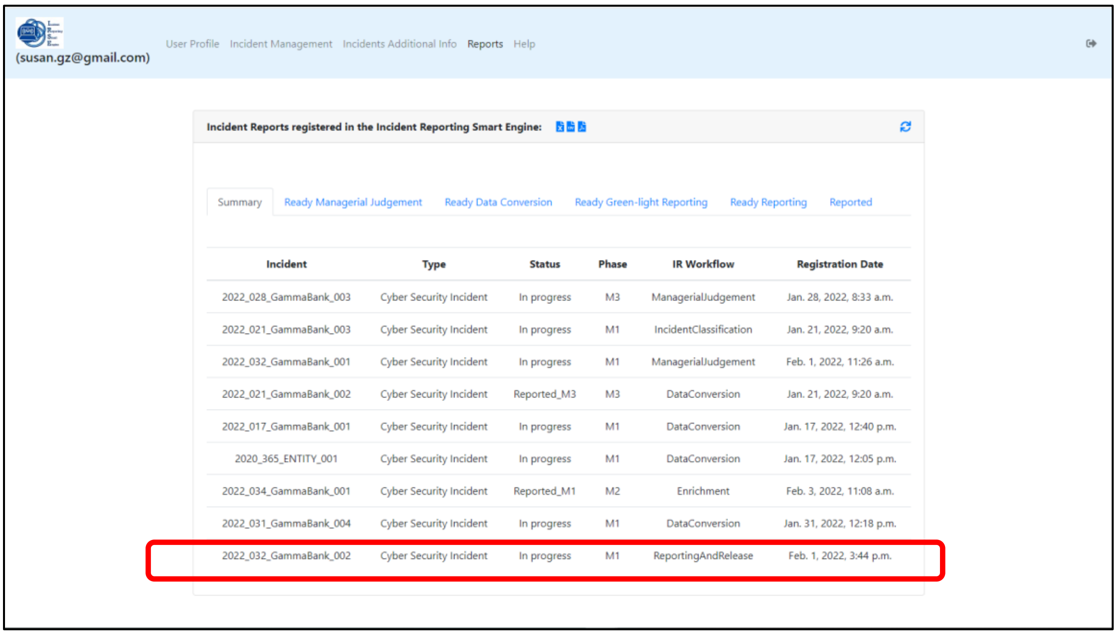
CS4EU ATOS Incident Management Team 02/01/22 16:44 2 days

List of tasks (7 of 7)

□	Group	Task	Date	Assignee	Actions
□ ✓	IMT	Data Collection Closed after *7 minutes*	02/01/22 16:45	CS4EU Incident Management Team	
□ ✓	IMT-ICLT	Data Enrichment Closed after *7 minutes*	02/01/22 16:52	CS4EU Incident Classification Team	
□ ✓	ICLT	Incident Classification Closed after *8 minutes*	02/01/22 17:01	CS4EU Incident Classification Team	
□ ✓	CONTROLLER	Managerial Judgement Closed after *a few seconds*	02/01/22 17:13	CS4EU Controller	
□ ✓	IRT	Data Conversion Closed after *2 days*	02/01/22 17:14	CS4EU Incident Reporting Team	
□ ✓	CONTROLLER	Green-light for Reporting Closed after *a few seconds*	02/03/22 15:52	CS4EU Controller	
□ ⌛	IRT	Reporting & Release Started *a few seconds ago*	02/03/22 15:52	CS4EU Incident Reporting Team	

Figure 166. New Reporting and Release Task.

The event is registered on the Summary of the Reports, Figure 167.



