Horizon 2020
European Union Funding
for Research & Innovation

Deliverable D3.2
CSIRT model dedicated to railway, final release

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:	M11 (end of October 2020)
Actual submission date:	30-10-2020
Responsible/Author:	Antonio López / Enrique Ruiz, Hit Rail BV
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	01/10/2020	First D3.2 draft after D3.1 feedback review
0.2	22/10/2020	D3.2 ready for interim review
1.0	29/10/2020	D3.2 ready for submission after internal review
2.0	10/12/2020	D3.2 resubmission addressing feedback from the Project Officer and Advisory Board

Report contributors		
Name	Beneficiary Short Name	Details of contribution
Frank Wilson	Hit Rail	Deliverable leader, all sections
Antonio López	Hit Rail	Deliverable leader, all sections
Enrique Ruiz	Hit Rail	Inputs and feedback on all sections
Alejandro Prada	Tree Technology	Inputs on model and platform; feedback on all sections
Marcos Sacristan	Tree Technology	Inputs on model and platform; feedback on all sections
Christine Hassoun	UIC	Review
Jean-Michel Evanghelou	UIC	Review
Adriá Farré	Ardanuy Ingenieria	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 provides a design of the **4SECURail output** on the **CSIRT model for the European railway sector.** The **CHIRP4Rail concept** – Collaborative tHreat Intelligence Platform for Rail – aims to coordinate the different Rail Operators of Essential Services' (OES) security teams in sharing cross border threat/incident information. In such a scenario, the model must clearly determine what can be shared, with whom, under what circumstances, and how (e.g. automated sharing of incident declaration).

The work presented in this report is extensively addressing all activities developed towards the achievement of the CSIRT model dedicated to the European railway sector (CHIRP4Rail). This includes firstly a detailed analysis of the operating context and related initiatives, and desk research on existing models and interactive research with surveys and interviews to the key stakeholders; secondly, the conceptualisation of the CHIRP4Rail concept; and finally, the definition and design of the CHIRP4Rail model and initial outline of the future CHIRP4Rail collaborative platform prototype fulfilling the specific needs of the railway sector.

An in-depth analysis on the relevant context analysed the key initiatives and stakeholders (especially relevant is the role of the ER-ISAC and the UIC; and the related Shift2Rail complementary initiative X2RAIL-3) as well as the position of 4SECURail in relation to them, thus sets the basis for this work.

Then, building on that context, the research leading to the definition of the 4SECURail CSIRT model was addressed following a twofold research approach:

- through desk research to analyse in detail and identify the connections and synergies with the relevant railway contexts (situation analysis); and
- through interactive research conducted using both surveys and interviews with the key stakeholders, including Infrastructure Managers (IM), Railway Undertakings (RU), Digital Service Providers (DSP) and Suppliers (as defined by the NIS Directive); and high-level stakeholders like the European Commission, and relevant agencies like ERA and ENISA.

The joint analysis resulted on the following main conclusions for the CHIRP4Rail concept model and functionality statement:

- The railway security stakeholders understanding of the **"CSIRT" extends beyond purely response to 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 intelligence building and information sharing 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.

Based on the above conclusions and the functionality statement, the 4SECURail CSIRT model has been elaborated. This model has been developed in this deliverable as follows:

Firstly, and most importantly, as the main goal of this report, the CHIRP4Rail Model was addressed from a threefold perspective, developing the functional, organisational and technical aspects of the proposed model:

- The **functional model** establishes at 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); and the CHIRP4Rail Platform Operator (CPO).
    - WHAT (the flows): Cyber Threats relevant for Rail (incidents and/or vulnerabilities) building Actionable Intelligence (bulletins, prevention, response).
    - HOW (the tools): a platform interconnecting RST's tool, enabling voluntary and anonymous sharing of information and guaranteeing cyber secure communications.
- The **organisational model** defines the organisation and process at three levels:
    - Roles and functions for each of the actors involved,
    - The management structure and
    - The detailed data and workflows, identifying the inputs (information sources), process (threat analysis and intelligence building), and outputs (results for information sharing).
- The **technical model** defines the data model, based on the MISP data standard, and defining the use of the core and attributes, tags, taxonomies and access control.

Secondly, in the final part of the report, an early outline of the key functional and technical aspects of the CSIRT platform (CHIRP4Rail) is presented as an anticipation, to be elaborated in further tasks.

This work presents a final version of the model after interaction and validation through workshops and interaction with key stakeholders and building on the previous deliverable D3.1. Our work will be further elaborated in the consequent task towards the 4SECURail CSIRT collaborative platform prototype supporting this model, which will be released in deliverable D3.3.

2 Abbreviations and Acronyms

2.1 Glossary

Abbreviation / Acronyms	Description
APT	Advanced Persistent Threat
CERT	Computer Emergency Response Team
CHIRP4Rail	Collaborative tHreat Intelligence for Rail Platform
CI	Critical Infrastructure
CISO	Chief Information Security Officer
COLA	Collaboration Agreement
CPO	CHIRP4Rail Platform Operator
CSIRT	Computer Security Incident Response Team
CTI	Cyber Threat Intelligence
CTP	Cyber Threat Provider
DOS	Denial of Service (attack type)
DSP	Digital Service Provider
ECG	European Cooperation Group (deals with NIS transposition)
ECN	European CSIRTs Network (supports / coordinates CSIRTs)
ER-ISAC	European Railway Information Sharing and Analysis Centre
GDPR	General Data Protection Regulation (applicable since May 25, 2018)
ICS	Industrials Control Systems
IM	Infrastructure Manager
ISO	Information Security Officer
ITS	Intelligent Transport Systems
NIS	Network and Information Security Directive of the EU
OES	Operator of Essential Services
RST	Rail Security Team
RU	Railway Undertakings
SCP	Security Contact Point
SERA	Single European Rail Area
SOC	Security Operations Centre

2.2 Key CSIRT definitions

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

Term	Definition
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
MALWARE	Software intentionally causing damage
RANSOMWARE	Malware linked to a ransom demand (payment or damage)
SUPPLIER	A company or organization that provides something needed such as a product or service
THREAT	Any circumstance or event with the potential to adversely impact an asset through unauthorized 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
APT	An advanced persistent threat (APT) is a stealthy computer network threat actor, typically a nation state or state-sponsored group, which gains unauthorized 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.

3 Background

3.1 Position of this document within 4SECURail Project

The present document constitutes the Deliverable D3.2 "*CSIRT model dedicated to railway, final release*" in the framework of the 4SECURail project, Grant Agreement number 881775 — IP/ITD/CCA — IP2, task 3.1 "*CSIRT Model*" 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.

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

4 Objective/Aim

4.1 Specific objectives of this document

The work stream 2 specific objectives within 4SECURail are:

- To define stakeholder requirements for a European Rail CSIRT collaborative activity, and to co-design with them a rail CSIRT model for open consultation.
- 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.
- To identify relevant platforms to support CSIRT collaboration and, based on requirements and CSIRT model, specify and adapt to meet CSIRT needs.
- To test and update the CSIRT collaborative environment so as to ensure meeting user needs.

This document has been prepared to especially address Objective 1, therefore **the main goal is to design a first version of the 4SECURail CSIRT model for the European railway sector:** the **CHIRP4Rail concept** – 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 concept). 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).

This will further support the other objectives in consequent tasks and deliverables:

- a revised version of this model after interaction and validation through workshop with key stakeholders will be documented in deliverable D3.2; and
- the 4SECURail CSIRT platform prototype supporting this model will be released in deliverable D3.3.

4.2 Collaboration with Complementary Activity

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

- “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*;”
- “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, then investigate how a 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 signed by X2RAIL-3 and 4SECURail (COLA), both projects have carried out several collaboration meetings (see section 7.4.2) to guarantee that the output of 4SECURail project would be used by X2RAIL-3 to define the challenges and recommendation for a railway specific CSIRT/ISAC.

In the case of **A**, above, 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 has been addressed through the following activities defining the structure of the document:

- **Section 5** provides an in-depth analysis about the relevant context to this work. Such section analyses the key initiatives and stakeholders as well as the position of 4SECURail in relation to them, thus sets the basis for this work at the time of this report.
- Then, building on that context, the research leading to the definition of the 4SECURail CSIRT model has been addressed following a twofold approach:
    - through desk research to identify and describe the relevant railway contexts (situation analysis). The findings have been documented in **Section 6**.
    - in parallel to that, interactive research have been conducted through both surveys and interviews with key stakeholders: online survey with key rail security stakeholders within Infrastructure Managers (IM), Railway Undertakings (RU), Digital Service Providers (DSP) and Suppliers as defined by the NIS Directive **[NIS]**; and interviews with high level stakeholders, the European Commission, and relevant agencies. The findings have been included in **section 7**.

  The joint analysis bringing together both research paths have finally been consolidated resulting on the main conclusions as compiled in **section 8**, in the form of the requirements giving place to the functionality statement.

- The 4SECURail CSIRT model has then been elaborated based on and building on such statement. This model has been developed in this document as follows:
    - Firstly, **section 9** addresses the main goal of D3.1 by outlining the CSIRT model from a threefold perspective, developing the functional, organisational and technical aspects of the proposed model.
    - Secondly, **section 10** adds to that by developing an early outline of the key functional and technical aspects of the CSIRT platform, to be elaborated in further tasks.

  While the main goal of this deliverable is the model as defined in section 9, section 10 takes the opportunity to advance on such basis for the work on the CSIRT platform to be further elaborated and implemented by the following tasks, in order to provide a more holistic vision of the CSIRT work stream and constituting the main output of the present deliverable, as input for the further research activities in 4SECURail.

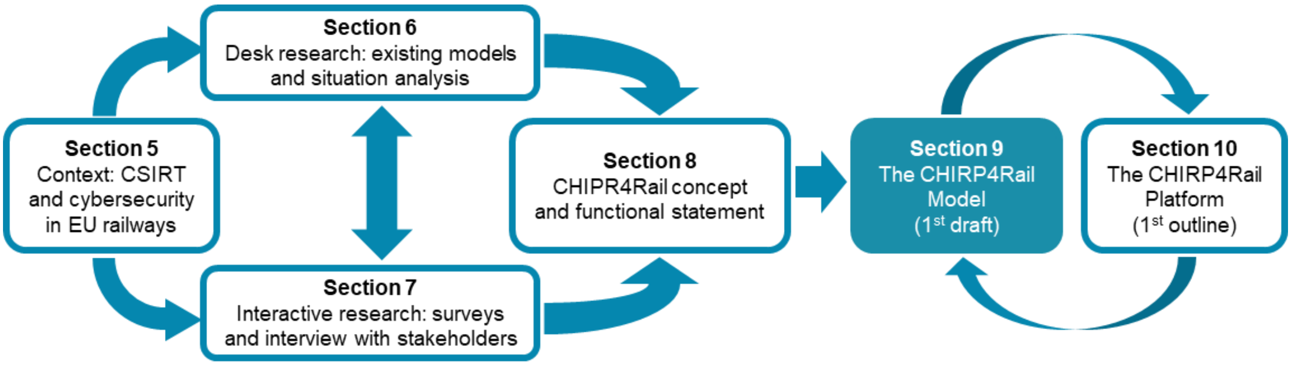

Section 6
Desk research: existing models and situation analysis
Section 5
Context: CSIRT and cybersecurity in EU railways
Section 8
CHIPR4Rail concept and functional statement
Section 9
The CHIRP4Rail Model (1st draft)
Section 10
The CHIRP4Rail Platform (1st outline)
Section 7
Interactive research: surveys and interview with stakeholders

Figure 1: Structure of the deliverable D3.2

The final sections of the document provide the conclusions (section 11), references (section 12) and appendices (section 13).

5 Context: Incident Report and Information Sharing in the EU railway community

5.1 EU Railway Collaboration for Cyber Security

The Shift2Rail open call for support to implementation of CSIRT to the railway sector emphasises the need for Railway collaboration, evident also in its various discussions and collaborations, as well as within the industry and its recent ER-ISAC. The basis of need is summarised here for reference.

5.1.1 Single European Railway Area: Need for Shared Security Response

Railways are a particularly strategic area of European Shared Infrastructure and are one of the most extensive cross-border and pan-European "essential services". Railways are conjoined by their physical and IT systems to operate the Single European Railway Area **[SERA]**. Within the SERA model, widely implemented by European railways, European economic activity benefits from open access operations on railway lines by companies other than those that own those railway lines. Such "open access" operations require not only the "lines" but also their supporting infrastructure (train signalling, routing, messaging for freight management, etc.). This means that all European railway infrastructure, both physical and IT, can be conceived as a single network. Within each country the different rail operators are interconnected (physical infrastructure and IT) to ensure management and coordination of passenger and freight services – inter-organisational collaboration. Between countries this is also true, and so SERA depends on cross-border inter-organisational collaboration to ensure effective and safe operation of European railway business.

The rise in cybercrime targeting Industrials Control Systems (ICS) converges with this development of Intelligent Transport Systems (ITS). Since these ITSs are not isolated, the increasing level of integration among transport systems brings increasing needs for cyber-security coordination between Operators of Essential Services (OES[2]). European railways are both OES and "Critical Infrastructures" (CI), where CI is the body of systems, networks and assets whose continued operation is required to ensure the security of a given country, its economy, and public safety.

Each Rail OES is *potentially open to threats* originating both within their "own" systems, and also via other access opportunities present in the integrated SERA.

Within a single organisation, *identification of threats and response to threats* can be more easily coordinated by an internal security team (e.g. an internal CSIRT), but between inter-connected and coordinated business entities, the "response" aspects will have to be coordinated between organisations – hence the potential benefit of a European Railway CSIRT involving security teams from multiple Rail OES.

5.1.2 EU Policy and Legal Context for Cyber Security: The NIS Directive

Under the EU Directive on the security of Network and Information Systems **[NIS]**, Operators of Essential Services (OES) are required to take appropriate and proportionate security measures to identify and manage risks to networks and information systems. They are also required to *notify serious incidents to the national competent authority*. In the case of EU Railway OES, their IT systems

[2] OES – Operators of Essential Services as defined by the **[NIS]** Directive

are interconnected in various ways, and the threats they face are *in common*, and so a *joint affirmative action is required* to ensure interconnected European railways can support each other, share knowledge, and *share response capacity* for common European benefit. Such actions can have multiple forms (see later).

NIS demands that Member State Governments, and OES such as Railways, take steps to ensure Cyber Security for European Society and Economy. The Member States National Frameworks and Strategies are supported by the European Cooperation Group (ECG[3]) to conjoin efforts across Europe concerning transposition of NIS into law. The Member State CSIRTs are supported by the European CSIRTS Network (ECN[4]) for coordination of shared response (see later). However, the European level, and National level, cannot be fully effective without parallel actions by Railway OES due to their "connectedness".

Railways as "OES" are mandated to report all Cyber Security incidents to their National cyber security teams. However, since a threat at one railway or one of its systems is potentially a threat at conjoined railways (via shared infrastructure, messaging, etc., or via common enemies promoting malicious or criminal actions), a pan-European collaboration is clearly demanded. This is further complicated by the dependence of Railway OES on Digital Service Providers (DSPs) who effectively deploy and manage systems and services on behalf of the National and pan-European Railway infrastructure of SERA.

The relationships subsumed under NIS are therefore somewhat hierarchic as shown in Figure 2.

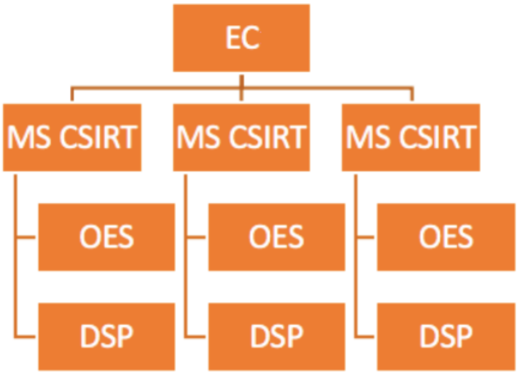


Figure 2: NIS Reporting Hierarchy

What is currently missing for Rail is the *horizontal coordination at the level of Rail OES and their essential DSPs*. This would most naturally be done via the security teams of OES who, as in the case of the ER-ISAC, would be the natural constituency for a European Rail CSIRT.

Some examples of horizontal security collaborations are in evidence and are discussed later.

[3] Cyber Security European Cooperation Group on NIS / Cyber Security: tasks defined in Article 11 of the NIS Directive. https://ec.europa.eu/digital-single-market/en/nis-cooperation-group

[4] European CSIRTs Network - https://www.enisa.europa.eu/topics/csirts-in-europe/csirts-network

5.1.3 EU Policy and Legal Context for Cyber Security: The Cybersecurity Act

On June 2019, the European Parliament and the Council of the European Union adopted the European "Cybersecurity Act" (CSA) Regulation. The Cybersecurity Act:

- Reinforce the new permanent mandate of ENISA to assist Member States in preventing and responding to cyber-attacks and
- Stablish the European cybersecurity certification framework to ensure Information and communication technology (ICT) products, services and procedures are cyber secure.

Most of the CSA's provisions support or advance provisions of the NIS Directive. However, the Act:

- Establishes an EU cybersecurity certification framework for ICT products, services, and processes.
- Requires Member States to designate one or more national cybersecurity certification authorities.
- Establishes assessment bodies to determine conformity with the Act.
- Requires Member States to determine penalties for certification violations and infringement of European cybersecurity certification schemes.

The opening clauses of the CSA (whereas 2) provide an extensive justification of the need to develop such as certification framework. ICT products and services "are not sufficiently built-in by design, leading to insufficient cybersecurity". The Act also notes that "the limited use of certification leads to individual, organizational and business users having insufficient information about the cybersecurity features of ICT products, ICT services, and ICT processes, which undermines trust in digital solutions."

In this context, any rail digital service providers, train builders, rail equipment suppliers or commercial cybersecurity threat intelligence providers offering ICT products, services, or processes within the EU to rail OES (IMs and RUs), are affected by the Cybersecurity Act and should begin monitoring the ENISA and EU websites for updates on EU cybersecurity certification schemes.

Furthermore, the CSA emphasises (whereas 92) that "it could be necessary in the future to impose specific cybersecurity requirements and make the certification thereof mandatory for certain ICT products, ICT services or ICT processes, in order to improve the level of cybersecurity in the Union". The CSA also points out that "The efficiency of the European cybersecurity certification schemes, and whether specific schemes should be made mandatory, should be assessed in light of the cybersecurity-related legislation of the Union, in particular Directive (EU) 2016/1148, taking into consideration the security of the network and information systems used by operators of essential services" (OES).

Therefore, the CSA will play, in the coming years, a key role in legally reinforcing the provisions set out in the NIS Directive for the operators of essential services (OES) to take appropriate and proportionate security measures to identify and manage risks to networks and information systems.

5.2 EU and ENISA Support for Cyber Security Networking

In addition to the preceding considerations of EU Support, both from EC and ENISA, there are numerous related initiatives designed to encourage and support Member States CSIRTs in different ways. Some key examples are considered here, and others can be found at the comprehensive **[ENISA]** website.

5.2.1 MeliCERTes: EU and ENISA Platform for CSIRT Collaboration

The MeliCERTes facility was developed under an open call in 2015, and provides facilities secure communications, incident and threat management, and artefact analysis using open source tools. MeliCERTes is hosted by ENISA and was developed and is maintained by and for Computer Security Incident Response Teams (CSIRTs) to support the CSIRTs Network under the NIS Directive. It facilitates cross-border co-operation including data exchange between 2 or more CSIRTs based on trust. In 2018 the Commission called for a manager to maintain and further develop MeliCERTes in cooperation with ENISA and the participating CSIRTs, including addition of new tools and functions (three-year contract).

The precise nature of MeliCERTes is not publicly known in detail, but its general aim and form are both interesting and relevant to 4SECURail, since they emphasise collaboration of CSIRTs (at National level, and together at EU level) in collectively addressing cyber security incidents, threat management, and artefact analysis.

Key tasks of interest to the European Rail CSIRT study include:

- *support operation of the platform in conjunction with ENISA (hardware and Helpdesk).*
- *maintain the software code (emphasised as open source), including bug fixing, vulnerability assessment, testing, and managing updates.*
- *further develop the platform to meet emerging needs of CSIRTs.*
- *extend the platform as a repository of open source tools developed by CSIRTs.*
- *deliver a sustainability strategy for the platform and its services.*

Although this platform supports national level CSIRTs in the context of the CSIRT Network, as defined under the NIS directive, its general form, and specific features, are clearly worthy of consideration in the context of 4SECURail and the Shift2Rail objectives concerning a European Rail CSIRT collaboration platform.

5.2.2 CEF Service Platform for ISACs

The European Commission, under a call in 2018, established a project to deliver a “service platform and cooperation mechanism for Information Sharing and Analysis Centres (ISACs)”. The title of the call was “Connecting Europe Facility (CEF): Cybersecurity digital service infrastructure establishment of a core service platform cooperation mechanism for Information Sharing and Analysis Centres (ISACs) facilities manager” (3-year project).

This project planned to support formation and delivery of specific sectoral ISACs, including “transport”. Support to be delivered included:

- *logistics (meetings, events, etc.).*

- *advice; analysis (e.g. cyber threat intelligence).*
- *IT platform-based support, and "subscription-based services" (undefined).*

The call emphasised ISAC as voluntary information sharing between trusted stakeholders, and improvement of "cybersecurity preparedness, situational awareness and coordinated vulnerability disclosure". This call did not emphasise the "response" phase or collaboration in response but does provide some general considerations of relevance to the 4SECURail task on providing a model and platform enabling collaboration between CSIRTs (as response entities).

5.2.3 European Aviation ISAC

The European ISAC in Aviation sector was initiated in February 2017 by the private sector in cooperation with ENISA and EASA[5]. The EA-ISAC will contribute to the safety of air travellers and the public by assisting in the establishment of acceptable levels of protection of its infrastructures: from design to decommissioning of aircraft; Communication, Navigation and Surveillance systems; and other critical services necessary to the safety of flight.

5.2.4 ER-ISAC

The ER-ISAC development was initiated at the security conference organised by Hit Rail in 2017, where a statement of understanding[6] was agreed by numerous RU and IM representatives. This was followed by discussions with DG-CNECT and DG-MOVE, and the introduction of Infrabel (the national Belgium railway IM) as an initial coordinator.

The ER-ISAC has since then developed its Terms of Reference (TOR), established its co-chairs and initial membership, and is strongly supported in its development by ENISA who provides experience and support. Planning for specialist groups, activities and services to members is well under way, but coordination of "response" is not included in the TOR or immediate plans. While this indicates an opportunity for a CSIRT collaboration around response, it should be recognised that the community of interest is the same, and so the relationship with ISAC activities should be carefully considered.

5.3 CSIRT and relation to ER-ISAC

5.3.1 CSIRT

A typical definition of a CSIRT holds that "A Computer Security Incident Response Team (CSIRT) is an organizational unit (which may be virtual) or a capability that provides services and support to a defined constituency for *preventing, detecting, handling, and responding to computer security incidents*, in accordance with its mission. A properly deployed CSIRT has a clear mandate, a governance model, a tailored services framework, technologies and processes to provide, measure and continuously improve defined services. "(FIRST CSIRT Framework v2.0 2019 [**FIRST_CSIRT**])

A similar definition is provided by ENISA, who holds that "A CSIRT is a team of IT security experts whose ***main*** business is to respond to computer security incidents. It provides the services to handle

[5] https://www.easa.europa.eu/newsroom-and-events/press-releases/easa-cooperate-cert-eu-cybersecurity
[6] https://www.hitrail.com/events/cyber-security-for-railways-conference-2017

them and support their constituents to recover from breaches" (ENISA CSIRT Setting-up Guide 2006 [ENISA_CSIRT, 2006]).

While the ENISA definition emphasises "response", the FIRST definition includes both "prevention" and "response", but both do follow very similar structures and functionality.

CSIRTs generally are often defined as internal to a specific organisation, yet the EU Member State CSIRTs are at national level, and each represents many government departments, and coordinates across a country to support multiple stakeholders under ECN coordination.

A Rail CSIRT would have to operate across the Rail transport sector (EU Rail – SERA), and would need a coordinated response approach, as well as possible prevention support. This latter aspect may be delivered by the ER-ISAC or by the CSIRT itself.

5.3.2 ER-ISAC

There is currently a European Rail ISAC (ER-ISAC - *Information Sharing and Analysis Centre*), which is not yet[7] fully established as a "centre" but a *network of collaborating Rail security experts*. This was initially established in 2019, following a Hit Rail conference in 2017 and several follow-up actions with DG-CNECT, ENISA, and Infrabel. The ER-ISAC has already progressed in initiating actions designed to help members improve Cyber Security capacity through education, sharing, preparatory / preventive actions, etc. It has also made clear that it will not, in the immediate future, go as far as implementing a "hot phase" ***response*** capacity such as is expected of a CSIRT.

While this difference between the CSIRT and ISAC are clear (preparation versus response, with some necessary overlap), it is necessary to recognise the parallel ER-ISAC activity to also identify any potential replication / overlap of actions, and to capitalise on collaboration and coordination where any such opportunity exists. Furthermore, key members of the ER- ISAC are the very CISOs and security teams that an EU Rail CSIRT would engage.

In future, there could be other cybersecurity activities outside the classical ISAC model that the ER-ISAC could consider. The ER-ISAC could formalise its collaboration by starting a joint rail EU-CSIRT in order to combine resources, which can help to professionalise the ER-ISAC and build its capabilities further (e.g.: automated sharing and acquisition of information, analysis and automated processing of threat information, etc.).

The classical ISAC model is intended as a precursor to the next steps, although of course there are other ways to achieve the same objective: an EU-CSIRT. Applying whatever suits, the rail EU-ISAC best should always be the main priority.

5.3.2.1 ER-ISAC Situation and Relation to Other Initiatives

In December 2019 the proceedings of the ER-ISAC second general assembly included a range of presentations and debates that brought various features of interest to our CSIRT study:

[7] Formulation of a physical "centre" for the ER-ISAC is proposed and under discussion as of December 2019.

ENISA on NIS Directive and Subsequent Actions

ENISA indicated the scope of the NIS directive, emphasising EU-level cooperation for improved cyber security. The network of National CSIRTs (emergency teams) is operational and the manner of coordination should be a key item of interest for 4SECURail since coordination of separate Railway security teams may be required of an ER-CSIRT. Notification of important cyber security incidents to national competent authorities is mandatory under NIS (vertical reporting), but any such incidents are of interest across the Rail sector (horizontal reporting requires a coordinated CSIRT approach). The support for "horizontal" action is evident in ENISA support activities, and further emphasised by Commission recommendations[8].

ENISA review of rail stakeholders (ongoing study to be completed in 2020) identifies, in addition to operators of essential services (OES) their digital service providers (DSPs), delivery chains, and other supporting activities which are part of the larger network of cybersecurity dependencies. This survey identifies "essential services" specifically as:

- Operate traffic on network
- Security of passengers and goods
- Maintain railway infrastructure and trains
- Plan operations and book resources
- Carry goods and passengers
- Provide "operations" information to passengers and customers
- Manage billing and finance
- Sell and distribute tickets

These essential services are therefore primary cybersecurity concerns for an ER-CSIRT.

ER-ISAC Coordination, Facilitator and Platforms

The ER-ISAC has decided[9] to place physical presence and coordination of the ER-ISAC within UIC, to adopt a "facilitator" 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. The last of these might cover some of the focus of the proposed CSIRT platform, but the precise intention is not yet known (apart from stating "Propagation method, assets impacted, confidentiality on causes, ...") and should be further investigated.

European ISAC Cooperation Group

Four European ISACs have agreed to collaborate to improve understanding and to share experience (Finance, Energy, Aviation and Railway). The first meeting[10] was held in October 2019, and there are plans to add ISACs in Telecom and Maritime.

[8] Recommendation on cybersecurity in Energy sector also mentions comparable needs in the transport sector: https://ec.europa.eu/energy/sites/ener/files/swd2019_1240_final.pdf

[9] ER-ISAC Facilitation: "ER-ISAC Facilitator.pdf" December 2019. ER ISAC Actions and Coordination: "ER-ISAC Note for information UIC.pdf", December 2019.

[10] Inter-ISAC first joint meeting: https://www.enisa.europa.eu/news/enisa-news/enisa-hosts-the-first-inter-eu-isac-meeting

X2RAIL-3 activity: CSIRT concept (DB Netz)

The purpose of the Shift2Rail initiative (X2RAIL-3 – CSIRT Concept) was not to build a single European CSIRT but rather define common criteria for its implementation and setup. This work was planned for completion in late 2020 and is already linked to 4SECURail by means of a Collaboration Agreement (COLA).