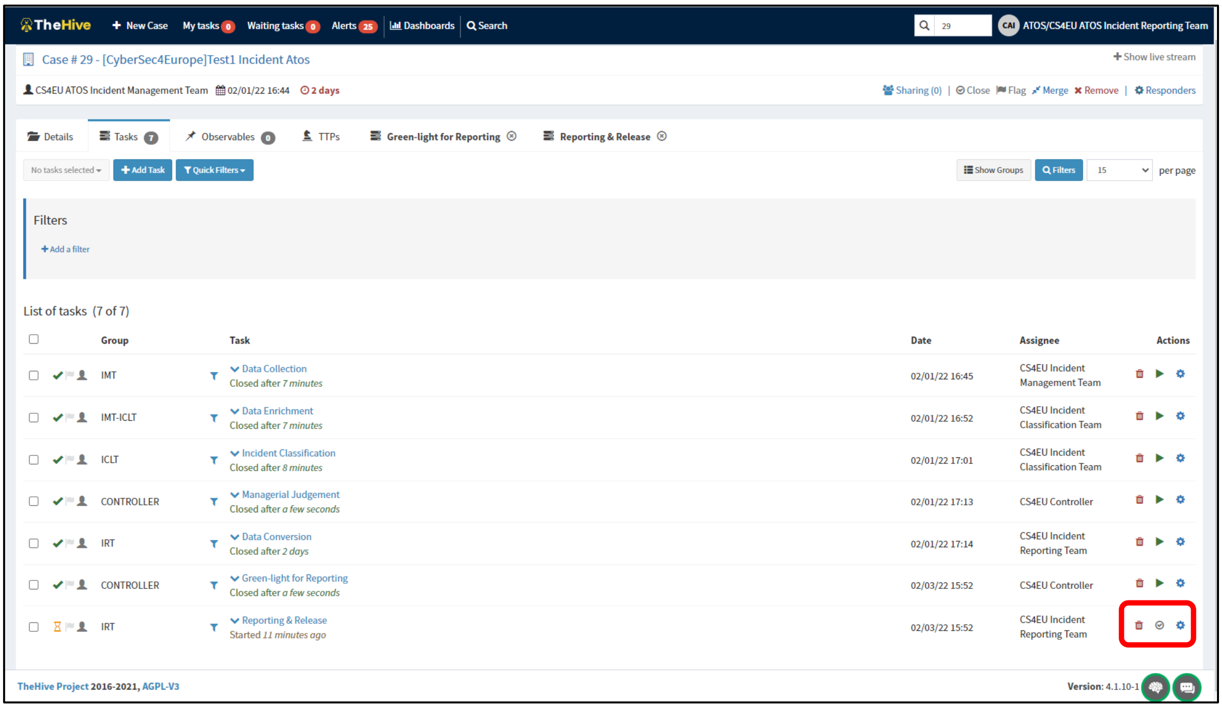
Incident Reports registered in the Incident Reporting Smart Engine:

Incident	Type	Status	Phase	IR Workflow	Registration Date
2022_028_GammaBank_003	Cyber Security Incident	In progress	M3	ManagerialJudgement	Jan. 28, 2022, 8:33 a.m.
2022_021_GammaBank_003	Cyber Security Incident	In progress	M1	IncidentClassification	Jan. 21, 2022, 9:20 a.m.
2022_032_GammaBank_001	Cyber Security Incident	In progress	M1	ManagerialJudgement	Feb. 1, 2022, 11:26 a.m.
2022_021_GammaBank_002	Cyber Security Incident	Reported_M3	M3	DataConversion	Jan. 21, 2022, 9:20 a.m.
2022_017_GammaBank_001	Cyber Security Incident	In progress	M1	DataConversion	Jan. 17, 2022, 12:40 p.m.
2020_365_ENTITY_001	Cyber Security Incident	In progress	M1	DataConversion	Jan. 17, 2022, 12:05 p.m.
2022_034_GammaBank_001	Cyber Security Incident	Reported_M1	M2	Enrichment	Feb. 3, 2022, 11:08 a.m.
2022_031_GammaBank_004	Cyber Security Incident	In progress	M1	DataConversion	Jan. 31, 2022, 12:18 p.m.
2022_032_GammaBank_002	Cyber Security Incident	In progress	M1	ReportingAndRelease	Feb. 1, 2022, 3:44 p.m.

Figure 167. Reporting And Release register in Summary of Reports.

NOTE: In case the Controller does not confirm proceeding with the actual reporting, the incident reporting process will finish, and the reports will be closed.

13. **Closing the reporting phase:** IRT user can close the task associated *Reporting & Release* from TheHive template. The report will appear in the dashboard under *Reports* tab in the status *Reported_M1*, changing the phase to *M2* and the workflow to a new *Enrichment*, Figure 168.



Case # 29 - [CyberSec4Europe]Test1 Incident Atos

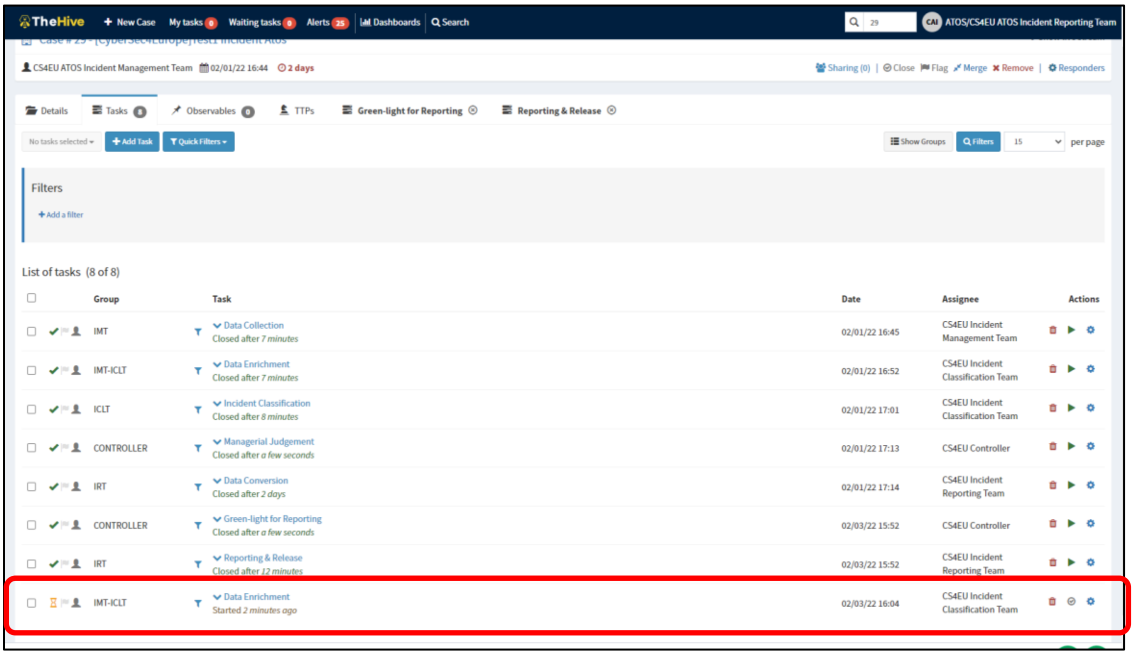
CS4EU ATOS Incident Management Team 02/01/22 16:44 2 days

List of tasks (7 of 7)

Group	Task	Date	Assignee
IMT	Data Collection Closed after *7 minutes*	02/01/22 16:45	CS4EU Incident Management Team
IMT-ICLT	Data Enrichment Closed after *7 minutes*	02/01/22 16:52	CS4EU Incident Classification Team
ICLT	Incident Classification Closed after *8 minutes*	02/01/22 17:01	CS4EU Incident Classification Team
CONTROLLER	Managerial Judgement Closed after *a few seconds*	02/01/22 17:13	CS4EU Controller
IRT	Data Conversion Closed after *2 days*	02/01/22 17:14	CS4EU Incident Reporting Team
CONTROLLER	Green-light for Reporting Closed after *a few seconds*	02/03/22 15:52	CS4EU Controller
IRT	Reporting & Release Started *11 minutes ago*	02/03/22 15:52	CS4EU Incident Reporting Team

Figure 168. Reporting and Release actions.

And a new task “Data Enrichment” will be opened in TheHive to enrich the information about the incident for the Interim Report (M2), Figure 169.