European Electricity ISAC (EE-ISAC)

The presentation from **[EE-ISAC, 2019]** shows that it operates as a community-of-communities, each being a grouping of stakeholders on cyber security and other topics. Within this they do include a community addressing "Enhancing quick response" in relation to cyber security, and so demonstrate inclusion of CSIRT-type activity as part of an ISAC. Other actions are similar to the ER-ISAC and emphasise sharing and collective learning around topics such as Vulnerabilities, Threat/Risk Analysis, Types of Incidents, Lessons/best practice, Alerts and Notifications, Standards, Relevant Research (esp. H2020). Future collaborations include a European Network of ISACs, demonstrating openness to sharing and learning for strength. MISP platform is already being used for threat sharing. A general sharing platform is powered by BroadVision, and permits sharing of documents, posts and chat among members and external peers. The ER-ISAC is using EE-ISAC as a reference for future actions.

ADIF Increase of Cyber Security Capacity

The presentation of **[ADIF, 2019]** showed emphasis on increased preparedness and prevention, as well as increased response and recovery planning. This latter action shows CSIRT-type features and is made part of an Information Security Management Systems (ISMS) consistent with / aligned with ISO 27001, ISO 27035 and ISO 27036. Acquisition of additional services and capabilities is emphasised, especially around detection and response, with an open question on whether future advances will involve self-implementation or acquisition from third parties (DSP and/or collaboration with other railways).

TRAFIKVERKET – Swedish Rail CSIRT Action

Trafikverket presented some challenges arising from Intelligent Transport Systems (ITS), and showed the complexity of interconnected concepts (thousands of km of rail track and associated signalling and control systems; huge number of points locations; hundreds of stations linked to information and control systems; thousands of bridges and road/railway crossing points; linkage to numerous ferry lines; etc.). Their "Cyber Centre" contains:

- Monitoring platforms
- Cyber Security Operation Centre (CSOC)
- Computer Emergency Response Team (CERT/CSIRT)

Any significant incidents detected by the CSOC Security Information and Event Management (SIEM) are escalated to the CERT for Incident Response, showing that formalised processes within Railway security teams do provide opportunities to share at ER-CSIRT level (either manually or automatically).

The CERT also conducts Penetration testing, Vulnerability Scanning, Security reviews, Threat hunting, Threat and vulnerability management, etc. and so covers more than pure response.

5.3.3 UIC

UIC is the worldwide organisation for international cooperation among railways and promotion of rail transport at a global level. Founded in 1922, it currently gathers more than 200 members on all 5 continents, among them railways, rail operators, infrastructure managers, etc. The mission of the association is to promote rail transport at world level with the objective of optimally meeting current and future challenges of mobility and sustainable development.

UIC maintains close cooperation links with all actors in the rail transport domain right around the world, including manufacturers, railway associations, public authorities and stakeholders in other domains and sectors whose experiences may be beneficial to rail development. The UIC's main tasks include understanding the business needs of the rail community, developing programmes of innovation to identify solutions to those needs and preparing and publishing a series of documents known as IRS that facilitate the implementation of the innovative solutions.

Beyond the role of facilitator for ER-ISAC, UIC, as a complement, is developing a new "Cybersecurity Solutions Platform", whose objective is to identify and categorize concrete industrial solutions to prevent railway critical networks form Cybersecurity threats. This initiative includes all the major European railways companies and will be developed in collaboration with manufacturers and suppliers specialized in Cybersecurity solutions.

Moreover, **UIC ARGUS** working group has developed two years ago guidelines for railways to support the rail industry in reducing its vulnerability to cyber-attacks.

5.4 Initial Requirements for a Rail CSIRT

Based on the preceding analysis, we identify some general requirements evident in ISAC discussions that help to scope the potential EU Rail CSIRT Model:

General requirements for ER-CSIRT functions (identified in ER-ISAC discussions)
• Collaboration in support for cyber security response. • Sharing of threat intelligence concerning new incidents, known threats, new threats, established mitigation strategies, new mitigation measures. • Team for handling collaborative response and supporting recovery. • Sharing "NIS notifications" horizontality among rail stakeholders. • Engagement of relevant digital service providers (DSPs) in collaborative response. • Ensure all "essential services" are addressed (as defined by ENISA ongoing study): o traffic operation o carried passenger and freight security o railway infrastructure and trains maintenance o "operations information" provision to customers o ticketing o billing and finance • Identify methods to enhance quick response.

- Manual or automatic sharing mechanisms, considering standards.
- Shared services where required (help your neighbour):
    - vulnerability scanning
    - security reviews
    - threat hunting, threat intelligence and vulnerability management

The above features are later considered in concert with other potential ER-CSIRT features arising from the different stages of our analysis.

6 Desk research: analysis of CSIRT Models

6.1 General Approaches and their Elements

Here, we consider selected examples just to illustrate the main features of relevance to our key task of defining "*information sources, workflows and data flows required for the implementation of the CSIRT dedicated to railway sector*". This requires identifying, and later agreeing/refining with stakeholders, the organisational form, the specific functions, and hence the *information exchanges and communication actions* that the CSIRT "*collaborative environment*" must support.

6.1.1 General Example: Carnegie Mellon CSIRT Workflow Model (Operational)

The Carnegie Mellon Software Engineering Institute have been leading developers and supporters of CSIRTs (originally CERT – Computer Emergency Response Team) since 1988 **[Carnegie Mellon CERT]**. Figure 3 below indicates some key flows and actions related to CSIRT operation.

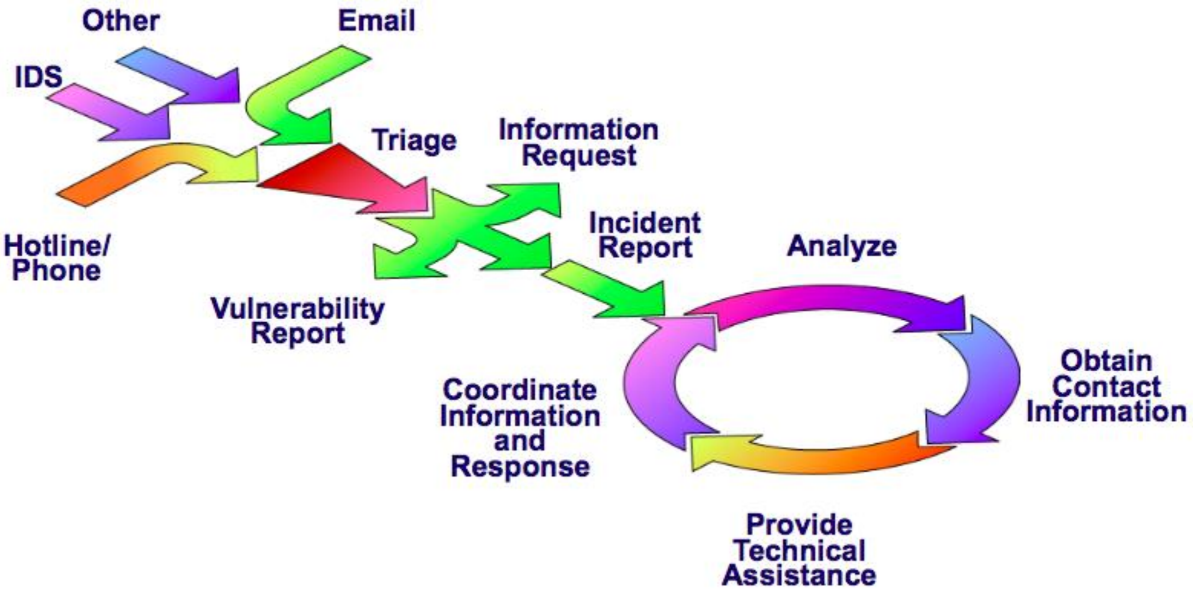


Figure 3: Cernegie Mellon CSIRT Workflow: From "Building Global CSIRT Capabilities" 2003.

The above diagram focuses "incidents", plus subsequent "response" via analysis/support, and illustrates an organisational CSIRT. It is unlikely that a multi-organisational structure such as SERA could easily adopt this model as a "unified organisation", since it would require live access to all IT/IDS in all railway companies simultaneously. Therefore, it seems safe to assume that an EU-level CSIRT could "coordinate" the different Rail CSIRTs in sharing threat / incident information. Each Rail-OES has a security team (CSIRT or other structure), or at least IT actors responsible for security (even in small concerns), and so the above-marked stages such as "vulnerability report" / "incident report" indicate opportunity to "share" between Rail-OES, facilitated by an EU-Rail-CSIRT. In such a scenario, it has to be determined what can be shared, with whom, under what circumstances, and how (e.g. automated sharing of "incident" declaration).

Based on the above model, and analysis of it, typical information flows concern a ***range of opportunities***: Incident Detection Alerts (IDS Alert); Incident Reports; Vulnerability Reports; Network Monitoring; Requests for Supporting Information/Services; among others.

For an EU-level Rail CSIRT, linkage between Rail-OES teams would require a collaboration environment able to e.g. *receive and share knowledge of incidents and how to mitigate them; share knowledge of current threats of relevance; support communication between actors*.

6.1.2 General Example: Organisational Model for EU-Rail CSIRT Collaboration

The organisational model for an EU Rail CSIRT must take into account the fact that it will be coordinating and supporting the collaboration of a number of EU Rail-OES (security teams / CSIRTs), as well as potentially establishing an EU-level role in relation to EU Cyber Security coordination (as in ECN).

Such a scenario suggests two levels of organisational model:

- Governance level.
- Operational level.

CSIRT Governance: Current Rail Cooperation on Security

At present the ER-ISAC engages a large number of Rail OES and their CISOs and so provides an example of how governance of a ***common security action*** can be achieved. The ER-ISAC uses a “terms of reference” (TOR) indicating key aspects: Purpose; Objectives; Membership criteria; Board; Rules of participation; Information sharing; Obligations; etc. Confidentiality and disclosure are key issues, addressed in some detail.

EU-level CSIRT Operation: Lessons from Current Practices in Europe

As suggested earlier, the operational workflow for an EU level Rail CSIRT would be somewhat different from the specific CSIRTs/Security Teams within OES and would be concerned primarily with coordination and support “across” OES security teams.

Taking the NIS directive as a reference, and focusing the aspects that determine National CSIRTs and their co-operation mechanism (now running as the ECN mentioned earlier), we can see some interesting operational features (extracted from **[ENISA NIS CSIRT, 2016]**) that might guide discussion of the EU Rail CSIRT.

Annex 1 of the NIS Directive: basic requirements for National CSIRTs and their tasks.

This annex puts requirements on CSIRTs to ensure a certain level of quality/reliability, e.g.:

- Highly available communication services, multiple means of communication, and communication channels well specified and known to users.
- Based in secure sites to ensure continuity.
- Having a system for managing requests, based on assured continuity infrastructure.
- Designed to participate in international co-operation networks.
- Key tasks include: Monitoring incidents; Early warning/alerts; Dissemination of information on risks and incidents to relevant stakeholders; Responding to incidents; Providing dynamic risk and incident analysis / situational awareness; Participating in the EU CSIRT network.
- Promote adoption and use of common or standardised practises for: 1. incident and risk handling procedures; 2. incident, risk and information classification schemes.

The selected features of National CSIRTs could be taken as an ideal start point for Rail-OES CSIRTs that intend to collaborate in a co-operation model for shared security in SERA.

Article 12 of the NIS Directive: CSIRT Network.
The Directive here proposes:

- A cooperation network run by CSIRT owners (MS).
- The CSIRT network shall support MS CSIRTs via specific tasks:
  - Exchange information on CSIRTs services, operations and cooperation capabilities,
  - Exchange and discuss non-commercially sensitive information related to an incident declared by a CSIRT and any associated risks,
  - Exchange and make available on a voluntary basis of non-confidential information on individual incidents,
  - Upon request from a CSIRT, discuss and identify a coordinated response to an incident that has been identified within the jurisdiction of that CSIRT,
  - Support CSIRTs (Member States) in addressing cross-border incidents on the basis of their voluntary mutual assistance,
  - Discuss, explore and identify further forms of operational cooperation (categories of risks and incidents; early warnings; mutual assistance; principles and modalities for coordination, when CSIRTs (Member States) respond to cross border NIS risks and incidents,
  - At the request of an individual CSIRT, discuss the capabilities and preparedness of that same CSIRT (advice and support),
  - Ensure CSIRT owners (MS in this example case) decide rules and procedures.

The above features of the CSIRT network, while aimed initially at national Government CSIRTs, could be taken as an initial outline of opportunities / options to consider when working with stakeholders (EU Rail CISOs and security teams) so as to encourage consideration of good practices, and also to ground the discussions.

Taken together, the above consideration of CSIRTs and their coordinating CSIRT Network, indicate a range of interesting features that offer opportunities for an EU-Rail CSIRT coordination. These are considered later in the proposed EU-Rail CSIRT Model, after consideration of the CSIRT analysis, and the results of the 4SECURail Survey and Interviews.

6.2 CSIRT Examples: Significant features of Relevance to EU Rail

Following the preceding high-level consideration of the general features of CSIRT models, and CSIRT coordination and collaboration, here we consider four well established CSIRT models that were chosen to support a baseline understanding of their general form, activities, services, role actors, and other salient features. Each is summarised in more detail in the Appendices , and all are discussed here. The detailed features are later discussed to identify opportunities for supporting an EU-level collaboration between the security teams of railway organisations.

6.2.1 CERT.NL

[CERT-NL] is a government model supporting governmental bodies as well as vital process providers essential for The Netherlands' core social and economic continuity. In addition to installing prevention and intrusion-detection solutions for government systems, the CERT provides services to analyse attempted or real intrusion events in relation to those systems. A 24-hour advice line is also in place to deliver support whenever it is required. For external partners (e.g. essential service operators) support is provided in understanding threats, selecting software for prevention and detection, as well as guidance on mitigation, and on-site support if required. Incident investigation also involves correlation of events to establish a broad situation analysis, engineering solutions to evident malware. Vulnerability assessment and protection advice is also actively delivered to community members.

6.2.2 CIRCL.LU

[CIRCL.LU] is a government model supporting all communes, private sector, and NGOs, as well as providing support to CSIRT development and MISP usage by European governmental actors and companies. Their primary aim concerns systematic response to cyber security incidents, and coordination of communication between involved stakeholders. Principle services involve delivery of alerts and warnings for Luxembourg users, incident handling and coordination, reporting and sharing of incidents, triage, and mitigation.

6.2.3 RAIL.IM

RAIL.IM is an anonymised EU Rail IM (see Appendices), supporting its operational systems and groups (*anonymised since it derives detail from both examination of public sources and our anonymous survey responses - see later*), and is selected as being fairly typical of EU Rail CSIRTs and Security Teams. The CSIRT is highly focused on prevention, through installing monitoring of all systems and networks, ensuring patches and adjustments to systems in reaction to emerging threats, and education/support to all IT and IT-security teams to ensure strongest prevention and response capacity. A systematic response capability includes standard procedures for *reporting* and *sharing* identified intrusion attempts or irregularities in logs or systems activities requiring investigation. Central support helps all teams.

6.2.4 NATO NCIRC

[NATO NCIRC] is an international organisation supporting its various sites and systems, along with its allies and strategic partners. Prevention involves deployment of latest IDT and analysis approaches, along with education and support of all systems, operating units, and IT teams, including sharing of threat intelligence and mitigation measures. Work with suppliers is identified as important for optimum prevention and shared response and mitigation measures. MISP is an important shared facility for exposing features of malware and incidents without exposing private details of the incident context. Response coordination involves Rapid Reaction Teams (RRT) to support all systems and networks.

6.2.5 ENISA essential model

The ENISA essential model is a general but very detailed CSIRT model and guidance derived by ENISA from its research, including collaboration with CERT-CC, and offered as support for European organisations developing a CSIRT. A primary emphasis is on prevention, supported by tools such as IDS, monitoring strategies, and threat databases, along with education and training, to ensure strongest preventive capability in the host organisation. Response emphasises organised alerting strategies, sharing of situation data, rapid response by technical experts to quickly control and remedy cyber events, collaboration with other relevant CSIRTs to limit effectiveness of new threats and to ensure broader community defence [ENISA_CSIRT, 2006].

6.2.6 Comparison of Examples

The preceding examples are provided in more detail in Annex 1 – Summarised CSIRT Examples, and are briefly analysed here to determine key features, the primary responsible for the activity, and who could provide added support. This latter aspect is essential here since we attempt to identify opportunities for a European Rail CSIRT Coordination function (referred to as ER-CSIRT for now) to provide relevant support to individual Rail CSIRTs and Security Teams.

Prevention and Preparation	**Main Stakeholders:**			
Key Activities:	**IM/RU**	**ENISA**	**ER-ISAC**	**ER-CSIRT**
Deploy a team of security experts to monitor systems and networks.	RE	AD	AW	-
Develop/Deploy Security Tools to monitor systems and networks.	RE, AD	AD	AW	-
Vulnerability management (cyclical, identify and mitigate).	RE, AD	AD	AW	-
Deploy forensic tools / IDS / threats databases etc. to support all activities.	RE, AD	AD	AW	-
Set up standard procedures to monitor and analyse events.	RE, AD	AD	AW	-
Provide intrusion detection services	RE, AD	AD	AW	-
Conduct security audits or assessments.	RE, AD	AD	AW	-
Conduct technology watch to identify emerging risks.	RE, AW	AD	AW	-
Share best practices with all teams.	RE, AW	AD	AW	-
Help selecting / installing software for logging / combatting cyber threats.	RE, AD	AD	AW	-
Analysis of malicious software / threats / likely intrusions (prep).	RE, AD	AD	AW	RE, DB
Provide database of known threats and mitigation actions (for preparedness).	RE	AD	AW	RE, CO, DB
Provide announcements to IT teams - risks and mitigation.	RE	AD	AW	AW
Ensure awareness - training - information dissemination to improve capacity.	RE	AD	AW	AW
Support for technical staff / showing how to deal with cyber threats / incidents.	RE	AD	AW	AW, DB
Collaborate with relevant bodies for shared capacity.	RE	AD, CO	CO	CO

KEY: RE-Responsible, AD-Advice, AW-Awareness, CO-Coordination, DB-Database (threats / mitigation).

In the preceding table of prevention and preparation activities, it is assumed that there is scope for an ER-CSIRT to provide support also at the prevention stage, by assuming responsibility for:

- *Provision of a database of known threats and mitigation*
- *Supporting its roles as Database holder by continually updating/analysing the threat intelligence landscape.*
- *Generating announcements of new threats or availability of support information etc.*
- *Supporting awareness and training, especially concerning use of the Database.*

- *Coordination with relevant bodies (ER-ISAC, Shift2Rail, ERA, ENISA, UIC, CER, EIM, etc)*.

The following table shows a similar analysis of opportunities in the response phase:

Response and Coordination	**Main Stakeholders:**			
Key Activities:	**IM/RU**	**ENISA**	**ER-ISAC**	**ER-CSIRT**
Deploy a team of security experts to respond to security incidents.	RE	AD	AW	-
Deploy an alert / warning system (actual incidents / new threats).	RE	AD	AW	RE, CO
Deploy communication facilities for sending/receiving alerts / guidance.	RE	AD	AW	RE, CO
Ensure 24/7 support.	RE	AD	AW	RE, CO
Incident identification.	RE	AD	AW	AD, DB
Vulnerability response coordination.	RE, CO	AD	AW	AD, DB
Generate alerts and warnings to other teams.	RE, CO	AD	AW	RE, CO
Incident handling, analysis, response coordination and support.	RE	AD	AW	CO
Analysis of malicious software / actual intrusions (response).	RE	AD	AW	CO, DB
Vulnerability assessment (identify risks, apply remedies).	RE	AD	AW	CO, DB
Provide advice on handling incidents (specific).	RE	AD	AW	DB
Coordinate response teams and communication between them.	RE	AD	AW	CO
Provide database of known threats and mitigation actions (support response).	RE	AD	AW	DB
Dynamic malware analysis platform.	RE	AD	AW	RE, DB
Communications platform for coordination.	RE	AD	AW	RE, CO

KEY: RE-Responsible, AD-Advice, AW-Awareness, CO-Coordination, DB-Database (threats / mitigation).

As indicated, there are potential opportunities for ER-CSIRT support in the response phase:

- *Deploying a coordinated alert/warning system* (between IM/RU)
- *Organising coordinated communications between IM/RU for alerts/notices of cyber-attacks or identified threats*
- *Sharing of incidents data* (type of attack /malware – links to DB)
- *Analysis of threat intelligence for updating the database* (as in prep' phase)
- *Providing a shared database of known threats and mitigation to support response actions*
- *Operating a communications/database platform for Europe-wide coordination of CSIRT knowledge sharing in relation to cyber security incidents*.

Main findings from example CSIRT examination
Based on a consideration of key activities in example CSIRTs, a number of actions are identified as prime candidates for implementation in an ER-CSIRT to enable coordination of cyber-security response by European IM/RU and their linked stakeholders: • Provision of a database of known threats and mitigation • Continually updating/analysing the threat intelligence landscape (for DB update) • Generating announcements of new threats or availability of support information etc. • Supporting awareness and training concerning use of the Database • Coordinating an alert/warning system (between IM/RU) • Sharing of incidents data (type of attack /malware – links to DB) • Operating the communications/database platform for Europe-wide coordination of CSIRT

knowledge sharing in relation to cyber security incidents
- Establishing a "virtual" team from participating IM/RU to deliver 1-7

The above initial list informs consideration of operational models, after considering examples of CSIRT coordination, then IM/RU/DSP Survey and Stakeholder Interview results.

6.3 CSIRT Coordination Examples: Coordinating CSIRTs

As we have seen in the preceding section, many CSIRTs appear to provide a "coordination" function so as to ensure that different security teams within a single organisation are working together, sharing necessary information, and organised as part of a coherent cyber defence and cyber response strategy. This model is sometimes referred to as the "campus" model where an organisation is "distributed", and so is relevant to EU Rail since that is effectively a distributed service system whose IT and Physical infrastructures are linked together right across Europe.

Here we examine some coordination examples of relevance to EU Rail cyber security collaboration, and as in the preceding section, seek to establish the specific features of relevance to EU Rail security coordination.

6.3.1 CERT-CC: CSIRT Coordination and Support

[CERT-CC] is the Computer Emergency Response Team "Coordination Centre". It was started in 1988 by the Defence Advanced Research Projects Agency (DARPA), a part of the U.S. Department of Defence, to support development of teams within key organisations for cyber security risk prevention and response/mitigation. CERT CC develops cyber intelligence, publishes alerts, and supports organisations at risk through training, advice, and on-site support. Other services include CSIRT (CERT) *coordination*, Incident reporting, security audit, sharing threat intelligence, artefact analysis, education of cyber experts.

6.3.2 FIRST CSIRT NETWORK: CSIRT Development and Support

[FIRST] is a confederation of trusted computer incident *response teams* (not all are configured as CSIRTS) who *cooperate* to support each other in handling security incidents. Members fund and support FIRST as a non-profit enterprise providing services to members. Members also develop and share technical information, tools, methods, and best practices. Services include security team development and support, training, threat intelligence sharing, coordinating members in supporting each other (best practices + during incident response). First provides information sharing tools (https://www.first.org/global/sigs/information-sharing/misp).

The FIRST security response teams are listed at: https://www.first.org/members/teams/

6.3.3 EC CSIRT Network: Member State CSIRT Coordination

[EC CSIRT Network] The CSIRT Network is established under the 2016 EU Directive on security of network and information systems (the *NIS Directive*). It ensures strategic cooperation between EU Member States in ensuring cybersecurity, including exchange of information on threats and incidents. Specific tasks are defined in the NIS Directive, being a matter of law in Member States, and including support for, and collaboration with, operators of essential services (OES). Primary activities include coordination of MS CSIRTs, promoting awareness of cyber security, reporting on threats and incidents, providing alerts, coordinating cross-border cyber security, pan-European exercises, and relevant studies and support for policy development.

6.3.4 Comparison of Examples

The preceding examples of coordination of security teams are provided in more detail in Annex 2 – Summarised CSIRT Coordination Examples, and are briefly analysed here (as was done in section 6.2) to determine key features, the primary responsible for the activity, and who could provide added support. This latter aspect is essential here since we attempt to identify opportunities for a European Rail CSIRT Coordination function to support collaboration of individual Rail security teams such as CSIRTs and other forms.

Rail CSIRT Coordination and Support	**Stakeholders:**			
Main Activities and Services:	**IM/RU**	**ENISA**	**ER-ISAC**	**ER-CSIRT**
Support understanding of NIS Directive and Cyber Security Act.	RE, AW	CO, RE, AD, AW	AW	AW
Support CSIRT formation / education / training.	RE	AD, AW	AD, AW	AW
Creation and support of active CSIRT Network for Rail.	RE	AD, AW	RE, AW	RE, CO
Coordinate CSIRTs for collaborative preparation and awareness.	AW	AD, AW	RE, AW	RE, CO
Coordinate CSIRTS for response to large scale / cross-border incidents.	AW	AD, AW	RE, AW	RE, CO
Providing hands-on support for cyber security response.	RE, AD	AD, AW	AD, AW	DB
Support NIS reporting security incidents.	RE	RE, CO	AW	AW
Focal point for documenting vulnerabilities, corrective measures.	RE, CO, AD	AD, AW	AD, AW	RE, DB, CO
Promote awareness/understanding of CSIRT developments.	AW	CO, RE, AD, AW	AD, AW	AW
Promote awareness of security trends and issues.	RE, AD	AD, AW	CO, AW	AW
Courses, Conferences, Training programmes.	AW	CO, RE, AD, AW	CO, RE, AD, AW	AW
Analyse threat intelligence to document risks/countermeasures.	RE, AD	RE, AD, AW	AD, AW	RE, AD, DB
Issue advice notes on threats and countermeasures.	RE, AD	RE, AD, AW	AW	AW
Identify/develop and share best cyber security practices.	RE, AD	AD, AW	AD, AW	AW
Provide/ manage database on cyber threats and countermeasures.	AD, AW	AW, AD	RE, AW, AD	RE, AW, DB
Generate / Share security Alerts / Announcements.	RE, AD	RE, AD	AW	AW
Vulnerability Analysis / Risk Analysis / Artefact Analysis	RE	AW	AW	AW
Auditing and Penetration Testing	RE	AW	AW	AW
Incident tracing	RE	AW	AW	AW
Promote development of quality security products, policies and services.	AD, AW	AD, AW	AD, AW	.-
Support for cyber security standards.	AD, AW	AD, AW	AD, AW	AD, AW
Analysis of CSIRT maturity / advice on development.	AW	RE, CO	AD, AW	.-
Pan-European Cyber Security Exercises.	AW	RE, CO	AW	AD, AW, DB
Studies on relevant security topics to benefit stakeholders.	AW	RE, CO	AW	.-
Support for policy development.	AD, AW	RE, CO	AD, AW	AD, AW
Support for Cyber Security certification schemes.	AD, AW	AD, AW	AW	AW

KEY: RE-Responsible, AD-Advice, AW-Awareness, CO-Coordination, DB-Database (threats / mitigation).

In the above table, there is opportunity for coordination and support of EU rail cyber security in several aspects, primarily:

- Create and support active CSIRT Network for Rail (parallel to ER-ISAC / with ER-ISAC).
- Coordinate CSIRTs for collaborative preparation and awareness (supported by ER-ISAC).
- Coordinate CSIRTS for response to significant / cross-border incidents.
- Focal point for documenting vulnerabilities, corrective measures + shared Database.
- Supporting sharing of incidents / vulnerabilities between security teams (response).

CSIRT Coordination Roles / Tasks	**Stakeholders:**			
Key Items:	**IM/RU**	**ENISA**	**ER-ISAC**	**ER-CSIRT**
Engage stakeholders and organise stakeholder membership	AW	AW	RE, CO	RE, CO
Identify educational needs and organise education	AW	AD, AW	RE, CO, AW	AD, AW
Organise and manage Specific Services	AW	AD, AW	AD, AW	RE, CO, AW
Facilitate communication between CSIRTs in networks (incidents, etc.)	AW	AD, AW	AW	RE, CO, AW
Operate Specific Services	AD, AW	AD, AW	AD, AW	RE, CO, AW
Implement / Manage Content / Operate Threats Database	AD, AW	AD, AW	AW	RE, CO, DB, AW
Facilitate communication between Security Teams (incidents, etc.)	AD, AW	AD, AW	AW	RE, CO, AW
Facilitate security training and Education.	AW	AD, AW	RE, CO, AW	AD, AW
Organise security workshops and conferences.	AW	AD, AW	RE, CO, AW	AD, AW
Organising and supporting Special Interest Groups (SIGs).	AD, AW	AD, AW	RE, CO, AW	AD, AW

KEY: RE-Responsible, AD-Advice, AW-Awareness, CO-Coordination, DB-Database (threats / mitigation).

Again, in the above table we can see opportunity for response coordination, mainly:

- Engage stakeholders (IMs, RUs, the ER-ISAC and the ER-CSIRT) to form collaboration group.
- Organise, operate, and manage services as previously identified.
- Facilitate secure communications between security teams in rail IMs/RUs.

Information Recorded / Exchanged	**Stakeholders:**			
Key Items:	**IM/RU**	**ENISA**	**ER-ISAC**	**ER-CSIRT**
Incident Reports.	RE, AD	AW	AW	RE, CO, AW
Threat library (risks and remedies).	AD, AW	AD, AW	AD, AW	RE, CO
New threats / new remedies (shared with stakeholders).	AD, AW	AD, AW	AD, AW	RE, CO, AW
Contacts information for other CSIRTs in the network.	AD, AW	AW	AW	RE, CO, AW
Threat intelligence and incidents via database.	AD, AW	AD, AW	AD, AW	RE, CO, AW
Supporting information (cases, reports, etc.).	AW	AD, AW	AD, AW	AD, DB
Alerts, Threat news and advice.	AW	AD, AW	AW	RE, CO, AW

Publications (Reports on Cyber Security topics; Info notes, e.g. threats and mitigation; Opinion papers, e.g. on ISACs)	AW	RE, AD, AW	AD, AW	AD, AW

KEY: RE-Responsible, AD-Advice, AW-Awareness, CO-Coordination, DB-Database (threats / mitigation).

Under this heading, we see coordination opportunities concerning:

- Recording and sharing incidents reports.
- Creating and maintaining a threat library for stakeholder usage.
- Identify and record new threats as part of library.
- Share threat intelligence of relevance to stakeholders.
- Deliver alerts, threat news and advice to stakeholders.
- Support communications between stakeholders.

Tools for Recording /Sharing Threat Intelligence	**Stakeholders:**			
Key Items:	**IM/RU**	**ENISA**	**ER-ISAC**	**ER-CSIRT**
CERT-CC Vulnerabilities Database: https://www.kb.cert.org/vuls/	AD, AW	AD, AW	AD, AW	AD, AW
National Vulnerabilities Database: https://nvd.nist.gov	AD, AW	AD, AW	AD, AW	AD, AW
Vulnerability Archive: https://github.com/CERTCC/Vulnerability-Data-Archive	AD, AW	AD, AW	AD, AW	AD, AW
Rail cyber threats database to be used and made accessible to all members.	AD, AW	AD, AW	AD, AW	RE, CO, AW
Library of news / security reports.	AW	RE, CO	AW	AW

KEY: RE-Responsible, AD-Advice, AW-Awareness, CO-Coordination, DB-Database (threats / mitigation).

Concerning tools there is opportunity to:

- Operate the database on behalf of stakeholders.
- Provide links to the other identified databases of value to stakeholders.
- Extract from relevant sources to enrich the hosted rail cyber threats database.

Other Salient Features	**Stakeholders:**			
Key Items:	**IM/RU**	**ENISA**	**ER-ISAC**	**ER-CSIRT**
Method for quick notification (speed reduces damage to all).	RE	AD	AW	-
Common policies and procedures.	RE	AD	AW	RE, CO
Automate incident handling tasks (speed reduces damage to all).	RE	AD	AW	RE, CO
Methods to collaborate and share information with others.	RE	AD	AW	RE, CO
Easy and efficient way to sort through incoming information.	RE	AD	AW	AD, DB

KEY: RE-Responsible, AD-Advice, AW-Awareness, CO-Coordination, DB-Database (threats / mitigation).

As part of its implementation, the collaboration models could include:

- Support development of common policies and procedures for collaboration.
- Automate incident reporting / sharing to reduce risk.
- Explore and develop further strategies for collaboration between rail security teams.
- Develop and implement information management approach (crisis management).

Main findings from examples of Security Teams Coordination
Organising • Organise stakeholders to create and support a CSIRT Collaboration Network for Rail. • Provide a focal point for declaring and sharing cyber security incidents. • Provide a focal point for documenting vulnerabilities, corrective measures (DB). • Support development of common policies and procedures for collaboration
Documenting • Create and maintain a shared threat database for stakeholder usage. • Extract from relevant sources to enrich the database. • Identify and record new threats as part of library. • Provide links to the other identified databases of value to stakeholders. • Implement other support tools as agreed by stakeholders.
Responding • Implement a response scheme to share incidents between security teams (response). • Coordinate CSIRTS for response to significant / cross-border incidents. • Record and share incidents reports. • Automate incident reporting / sharing to reduce time / risk. • Share threat intelligence of relevance to stakeholders (emergent issues).
Operating • Collectively organise, operate, and manage required services. • Facilitate secure communications between security teams (response).
Extending • Explore and develop further strategies for collaboration between rail security teams. • Develop and implement information management approach (crisis management).

7 Capturing the vision of the key EU stakeholders: surveys and interviews

4SECURail has followed a twofold approach to capturing the key stakeholders' vision on a future CSIRT model in the railway sector at the European level, by conducting an online survey to a number of critical stakeholders followed by individual interviews with the most active and key individuals resulting from that. This section describes the process as well as compiles the key findings.

7.1 European Survey of Railway Security Stakeholders/Experts

An online survey was collaboratively designed with a small sample of stakeholders and was informed by the "situation analysis" conducted at the start of the project. The survey was hosted on the **[EU SURVEY tool]**, provided by the European Commission, and was anonymous to allow respondents to freely express views.

Invitations and Response Rate

A total of 60 railway organisations were invited to take part, including 28 IMs, 26 RUs, and 6 Suppliers of Services (DSP), Systems, and Equipment.

From the period 5th February 2020 till 15th March 2020, we received detailed responses from 26 organizations (***43%***). This is substantially higher than the typical 10% response rate for broad surveys like this and reflects the interest and commitment of IM/RU security teams. To this were added a small sample of higher-level stakeholders such as Policy Makers, Rail Associations and Regulatory Agencies, and their views are taken into account of later since they were also interviewed to elaborate issues arising (see Stakeholder Interviews section).

The main survey findings (from IM/RU/DSP/Systems/Equipment) are summarised below, and follow the structure of the survey, followed by a general summary.

7.1.1 General Profile of Respondents

Respondents' Personal Role in Railway Security

The survey respondents demonstrated a range of roles and included different levels of explanation. Key roles were:

- Director/Manager of Information Security.
- CISO + roles such as Team Leader for specific areas (e.g. networks).
- Deputy CISO + roles within specific areas.
- ISO + roles within specific areas.
- CIO with role supporting security teams.
- Cybersecurity platform manager.
- Secure Info Systems Architect / Network Engineer.

Additional information provided on roles and responsibilities emphasised:

- Managing Cyber Security Teams (Protection + Response).
- Ensuring Systems and Information Security (Operational).
- Providing Response to Cyber Incidents and Threats (Operational).
- Managing Secure Platforms (linking security teams).

- Ensuring Security in Signalling Systems.
- Designing Secure Information and Service Systems.
- Designing Network Security for Railways.
- Specifying Security Requirements with Suppliers.
- Managing Secure Technical Systems.

From these two preceding factors, we can be confident of a relevant and useful spread of professional perspectives, representing all key aspects of cyber security.

Respondent's Organisations

Survey responses indicate participation by:

- 12 Infrastructure Managers (IM)
- 10 Railway Undertakings (RU)
- 2 Digital Service Providers (DSP for numerous European railway companies)
- 2 Suppliers of Systems and Equipment (both large organisations with large customers in several European countries).

So, again we can be confident of a useful and relevant spread of organisational perspectives being reflected in the survey.

Respondents Main Interests

Concerning their key interests, 80% of respondents stated they were interested in both prevention and response, while 12% suggested mainly prevention, and 4% suggested mainly response.

7.1.2 Sharing Cyber Threat Information

Receiving and Providing Alerts and Warning of Incidents and Threats

In total, 25 of 26 respondents stated that they want to receive warnings of threats, intrusions, or other cyber incidents experienced by European railway stakeholders. These same 25 stated that they are also willing to share declarations of incidents and threats they themselves have experienced.

The single exception stated that it should be a matter of choice at the time (see next point) and so we interpret this as a willingness to receive/share, depending on circumstances.

Attribution of Threat Information

Participants were asked if shared information should be "attributed", i.e. provider should be identified. The results indicate (in order of preference):

- 23 – A matter of choice at the time.
- 3 – Yes, attribute origin of shared information (incident, threat).
- 0 – No, keep all sharing anonymous.

Therefore, it appears there is a very strong majority in favour there being a choice, at the time of declaring event information to be shared, whether to say who the contributor is. Since the organiser of a collaboration mechanism/platform requires of course to know its contributors, then specific requirements are present here:

- Platform organisers must know identity of contributors (trust mechanism).
- Platform organisers must preserve identity of contributors when requested.
- Platform organisers must "anonymously" relay information from "trusted" members.
- Platform must declare contributor identity when requested by contributor.

European Railway Cyber Response Coordination

Respondents were also asked if they perceive value in exploring a *future* European level "Response Coordination" action, to coordinate exchanges between Security Teams concerning threats and actual incidents intrusions, including during Incident Response / Mitigation (European Railway CSIRT coordination).

a. 23 of 26 respondents stated YES.
b. 3 of 26 respondents stated NO.

Of the 3 who stated NO, all three were from Railway Undertakings (RU) and provided rationale as follows:

- One RU states they do not own or operate their IT network infrastructure, and so we assume they rely on their IM and/or suppliers to ensure security. This latter aspect is relevant since the same RU has a cyber security team, with clear roles, and is ISO 27001 compliant (a standard for an information security management system, indicating both information security and "system"). There may be some possible confusion in this case. Even if they rely on IM and Suppliers to look after security, their ISO27001 compliant team might want to know of Europe-wide or cross-border incidents threatened their systems and processes (e.g. new threats or attacks on railways). This RU also agrees to sharing as a "matter of choice" at the time (see earlier).
- One RU states that they share with the national CSIRT/NCSC and so expect that European level collaboration could be organised through such a system. The previous discussion of CSIRT Network and EU-level cooperation indicates that a sector-specific exchange for rail is not evident and so cannot be depended upon. This RU is not a declared member of the ER-ISAC, and so may not fully understand the current climate/debates around railway security information sharing.
- The third RU declaring "NO" did not provide any explanation.

The results here suggest that there is a *strong approval for a future European level railway cyber security response coordination*. However, the three voices of dissent suggest a need to *engage with RUs more closely* and to understand their perspective more fully on sharing cyber security information.

Other Issues Identified

When asked to identify any further issues relating to "sharing" of cyber threat information, respondents were quite forthcoming and noted a range of issues, summarised here:

- Sharing cyber threat inside the rail sector is vital to increase the cyber resilience of the whole sector.

- There is a need for a structural approach with guidelines and specific rules attuned to the Railway Industry and its context.
- Coordination could be led by several IMs with good security teams and facilities yet include and benefit all stakeholders.
- We need a legal framework for sharing information regarding systems from different technology providers.
- The issues around GDPR should be clarified.
- Trust-building activities should be addressed since trust is required for information exchange.
- Protection against cyber threats is a shared responsibility between stakeholders (product suppliers, integrators and operators) - so disclosure of attack/threat details must be coordinated between the different involved parties.
- We need to clarify the roles of the suppliers in European rail cyber security.
- The choice of whether to identify the *sharing organisations* depends on whether/which other actors are affected through that specific organisation, or whether some are potentially affected by the declared threat in a more general way.
- The coordination at European level depends on the number of organisations in different countries that could be affected by the same case.
- Exchange should not be mandatory, and those who are willing should proceed.
- There is a lack of an active platform or community to support response collaboration.
- Obligation to *notify* under the NIS directive exists for some parties and should be accounted for (e.g. what they have to *notify* may be relevant to other rail actors).

From this list of key points (echoed by many respondents), the *main additional issues are*:

- Establishing trust between stakeholders, and protecting information/identities,
- Establishing guidelines for a common approach,
- Ensuring shared facilities and supporting actors (management and operational),
- Using secure communication channels.
- Engaging suppliers (DSP/Network/Systems/Equipment) in appropriate roles.

7.1.3 Help in Defining/Testing a Cyber Security Collaborative Platform

Some questions were asked to test level of interest in helping define and test a platform for European Railway security teams' collaboration. The survey indicated that the platform is intended to deploy secure EU open source solution for use by any/all EU railways.

Participation in Defining and Testing the Platform, and Joining a Co-Design Workshop

Respondents indicate that the majority would be keen to participate in further defining the collaborative platform, and in joining a co-design workshop to support its refinement. A total of 24 out of 26 would participate (92%), which is a very positive response. It will be important, therefore, to ensure widest possible opportunity for stakeholders to continue guiding such an action. While a workshop, for practical purposes, may be limited in size, other strategies for participative co-design should be employed to ensure inclusion.

Other Issues Identified

The survey responses here were very clear on several key issues:

- A planned approach is required to allow a *detailed assessment*.
- Information should be provided on *comparable relevant initiatives* to ground the discussion and enable comparison.
- In advance of a workshop or other activity there should be a *preview of the proposed model and platform* to allow consideration before the event.
- Any structure for the workshop, such as themes or key questions, should be *known in advance to allow preparation* of ideas and suggestions.
- The model and suggested platform should include *definition of a clear relationship with other relevant initiatives such as the ER-ISAC, the National CSIRTs*, and any other European collective actions supporting coordinated response to threats.
- The workshop should *involve IM/RU specialists/experts who investigate new ways of security information exchange*, since these are advisors to decision makers in railway.
- Testing *should be like a field test with several stakeholders sharing realistic example* intrusion or threat incidents.

Overall, the responses were very positive, and the above key issues should be carefully considered when developing the participative co-design workshop, and any wider co-design actions to ensure a broad inclusion of perspectives.

7.1.4 Respondent Organisation's Cyber Security Actions

Several questions addressed the cyber security actions deployed by the respondents’ organisations, and the results of these are summarised below.

Security Team Form / Structure

Here, 23 of 26 respondents (88%) declared that their organisation has a well-defined (cyber) security team with clear roles. Those who said they did not have such an arrangement were two RUs and one IM. Two (RU) declare there is no “centralised” cybersecurity team, but a team of technicians in IT address all IT issues including security. The third (IM) declares they are in the process of defining a cyber security team specifically for signalling systems, as part of an initiative to develop a national cyber security action on signalling.

For those who did declare a formally defined cyber security team, only 9 of 26 (35%) stated that it followed a classical CSIRT or SERT model (see CSIRT classic models in earlier sections of this report). The others, in describing security team arrangements, show similar general features, but with some interesting differences/specialisms:

- Established as a loose organisational network, with Technical Director/Security Manager, overseeing team leaders for Networks, Systems, and Services, plus nominated experts linking to Suppliers and Customers.
- Established as a Security Operations Centre (SOC - more formal) overlooking security teams in different areas. Additional support is given such as delivery of (or training team members to conduct) log/activity analyses, penetration testing, using technologies for identifying intrusions (IDS).

- In addition to the above, several mention specific additions:
  - Risk & Regulatory Framework Officer / Expert.
  - A Cybersecurity Coordination Centre coordinating the teams (CSIRT form).
  - A Cybersecurity Laboratory or Technical Analysis Centre (Forensics etc.).
  - A specialist in Data Privacy.
- There is evidence of usage of the ENISA guidance document (CSIRT Guidance ADD LINK) to help shape security teams.
- Some mention having a security coordination team above the SOC to decide policies and procedures for SOC and Teams.
- Suppliers show separation of teams for IT and OT, with detail of activity focus (e.g. IT cybersecurity teams cover design, manufacturing, and validation/testing for cybersecurity – e.g. OT cybersecurity team ensures that products meet the customer cybersecurity expectations and nominated standards). Both focus internal standards such as ISO/IEC 27001:2013 and NIST Special Publication 800-53 Revision 5 (framework).

Security teams are clearly quite diverse in form and structure, some being centralised or established as a single entity, while others are distributed and use sub-teams or specialist teams for different systems / functions. While some do not declare their security team a “CSIRT” they do follow the general form and function (see later).

Key Roles in Railway Cyber Security Teams

The main cyber security roles in respondents’ cybersecurity teams can be summarised:

- Cyber Security / Security Manager.
- Team leaders in specific areas (e.g. Network, Systems, Services, OT).
- Security Responder.
  - Triage staff.
  - Incident Handler / Analyst.
  - Response advisor / Remediation.
  - Security experts for advice.
  - Forensics experts.
- Data Protection Officer (DPO).
- Platform manager (connects teams and supplies information / communication).
- Risk analyst / Risk & Regulatory Framework Officer.
- Security designers (for equipment / IT suppliers and DSPs).
- Security Architecture design (esp. supplier).
- Project security integration expert.
- Security tester / Penetration Tester.
- Data Privacy Officer (GDPR)
- Physical Security expert.
- Specialist technicians working with system/equipment suppliers (IT/OT).

These range of roles indicate some variability in how security teams are made up. Collaboration between organisations might therefore require a range of activities in Rail security teams and should also be taken as reflective of the variability between teams. Collaboration through linkage to specific actions may be quite complex, and so linkage via a single point of contact may be more practical.

That could require that teams adapted their internal practices to ensure intelligence was channelled to the point of contact.

Primary Tasks evident in Railway Security Teams

The main cyber security tasks identified for the above described roles are mainly self-evident from the role descriptions, and include:

- Define and deploy the cybersecurity strategy for the organisation.
- Conduct risk analysis (all IT systems, Networks, Equipment/OT).
- Ensure a “business continuity” plan for all identified risks.
- Organise and lead (Cyber Security / Security Manager).
- Organise and lead specific areas (e.g. Team Leaders - Network, Systems, Services).
- Provide data protection advice (both concerning system data, and GDPR).
- Conduct GDPR audit / Personal Identifiable Information (PII) analysis.
- Identify and monitor “insider threats” and Human Resource risks.
- Conduct security tests and penetration tests.
- Design security strategy for IT/OT (and for products, if supplier / DSP).
- Advise on evident risks and applicable regulatory frameworks.
- Conduct monitoring of all infrastructure at risk (via logs, IDS, traffic analysis etc.).
- Identify threats /attempts / intrusions.
- Provide security response for incidents:
    - Handle incident / organise activities and specialists.
    - Conduct triage / incident analysis.
    - Advise on response and remediation.
    - Conduct forensic analysis (establish threat strategy, penetration, artefacts).
    - Advise on follow-up actions / clean-up.
- Manage platform services to security teams.
- Manage communications services linking security teams.
- Provide security integration in projects (especially interconnected systems).
- Provide security oversight and assurance with suppliers of equipment, IT, networks, OT and services.
- Maintain vulnerability watch (all potential threats and risks in all areas).
- Services to business units and customers (ethical hacking, testing, advice, etc.).
- Provide 24/7 helpline and assistance to all key stakeholders.

These key tasks can be seen as indicative of the range of activities in Rail security teams and should also be taken as reflective of the variability between teams. Collaboration through linkage to specific actions may be quite complex, and so linkage via a single point of contact may be more practical. That could require that teams adapt their internal practices to ensure intelligence will be channelled through the point of contact.

7.1.5 Threat Intelligence Tools and Information Sharing

A number of questions examined how technologies and processes are used to coordinate intelligence gathering and sharing.

Use of Platforms and Tools within Security Teams

In response to questions about use of platforms and tools within security teams, it was shown that *platforms* are used by more than *90%* of respondent organisation security teams. The two organisations who do not use platforms to support security teams offer no further explanation.

Detection Tools are used by almost 90%, with only 3 of 26 not yet using detection tools themselves but relying on system providers to install their own measures. Mentioned detection tools in use can be summarised as follows:

- Security information and event management (SIEM) installations of different kinds.
- SIEM key components such as manager/analyser using real-time alerts/data from multiple applications and network hardware.
- Specific/separate log managers of different kinds for centralised management of log data.
- SIEM components designed to attract attention / deflect attacks (Honeypots, Honeytokens) as part of "detection" strategy.
- Specific products combining features - ArcSight, DEVO, Darktrace, Nozomi, Qualys VMDR, Splunk (monitoring, detection, vulnerability scans, investigation, correlation, etc.).
- Bespoken SIEM from suppliers (not defined).
- Web Application Firewall (WAF) for HTTP applications, including some specific products such as Palo Alto Firewall NG.
- Other security analytics such as included in IBM QRadar or AKAMAI cyber suite for Cloud.
- Tools (not specified) installed by equipment/network/systems providers.
- Various Intrusion Detection Systems (IDS), network intrusion detection (NIDS), host intrusion detection (HIDS) – not named, and installed by suppliers.
- Endpoint detection response (EDR), and Endpoint Threat Detection and Response (ETDR), not named products but mentioned.
- Vulnerability Scanners / Analysers.
- Risk assessment tools, e.g. Monarc.
- Two mention that further tools are being tested (but not which).
- Four mention that they will only release details in face-to-face discussion (caution).

These results indicate that there is a wide variety of activity around detection, with a range of solutions being used, often integrated in systems supplied by vendors. This further emphasises the need to work with suppliers to ensure shared responsibility.

Collaborative Prevention Tools

It can be learned from the preceding that the majority are using different tools / suites of tools for combined detection and prevention, in many cases provided by systems suppliers. However, concerning collaborative prevention tools, only 11 of 26 declare usage (42%).

The declarations include mention of:

- MISPs (Malware Information Sharing Platform) (4 are already using + 4 are in test / training).
- Proprietary tools to coordinate cybersecurity actions (4 respondents).
- Other systems and components mentioned included:
  - Honeypots / Honeytokens as preventive measure (also see detection).

- Sandbox facilities to separate untrusted/untested programs.
- AKAMAI Net Storage (Cloud - shared security management aspects)
- SAT-INET (Internet Early Warning - shared management aspects)
- Qualys VMDR (Detection and Response management aspects).
- Symantec CASB (Cloud Access Security Broker - shared access control).
- Symantec DLP (data loss prevention)
- Anti-Virus software (AV).

Two respondents indicate they might discuss face-to-face only.

Again, we see a variety of solutions and strategies mentioned, but with significant emphasis on MISP (see earlier analysis for MISP details and analysis). It is worthy of note that MISP instances can be linked for wider sharing (see later, under outline platform).

Organising Threat Intelligence Sharing Among Stakeholders

Respondents were also asked about their strategies for sharing threat intelligence among stakeholders, and results indicate a variety of strategies in place:

- Company defined procedures and protocols (including reporting mechanisms).
- Regular monthly reporting and timely threat alerts
- Sending Alerts, Bulletins, Advisory Notices.
- Declare new threats via Intranet lists and alerts with emails.
- Relay news to Intranet, email and text about new threats from outsider sources (like ENISA web and supplier notices).
- Share indicators of compromise (IOC) through MISP and by email.
- Text warnings sent to key staff phones.
- Multi-Layered MISP cluster (sharing between MISP instances).
- Regular Meetings, Blogs, Collaboration Tools (not specified).
- Ad hoc basis, depending on issues arising / events.
- Using standard Microsoft tools (Teams, mail)
- No organised sharing within organisation but sharing with governmental cyber security centre.
- Threat intelligence for company not dedicated to OT scope.
- Alerting suppliers.

The list indicates some degree of variability, with a range of examples that can together effectively ensure awareness by key stakeholders. These should be carefully considered in further co-design of the model and platform.

Further Issues on Cyber Security Organisation, and Threat Intelligence Sharing

When asked for any other comments on Cyber Security organisation, and Sharing of Threat Intelligence (free inputs), the respondents advised as follows:

- Some indicate that national authorities provide secure platforms to share cyber intelligence where all rail stakeholders can contribute, and in some cases must contribute notifications (but it was not indicated how these stakeholders can share with each other).

- One respondent suggests that a framework based on Best Practices should be developed and shared, then further matured jointly by rail stakeholders.
- One respondent indicates they are following the ENISA best practice model to develop their own company CSIRT further, and then want to share with "trusted" rail stakeholders around Europe.
- It is suggested that sharing (between IMs in the case of the contributor) would have to come from SOC leadership, not directly from each team, i.e. a point of contact per company.

These additional issues should also be considered in the analysis supporting model and platform definition.

7.1.6 Access to Information

Respondents were asked their views on intrusion and/or threat information between organisations.

Restriction of Access

When asked if threat/intrusion (cyber intelligences) information shared between organisations be restricted to CISOs, the group was split, with 11 saying Yes and 15 saying No. Those who said no, indicated a range of reasons:

- It depends on the organisational structure and where the security team / unit is located: cyber intelligence should be made available where it is needed / to those who have to act on the information.
- It should be 'trusted' persons (not just CISOs), to ensure information is available to those persons best placed to analyse and act upon it.
- CIOs and IT staff.
- CISOs could present a 'bottleneck'.
- The CISO must have all the information to coordinate the different teams/areas.
- The trusted network should be limited to cyber security professionals to prevent confusion or panic.
- Relevant information should be distributed to expert analysts and potentially to testers or designers.
- It depends on the size of the organisation, number of people involved in security.
- For sharing information inside the organisation, a confidentiality policy controls distribution of information inside the organisation (anonymised if required).
- IT manager level.
- Information sharing must start on a technical level. CISOs usually do not have the capability to present and consume this information in an appropriate way.
- SOC leads in our company so SOC leader or SOC contact is an ideal point for sharing.

While there are some conflicting views expressed, the general consensus seems to be that for each organisation, they have to *decide on the main point of contact*, and the *internal policy for distribution*. Relevant shares include cyber security professionals (analysis and policy adjustment), system designers and engineers etc. (repair/mitigation).

Interestingly, when sharing with a wider group (CISO and other team members) only 26% of respondents suggest recipients should receive all the cyber intelligence. The majority (74%) suggest they should receive only part of the information, depending on their role (i.e. only what is relevant to their job).

If information of cyber threats/incidents is shared between railway stakeholders, via a trusted point of contact, the decision on who to provide with "selected" information might be part of the trust relationship (i.e. decided by internal policy).

7.1.7 Platform Facilities

Respondents were asked a series of questions concerning the facilities that a collaborative platform might include.

Threat Library + Library of Defensive Measures

All but one of the respondents (96%) agreed that a European collaborative platform for rail should include an updated library/repository of relevant cyber threats. In addition, all respondents (100%) agreed that such a platform should provide an updated library/repository of defensive measures in relation to threats (mitigation).

Communication Facilities – Sharing Intrusion / Threat Information

All respondents also agreed (100%) that a platform should include a facility to tell other participants (e.g. via Security team leader, CISOs of IM, RU, etc.) about a recent intrusion/attack.

In relation to this facility, respondents indicated preferences as follows:

- 20% - A facility to communicate / send messages to all participating CISOs/Teams.
- 17% - A facility to choose participating CISOs/Teams for communication.
- 4% - Use email privately.
- 59% - Choose between the 3 options at the time.

So, to seems the majority prefer to choose between an "all" or "selected" group share, but with a small minority selecting private email as an option.

Analytics Module

The majority (85%) of respondents stated it would be desirable to have an analytics module showing e.g. same threats / events declared by different users. Such features appear in many large-scale in order to help higher level analysis of the threat landscape.

Other Issues

Other comments on platform facilities were received from half of respondents and can be summarised as:

- Examine how EU-level collaboration between CSIRTs is being handled since that could be a good model.
- A central library/repository governed centrally would be the best and secure option to inform, share, maintain and evolve.
- We need trust and willingness to have an equal role, and so level playing field.

- If the "analytics module" is embedded into the platform, it could be interesting, but if externalised e.g. in another SaaS platform, it could be problematic for confidentiality.
- The platform should share any information about the known attackers' groups, and their attack methods.
- The platform should offer actuation guides about the different known cyber threats/intrusions for all Railway organisations to respond in the same manner (e.g.: expanded activity of Malware like EMOTET, or expanded Phishing activity, etc.).
- Information should be well secured, covered by a non-disclosure agreement (NDA) and only accessible to authorised people.
- Sharing may be with a connected railway or supplier only or may be for everyone if it is a new threat or something for all - a choice for the contributor.
- Given the specific nature of cyber infrastructures, large differences in exposure, risk and remediation potential exist between different organisations, and so generic analytics will provide limited added value - analytics of railway specific data is needed.
- We should be able to share what happens (threat intelligence) with our national security contact under NIS.
- It could help people if they could ask questions - like a private discussion area for security experts who can discuss issues they are trying to address.