CS4EU ATOS Incident Management Team 02/01/22 16:44 2 days

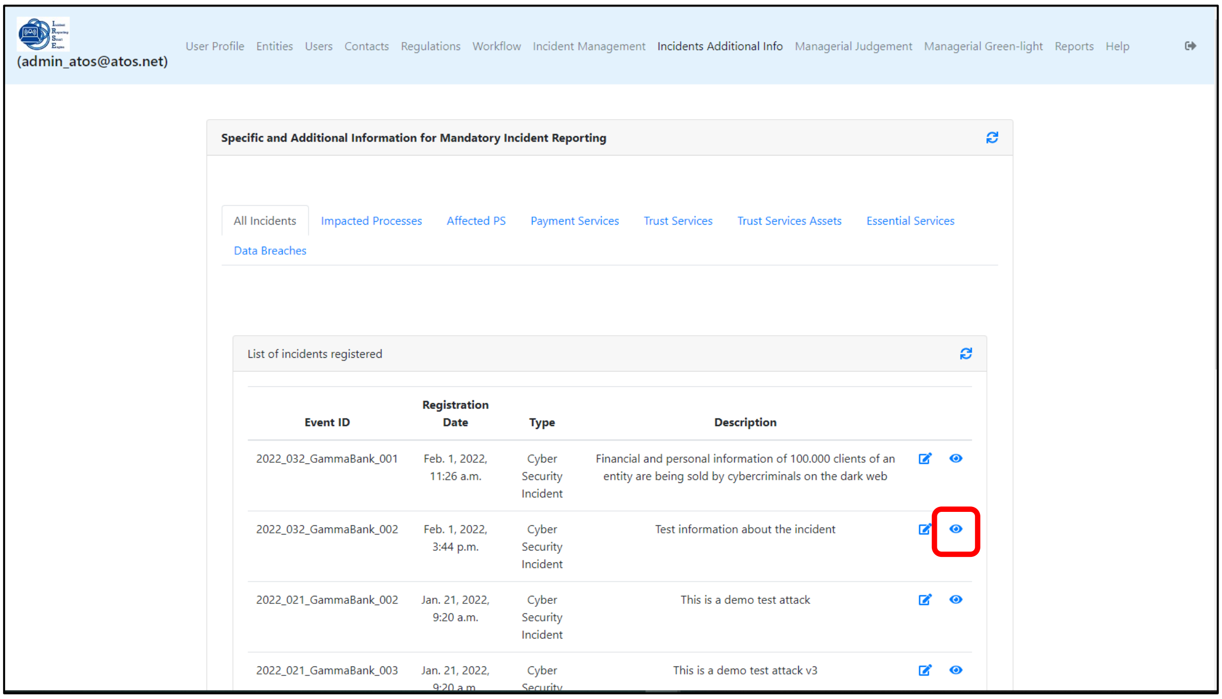
List of tasks (8 of 8)

Group	Task	Date	Assignee
IMT	Data Collection Closed after *7 minutes*	02/01/22 16:45	CS4EU Incident Management Team
IMT-ICLT	Data Enrichment Closed after *7 minutes*	02/01/22 16:52	CS4EU Incident Classification Team
ICLT	Incident Classification Closed after *8 minutes*	02/01/22 17:01	CS4EU Incident Classification Team
CONTROLLER	Managerial Judgement Closed after *a few seconds*	02/01/22 17:13	CS4EU Controller
IRT	Data Conversion Closed after *2 days*	02/01/22 17:14	CS4EU Incident Reporting Team
CONTROLLER	Green-light for Reporting Closed after *a few seconds*	02/03/22 15:52	CS4EU Controller
IRT	Reporting & Release Closed after *12 minutes*	02/03/22 15:52	CS4EU Incident Reporting Team
IMT-ICLT	Data Enrichment Started *2 minutes ago*	02/03/22 16:04	CS4EU Incident Classification Team

Figure 169. New Date Enrichment Task.

The cycle will be repeated to generate the Interim and Final reports depending on the regulations selected as active for the entity and the last phase configured.

14. **Security Event Lifecycle:** Under *Incidents Additional Info* menu, the *Security Event Lifecycle* of *All Incidents* can be consulted, Figure 170.