A number of these additional comments confirm the strong willingness to share, and to use a collaborative platform. At the same time there is concern about ensuring security of content on the one hand, but freedom to share with national security authorities on the other, indicating a need to define the "stakeholders" as both key railway stakeholders and trusted third parties.

7.1.8 Relationship to ER-ISAC & NIS Directive

Respondents were asked if their organisation is a partner/participant in the ER-ISAC:

- Half of respondents (50%) stated that they were partners.
- A fifth (20%) stated that they were not.
- Almost one third (30%) stated they were unsure or were in the process of becoming so.

From those who were established members, 38% stated that the ER-ISAC should deploy the collaboration model for response (referred to in 4SECURail as CSIRT) to enable a shared "response capability". The remainder (62%) suggested that the CSIRT collaboration should be a separate action/facility.

Those who are not yet members of the ER-ISAC were not asked their view on the above aspect. However, all were asked "***How should a future EU Rail CSIRT coordination be implemented or hosted***". In response to this open-ended question, respondents suggested several observations and ideas as follows:

- EU-Rail CSIRT collaboration activities should be carried out by a dedicated team, and a link must be established with ER-ISAC.
- The ER-ISAC can be a Governance Authority, with something else (e.g. *collaborative platform + initiative)* on a more practical and active level.

- The ER-ISAC should contribute to building a future EU-Rail-CSIRT with activities performed by dedicated teams. Links (*from 4SECURail*) should be established with ER-ISAC.
- The ER-ISAC should be the platform for exchange of cybersecurity threats and issues in the sector, and so should "*deploy*" the future CSIRT and collaboration platform.
- Although the CSIRT can be a separate action/facility it must be accessible to the ER-ISAC participants (*maybe through their platform*), because sharing information and news about incidents is a part of the objectives of the ER-ISAC.
- It should really be the IMs who do it together. It can be a part of ER-ISAC, or a separate thing, but both would still be a European railway collaboration, so strong link to ER-ISAC will be there anyhow.
- It can be "separate" but still ER-ISAC partners, and so can be linked. The jobs to be done can be shared between partners. The leaders can be companies with well-developed teams. RU should be involved, not just IM.
- Apart from the platform there should also be a discussion on whether the EU Rail CSIRT should have staff for coordination and / or response activities.
- The future collaboration model and CSIRT collaborative platform require an agreed implementation procedure.
- The CSIRT collaboration model and collaborative platform should be implemented as a bottom-up approach.
- The platform must include the main operators and integrators in order to share and build a common up-to-date cybersecurity context.
- The platform should have the capability to activate a cybersecurity manager and expert network in order to answer to any imminent cybersecurity threat or to provide a consistent and quick response to any cybersecurity attack.
- The simplest functionality would be only to provide an information sharing platform, and more advanced functionality would be needed for coordinated reaction.
- The choice of location for the CSIRT collaboration can be with many companies and not just with one - would teach more people, and the leader should be large rail with good CSIRT and tools for leadership.
- This could be considered as a European railway SOC, eventually linked with local company SOCs, and so provide SOC services to railways companies.

The above ideas are quite challenging and indicate a number of key issues for discussion:

- Choice of governance – under ER-ISAC or as a separate but linked action.
- Need for dedicated team, with emphasis on using people already situated in security teams (distributed and "virtual" organisation).
- Emphasis on using "leaders" – companies with well-developed CSIRT/CERT/Security teams.
- Links to integrators and suppliers need to be developed since they are key actors in analysis and repair.
- Need to ensure quick response to calls for assistance form all EU rail actors.
- Support from, and advised by, ER-ISAC since that is the same community of interest.

NIS Directive Notification Obligations

Concerning obligations to "notify" cyber security incidents according to NIS directive, 46% of respondents indicated they were obliged as Operators of Essential Services (OES). Four respondents (16%) stated that they were not obliged, and the remainder, while 40% state they are unsure!

For those who do notifications, methods stated were:

- Formal process with national CERT/CSIRT via an online platform (+email in some cases).
- Additionally, with the national Telecommunication Authority via agreed protocol.
- Additionally, through the FIRST forum to share with other CSIRTs.

As discussed earlier in this report, there is still some uncertainty around which countries identify Rail as OES, with some even separating rail into different classes for inclusion/exclusion. This suggests the collaboration model and platform can, through its outputs, provide information of relevance for European level analysis by Member States, but it would rely on uncertain pathways within countries.

7.1.9 Respondents Advice and Comments to the Study

Despite an extensive survey, participants provide some additional advice in the final open comment section as follows:

- A key challenge is to prove, show and create a community with active members.
- We need a demonstration to convince people through experience, e.g. by presenting to ER-ISAC. If there are public reports, make sure all ER-ISAC people are sent copies.
- The model should include cooperation with relevant European CSIRTs and ISACs.
- There are many rail initiatives in Europe, and they compete for attention, so it is necessary to link concerns together to solve the problem of collaboration.
- Optimal use should be made of existing models and platforms already in use or under development to support international exchange and cooperation between CISRTs.
- Even if large rail companies lead the CSIRT all rail companies can be supported for European strengthening.
- To make all European railways safe needs all railway companies and their system providers to be open and share problems.
- Focus on both IT and OT systems for railways so as to have an end-to-end view.
- ER-ISAC should contribute for EU-Rail-CSIRT building.

Main survey findings
Profile of Respondents • Both IM and RU seek collaboration around Prevention and Response. • Key stakeholders within rail security teams fulfil a range of roles. • Point of contact for collaboration will vary between different railway security teams
Supporting Co-design on Model and Collaborative Platform • The majority of IM/RU wish to support 4SECURail co-design and workshop activities.
Sharing Cyber Threat Information • The majority of key stakeholders wishes to share threat intelligence. • Choice of anonymity is context-dependent and linked to "trust". • Coordination of different security teams' response is seen as highly attractive / beneficial. • Sharing is mainly around likely threats and actual incidents.

• Required shared facilities include database (IoC, etc.) and Communications (alerts/warnings).
Company Cyber Security Actions • The majority have clear security teams / responsibilities - not all follow CSIRT model. • Roles and tasks are highly variable. • ENISA guidance on CSIRTs is being used by many and stated as being of high value.
Threat Intelligence Tools and Information Sharing • The majority use a platform of some kind to link cyber security actors internally. • Detection tools are used in most cases, with a wide variety of types/instances. • Less than half use collaborative prevention tools, with “MISP” being highest example. • A variety of strategies / mechanisms are used to share threat intelligence with stakeholders.
Sharing Security Intelligence Between Organisations • Point of contact for sharing between organisations is local choice (not just CISO). • A trusted network must be organised around trusted parties. • Distribution / sharing within an organisation is a matter of internal policy.
Suggested Platform Facilities • Inter-organisational sharing of threat intelligence should include a platform with: o Library of threat intelligence (up-to-date library of threats + defensive measures). o Communication facilities for rapid Alerts, Awareness bulletins. o Analytics module (threats experienced by different users / locations / times, etc.).
Relationship with ER-ISAC and NIS Directive • The collaboration platform/initiative should be linked to ER-ISAC. • Governance will be a key issue, but a new organisation should be avoided: it needs a “virtual” team of IM/RU points of contact, plus a “host” for platform facilities. • NIS “notifications” could also be shared via the platform to “speed” intelligence
Respondent Advice to Remainder of Study • Exploit platforms already in use for exchange and collaboration. • Demonstration will convince people through experience

7.2 Interviews with Key EU Railway Security Stakeholders

As a further triangulation point concerning European railway cyber security stakeholders, a sample of high-level stakeholders were invited for interview (DG MOVE, ERA, ENISA, ER-ISAC, ERTMS, X2RAIL-3, ALSTOM, Infrabel, DB-Netz and DB-Systel). The set was chosen to include views from the main types of stakeholders and leaders in rail security development (European Commission, Agencies, Suppliers, ER-ISAC, Complementary project in Shift2Rail, Leaders in rail cyber security). A standard set of topics was used to allow comparison (structure of this section), followed by open discussion to encourage sharing of ideas. The results are integrated and summarised as follows, including only commonly shared views. Alternate views will be explored at the workshop stage.

7.2.1 Current and Future Needs

7.2.1.1 Collaboration and Support for Response

- There is a need to help rail security stakeholders collaborate concerning response and requires critical information sharing (both incidents and potential threats) – especially for trans-border incidents (same risk/attack in different countries / organisations).
- At detection of an intrusion or an attempted intrusion, rail needs to share between security teams in all relevant rail IM/RU “instantly” or near-instantly.

- Rail needs a way of exchanging information rather than “coordinating” a response, since the actual response will be decided by the IM/RU and their internal experts.
- Rail needs a “virtual” team, not an “organisation” - with clear tasks and functions to support information exchange for collaboration. A legal framework may be required.
- Further exchanges (IOC, architectural problems / solutions, etc.) would add benefit.
- Short term emergency situations need more than the ER-ISAC model.
- Further collaboration between security stakeholders can use the ER-ISAC, CSIRT Network, FIRST etc.

7.2.1.2 Issues for Sharing Threat Experience

- EU rail is in a semi-public environment, so exchange of information could be sensitive, especially where there is a link between rail and military.
- IM might be hesitant to share with clients (RUs), as might suppliers.
- Anonymous exchange would be easier (from IM via platform to RU and other IMs).
- Sharing in the ER-ISAC is informal. We need a reliable framework in 4SECURail.
- Trust is critical. The platform itself must be highly secure and tested / proven.
- The platform must gather and share in a practical way for all (easy access).

7.2.1.3 Other Support and Services

- Detection happens within organisations, so we need to identify what will trigger the sharing processes – receiving triggers (monitoring / notifications of incidents / threats, situational awareness).
- There should also be a long-term plan to add services in future, e.g. analytics etc.
- Proactive info sharing would ensure people are prepared (alerts, awareness bulletins).
- Legal obligations must be considered.
- Training is of interest (e.g. CSIRT formation), probably via the ER-ISAC/ENISA.
- Exchange of experience is a benefit, and helps to speak with one voice to manufacturers, so there must be sharing with ER-ISAC who will coordinate such aspects.

7.2.2 Future Implementation

7.2.2.1 Form of the Collaboration Group Relationship

- Technically, the easiest approach is that somebody hosts and supports the platform (a service), while actors in IM/RU security teams act like a sharing team.
- A “virtual” team model would be the most flexible, formed by EU Rail security stakeholders, having a primary contact at each company. This flexible approach can then be adopted into any initiative or organisation as required.
- It is the functionality that is most important - what it does and how.
- A group allowing direct and fast sharing (e.g. not via national CSIRTs) can be linked to any organisation at EU / sectoral level as EU collaboration develops. This would need a mandate from partners.
- The group should be driven by “leaders” in response.
- Collaborating with / linkage to the ER-ISAC would reduce overhead (same constituency).

7.2.2.2 Key Roles and Tasks in the Collaboration Group

- The main relevant roles/tasks are identifying alerts, communicating events (threats/intrusions), recording events (logging), maintaining a database.
- There are two sets of roles: platform hosting (maintain database and communication facilities, receive information to share, share information with relevant targets, provide centralised analysis); group collaboration (formation, participation in sharing).
- Actors in IM/RU identify risks and “share” to the virtual team via their point of contact.
- Point of contact is a key role – deciding what is to be shared and with whom.
- Platform actors can also channel other threat intelligence (news, bulletins, etc.).
- Some info may be for IM only / RU only / for all - this has to be managed.
- Technical experts adding data from authoritative data sources.

7.2.2.3 Technical Facilities

- Database and communications for holding and sharing security information.
- Collect from known threat databases and add new events and experiences.
- MISP is commonly used for the above functions and to link different work groups within rail companies, and so fulfils a few needs (should be considered).
- MISP can have multiple instances, allowing for a centralised reference instance, plus installed instances within participating IM/RUs.
- MISP allows for a rule-based filter to select what is required from feeds. This facility can be used within rail partners to target their analysis and can be used in a central instance to ensure selection of relevant information.
- This model would need a) technical support, and b) threat analyst – this could then support a network of primary contacts in railways (IM/RU) shaped as SOC, CSIRT or other team form.
- MISP clusters can even be coordinated within a company, and some railway actors are doing this, so coordination between companies would be made easier by following this model.
- Adopting MISP would require support for smaller companies to adopt (e.g. via ENISA).
- MISP allows automated usage of outputs, and so can be well integrated with company systems / processes.
- The platform must be secure and tested to ensure control of data.
- Cross organisational is not necessarily a big problem, so it should be kept simple but secure.

7.2.3 Membership

- The main participants should be IMs and RUs.
- Digital service providers (DSPs) are also a key element of secure rail IT/OT.
- Suppliers could be invited if their systems are implicated – especially those who operate systems for participants and provide close support.

7.2.4 Other Issues and Ideas

- Throughout the interviews it was questioned why the initiative is referred to as a “CSIRT” since that structure tends to be “within” organisations. It was recognised that EU Support for national CSIRTs was aimed at governmental bodies coordinating a range of ministries/ departments/ agencies: appropriate since the country government was in common. It was strongly suggested that a suitable name is required for the 4SECURail model and platform to indicate that it is a collaborative information sharing initiative between European rail cyber security actors. This guidance is accepted, and a name is offered later in this document (see model).

- The ER-ISAC works at a strategic level and is a membership organisation. 4SECURail operational collaboration model should acknowledge the ER-ISAC as complementary.
- The supply chain will analyse indicators of compromise (IoC) after events.
- Organisational contact points can "trigger" activities at operational level (via the collaborative platform) which later shares with ER-ISAC (what has happened).
- If future rail CSIRTs worked the same way, then that would be advantageous, and can be supported by ENISA / ER-ISAC.

7.2.5 Further Collaboration

All interviewees offer further support and collaboration, through developing links, providing support of different kinds, and further participating in the co-design and workshop actions.

Main Interview findings
Current and Future Needs / Collaboration Group • Collaboration is required primarily for exchange of threat intelligence. • Best form is a "virtual team", using hosted facilities. • Key roles: platform hosting (maintain database and communication facilities, receive information to share, share information with relevant targets, provide centralised analysis); group collaboration (formation, identifying contact points, participation in sharing). • Technical experts add data from authoritative data sources. • Membership should be IM/RU, with links to DSP and Suppliers
Issues around Sharing / Supporting Services • Sharing may have to be anonymised, and trust is critical for team success. • Organisations need to agree what triggers sharing - events and information of interest. • Identified items are alerts (incident or attempt), bulletins (security news), awareness. • Training and exchange of experience can be supported by ISC / ENISA
Technical Facilities • Database and communications for holding and sharing security information. • Target technology is MISP since it is already in use in rail. • MISP central instance linked to IM/RU local instances addresses requirements. • Rule-based filters can allow selection of preferred content. • Platform hosting should be secure and tested to ensure control of data
Additional Issues • Naming the initiative CSIRT is misleading, ad so new name is required. • Sharing with the ER-ISAC should be formalised

7.3 The first 4SECURail Workshop on Rail CSIRT

On June 9th, 2020 4SECURAIL organised a first workshop with several key stakeholders in European Rail Security. The 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 9th, 2020, from

10.00 am to 12.30 pm CEST, with 25 participants (16 external participants plus 9 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 and The Netherlands**) and the **UIC**; stakeholders from the CSIRT regulation such as **ENISA** and **ERA**; and representatives from the collaborator project **X2RAIL-3**.

This workshop was organised in the latest stages before completing this deliverable. The 4SECURail CSIRT team had already completed its initial survey and interviews as well as its background research period (as presented in the previous sections) and it was in the process of defining a draft CSIRT model and plans for a collaborative platform. This first draft model and outline collaboration platform was presented for open debate at this workshop. The open discussion and feedback received in the workshop is here presented and summarised, as it was carefully processed giving place to the 4SECURail CSIRT model. The workshop community will continue to be involved in project consultation towards completing the project, thus following a co-creation approach.

This workshop was the starting point for the creation of the key stakeholders' community, 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 aim to ensure that the outcomes of 4SECURail CSIRT feed forward towards a best common approach for collaborative rail cyber security by the CSIRT collaboration model and platform being collaboratively designed with the key stakeholders, as a resource for uptake.

Main workshop findings
Current and Future Needs / Collaboration Group • EU-ISAC vs EU-CSIRT are two different platforms and there is a need to understand the bridges and connections between both. These are two different organisations, but they need to work together. • Vision for staff: dedicated or a shared team, human resources to be involved; based in a physical site vs virtually connected.
Issues around Sharing / Supporting Services • Confidentiality, roles in terms of access to information by the stakeholders and how to protect the legal aspects for information sharing. The Legal requirements must be considered even beyond NIS. • Governance of the platform: o Who can and who cannot connect (outside EU) to the platform? o What are the rules to be able to connect and provide/receive information? o Obligations of the members and the platforms. o Reporting process. o Sovereignty aspects. • The role and involvement of the supply chain and digital service providers should be considered. • Roles and responsibilities within the model should be considered, including for example: o Decision-making in the information sharing and data flows. o Decisions on dissemination and access to information. o Legal responsibilities about the decisions taken and implications, liability.
Technical Facilities • Common architecture and products used in Rail, must be aligned with the process of onboarding and the role of the suppliers and DSPs in the CSIRT model. • Interoperability with existing platforms and processes in place (e.g. CSIRTs at the organisations, and

national level CERTs). • Automated information sharing, with input from the community and the option for members to choose what to share + one facilitator for contacts could be specified in the model. This should take into account the compromise between information overload and not missing what is relevant.
Additional Issues • Cooperation with X2RAIL-3 is essential, some aspects (e.g. legal) will be developed by X2RAIL-3 project which is responsible to develop a feasibility study on a pan-European CSIRT dedicated to rail.

7.4 Actions with stakeholders on Rail CSIRT draft model refinement

7.4.1 CSIRT Advisory Board

In 4SECURail project, the **Advisory Board is a group of external, independent experts** of recognized knowledge in different kinds of background and areas of expertise including market, technological trends and standards. The Advisory Board is in charge of discussing how the project will be able to provide relevant input and impact on the rail cybersecurity landscape and to contribute to the future mobility concept with railways as a backbone. The CSIRT Advisory Boards is compound of experts from DG MOVE, EXPLEO (CSIRT expert), CERVELLO (ex CISO Israel Railways) and UNIFE.

In this context, during the preparation of deliverable D3.1 “CSIRT model dedicated to railway: 1st release”, a meeting of the CSIRT Advisory Board was held in June 2020. The main contributions of the members were as follows:

- Sharing experiences is a key point **building trust between the stakeholders**: “you have to share something to get something”.
- Trust from the members need to be built, value must be shown. Gentlemen agreements could a way to start: “We can’t force people to share”.
- It is important to select the right cybersecurity partner to manage the CSIRT collaborative platform.
- The platform must **add value** – how the one consuming information could also help to improve the security measures. playbooks, documentation, etc.
- The challenge is to choose what is the **policy for publishing/prioritising** or not: problems with duplication, information overload, lack of added value from the information shared, etc.
- The platform is not the focus of the discussion: it is only one tool of building trust for sharing.

7.4.2 X2RAIL-3 / 4SECURail Collaboration Meetings

Following the release of deliverable D3.1 “CSIRT model dedicated to railway: 1st release” in June 2020, a series of collaboration meetings with X2RAIL-3 were organised between July and October, along with a review process on the D3.1 for X2RAIL-3 to provide detailed feedback on it towards addressing the remarks in the preparation of this final report D3.2 “CSIRT model dedicated to railway, final release”.

While X2RAIL-3 members already attended the first 4SECURail workshop on Rail CSIRT (see the previous section 7.3), a dedicated collaboration meeting with X2RAIL-3 was organised following the workshop for a more detailed discussion (July 9th 2020, online). Within this meeting, early feedback was provided by X2RAIL-3 to the main topics addressed by D3.1, but a formal review process for detailed feedback was organised for the next weeks: first, using an agreed template, the remarks, comments and observations from X2RAIL-3 members were received until the end of August 2020; second, the 4SECURAIL CSIRT team worked on these comments to enhance and advance on the corresponding aspects in the document to address such remarks and observations; and then, the response and actions taken for each comment were provided back to X2RAIL-3 for further discussion in the subsequent collaboration meetings.

In particular, a new collaboration meeting was organised in October (October 6th, 2020, online). In this meeting, X2RAIL-3 and 4SECURAIL CSIRT teams went through all the comments and remarks in order to agree on the actions taken and final improvements to be included in the final release.

7.4.3 3rd ER-ISAC General Assembly

In July 2020 the proceedings of the ER-ISAC third general assembly included a range of presentations and debates that brought various features of interest for capturing the vision of the key EU rail stakeholders towards our final CSIRT model after the first release (see deliverable D3.1):

ER-ISAC Platforms

The ER-ISAC has decided to deploy a "Generic IT Platform Services" to support ER-ISAC activity. The platforms are named as Knowledge Exchange (secure web, conferencing, discussion forum, shared planner, webinars, document sharing, mailing list and E-Learning), External Presentation (public website and reporting), Knowledge Selling Portal, Analysis & Collaboration (analysis tools and data exchange) and the corresponding Underlying Services (IAM, logging and monitoring, encryption, hardening, anti-malware and security testing). Several of these platforms might cover some of the focus of the proposed 4SECURail CSIRT platform, but the precise intention is not yet known and should be further investigated.

ENISA study on Cybersecurity in the Rail sector

ENISA provided an update on the ongoing study on Cybersecurity in the rail sector to be completed by the end of 2020. The main scope of the study is to identify the most critical areas of the railway system architecture. This survey, answered by 32 rail OES (IMs/RUs) in 23 Member States, identifies "most critical areas" specifically as:

- Security and Safety
- Pre-operations
    - Network allocation
- Operations
    - Signalling
    - Command and Control
    - Telecom
    - Auxiliary
    - Passenger comfort and services

The study also identifies the most important challenges for the rail sector as follows:

- Lack of digital and cybersecurity culture and awareness

- Strong dependencies with supply chain regarding technical and cybersecurity standards and requirements
- Specificities due to the nature of the distributed rail infrastructure and the existence of legacy systems
- Difficulty reconciling safety and cybersecurity worlds (accreditation, culture, jurisdiction)
- Costs: Need to find the right balance between security and both competitiveness and operational efficiency
- Complexity of regulatory ecosystem regarding cybersecurity: differences in national transposition of the NIS Directive

These critical areas and challenges are therefore primary cybersecurity concerns for a rail ER-CSIRT.

EUROCONTROL EATM-CERT

EUROCONTROL is an inter-governmental, pan-European, civil-military organisation dedicated to supporting the European Aviation sector. It is compound of 41 Member States and the European Union. The presentation from EUROCONTROL showed that its regional sectorial ATM-CERT combines cybersecurity and aviation domain expertise. Within this the stakeholders exchange mainly alerts and relevant incidents while the regional CERT provides cyber intelligence as well as logs and recommendations.

Shift2Rail Cybersecurity Activities (X2RAIL-3 & 4SECURail)

Shift2Rail Innovation Package 2 (Advanced Traffic Management & Control System) has defined a Technical Demonstrator (TD2.11) dedicated to Cyber Security. Within TD2.11 several Call For Members (CFM) projects (X2RAIL-1 and X2RAIL-3) as well as Open Call (OC) projects (CYRAIL and 4SECURaial) are contributing to propose a comprehensive cybersecurity framework for rail.

In this context X2RAIL-3 and 4SECURail initiatives are already linked by means of a Collaboration Agreement (COLA). Both presentations to the 3rd ER_ISAC General Assembly focussed on the information sharing process for the European Rail (ER) CSIRT Concept:

- On one hand, X2RAIL-3 task 9.7 is concentrated on defining what, when, why, who and how to share information with as well as the common criteria for ER-CSIRT/ISAC implementation as setup such as legal structure, governance, organisation, business model, etc.
- On the other hand, 4SECURail is concentrated on a) defining stakeholder requirements for an ER-CSIRT collaborative activity and to co-design with them an ER-CSIRT model and b) testing and validating the ER-CSIRT collaborative platform (most likely MISP) to support ER-CSIRT collaborative model.

RENFE Cyber Security Organisation

The presentation of **[RENFE, 2020]** showed emphasis on RU organisation dealing with IT and OT security issues and the relationship with ADIF, the Spanish Infra Manager. This “Information Security Organisation” shows CSIRT-type features. Services and capabilities of such organisation are emphasised, especially strategy and awareness, regulatory framework, coordination centre for incident management as well as additional services (ethical hacking, testing of products/services and intelligence analysis).

IP – Infraestruturas de Portugal NSOC Action

Infraestruturas de Portugal **[IP, 2020]** presented the Network and Security Operations Centre (NSOC-CSIRT) and showed the complexity of managing thousands of km of rail tracks and roads. The NSOC-CSIRT is responsible for cybersecurity incident response in public rail and roads as well as the cooperation with the CERT.PT, a service of the National Authority CNCS, as operator for Essential Services and Critical Infrastructures as well as Digital Service Providers. It also interacts with the National CSIRT network as country focussed ISACs.

Alstom – Contribution to the ER-ISAC initiative

The presentation of **[ALSTOM, 2020]** highlighted the possible areas of contribution of a train builder like Alstom to the development and consolidation of the ER-ISAC initiative. The areas of contribution are defined as follows:

- Cybersecurity White Papers
- Definition of railway cybersecurity context
- Definition of generic countermeasures
- Definition of railway cybersecurity architecture principles
- Common cybersecurity referential for railway equipment suppliers/manufacturer
- New innovative subjects such as cybersecurity and artificial intelligence and machine learning applied to railway systems.

The Empowering EU ISAC Consortium (isacs.eu)

The European Commission is fostering the establishment and development of EU ISACS across essential industrial sectors. The Empowering EU-ISAC Consortium aims to facilitate the set-up and further development of Information Sharing and Analysis Centers, ISACs. The mission of the ISAC Consortium is to:

- Empower European ISACS
- Promote horizontal structured coordination among various European ISACs.
- Offer business services and technical solutions to support ISACs in their daily operations.
- Mobilise public and private actors to establish and further develop European ISACs across different industry sectors.

The services to be offered by the ISAC Consortium are as follows:

- ORGANISATIONAL SUPPORT
    - Consult with Consortium business experts for ISAC's optimal structure and way of working.
- TECHNICAL SUPPORT & SOFTWARE SOLUTIONS
    - Use Consortium cloud-based toolkit to collaborate within sectorial ISAC members.
- CONFERENCES & WORKSHOPS
    - Get in touch with other sectorial ISACs to address contemporary issues to continuously improve ISAC's services.
- LEGAL SUPPORT
    - Get in touch with Consortium legal experts for an optimised governance for sectorial ISACs.

As an example of the Empowering EU ISAC Consortium activities, a Thematic Workshop session was held on October 5, 2020 to cover **the role of the ER-ISACs and the Community of European Railways (CER) in the Legislative and Regulatory Landscape**. It addressed the question of how an ISAC can be of added value by being the voice of their constituents in the (European) legislative and regulatory cybersecurity landscape.

The creation of the Empowering ISAC Consortium supported by the European Commission demonstrates the openness of the different European ISACs (aviation, railway, finance, maritime, etc.) to sharing and learning for strength.

8 Functionality statement: an information sharing and intelligence building model between EU rail security actors

8.1 Rationale: the CHIRP4Rail concept

Previous sections have presented the key needs identified in the desk research (section 6) and interactive research (surveys and interviews in section 7). As a conclusion of this research, this deliverable states that there is an evident need to coordinate information exchanges between rail cybersecurity teams for EU-wide cyber security: **the CHIRP4Rail concept** – Collaborative tHreat Intelligence Platform for Rail – 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). Furthermore, the exchange of data under the CHIRP4Rail concept should be "GDPR proof" (see section 9.2.4).

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.

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 establishing 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

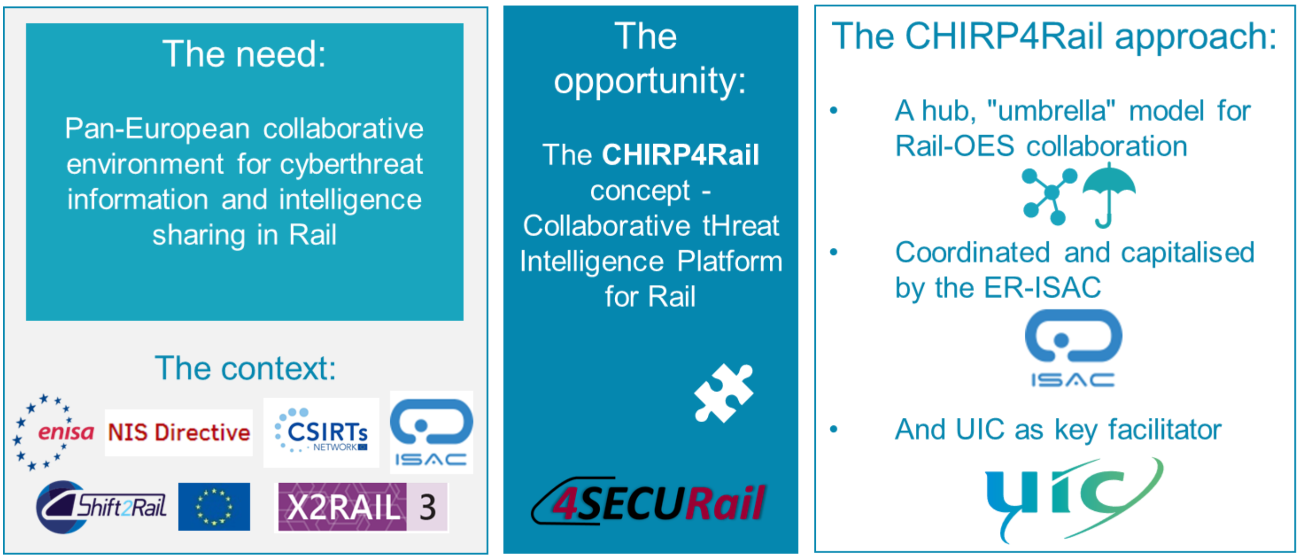
NIS directive, its general form and features are worthy of consideration in the context of the X2RAIL-3 and 4SECURail concerning a European Rail CSIRT collaborative platform

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 4:



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 4: The CHIRP4Rail concept rationale

This vision suggests a model that is data driven, horizontal and bottom up:

A. identifying what data is to be shared between rail security teams.
B. identifying an operational strategy to enable exchange, supported by technical and operational schemes.
C. identifying a suitable management model to facilitate and ensure both A and B.

The bottom-up approach for this model is schematised in Figure 5 below:

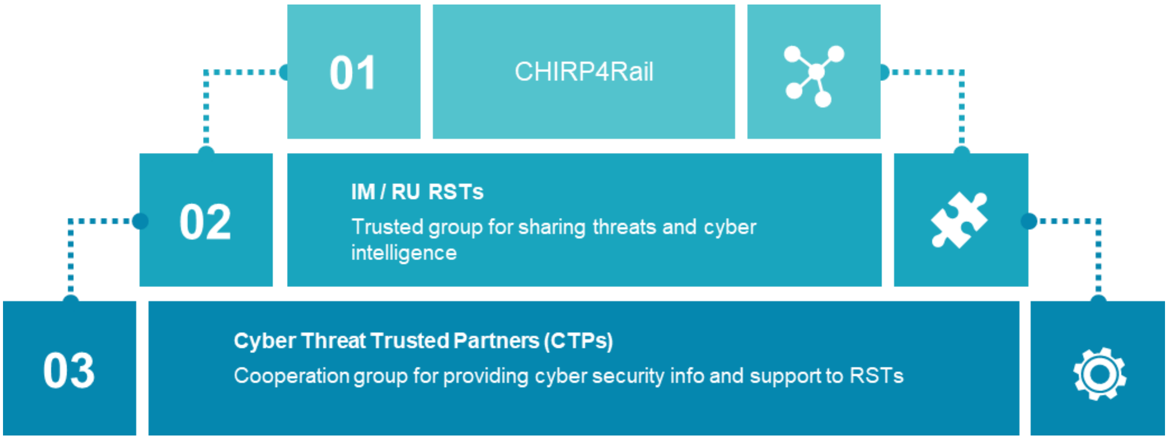

01
CHIRP4Rail
02
IM / RU RSTs
Trusted group for sharing threats and cyber intelligence
03
Cyber Threat Trusted Partners (CTPs)
Cooperation group for providing cyber security info and support to RSTs

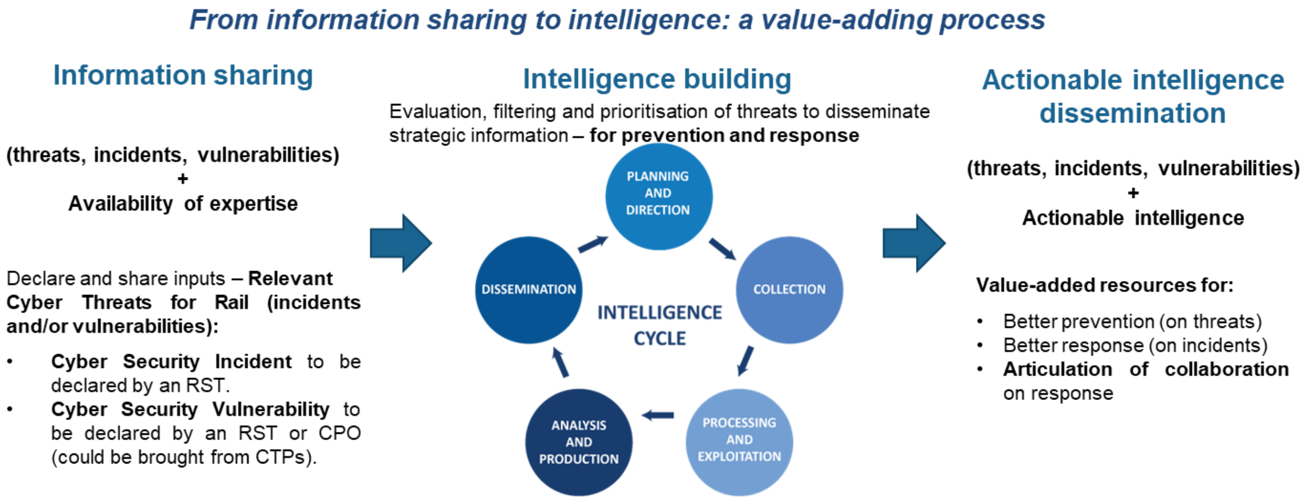
Figure 5: The CHIRP4Rail bottom-up approach

The information needs (A) have been identified in the various preceding analysis sections and are summarised in the next subsection, followed by a broad consideration of the necessary operational / technical support (B) to ensure easy and effective exchange. Confirmation / adjustment of these in the workshop and subsequent dialogue will support a more detailed determination of an appropriate management approach (C) which is initially outlined in section 9 below.

8.2 Functionality: from data and information exchange to intelligence

Based on the information collected in the reported activities (preceding sections), we identify the need for exchanges of different kinds of information, with implied data and flows identified. These are the primary determinants of the outline model provided later and will also determine to a significant degree the necessary operational and organisational features required to support such exchanges.

The vision of CHIRP4Rail, presented in Figure 6 below, is based on fostering and supporting a value-adding process evolution **from information sharing to intelligence**. On the basis of generating trust among the key actors for sharing information on relevant threats and incidents, such trust should be based on added value generated for the community as a whole. In order to achieve such vision, the process functionality will build from **aggregating and sharing inputs** (relevant cyber threats for Rail i.e. incidents declared by RSTs, and vulnerabilities by an RSTs, CPO, suppliers and DSPs; together with the availability of expertise), through a **process of evaluation, filtering and prioritisation** to disseminate **strategic information**, towards resulting on **actionable intelligence**, creating value-added resources **for prevention and response.**



From information sharing to intelligence: a value-adding process

Information sharing

(threats, incidents, vulnerabilities)
+
Availability of expertise

Declare and share inputs – **Relevant Cyber Threats for Rail (incidents and/or vulnerabilities):**

- **Cyber Security Incident** to be declared by an RST.
- **Cyber Security Vulnerability** to be declared by an RST or CPO (could be brought from CTPs).

Intelligence building

Evaluation, filtering and prioritisation of threats to disseminate strategic information – **for prevention and response**

Actionable intelligence dissemination

(threats, incidents, vulnerabilities)
+
Actionable intelligence

Value-added resources for:

- Better prevention (on threats)
- Better response (on incidents)
- **Articulation of collaboration** on response

Figure 6: The CHIPR4Rail functionality vision: from information sharing to intelligence

8.2.1 Registration / signup: declaring a Rail Security Team (RST)

A rail security team (RST) can be a member of the CHIRP4Rail aspect of a future ER-_CSIRT and can itself be formed as a CSIRT, CERT, SOC, or any other operational form. The RST should be able to declare:

- Organisational parent organisation
- Security Contact Point (SCP)
- Contact details.
- Description of its formulation.

There should be an approval process determined by the management stakeholders.

8.2.2 Information sharing

8.2.2.1 Declare Cyber Security Incident

An RST via its SCP can declare a security incident to have transpired, providing at least:

- Incident description.
- Identification of intrusion agent (e.g. specific malware if known).
- Identification of means of intrusion – if known – i.e. Indicator of Compromise (IoC).

The CHIPR4Rail model will detail the event model and the required fields for an incident notification. This is detailed in further sections (see section 9).

8.2.2.2 Declare Cyber Security Threat

An RST via its SCP can declare a new / changed cyber security threat. Threats may also be published by the central CHIRP4Rail, or identified from external sources like cyber threat intelligence providers such as national CERTs monitoring services, the cybersecurity industry feeds, etc.

8.2.2.3 Declare Cyber Security Vulnerability

An RST via its SCP can declare a new / changed cyber security vulnerability affecting their networks or equipment.

Vulnerabilities may also come from other actors in the ecosystem such as suppliers or digital service providers in rail.

8.2.3 Intelligence building: aggregation, analysis, filtering, prioritisation for a Rail Security Intelligence Database

With the gathering, analysis and prioritisation of the relevant information declared by RTSs and also intelligence developed by the CHIRP4Rail and external actors, the CHIRP4Rail operator team can make available to the members via SCPs, access to a database of threat intelligence of relevance to European Rail:

- Indicators of Compromise (IoC).
- Targeted attacks and attacks strategies of relevance.
- Threat intelligence of relevance.
- Vulnerability information.
- Correlation of malware, or attacks, or campaigns etc.
- Linked data model to support member's own analyses.
- Ability to share data (e.g. user has own database, easy export, etc.).
- Threat taxonomy for allowing teams to categorise quicker threats.
- Easy integration of the database with interested railway organisations.
- Allow pseudo-anonymous information in order to avoid spreading the name of an organisation involved in a security incident.
- Signatures and Rules such as Yara, Snort or Suricata and Sigma for early mitigation and detection of cyberattacks.

8.2.4 Actionable intelligence dissemination

8.2.4.1 Information Request (IR)

An RST via its SCP can make a request asking for more information to the community to support an analysis or to complete the information about a threat. There can be different types of information that can asked, such as:

- Request a sample (binary) of the malware for further analysis.
- Request more related samples of the malware.
- Request the context of the threat.
- Request more information about a threat.
- Request a technical analysis of the threat.
- Request detection signatures for the threat.
- Platforms such as MISP, address this requirement with a collaborative intelligence taxonomy which allows to tag an event with common needs of cybersecurity teams and threat intelligence analysts (e.g. malware samples, context, more information).

8.2.4.2 Security Intelligence Alert (SIA)

The ER-CSIRT can broadcast an alert to all members contact points (SCP) to share a declared security incident:

- Automated and sent to all (should this be moderated? – if so, how?)
- Automated and sent to selected targets/recipients (as above moderated?)

- Manual and sent by ER-CSIRT team member after checking.

Some additional discussion is needed (at workshops) to understand concerns / preferences.

8.2.4.3 Security Intelligence Bulletin (SIB)

The ER-CSIRT can broadcast news bulletins towards all members contact points (SCP) to share threat intelligence of different kinds:

- New cyber security threats.
- Changes to known cyber security threats.
- Sharing relevant alerts from supplier industry.
- Generating their own intelligence by analysing intern threats (i.e. not only broadcast Intelligence from external data sources).

8.3 Organisational Requirements: managing collaboration

The operational and technical coordination of exchanges between rail security teams in different railway organisations has been outlined in the preceding sections and is now considered as a management / organisational challenge.

This 'virtual' CSIRT should act as a hub by forwarding and coordinating intelligence among cross-border rail organisations and stakeholders in the EU. Besides, this CSIRT would also generate its own Cyber-intelligence. The purpose is to coordinate cross-border threat intelligence and cybersecurity incidents within the railway sector, acting as a centre of cybersecurity expertise, but without providing response to those incidents, assuming the majority of railway companies (IM and UR) have their own CSIRT teams established and operating.

This vision to a collaboration model is similar to the Europol model in Law Enforcement Agencies (LEA), where Europol supports the different agencies of the member states in intelligence and other activities, without prosecuting or starting investigations which is the role of the national and regional or local LEAs according to jurisdiction. Europol provides support, training, and at the same time they act as hub for exchanging intelligence among the EU members and their respective LEAs.

9 The CHIRP4Rail Model

9.1 Functional Model

The vision of the 4SECURail CHIRP4Rail concept, as previously presented in section 8.1, 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 7 below shows an overview of the 4SECURail functional model vision:

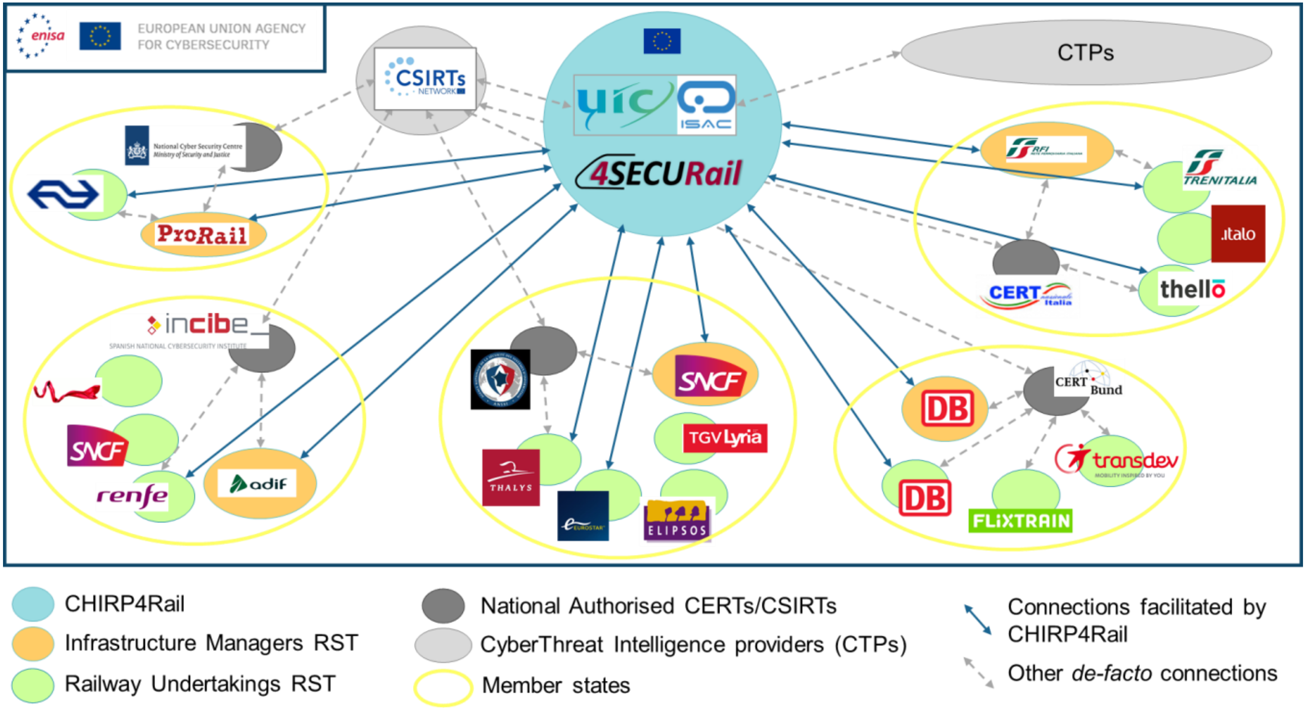

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY
CSIRTs NETWORK
uic
ISAC
4SECURail
CTPs
National Cyber Security Centre Ministry of Security and Justice
ProRail
RFI
TRENITALIA
italo
CERT Italia
thello
incibe
SPANISH NATIONAL CYBERSECURITY INSTITUTE
SNCF
renfe
adif
SNCF
TGV Lyria
THALYS
EUROSTAR
ELIPSOS
DB
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 7: 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 described in Annex 4 – Good practices in Threat Intelligence.

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 following sections identifies the organisational (section 9.2) and technical (section 9.3) aspects of the proposed CHIRP4Rail model.

9.2 Organisational model

9.2.1 Actors, roles and functions

The main actors involved in the model have been classified as:

- **IM / RU Rail Security Teams (RSTs)**: are the key participating members of the ER-CSIRT community. Formed as a CSIRT, CERT, SOC or any other existing operational form operating at national level.
- **The CHIRP4Rail Platform Operator (CPO)**: is the EU level Rail CSIRTs Threat Intelligence coordinator, thus operating at EU level with an intelligence coordination role. The CPO may take a twofold role:
  - **As the platform operator**: a horizontal role in support for the CHIRP4Rail platform.
  - **As an in-house analyst**: an executive role performing in-house threat intelligence tasks.
- **The ER-ISAC hosted by the UIC**: is the natural steerer of the model as the current initiative hosting the rail CSIRT community discussion, thus providing the ideal framework for the hosting of the CPO.

Other actors – as **Cyber Threat trusted Partners (CTPs)**: are those external trusted threat intelligence providers such as public bodies (e.g. National CERTs, European CSIRT Network –ECN–), rail Digital Service Providers, train builders, equipment suppliers, or commercial cybersecurity threat intelligence providers (e.g. cybersecurity industry).

The proposed model shall be expressed as an organisational form among these key actors, based on key role and main functions, as defined in the following table:

Actors	UIC/ER-ISAC	IM/RU RSTs	CTPs	CPO
Role	Steerer of the CHIRP4Rail Model	Main members of the CSIRT community	Trusted Partner (3rd parties)	Manager of the collaborative platform

Functions	• Manage the CHIRP4Rail Model • Coordinate with the European CSIRT Network (ECN	• Share relevant threats • Receive actionable intelligence • Coordinate with national CSIRT and rail DSPs and suppliers	• Share relevant vulnerabilities for rail • Coordinate with national CSIRT and RSTs • Consulted for analysis, investigation, mitigation and countermeasure	• Provide a secure communication platform • Guarantee voluntary and anonymous information sharing • Provide actionable intelligence • Provide technical support to RSTs and CTPs

9.2.2 Management and Services

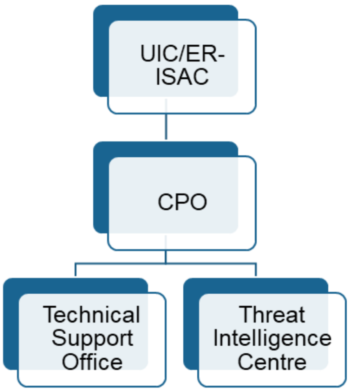
Based on the above proposed organisational model, the management structure should be simple and based on the ER-ISAC hosted by the UIC and the trusted CPO.

The **UIC and ER-ISAC** bodies should:

- Select the trusted CPO,
- Manage on day-to-day basis the selected CPO,
- Coordinate activities with the European CSIRT Network (ECN).

The **CPO** should provide the following services:

- Highly available and secure multiple communication channels.
- A secure platform (databases and tools) for information sharing and actionable intelligence dissemination.
- A technical office supporting all the actors involved.
- A centre for threat intelligence expertise.



9.2.3 Information and data workflow: a value-adding process

Figure 8 summarises the interconnections among the key actors involved in the information sharing process and the type of data and information provided on the different transactions:

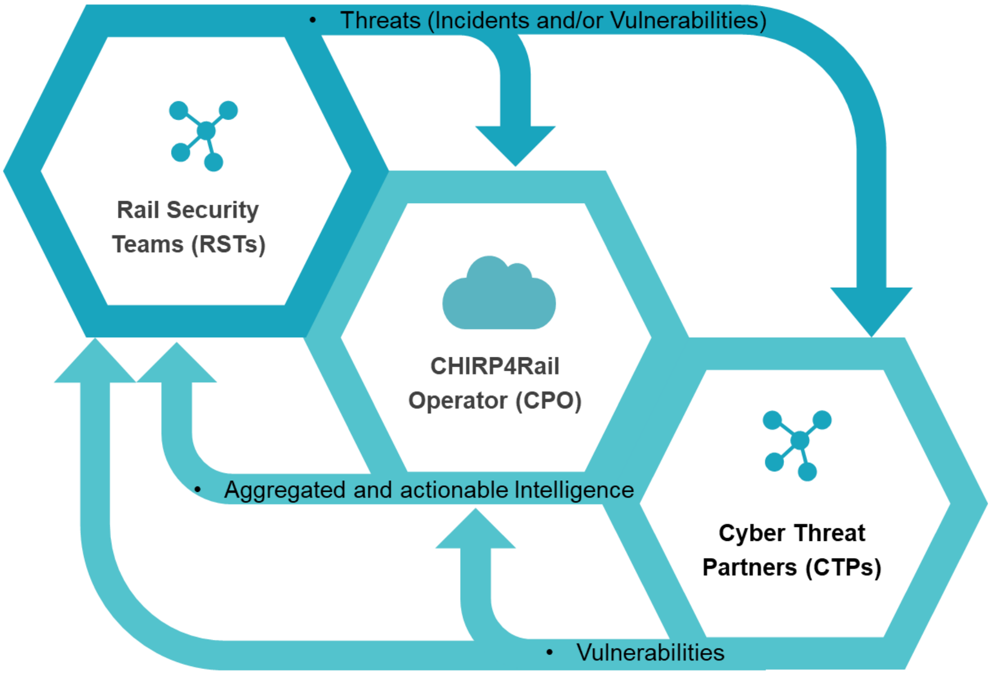

• Threats (Incidents and/or Vulnerabilities)
Rail Security Teams (RSTs)
CHIRP4Rail Operator (CPO)
Cyber Threat Partners (CTPs)
• Aggregated and actionable Intelligence
• Vulnerabilities

Figure 8: Schematic of connections among the key actors

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 9 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 10: The CHIRP4Rail process: low level view (detailed workflow):

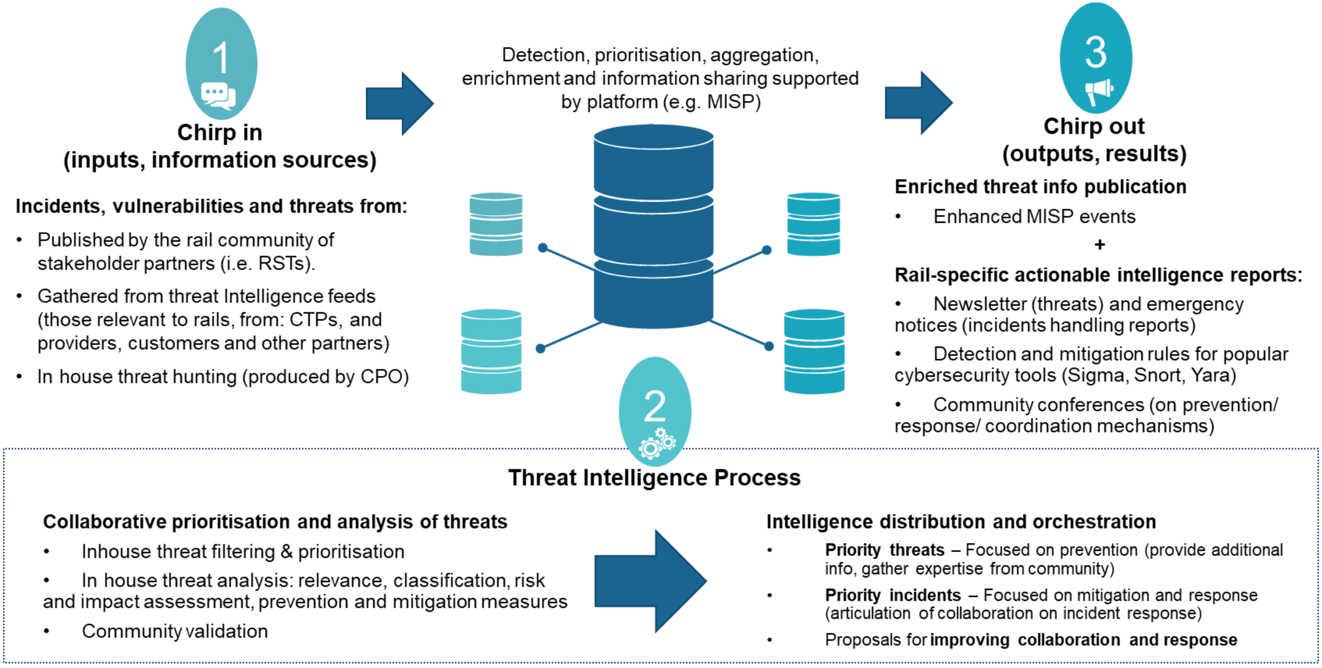

1
Chirp in
(inputs, information sources)
Incidents, vulnerabilities and threats from:
• Published by the rail community of stakeholder partners (i.e. RSTs).
• Gathered from threat Intelligence feeds (those relevant to rails, from: CTPs, and providers, customers and other partners)
• In house threat hunting (produced by CPO)
Detection, prioritisation, aggregation, enrichment and information sharing supported by platform (e.g. MISP)
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)
2
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 9: 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 10: The CHIRP4Rail process: low level view (detailed workflow)):

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 which 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.

STEP 3: CHIRP OUT (outputs, results)

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 10Figure 10: The CHIRP4Rail process: low level view (detailed workflow) below presents the detailed workflow diagram of the CHIRP4Rail process identifying and detailing the concepts previously described:

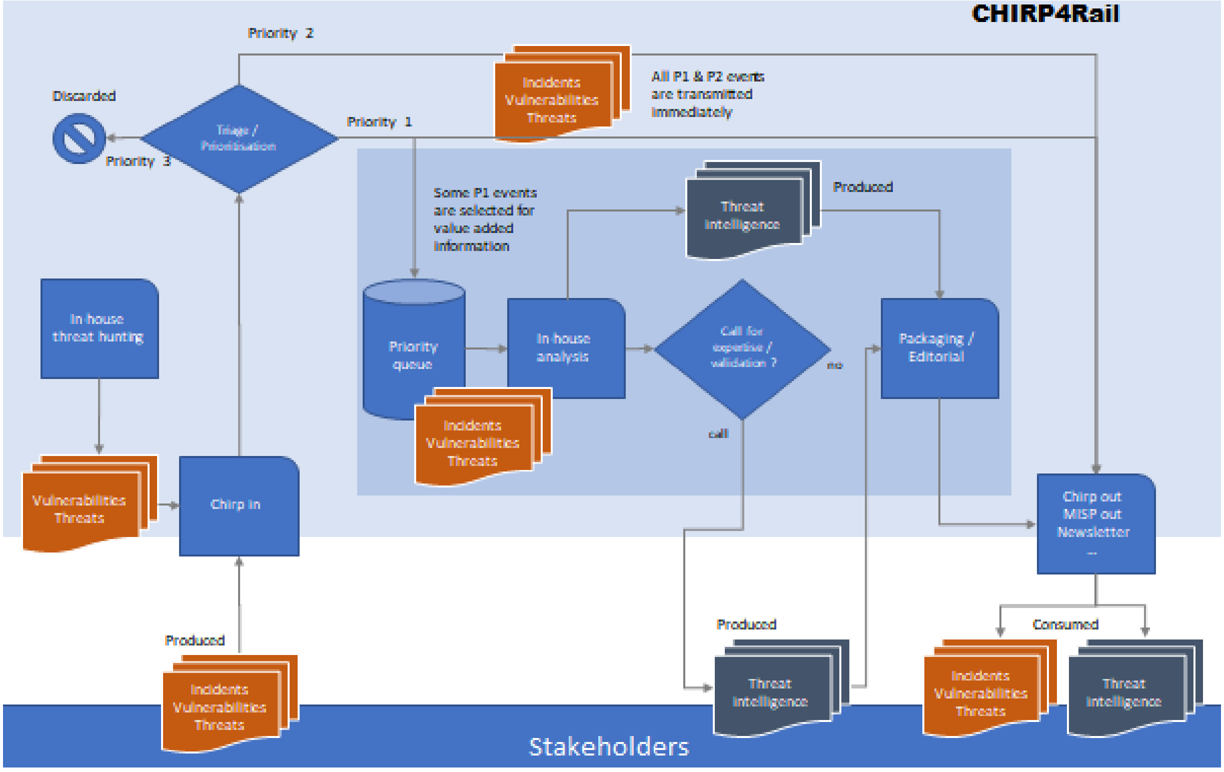

CHIRP4Rail
Priority 2
Discarded
Triage / Prioritisation
Priority 3
Priority 1
Incidents Vulnerabilities Threats
All P1 & P2 events are transmitted immediately
Some P1 events are selected for value added information
Threat intelligence
Produced
In house threat hunting
Priority queue
In house analysis
Call for expertise / validation ?
no
Packaging / Editorial
Incidents Vulnerabilities Threats
call
Vulnerabilities Threats
Chirp in
Chirp out MISP out Newsletter ...
Produced
Incidents Vulnerabilities Threats
Produced
Threat intelligence
Consumed
Incidents Vulnerabilities Threats
Threat intelligence
Stakeholders

Figure 10: The CHIRP4Rail process: low level view (detailed workflow)

9.2.4 GDPR and data privacy

The European General Data Protection Regulation [GDPR] looks after the protection of natural persons (citizens of the European Union) with regard to the processing of personal data and on the free movement of such data. The regulation was put into effect on May 25, 2018. Personal data is any information that relates to an individual who can be directly or indirectly identified. Names and email addresses are obviously personal data. Location information, ethnicity, gender, biometric data, religious beliefs, web cookies, and political opinions can also be personal data.