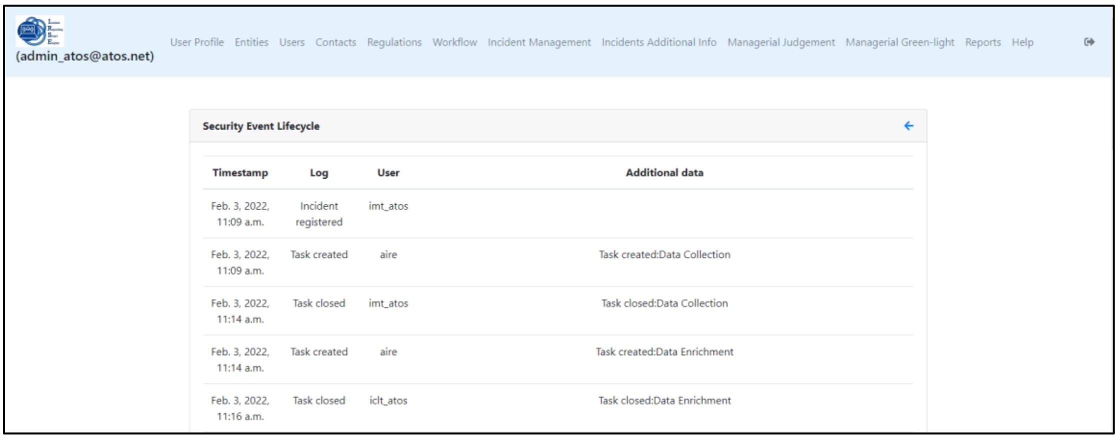
Specific and Additional Information for Mandatory Incident Reporting

List of incidents registered

Event ID	Registration Date	Type	Description
2022_032_GammaBank_001	Feb. 1, 2022, 11:26 a.m.	Cyber Security Incident	Financial and personal information of 100.000 clients of an entity are being sold by cybercriminals on the dark web
2022_032_GammaBank_002	Feb. 1, 2022, 3:44 p.m.	Cyber Security Incident	Test information about the incident
2022_021_GammaBank_002	Jan. 21, 2022, 9:20 a.m.	Cyber Security Incident	This is a demo test attack
2022_021_GammaBank_003	Jan. 21, 2022, 9:20 a.m.	Cyber Security	This is a demo test attack v3

Figure 170. Consult of Security Event Lifecycle.

This shows the log with timestamps for all events related with an incident, Figure 171.

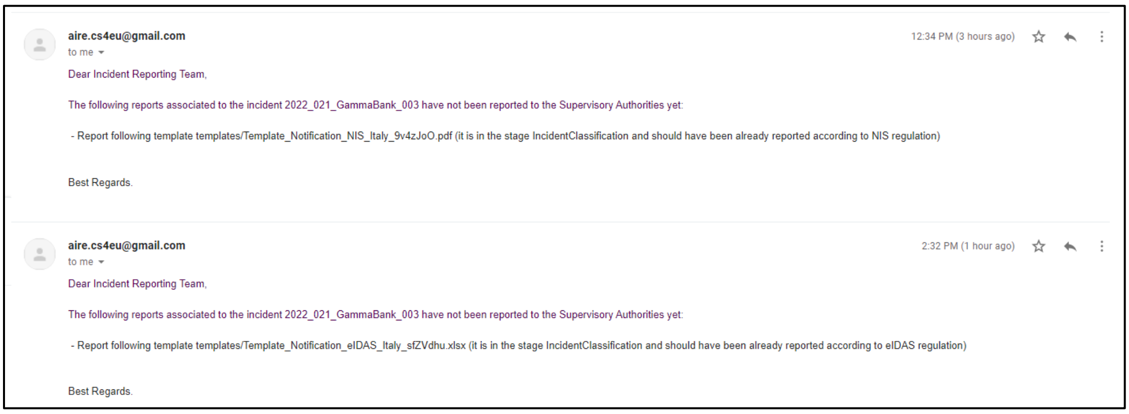


Security Event Lifecycle

Timestamp	Log	User	Additional data
Feb. 3, 2022, 11:09 a.m.	Incident registered	imt_atos	
Feb. 3, 2022, 11:09 a.m.	Task created	aire	Task created:Data Collection
Feb. 3, 2022, 11:14 a.m.	Task closed	imt_atos	Task closed:Data Collection
Feb. 3, 2022, 11:14 a.m.	Task created	aire	Task created:Data Enrichment
Feb. 3, 2022, 11:16 a.m.	Task closed	iclt_atos	Task closed:Data Enrichment

Figure 171. Security Event Lifecycle.