When processing personal data, seven protection and accountability principles have to be taken into account:

1. **Lawfulness, fairness and transparency** — Processing must be lawful, fair, and transparent to the data subject.
2. **Purpose limitation** —processing of data should take place for the legitimate purposes specified explicitly to the data subject when collected.
3. **Data minimization** —collection and processing of data should take place only as much as absolutely necessary for the purposes specified.
4. **Accuracy** — the personal data must be kept accurate and up to date.
5. **Storage limitation** — storage of personally identifying data may take place for as long as necessary for the specified purpose.
6. **Integrity and confidentiality** — Processing must be done in such a way as to ensure appropriate security, integrity, and confidentiality (e.g. by using encryption).
7. **Accountability** — The data controller is responsible for being able to demonstrate GDPR compliance with all of these principles.

The question that arises is whether the information that is being exchanged between the key actors under the CHIRP4Rail model should contain personal data or whether a reference to the (ab)use and role of personal data in the information that is exchanged, is sufficient.

In case it will be necessary and allowed to process personal data for the CHIRP4Rail purposes, the role of the respective actors will have to be considered, for example whether they act as Data Controller or Data (sub) Processor and/or whether their role might change along the exchange process.

The outcome of the forementioned investigations should be the guide for a decision on how to go (or not to go) about the need of processing personal data for purposes of the CHIRP4Rail platform and to verify whether such use would be allowed. In case all the before questions are positively responded, the respective actors should enter into an overall agreement that secures each of their compliance with the GDPR.

9.2.5 Stakeholders' adoption and involvement

In order to ensure that the stakeholders involved in the CHIRP4Rail model will be willing to provide the necessary inputs to make the CHIRP4Rail model a success, the management structure, basically the ER-ISAC hosted by the UIC and the trusted CPO, should define community engagement mechanisms to encourage contributions from the RSTs and the CTPs.

The main problems to be faced once the CHIRP4Rail platform will be implemented is first to ensure value-added and second to build confidence. Building trust among the stakeholders is essential not only for the success of the collaboration but also for the platform to provide added value to the RSTs community.

Another important challenge for CHIRP4Rail's adoption and stakeholders' involvement is expectation management. The CHIRP4Rail model will be acting in a very complex environment, managing collaboration between heterogenous stakeholders. In this context, it must be clear what CHIRP4Rail could offer, what the stakeholders can get and what the stakeholders need to give in order to take.

To enhance the trust building process and being able to manage stakeholders' expectations, several initiatives have been identified as follows:

9.2.5.1 ER-ISAC and UIC support

It is of capital importance to get full approval and support from the management of the ER-ISAC and the UIC. This support should be explicit and clearly disseminated to all the CISOs participating in the ER-ISAC initiative, either as members or as partners.

Dissemination activities could include official declarations from the ER-ISAC management board, web articles, webinars, case studies, white papers, social media (LinkedIn, twitter, Facebook, etc.), workshops, etc. Promotion of the CHIRP4Rail platform needs that major rail IMs and RUs, suppliers and decision-makers are fully aware of the initiative since the very early stages of the implementation, committed to its further support and involved in the collaboration environment.

9.2.5.2 Early adopters

The management of the ER-ISAC and the operator of the platform (CPO) should fully collaborate to get early adopters of the platform. Once the platform can get key early adopters, the platform will get traction and others will follow. The early adopters are expected to be the rail security teams (RSTs) from the big rail IMs and RUs, as they are in the natural leading position and have the power to lead the European RSTs community. They could also act as sponsors and users (RSTs) at the same time. Additionally, other ER-ISAC's partners, as for instance, big manufacturers and EU Agencies also qualify as early adopters as sponsors and/or users (CTPS) to get traction and momentum for the benefit of the platform.

9.2.5.3 Valuable information sharing

In a collaborative environment intended for information sharing, the added value comes from the information being shared. Although no specific and mandatory commitment should be requested for information sharing by the users of the platform, the participants should be committed to share only relevant and valuable important information to avoid noise and information overload in the platform.

9.2.5.4 Actionable intelligence reports

The best way to encourage users to participate in the platform is that they realize the value they will gain from using it. This is a process that takes time, but since the beginning, the platform should deliver not only information sharing but also actionable instructions on how to prevent or mitigate real threats relevant for the railway sector. If the platform can do so, the users will quickly start using it on a daily and practical basis.

9.2.5.5 Easy to use and secure trusted platform

To success, CHIRP4Rail should be a trusted platform. To achieve that objective, the CPO must guarantee an easy to use and highly secure platform.

The platform must be easy for users to access and to use it. The CPO should provide specific technical support to the users for coordinating and synchronising the user's cybersecurity platforms. For instance, in case of MISP usage, the users with their own MISP instances could be connected and synchronised with CHIRP4Rail's MISP by pushing events from their own MISP instances and vice versa.

Due to the sensitivity of the information that the CHIRP4Rail platform will hold, and the fact that it will contain data that relates to railway companies' vulnerabilities, it is essential to safeguard this data with the highest security methods. To guarantee the highest level of cybersecurity for the CHIRP4Rail platform, the platform must be accessible via Internet and/or a railway trusted virtual private network using secure IPsec protocol; therefore, only authorised users can connect. Two-factor authentication could also be implemented.

To be considered a trusted platform, CHIRP4Rail must also guarantee voluntary and anonymous sharing of threat intelligence information to allow stakeholders to freely share information. CHIRP4Rail must anonymously relay information from trusted members. Choice of anonymity must be context-dependent and linked to trust.

9.2.5.6 Training

The CPO managing the CHIRP4Rail platform should provide training in the platform to the RSTs. It will be helpful to gain adoption by the users and can be implemented from day one or at a later stage as the adoption process evolves.

9.2.5.7 Technical Forum

To properly operate and manage the CHIRP4Rail collaborative platform is not enough to be successful. It is also recommended to provide additional community tools such as a Technical Forum to encourage open discussions among the RSTs members. From a technical standpoint this forum would be independent from the CHIRP4Rail platform, but it would help in supporting open discussions among the RSTs members beyond information sharing features.

The technical forum could be organised in different subgroups for specific focused issues and could generate additional technical reports to CISOs and ER-ISAC members.

9.3 Technical model

Cybersecurity terms such as cyber-threats, vulnerabilities, and risks are often used for describing cybersecurity incidents and cyber-attacks. As defined in section 2.2, according to the [ENISA glossary]:

- **Cyber-threat** is "any circumstance or event with the potential to adversely impact an asset through unauthorized access, destruction, disclosure, modification of data, and/or denial of service".
- **Vulnerability** is used to refer to" 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".

As presented in the 4SECURail CSIRT vision, security teams need to share and to exchange information regarding threats, vulnerabilities and risks. It's crucial in the 4SECURail CSIRT model to assure a flexible data model where these concepts are mapped into a one single model. The 4SECURail CSIRT data model, taking the **[MISP data standard]** as a reference, will use a higher-level concept "**Event**", acting as a high-level entity grouping together the above-mentioned concepts (threat, vulnerability, risk).

For the further classification, 4SECURail will make use of the concept of **taxonomies, also used by MISP**. Taxonomies are used for organising and classifying different entities, and in this case, the 4SECURail taxonomy will be used within the "event" model for classifying cyber-threats focused on the rail sector, which might be related to an exploitation of a vulnerability and associated with one or more risks. Nevertheless, MISP standard provides a list of public taxonomies that are widely used for tagging the events such as the Admiralty Scale by NATO for evaluating the **reliability of a source**.

Although this data model has taken as a reference the format used by MISP, other Threat Intelligence formats are used in Threat Intelligence landscape, such as **[OpenDXL]** and **[STIX2.1]**. In order to assure format interoperability there are existing tools in the state of the art (including open source) for converting MISP format to others, and vice versa. Therefore, the 4SECURail will assure interoperability with existing standards and legacy systems and tools.

9.3.1 Event model

According to the **[MISP data standard]**, an event is a simple meta structure scheme where attributes and meta-data are embedded to compose a coherent set of indicators. An event can be composed from an incident, a security analysis report or a specific threat actor analysis. The event model is therefore flexible to admit a large variety of fields for supporting security teams to identify the different events that they might face. The meaning of an event only depends of the information embedded in the event.

The following sections summarise the data model used in 4SECURAIL. The information about the data model used is detailed at the MISP standard website (https://www.misp-standard.org/).

9.3.1.1 Core of the event

The following list summarizes the core fields in the 4SECURail event model

- **UUID**: a global identifier of an event.
- **ID**: id represents the human-readable identifier associated to the event for a specific MISP instance.
- **Published**: represents the event publication state. If the event was published, the published value MUST be true. In any other publication state, the published value MUST be false
- **Orgc**: represents the creator of the event. An Orgc object is composed of the following fields:
    - **Uuid**: represents the Universally Unique IDentifier (UUID) of the organisation. The organisation UUID is globally assigned to an organisation and shall be kept overtime.
    - **Name**: The name is a readable description of the organisation.
    - **Id**: The id is a human-readable identifier generated by the instance and used as reference in the event.
- **Org**: represents the current handler of the event on a specific instance. An Org object is composed of the following fields:
    - **Uuid**: represents the Universally Unique IDentifier (UUID) of the organisation. The organisation UUID is globally assigned to an organisation and shall be kept overtime.
    - **Name**: The name is a readable description of the organisation.
    - **Id**: The id is a human-readable identifier generated by the instance and used as reference in the event.
- **Date**: the date of occurrence of the event in ISO 8601 format (date only: YYYY-MM-DD).
- **Timestamp**: a reference time of creation or last updated. Timestamp is expressed in seconds since 1st of January 1970 (Unix timestamp). The time zone is UTC.
- **Publish_timestamp**: a reference time when the event was published on the instance. This value is expressed in seconds (decimal) since 1st of January 1970 (Unix timestamp). The time zone is UTC.
- **Threat Level id**: risk level of the event [low / medium / high].
- **Info**: brief and concise event description.
- **Tag**: classifies an event with a simple string (array accepting multiple values) – optional.
- **Distribution**: distribution represents the basic distribution rules of the event. This field might take the following values:
    - Your Organisation Only
    - This Community Only
    - Connected Communities
    - All Communities
    - Sharing Group
- **Sharing group id**: represents a human-readable identifier referencing a Sharing Group object that defines the distribution of the event.Analysis: current stage of the analysis of the event [Initial / ongoing / completed].
- **Attribute count**: represents the number of attributes in the event.
- **Extends_uuid**: represents which event is extended by this event. The extends_uuid is described as a Universally Unique IDentifier (UUID)

The MISP standard website provides more details for further explanation of the fields.

9.3.1.2 Event attributes

While the above list presents the fields that are core in the event, the model is kept flexible for further information details. Thus, an event entity may add attributes to extend the information and details. These attributes might be related to Indicators of Compromise (IoC's) such as hashes, filenames, IP's or domain names, but also with vulnerabilities or TTP's of attackers. Each attribute will have its own data model based in the following fields:

ID:
Represents the human-readable identifier associated to the event for a specific MISP instance.

Category:
This field describes the category of the attribute. The list of categories is based on the MISP format:

- **Antivirus detection**: all the info about how the malware is detected by the antivirus products
- **Artifacts dropped**: any artifact (files, registry keys etc.) dropped by the malware or other modifications to the system
- **Attribution**: identification of the group, organisation, or country behind the attack
- **External analysis**: any other result from additional analysis of the malware like tools output
- **Financial fraud**: information about finacial details (e.g bitcon address, IBAN, etc)
- **Internal reference**: reference used by the publishing party (e.g. ticket number)
- **Network activity**: information about network traffic generated by the malware
- **Payload delivery**: information about how the malware is delivered
- **Payload installation**: info on where the malware gets installed in the system
- **Payload type**: information about the final payload(s)
- **Persistence mechanism**: mechanisms used by the malware to start at boot
- **Social network**: social networks and platforms
- **Support Tool**: tools supporting analysis or detection of the event
- **Targeting data**: internal Attack Targeting and Compromise Information.
- **Person**: any reference to a person such as first name, last name, phone number, pgp public key, passport number, etc.
- **Other**: for cases where the above categories do not suit with the attribute found

Type:
This field describes what the attribute is. The list of attribute types is based on the MISP format and due to the extension, this has been detailed in Annex 3 – Attributes type in the MISP format.

Distribution:
Access control for the attribute. The attributes will inherit the level of distribution from the event by default, but the creator of the event can also control what attributes are can be seen by the community and which ones are only for internal use within the organisation. This field might take the following values:

- Your Organisation Only
- This Community Only
- Connected Communities

- All Communities
- Sharing Group

Value:
The value of the attribute.

UUID:
A global identifier of an attribute.

Comment:
This field will help to the audience to put into context the attribute.

Tag:
This field classifies an attribute with a simple string. This field is an array and it accepts multiple values. Its use is optional.

To_ids:
Represents whether the attribute is meant to be actionable and it can be used in automated process such as Host or Network Intrusion Detection Systems.

Event_id:
Represents a human-readable identifier referencing the Event object that the attribute belongs to.

Deleted:
Represents a setting that allows attributes to be revoked.

Data:
Contains the base64 encoded contents of an attachment or a malware sample. For malware samples, the sample must be encrypted using a password protected zip archive, with the password being "infected".

Related Attribute:
An array of attributes correlating with the current attribute.

Shadow Attribute:
An array of shadow attributes that serve as proposals by third parties to alter the containing attribute. The structure is similar to that of an Attribute, which can be accepted or discarded by the event creator. If accepted, the original attribute containing the shadow attribute is removed and the shadow attribute is converted into an attribute.

Sharing group id:
Represents a human-readable identifier referencing a Sharing Group object that defines the distribution of the attribute.

First_seen:

Represents a reference time when the attribute was first seen. *firstseen* is expressed as an ISO 8601 datetime up to the micro-second with time zone support.

Last_seen:
Represents a reference time when the attribute was last seen. *lastseen* is expressed as an ISO 8601 datetime up to the micro-second with time zone support

Timestamp:
This field represent a reference time when the event was created or last updated. Timestamp is expressed in seconds since 1st of January 1970 (Unix timestamp). The time zone must be UTC.

9.3.2 Tags

A tag is a simple method to classify an event with a simple string. The tag name can be freely chosen. The tag name can be also chosen from a fixed machine-tag vocabulary called [**MISP taxonomies**] as previously introduced at the beginning section 9.3.

9.3.3 Sighting

A sighting is an ascertainment which describes whether an attribute has been seen under a given set of conditions. The sighting can include the organisation who sighted the attribute or can be anonymised. This value might take the following values:

- 0: denotes an attribute which has been seen.
- 1: denotes an attribute which has been seen and confirmed as false-positive.
- 2: denotes an attribute which will be expired at the time of the sighting.

9.3.4 Taxonomies: CERT XLM map with SoTA of X-RAIL-EC1

The use of a taxonomy in the 4SECURail CSIRT Model will help to classify the events reported by the different organisations. This taxonomy will allow to understand better and quicker the events, summarizing 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 taking into account references such as the **[ISO 27005:2011]**, **[ENISA Threat Taxonomy]** and the **[BSI Threats Catalogue]**.

The selected taxonomy identifies the following categories, and for each of those, a set of possible threats, as reflected in the table below:

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

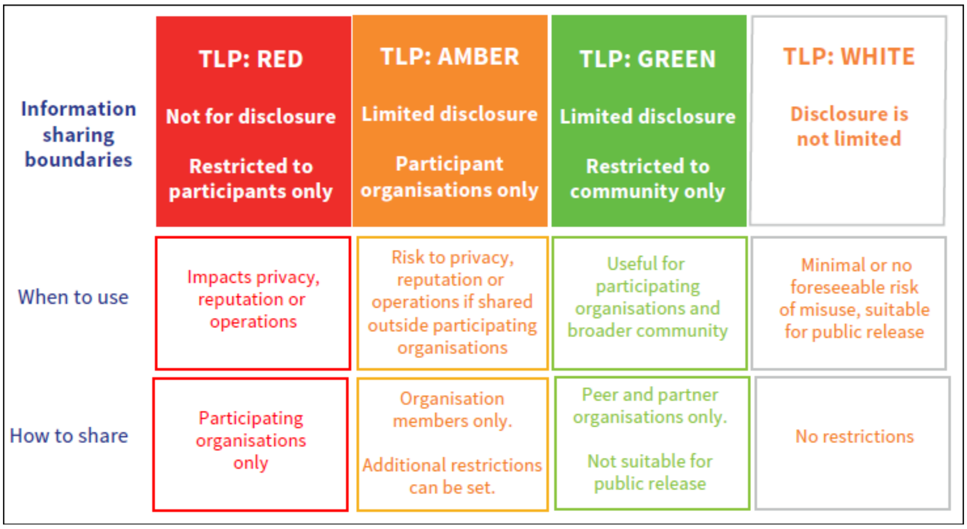
	• Disturbance due to radiation • Remote spying • Eavesdropping and reconnaissance • Theft of media, equipment or documents • Loss of media, equipment or documents • Retrieval of recycled or discarded media • Disclosure • Data from untrustworthy sources • Tampering with hardware • Tampering with software • 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

In the event model, as presented in the previous section, the field “Tag” will contain the value of the taxonomy with the following format: “Name of Taxonomy: Category": "Threat”. For instance, “X2-Rail-1: Unauthorised actions” =” Malicious software”.

9.3.5 Access control management

One of the requirements identified in the previous analysis is the need to provide a control mechanism for access to the data handled and shared along the threat intelligence process. Sensitivity of data in threat intelligence may differ depending on the nature or type of event, its severity, or the additional attributes and information provided.

In order to control how widely the information is allowed to be shared, it’s therefore highly recommendable to include as part of the model an indicator of the level of sensitivity of the information. To achieve this, the Traffic Light Protocol **[TLP]** will be used, which is popular among the intelligence community. This protocol (Figure 11) provides a simple and intuitive schema for indicating when and how sensitive information can be shared, facilitating more frequent and effective collaboration. In the event model, as presented in the previous section, the field “Tag” will contain the value of the TLP desired by the creator of the event.

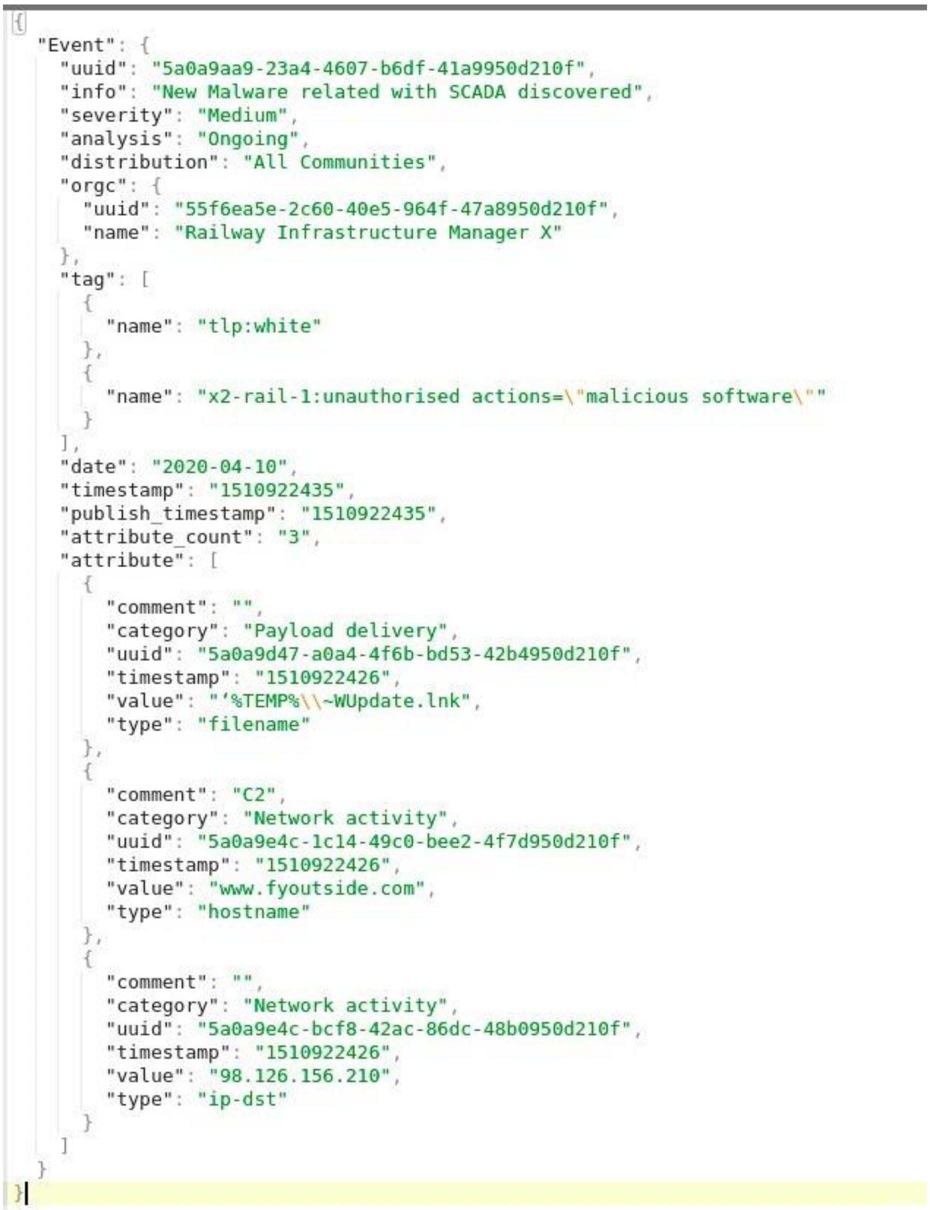


	TLP: RED	TLP: AMBER	TLP: GREEN	TLP: WHITE
Information sharing boundaries	Not for disclosure Restricted to participants only	Limited disclosure Participant organisations only	Limited disclosure Restricted to community only	Disclosure is not limited
When to use	Impacts privacy, reputation or operations	Risk to privacy, reputation or operations if shared outside participating organisations	Useful for participating organisations and broader community	Minimal or no foreseeable risk of misuse, suitable for public release
How to share	Participating organisations only	Organisation members only. Additional restrictions can be set.	Peer and partner organisations only. Not suitable for public release	No restrictions

Figure 11: Traffic Light Protocol scheme

9.3.6 Data model example

Figure 12 below shows an example of a 4SECURail Event model describing a new malware found by the Railway Infrastructure Manager X, as shown by the field “orgc”. The field “tag”, contains the value of Traffic Light Protocol (TLP), which in this case is green (Restricted to community only). A second “tag” is used to classify the type of threat shared according to the taxonomy as defined by X2Rail-1 (e.g. in this case the threat is classified as a “malicious software” within the category: “Unauthorised actions” of the X2-Rail-1 taxonomy).



```
{
  "Event": {
    "uuid": "5a0a9aa9-23a4-4607-b6df-41a9950d210f",
    "info": "New Malware related with SCADA discovered",
    "severity": "Medium",
    "analysis": "Ongoing",
    "distribution": "All Communities",
    "orgc": {
      "uuid": "55f6ea5e-2c60-40e5-964f-47a8950d210f",
      "name": "Railway Infrastructure Manager X"
    },
    "tag": [
      {
        "name": "tlp:white"
      },
      {
        "name": "x2-rail-1:unauthorised actions=\"malicious software\""
      }
    ],
    "date": "2020-04-10",
    "timestamp": "1510922435",
    "publish_timestamp": "1510922435",
    "attribute_count": "3",
    "attribute": [
      {
        "comment": "",
        "category": "Payload delivery",
        "uuid": "5a0a9d47-a0a4-4f6b-bd53-42b4950d210f",
        "timestamp": "1510922426",
        "value": "'%TEMP%\\~WUpdate.lnk",
        "type": "filename"
      },
      {
        "comment": "C2",
        "category": "Network activity",
        "uuid": "5a0a9e4c-1c14-49c0-bee2-4f7d950d210f",
        "timestamp": "1510922426",
        "value": "www.fyoutside.com",
        "type": "hostname"
      },
      {
        "comment": "",
        "category": "Network activity",
        "uuid": "5a0a9e4c-bcf8-42ac-86dc-48b0950d210f",
        "timestamp": "1510922426",
        "value": "98.126.156.210",
        "type": "ip-dst"
      }
    ]
  }
}
```

Figure 12: Example of 4SECURail Event model

On the other hand, the severity of this Event has been flagged as medium level, which implies that is something more specific that a common malware, such as an APT. The creator of this Event has also added 3 attributes regarding the network activity and the payload delivered by the malware.

9.3.7 Threat Intelligence Exchange communication protocol

Exchanging intelligence among trusted parts in a secure way is the critical point in the Threat Intelligence context. There are existing Threat Intelligence Exchanging protocols at the application level such as **[TAXII]**, **[OpenDXL]** or **[MISP Sync]**. These protocols use HTTPS as channel for exchanging communication, enabling organisations to share and exchange cyberthreat intelligence by defining an API with a common sharing model.

4SECURail acknowledges the existence of CSIRT information and Threat Intelligence Platforms (TIPs), and thus will seek interoperability with existing and legacy threat intelligence tools by assuring compliance with these communication protocols (providing specific connectors or bridges when required) widely adopted by the Cybersecurity community, thus allowing threat information exchange regardless the particular TIP used on each side of the communication.

10 Outline CHIRP4Rail Platform and future steps

Based on the preceding considerations, especially the model outlined in section 9 concerning information exchange, technical support, and operational level activities, this section outlines an early plan for the collaborative platform to be conceptualised and materialised in 4SECURail. This work is to be further elaborated in task T3.2 and D3.3, thus this deliverable provides only the early concepts, offered for consideration.

From the previous conclusions arising from the surveys and interviews, it has been made clear that information sharing is an essential part of the cybersecurity strategy and the CSIRT model conceived by 4SECURail should reflect 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. Technical solutions and platforms are used for sharing security relevant data, usually known as Threat Intelligence Platforms (TIP). There are many 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. The following section provides and overview of existing solution, concluding on a motivated selection for the 4SECURail approach.

10.1 Threat Intelligence Platforms (TIPs)

10.1.1 Review of existing TIPs

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 is presented in the table:

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 (at the time of this report) 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 anymore, an immature and experimental initiative, it has reached production environments and is used by many popular organisations such as NATO, FRST or CiviCERT (just to name a few), as well as many other private organisations.

It is however 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 will be easily transferable to and supported by any other TIP.

10.1.2 The Malware Information Sharing Platform (MISP)

The Malware Information Sharing Platform (MISP) is an open source Threat Intelligence platform. The project develops utilities and documentation for more effective Threat Intelligence, by sharing Indicators of Compromise. 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 will create an Event (Figure 13) and he 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, he will use an object to group those attributes together.

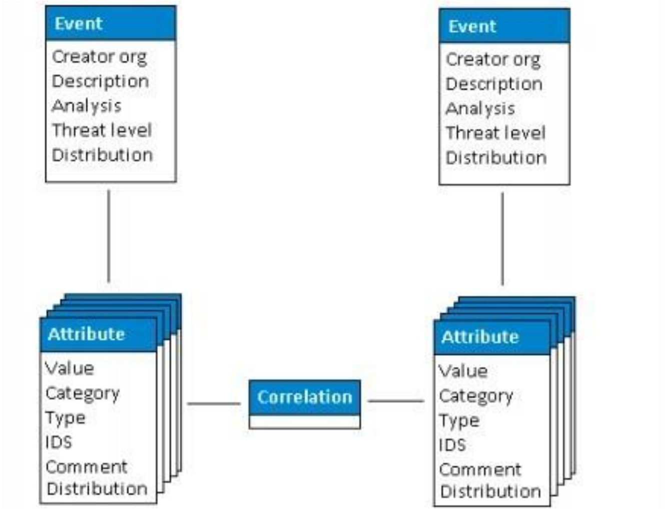


Figure 13: Event in MISP

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 14) for tagging properties in events or attributes.

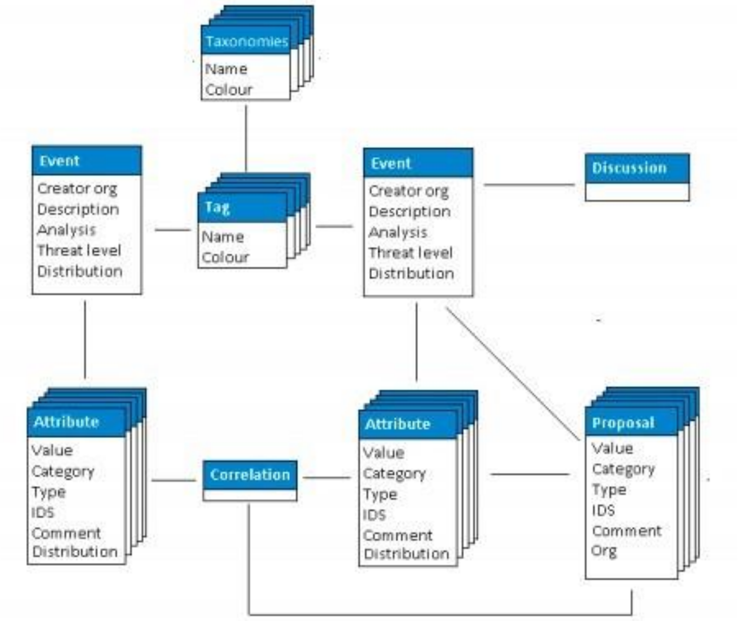


Figure 14: Taxonomies in MISP

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 15.

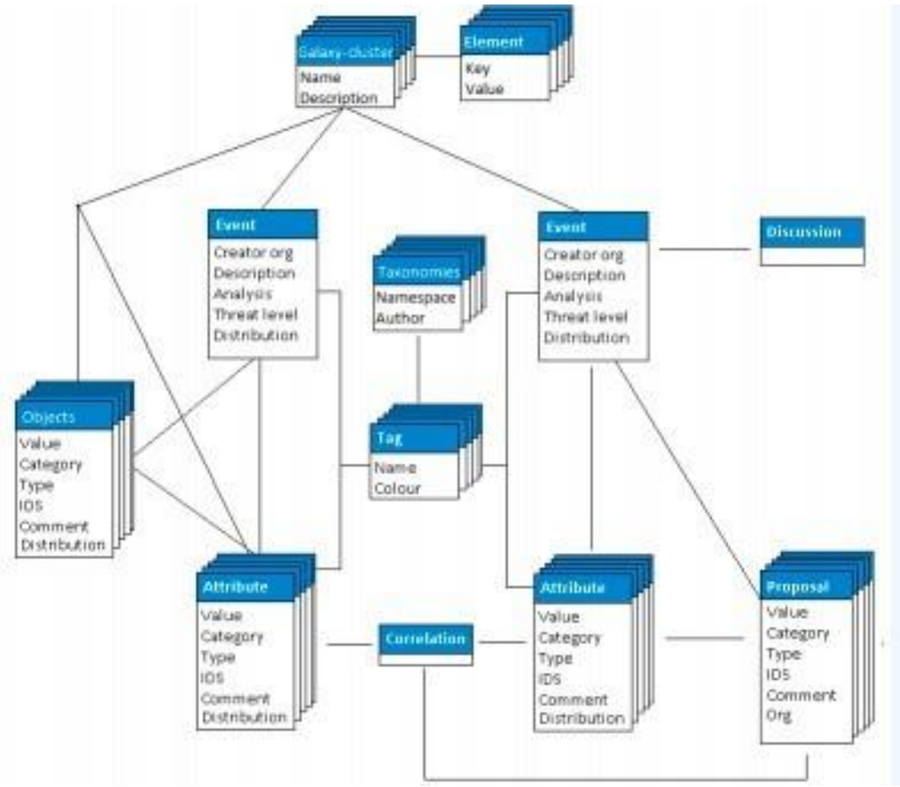


Figure 15: Galaxies (clusters) in MISP

Since MISP is a collaborative tool, it allows to propose attributes to events that were created by someone else and published to the instances of the community, as showed in Figure 14 and Figure 15. 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 customize its own MISP instance, configuring also with whom and what are the data that they want to share. The image shows an example of synchronisation between two instances.

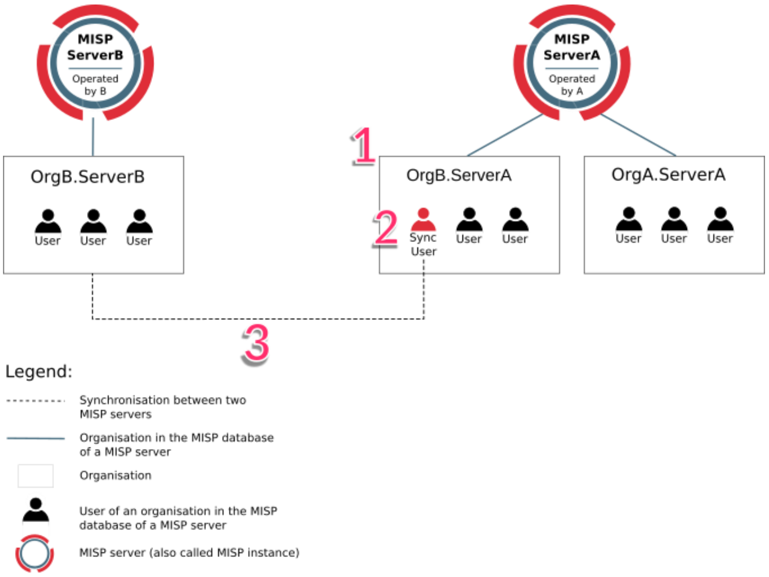

MISP
ServerB
Operated by B
MISP
ServerA
Operated by A
1
OrgB.ServerB
User
User
User
OrgB.ServerA
2
Sync User
User
User
OrgA.ServerA
User
User
User
3
Legend:
Synchronisation between two MISP servers
Organisation in the MISP database of a MISP server
Organisation
User of an organisation in the MISP database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

Figure 16: Sharing data between two MISP instances

Figure 16 above 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 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 API and a set of tools called MISP modules that extend the functionality of the platform, allowing to transform MISP Events to other formats and protocols used in Threat Intelligence information sharing such as STIX and TAXII, or even to transforms MISP Events into PDFs for other channels (e.g. email, SFTP, Collaboration tools, etc).

10.2 The CHIRP4Rail: Collaborative tHreat Intelligence Platform for Rail approach

Figure 17 illustrates the 4SECURail approach to a Collaborative tHreat Intelligence Platform for Rail approach (CHIRP4Rail) among different stakeholders in the railway sector at the European level.

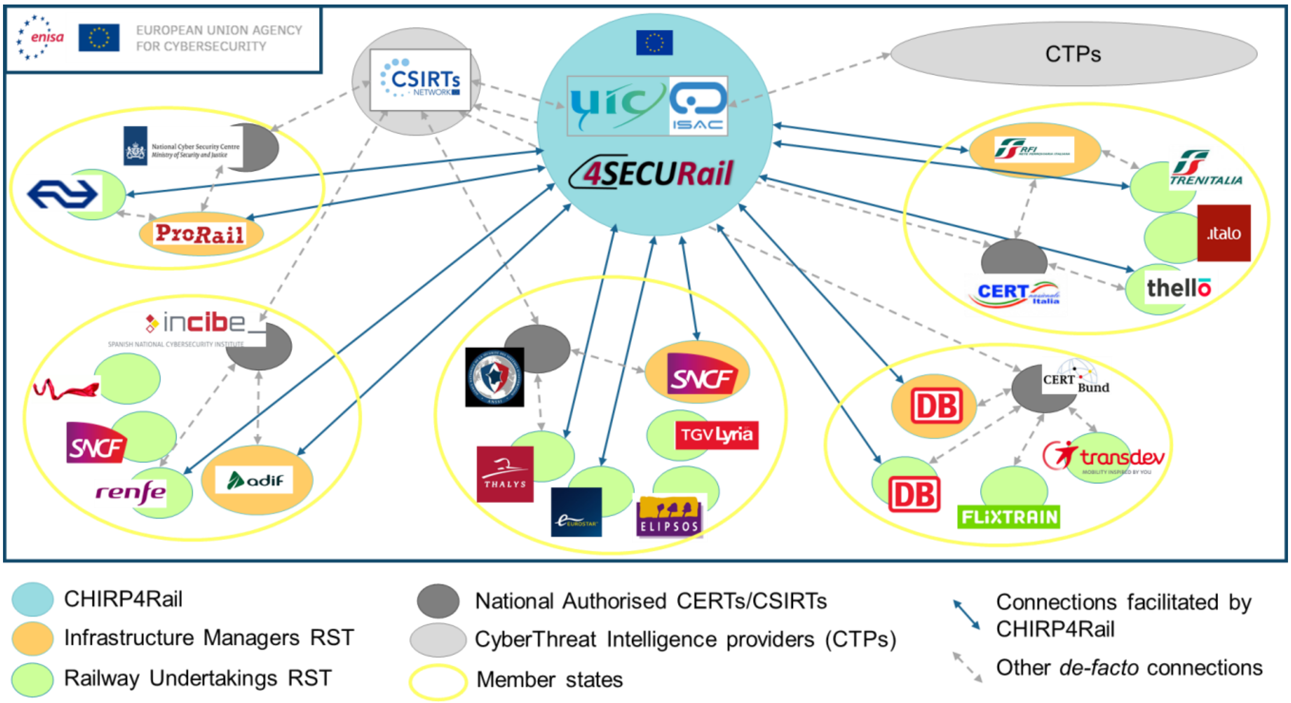

EUROPEAN UNION AGENCY FOR CYBERSECURITY
enisa
CSIRTs NETWORK
UIC
ISAC
4SECURail
CTPs
National Cyber Security Centre Ministry of Security and Justice
ProRail
RFI
TRENITALIA
italo
CERT Italia
thello
incibe
SPANISH NATIONAL CYBERSECURITY INSTITUTE
SNCF
renfe
adif
SNCF
TGV Lyria
THALYS
EUROSTAR
ELIPSOS
DB
CERT Bund
transdev
DB
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 17: 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.

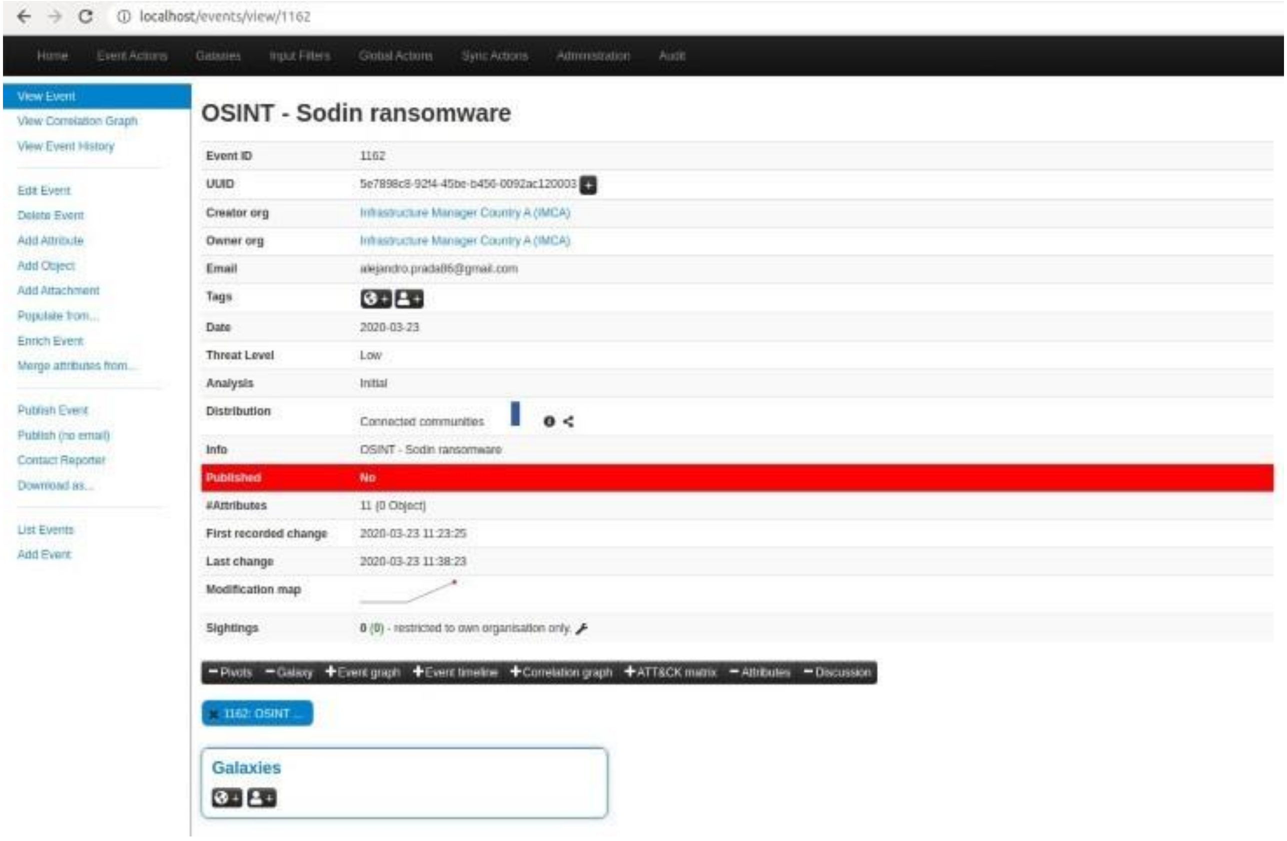
10.2.1 Sharing Intelligence among different entities

TIPs in general, and MISP in particular, allow to define communities for sharing information about threats or Indicators of Compromise (IoC) among different organisations. A community is composed of the local organisations on a MISP servers and the remote organisations connected by a MISP special user called “sync” users, which enables the synchronisation among members of the community.

In the case of 4SECURail, there could be one community for exchanging intelligence among the central instance of MISP and the infrastructure managers of each country, another one for exchanging intelligence among CHIRP4Rail the different Railway Undertaking and finally, one community which includes both types of organisation The CHIRP4Rail will be responsible of warning to the different organisations of potential threats and vulnerabilities that could have a potential impact in their infrastructures.

Although there is no need of having a MISP instance for each organisation, it is quite recommendable, since it gives more control of their data to the organisations. In case that an organisation doesn't host a MISP instance, they would have the alternative to be users in a TIP hosted by other organisation such as CHIRP4RAIL or even a TIP hosted by the IM of the country in the case of the RU's.

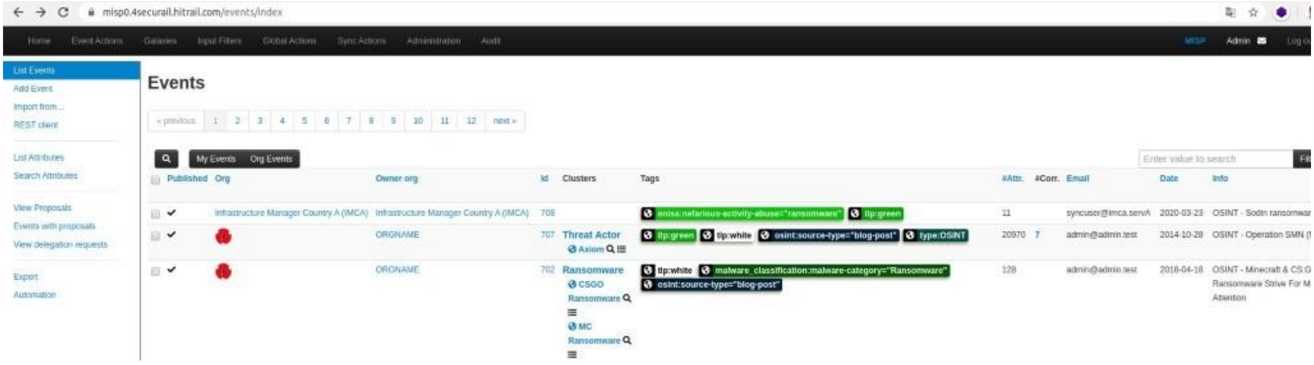
Using this approach, the security teams of rail organisations (RSTs in the IM's/RU's) within a community will be notified when an RST of any organisation publishes a new event with a potential threat. Figure 18 and Figure 19 show the synchronizations between 2 instances, e.g. the CHIRP4Rail and an IM MISP instance.



OSINT - Sodin ransomware

Event ID	1162
UUID	5e7898c8-92f4-45be-b456-0092ac120003
Creator org	Infrastructure Manager Country A (IMCA)
Owner org	Infrastructure Manager Country A (IMCA)
Email	alejandro.prada86@gmail.com
Tags	
Date	2020-03-23
Threat Level	Low
Analysis	Initial
Distribution	Connected communities
Info	OSINT - Sodin ransomware
Published	No
#Attributes	11 (0 Object)
First recorded change	2020-03-23 11:23:25
Last change	2020-03-23 11:38:23
Modification map	
Sightings	0 (0) - restricted to own organisation only.

Figure 18: 4SECURail MISP IM creates an event



Events

Published	Org	Owner org	Id	Clusters	Tags	#Attr.	#Corr.	Email	Date	Info
✓	Infrastructure Manager Country A (IMCA)	Infrastructure Manager Country A (IMCA)	708		enisa:nefarious-activity-abuse="ransomware" tlp:green	11		syncuser@imca.servA	2020-03-23	OSINT - Sodin ransomwar
✓		ORGNAME	707	Threat Actor Axiom	tlp:green tlp:white osint:source-type="blog-post" type:OSINT	20970	7	admin@admin.test	2014-10-28	OSINT - Operation SMN (I
✓		ORGNAME	702	Ransomware CSGO Ransomware MC Ransomware	tlp:white malware_classification:malware-category="Ransomware" osint:source-type="blog-post"	128		admin@admin.test	2016-04-18	OSINT - Minecraft & CS:G Ransomware Strive For M Attention

Figure 19: CHIRP4Rail – MISP Central Instance receives the event automatically

10.2.2 Key aspects of the Threat Intelligence Sharing Platform

10.2.2.1 Updated database of known threats and mitigation

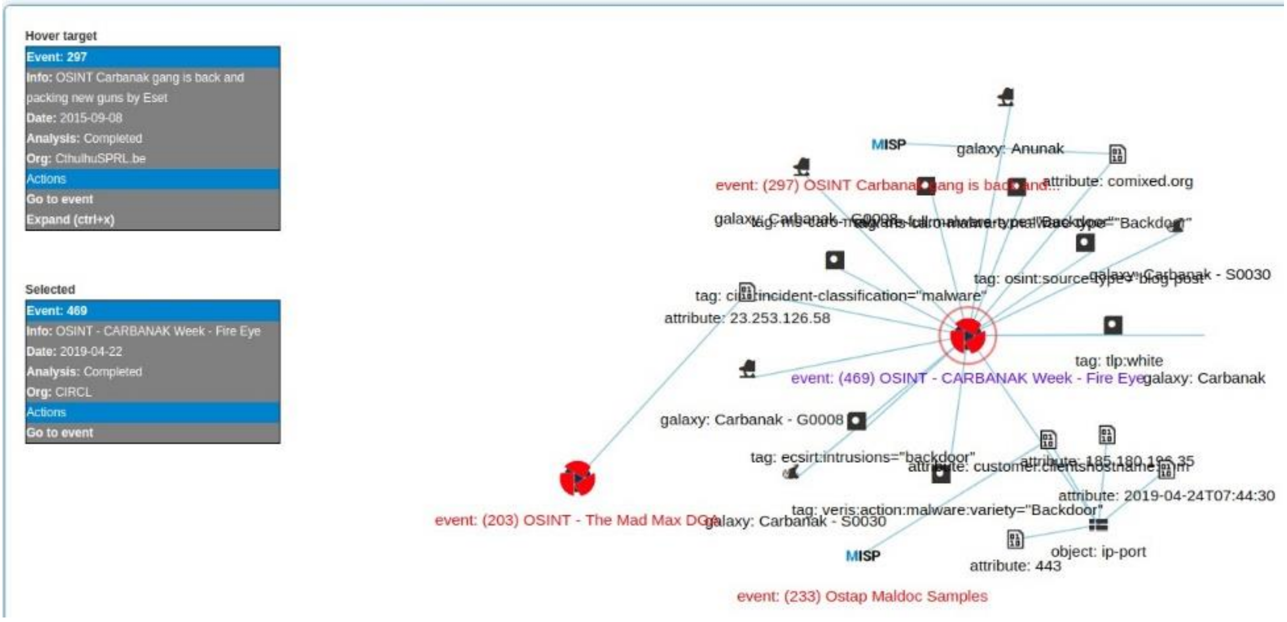
One advantage of MISP is the possibility to import threats and alerts from remote sources in an easy way. MISP allows to connect with other MISP communities, such as the CIRCL community, that is very active on MISP. It also provides a Python library, PyMISP, that allows to import threats and alerts automatically from other sources that are not using MISP, such as the ICS-CERT, the United States CERT for Critical Infrastructures that uses STIX. This feature will allow to the CHIRP4RAIL to be aware of last threats and vulnerabilities in IT/OT reported by public and private organisations.

10.2.2.2 Generating announcements of new threats or availability of support information

MISP provides a mechanism for receiving alerts every time there is a new event from a remote instance pushed to the system or someone add and event in the local instance. This functionality allows to the teams to be up to date of new events and threats, as well as corresponding possible countermeasures and mitigations measures.

10.2.2.3 Correlation of Events

Analyst at the different organisations can take advantage of the automatic correlation of events, making possible to find relationships between attributes and indicators of compromise. The platform provides a functionality to show the correlation of events as a graph (Figure 20), making easier to the user to find “matches” among different incidents.



Hover target

Event: 297
Info: OSINT Carbanak gang is back and packing new guns by Eset
Date: 2015-09-08
Analysis: Completed
Org: CthulhuSPRL.be
Actions
Go to event
Expand (ctrl+x)

Selected

Event: 469
Info: OSINT - CARBANAK Week - Fire Eye
Date: 2019-04-22
Analysis: Completed
Org: CIRCL
Actions
Go to event

MISP
galaxy: Anunak
event: (297) OSINT Carbanak gang is back and...
attribute: comixed.org
tag: osint:source-type="blog-post"
galaxy: Carbanak - S0030
tag: circl:incident-classification="malware"
attribute: 23.253.126.58
tag: tlp:white
event: (469) OSINT - CARBANAK Week - Fire Eye
galaxy: Carbanak
galaxy: Carbanak - G0008
tag: ecsirt:intrusions="backdoor"
attribute: customer.clientshostname.com
attribute: 185.180.196.35
attribute: 2019-04-24T07:44:30
tag: veris:action:malware:variety="Backdoor"
event: (203) OSINT - The Mad Max DGA
galaxy: Carbanak - S0030
MISP
object: ip-port
attribute: 443
event: (233) Ostap Maldoc Samples

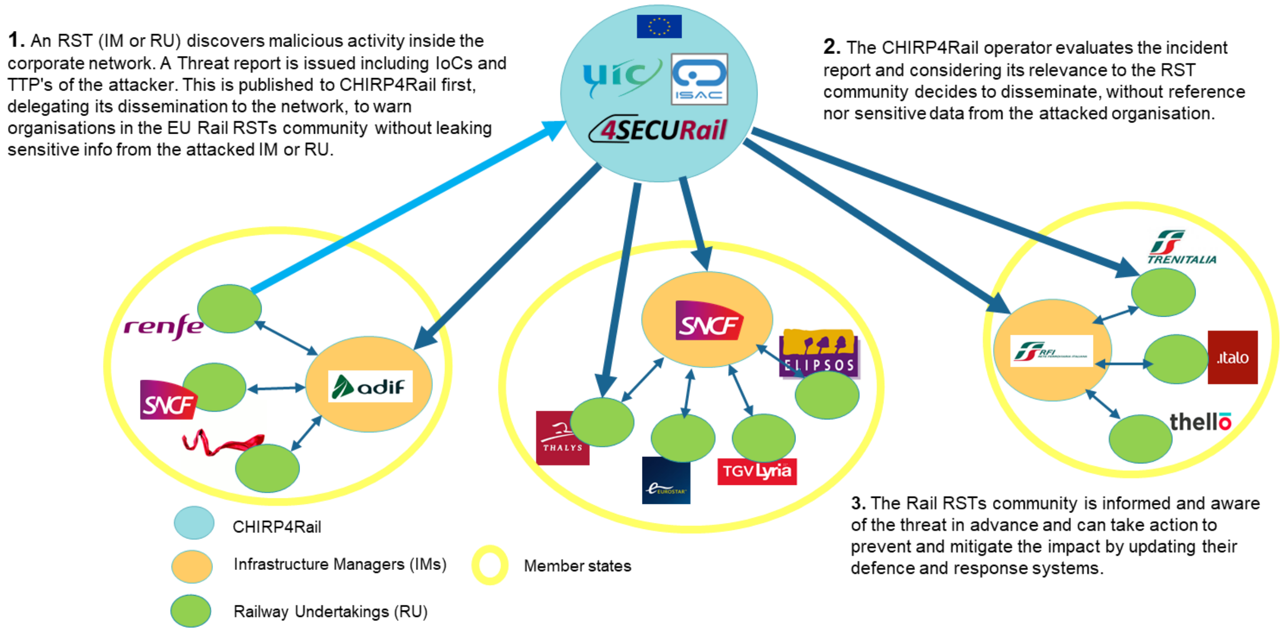
Figure 20: Correlation graph functionality

10.2.2.4 Flexible format

The platform allows different formats such as MISP, STIX, OpenIOC, CSV, Plain text, JSON or XML. Besides, analyst can export rules to popular IDS (Intrusion Detection Systems) such as Snort, Suricata or Bro.

10.2.2.5 Delegation of publication

In some situations, an organisation wants to alert of an incident without linking their name to the event due to sensitivity issues. MISP allows to delegate the publication of an event to other organisations. IM's and RU's will delegate the publication of an event to the CHIRP4RAIL. Figure 21 below shows the process of delegating the publications of an event within the community without associating the name of the organisation affected.



1. An RST (IM or RU) discovers malicious activity inside the corporate network. A Threat report is issued including IoCs and TTP's of the attacker. This is published to CHIRP4Rail first, delegating its dissemination to the network, to warn organisations in the EU Rail RSTs community without leaking sensitive info from the attacked IM or RU.

2. The CHIRP4Rail operator evaluates the incident report and considering its relevance to the RST community decides to disseminate, without reference nor sensitive data from the attacked organisation.

3. The Rail RSTs community is informed and aware of the threat in advance and can take action to prevent and mitigate the impact by updating their defence and response systems.