In case there is a delay in the reporting process and the reports have not been reported and released on the time configured for some regulations, a notification similar to the one shown in the Figure 172 will be sent to the email configured as Contact User in the incident template.



aire.cs4eu@gmail.com
to me

12:34 PM (3 hours ago)

Dear Incident Reporting Team,

The following reports associated to the incident 2022_021_GammaBank_003 have not been reported to the Supervisory Authorities yet:

- Report following template templates/Template_Notification_NIS_Italy_9v4zJoO.pdf (it is in the stage IncidentClassification and should have been already reported according to NIS regulation)

Best Regards.

aire.cs4eu@gmail.com
to me

2:32 PM (1 hour ago)

Dear Incident Reporting Team,

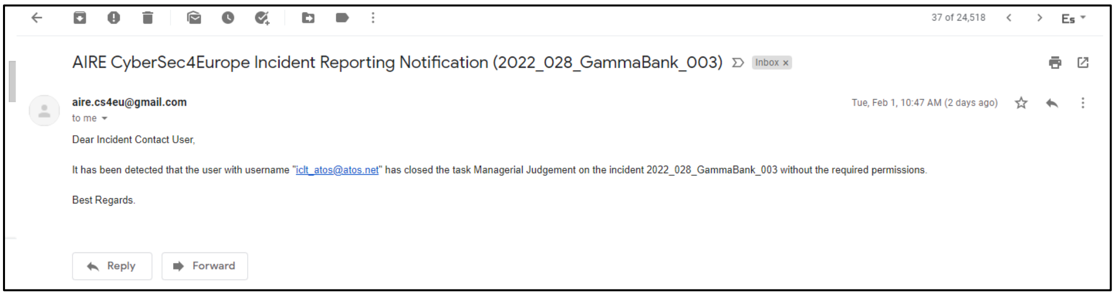
The following reports associated to the incident 2022_021_GammaBank_003 have not been reported to the Supervisory Authorities yet:

- Report following template templates/Template_Notification_eIDAS_Italy_sfZVdhu.xlsx (it is in the stage IncidentClassification and should have been already reported according to eIDAS regulation)

Best Regards.

Figure 172. Email to Contact User reminding of pending reports.

A notification also be sent to the Contact User in case some exception is detected regarding the Incident reporting workflow. For example, if a user without permissions is closing a task which is not assigned to that profile/role, Figure 173



AIRE CyberSec4Europe Incident Reporting Notification (2022_028_GammaBank_003)

aire.cs4eu@gmail.com
to me

Tue, Feb 1, 10:47 AM (2 days ago)

Dear Incident Contact User,

It has been detected that the user with username "iclt_atos@atos.net" has closed the task Managerial Judgement on the incident 2022_028_GammaBank_003 without the required permissions.

Best Regards.

Figure 173. Notification of closing task without permission.

I.IV.II INPUT METHODS

The process of incident management and reporting to authorities can be automated through the AIRE APIs, which allow starting, updating, and closing the enforcement processes. Furthermore, the incident management submodule, TheHive, can receive alerts from SIEMs within the system and IoCs from MISP instances, which contain relevant information about events occurred in other related companies.

I.IV.II.I REST API

Using the REST API, other systems can interact with AIRE's security incident reporting service, advising of finished tasks, or demanding the end of pending tasks [1]. Users can also consult security incident information and classify the incidents, which must be validated by managerial judgement. Furthermore, they can report to the competent authority. The action that a user can perform depends on its role and the workflow stage of the item. The **aire-workflow-enforcement** service supports the creation of new incidents and assignment of tasks to the different users, depending on their role. The API contains the following functions:

Table 3: aire-workflow-enforcement REST API

HTTP Method	URI	Description
POST	/aire/startProcess	Start AIRE workflow enforcement process when a new incident is registered.
POST	/aire/endProcess	End AIRE workflow enforcement process when a registered incident is closed.
POST	/aire/taskChangeNotification	Notify to trigger the next step in the Incident Reporting Workflow.
POST	/aire/checkWorkflowAuth	Receive a notification to check if a user has permissions to execute an action on an incident in the current workflow stage.
GET	/aire/managerial_judgement/{incidentId}	Get managerial judgement form for an incident.
POST	/aire/managerial_judgement	Submit managerial judgement.
GET	/aire/green_light/{incidentId}	Get green-light form for reporting for an incident.
POST	/aire/green_light	Submit green-light managerial judgement

The **aire-reports-generator service** transforms the information on security incidents to the different report templates. Then, they are sent to the Competent Authorities based on the regulations. The following table summarizes the API offered by the aire-reports-generator service:

Table 4. aire-reports-generator service REST API

HTTP Method	URI	Description
GET	/aire/generateReports/{incidentId}	Generate report templates for a specific incident.

The **aire-thehive-plugin** service is a middle layer that uncouples the incident management and response tool of organizations from the AIRE engine. It catches actions executed by users inside TheHive and calls the associated actions from AIRE engine, Furthermore, it supports a REST API endpoint to execute actions in TheHive or responders. Such as, checking the user authorization for an action or launching DataConversor Responder, which generates a report of the incident.

Table 5: aire-thehive-plugin service REST API

HTTP Method	URI	Description
POST	/aire/webhook-collector	TheHive Webhook Collector
POST	/aire/executeIR-action	Execute action requests on TheHive

POST	/aire/checkAuthorization	Check authorization for a TheHive Responder execution
GET	/aire/generateReport/{caseId}	Generate report templates for a specific incident.

TheHive features its APIs[11] to control the distinct parts: Organizations, Alerts, Cases, Tasks, etc. This documentation focuses on APIs that are used in automatic mode by other components, such as create new alerts, update a case, or close a task. For this reason, the list of functions is not exhaustive.

- Cases:

Table 6: The Hive REST API for Cases

HTTP Method	URI	Description
POST	/api/case	Create a Case
PATCH	/api/case/{id}	Update a Case
DELETE	/api/case/{id}?force=1	Permanently delete a Case
POST	/api/v0/case/{id1}/_merge/{id2}	Merge two Cases in a single Case
POST	/api/v0/query	List alerts merged in a Case; case ID passed in Request Body

- Alerts:

Table 7: The Hive REST API for Alerts

HTTP Method	URI	Description
POST	/api/v1/query?name=alerts	List of Alerts
POST	/api/alert	Create an Alert
DELETE	/api/alert/{id}?force=1	Delete an Alert
PATCH	/api/alert/{id}	Update an Alert
POST	/api/alert/{id1}/merge/{id2}	Merge an Alert into an existing Case
POST	/api/alert/{id}/createCase	Promote an Alert as a new Case

- Tasks:

Table 8: The Hive REST API for Tasks

HTTP Method	URI	Description
POST	/api/v0/query	List Tasks of a case; case ID passed in Request Body
POST	/api/case/{id}task	Create a Task
PATCH	/api/case/task/{id}	Update a Task
GET	/api/case/task/{id}	Get Task of a case
POST	/api/v0/query	List all waiting Tasks

[11] http://docs.thehive-project.org/thehive/api/

I.IV.II.II OTHER APIs

TheHive can receive security events related to the current infrastructure from other systems, for example, alerts from Wazuh SIEM or IoC from MISP instances. It registers the security events and displays them in a dashboard, where users can monitor the system and transform the alerts into incidents with a button on the view.

On one hand, TheHive can receive the alerts generated and sent by Wazuh to a Kafka broker[12]. Wazuh must send the alerts to the topic *wazuh-alerts*. Then, these alerts are transformed from wazuh format to TheHive alert format and registered in its API.

On the other hand, TheHive can monitor the IoC from MISP instances and shows them in the alert dashboard. To enable this feature, it is necessary to configure the tool, adding in application.config file. It queries the events from the *misp.url.instance* every *1 hour* for the tags *SUNRISE1* and *SUNRISE2*, and then, it creates alarms for the events, which are displayed in the alarm dashboard.

```
misp {
 servers: [
  {
   name = "MISP-NAME"
   url = "https://misp.url.instance"
   auth {
    type = key
    key = "XXXXXX"
   }
   caseTemplate = "Incident Report"
   tags = ["SUNRISE1", "SUNRISE2"]
   #filters
   max-age = 7 days
   max-attributes = 1000
   max-size = 1 MiB
   includedTheHiveOrganisations = ["*"]
   excludedTheHiveOrganisations = []
   #indicate if the tags of the case should be exported to MISP event (default: false)
   #exportCaseTags = True
  }
 ]
 # Interval between consecutive MISP event imports in hours(h)or
 # minutes(m).
 interval: 1 hour
}
```

[12] https://kafka.apache.org/