Figure 21: Sharing an incident without exposing the identity of victim to the community

10.2.2.6 Customisation

One of the best parts of MISP, is the possibility of adding new features using "MISP modules". These modules are autonomous modules that can be used for expanding the functionalities of the platform, as well as to import and export data. Currently there is a list of an available modules that enables integration with well-known cybersecurity tools such as Shodan, Yara, VirusTotal or event Maltego, that can be used for further analysis of attacks. An example is presented in Figure 22:

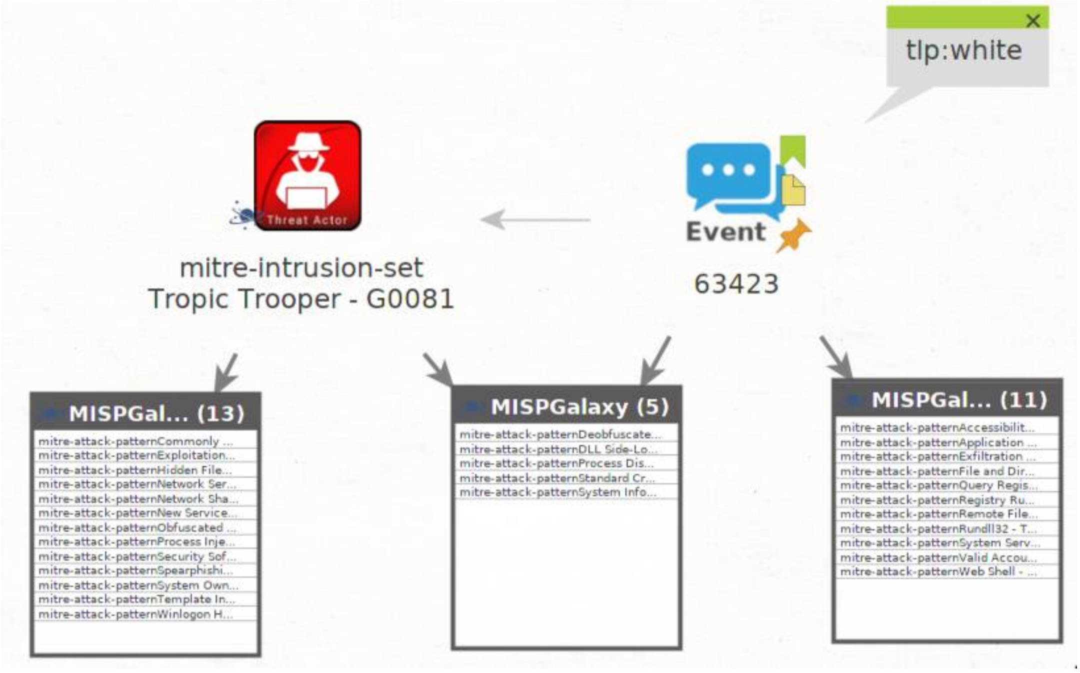

tlp:white
Threat Actor
mitre-intrusion-set
Tropic Trooper - G0081
Event
63423
MISPGal... (13)
mitre-attack-patternCommonly ...
mitre-attack-patternExploitation...
mitre-attack-patternHidden File...
mitre-attack-patternNetwork Ser...
mitre-attack-patternNetwork Sha...
mitre-attack-patternNew Service...
mitre-attack-patternObfuscated ...
mitre-attack-patternProcess Inje...
mitre-attack-patternSecurity Sof...
mitre-attack-patternSpearphishi...
mitre-attack-patternSystem Own...
mitre-attack-patternTemplate In...
mitre-attack-patternWinlogon H...
MISPGalaxy (5)
mitre-attack-patternDeobfuscate...
mitre-attack-patternDLL Side-Lo...
mitre-attack-patternProcess Dis...
mitre-attack-patternStandard Cr...
mitre-attack-patternSystem Info...
MISPGal... (11)
mitre-attack-patternAccessibilit...
mitre-attack-patternApplication ...
mitre-attack-patternExfiltration ...
mitre-attack-patternFile and Dir...
mitre-attack-patternQuery Regis...
mitre-attack-patternRegistry Ru...
mitre-attack-patternRemote File...
mitre-attack-patternRundll32 - T...
mitre-attack-patternSystem Serv...
mitre-attack-patternValid Accou...
mitre-attack-patternWeb Shell - ...

Figure 22: Integration with Maltego for analysing of an attack in a visual way

Besides this official list of MISP modules, organisations can develop their own modules for integrating MISP with their tools and adapt it to their cybersecurity processes and technologies.

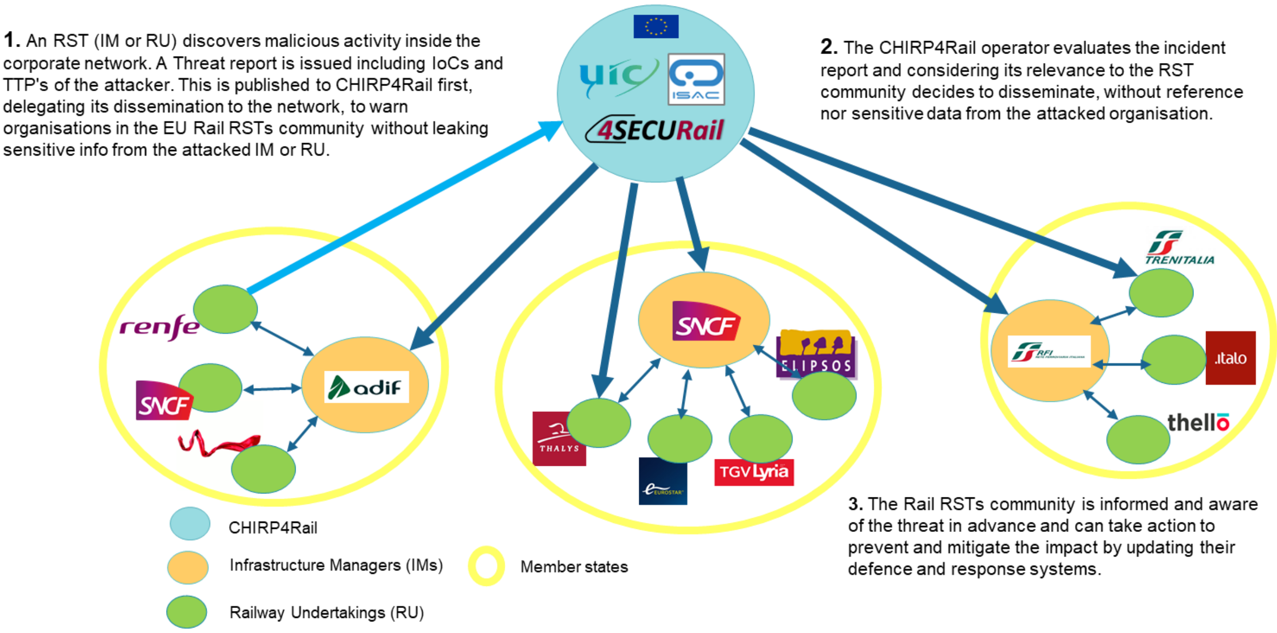
10.2.3 Exemplifying use cases for the Threat Intelligence Sharing Platform (dataflows)

The final section proposes a few scenarios as exemplifying workflows use cases for the purpose of showcasing how the CHIPR4Rail model and platform could be operated as well as for testing and evaluating the good practises implemented during the project for sharing Cyber-Threat Intelligence in the railway sector.

10.2.3.1 Scenario 1: incident report from a Railway Operator.

There aren't many public incidents in this sector, but in May of 2018, the Danish state rail operator was hit by a DDoS cyberattack, causing a breakdown which prevented train passengers across the country from buying tickets on that day.

This scenario, presented in Figure 23, represents information sharing of a cyber-security incident in the network of a RST, the steps and procedures to inform the community without compromising the reputation of the victim nor the operator, supporting CSIRT operations and threat intelligence.



1. An RST (IM or RU) discovers malicious activity inside the corporate network. A Threat report is issued including IoCs and TTP's of the attacker. This is published to CHIRP4Rail first, delegating its dissemination to the network, to warn organisations in the EU Rail RSTs community without leaking sensitive info from the attacked IM or RU.

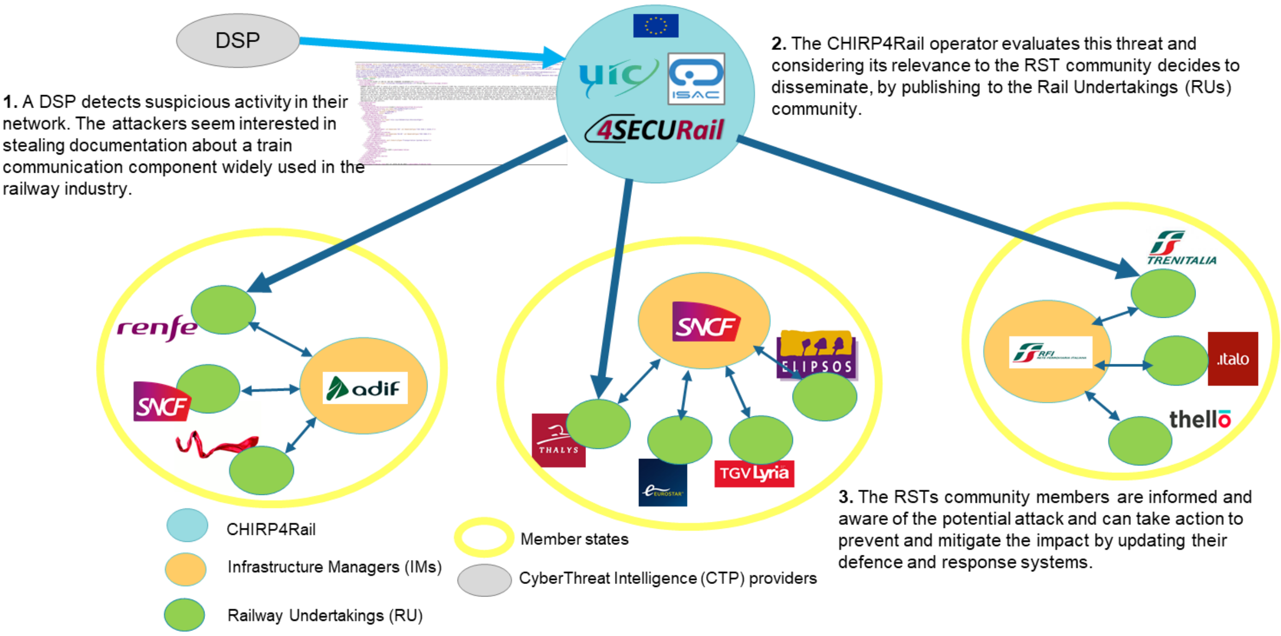
2. The CHIRP4Rail operator evaluates the incident report and considering its relevance to the RST community decides to disseminate, without reference nor sensitive data from the attacked organisation.

3. The Rail RSTs community is informed and aware of the threat in advance and can take action to prevent and mitigate the impact by updating their defence and response systems.

Figure 23: Scenario 1 – incident report from a Railway Operator

10.2.3.2 Scenario 2: railway APT declared by a Digital Service Provider

This scenario, presented in Figure 24, presents information sharing of a cyber-security incident in the network of a DSP. As an external stakeholder (not directly a RST, but a member of the supply chain), the steps and procedures to inform the community are handled by the CHIPR4Rail Platform Operator (CPO).



1. A DSP detects suspicious activity in their network. The attackers seem interested in stealing documentation about a train communication component widely used in the railway industry.

2. The CHIRP4Rail operator evaluates this threat and considering its relevance to the RST community decides to disseminate, by publishing to the Rail Undertakings (RUs) community.

3. The RSTs community members are informed and aware of the potential attack and can take action to prevent and mitigate the impact by updating their defence and response systems.

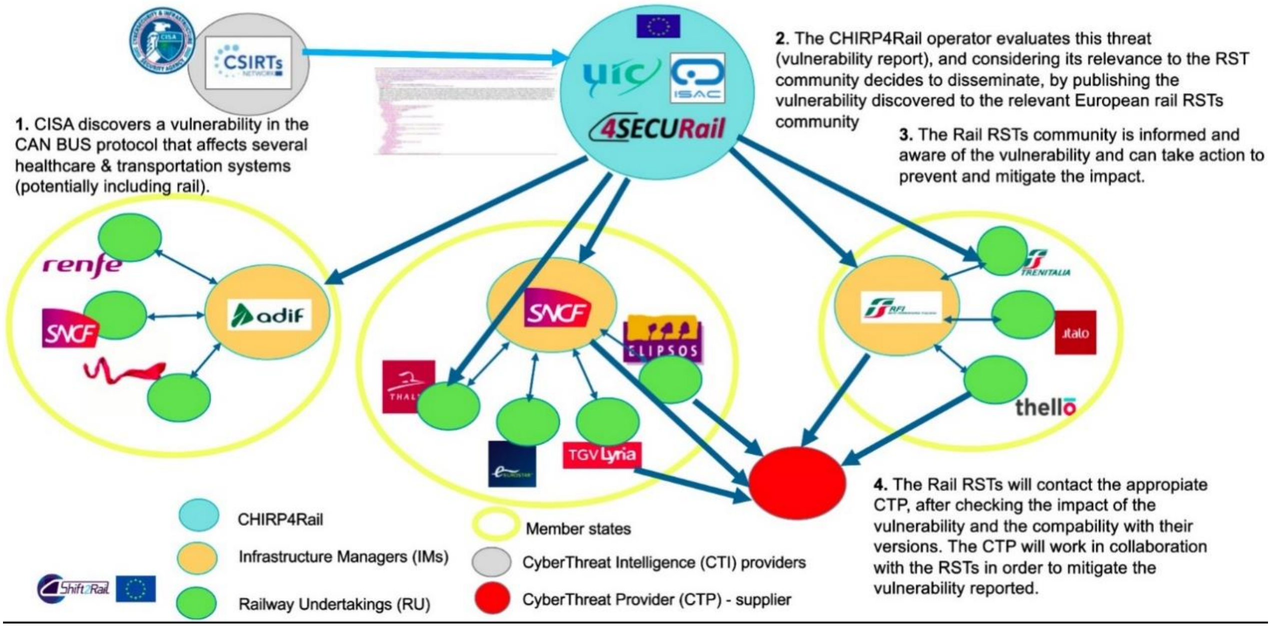
Figure 24: Scenario 2 – Railway APT threat identified by a Digital Service Provider

10.2.3.3 Scenario 3: vulnerability in a critical device (ICS)

ICS (Industrial Control Systems) is a general term that describes industrial automation systems responsible for data acquisition, visualization and control of industrial processes. They are very common in industrial sectors and Critical Infrastructures. They play a critical role not only in maintaining the continuity of industrial processes but also to ensure functional and technical safety, to prevent personal damage and damage to property.

According to the report "Analysis of ICS-SCADA Cyber Security Maturity Levels in Critical Sectors "by ENISA, the ICS-SCADA environment is a key component for the European Critical Infrastructures. Most sectors rely on ICS-SCADA to ensure process control and safety which ensure continuity of national critical functions. A vulnerability in this kind of devices, could have a huge impact in a Critical Infrastructure and there have been several cases where malicious actors have been targeting ICS such as the Triton malware or the notorious Stuxnet worm.

This seems a likely scenario within the transportation industry, where many assets are controlled by ICS/SCADA. Figure 25 shows the process of how a hardware provider reports a vulnerability in his products and this information is shared and extended among the different stakeholders within the railway sector (CERT's, IM's, RO's):


CSIRTs
uic
ISAC
4SECURail
renfe
SNCF
adif
SNCF
THALYS
CLIPSOS
TGV Lyria
TRENITALIA
RFI
italo
thello
CHIRP4Rail
Infrastructure Managers (IMs)
Railway Undertakings (RU)
Member states
CyberThreat Intelligence (CTI) providers
CyberThreat Provider (CTP) - supplier
Shift2Rail

1. CISA discovers a vulnerability in the CAN BUS protocol that affects several healthcare & transportation systems (potentially including rail).

2. The CHIRP4Rail operator evaluates this threat (vulnerability report), and considering its relevance to the RST community decides to disseminate, by publishing the vulnerability discovered to the relevant European rail RSTs community

3. The Rail RSTs community is informed and aware of the vulnerability and can take action to prevent and mitigate the impact.

4. The Rail RSTs will contact the appropiate CTP, after checking the impact of the vulnerability and the compability with their versions. The CTP will work in collaboration with the RSTs in order to mitigate the vulnerability reported.

Figure 25: Scenario 3 – Vulnerability identified within a critical service

10.2.3.4 Scenario 4: ransomware attack

This scenario is based in the WannaCry ransomware campaign in May of 2017, a global cyberattack that have a huge impact in many sectors, including railway, where the German Infrastructure Manager Deutsche Bahn was hit by the ransomware and some screens at train stations showed the ransomware message demanding money (see Figure 26).

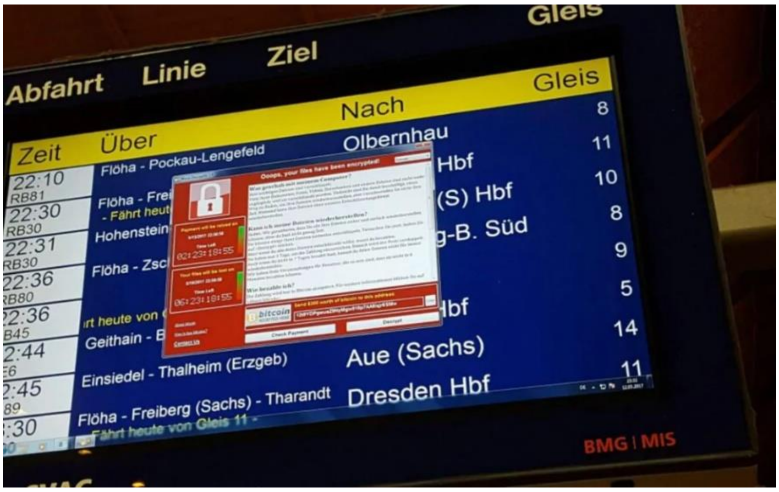
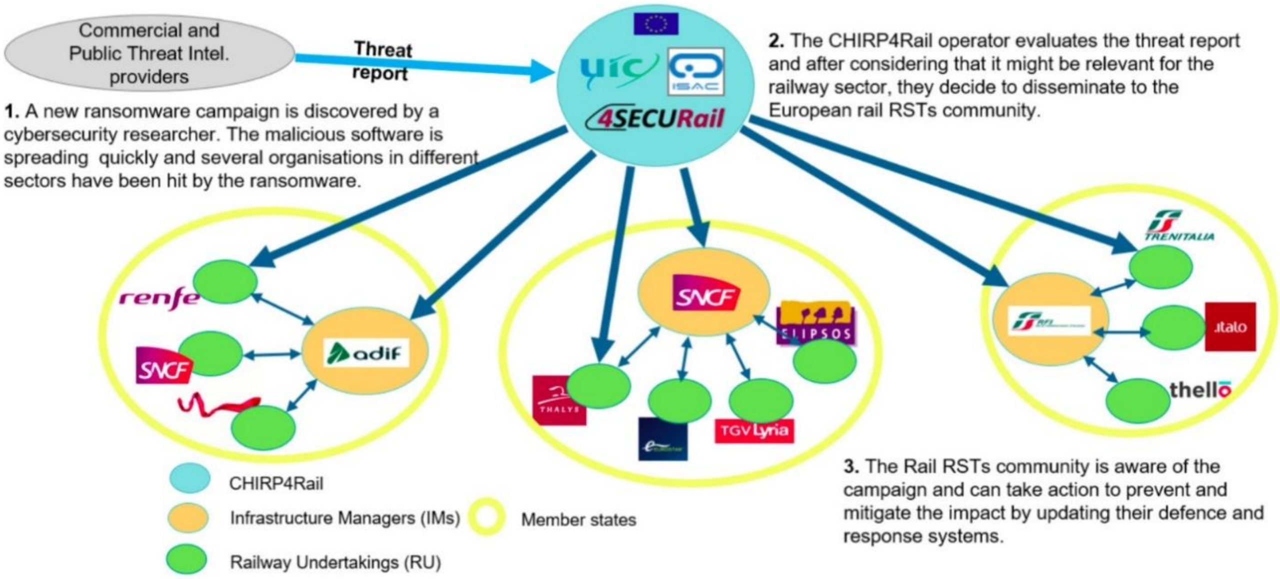


Figure 26: Wannacry ransomware hit train stations in Germany

Ransomware is on the rise and many sectors have suffered its consequences, including Transportation. For instance, the San Francisco Municipal Transport Agency (MTA) was attacked by a ransomware in 2016 and it forced the MTA to open the gates and allow passengers to ride without paying. The idea of this use case is to show the flow of information in the platform as well as the intelligence sharing good practises with a common cyberattack such as ransomware when information is provided from external intelligence providers (such public or commercial threat intelligence providers). Figure 27 below shows the process in such type of threat information sharing:



1. A new ransomware campaign is discovered by a cybersecurity researcher. The malicious software is spreading quickly and several organisations in different sectors have been hit by the ransomware.

2. The CHIRP4Rail operator evaluates the threat report and after considering that it might be relevant for the railway sector, they decide to disseminate to the European rail RSTs community.

3. The Rail RSTs community is aware of the campaign and can take action to prevent and mitigate the impact by updating their defence and response systems.

Figure 27: Scenario 4 – Ransomware attack

This scenario shows an example of how the CPO acts as an active coordinator among the national RSTs community members in researching and analysing the details to react and prevent the threat.

10.2.3.5 Scenario 5: ERTMS attack

The European Railway Traffic Management System (ERTMS) is a major industrial project that aims to replace the many different national train control and command systems in Europe with a standardised system. Nevertheless, although this upgrade introduces many advantages such as the interoperability between networks and reduces maintenance costs, it also increases the risk of cyber-attack on the rail infrastructure, since it brings more systems under centralised control, increasing the attack surface.

In "*The risk assessment of ERTMS-based railway systems from a cyber security perspective: methodology and lessons learned*", **[Bloomfield et al., 2016]** perform a high-level risk assessment on attacks to the railway signalling and control system that could have a high impact such as:

- Cyber-attacks that result in unsafe train movements. (e.g. a collision involving multiple trains, a derailment of a train)
- Cyber-attacks that result in loss of service that could lead to serious transport disruptions. (e.g. widespread disruption of train service over a large area)

These kinds of attacks could have a serious impact in rail operators, causing loss of service (economic and/or reputation damage) for several days, or even a large number of deaths in a worst-case scenario (e.g. a cyber-terrorist group attacking a train). Figure 28: ERMTS attack scenario below represents a cyber-attack by eavesdropping GSM-R data for bypassing the authenticating system (e.g. EuroRadio) and being able to send malicious orders to the train.

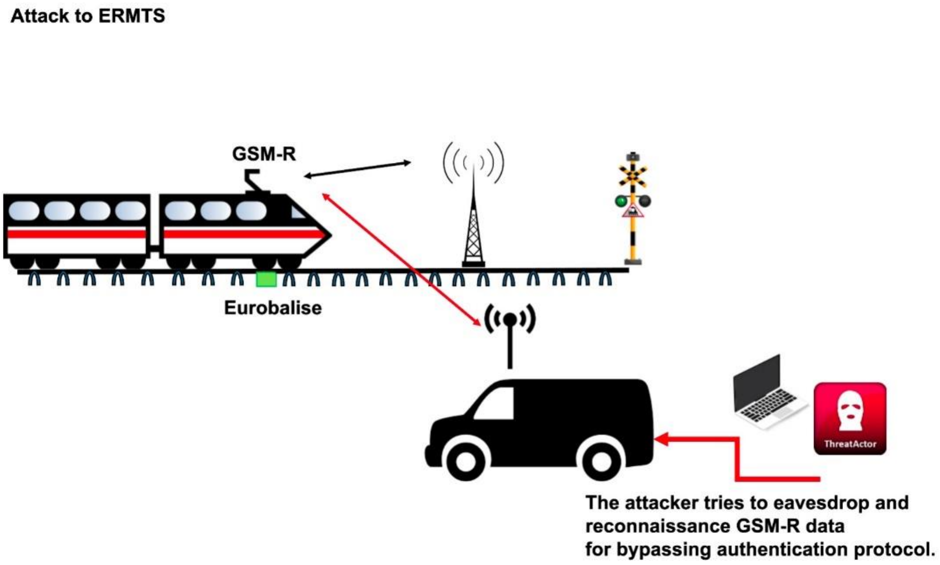
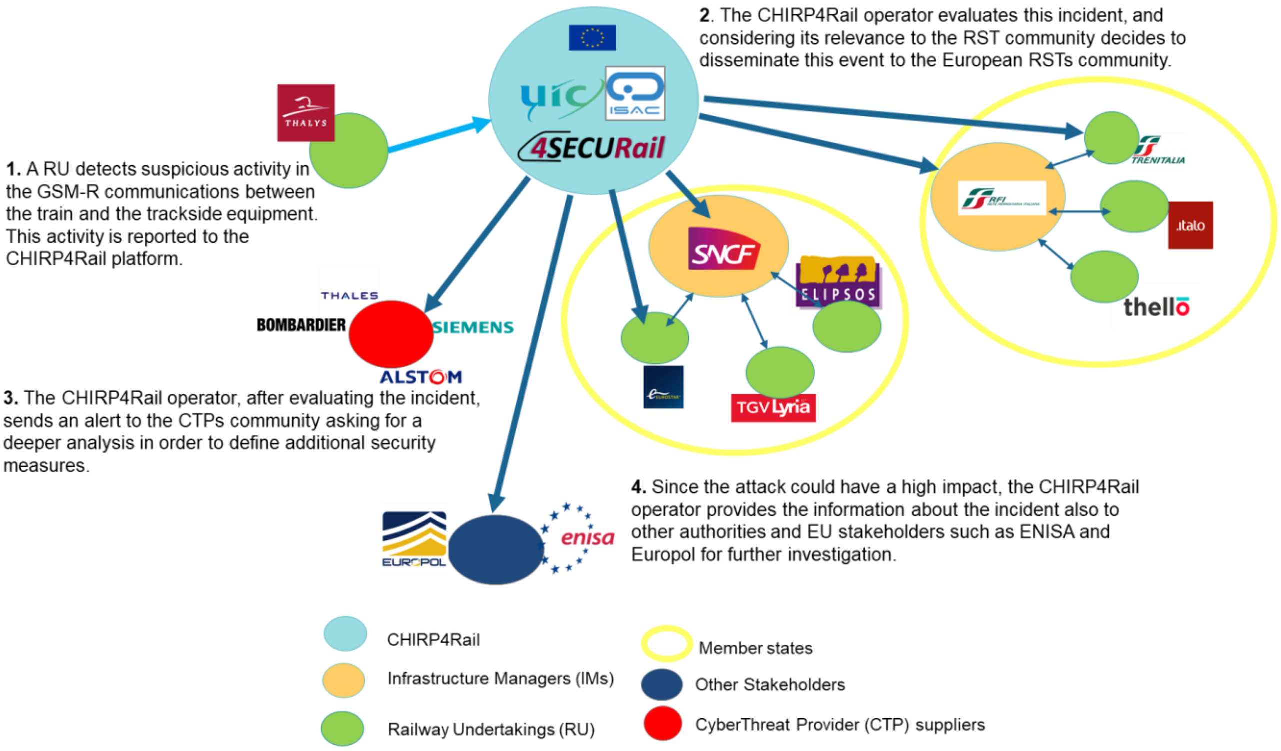

Attack to ERMTS
GSM-R
Eurobalise
ThreatActor
The attacker tries to eavesdrop and
reconnaissance GSM-R data
for bypassing authentication protocol.

Figure 28: ERMTS attack scenario

In this scenario, a threat actor is interested in sending malicious messages to the train and to achieve this, the first step is to eavesdrop the encrypted data that the train and trackside equipment exchanges using GSM-R protocol. The aim of the attacker at this stage is to bypass the authentication and verification message system used and to send malicious orders to the train in a second stage of the attack.

The attempt of bypassing the authentication protocol has been detected by the security measures of the train and this information has been reported to other stakeholders using the CHIRP4Rail platform. Figure 29 below presents the information flow once the attack has been detected.



1. A RU detects suspicious activity in the GSM-R communications between the train and the trackside equipment. This activity is reported to the CHIRP4Rail platform.

2. The CHIRP4Rail operator evaluates this incident, and considering its relevance to the RST community decides to disseminate this event to the European RSTs community.

3. The CHIRP4Rail operator, after evaluating the incident, sends an alert to the CTPs community asking for a deeper analysis in order to define additional security measures.

4. Since the attack could have a high impact, the CHIRP4Rail operator provides the information about the incident also to other authorities and EU stakeholders such as ENISA and Europol for further investigation.

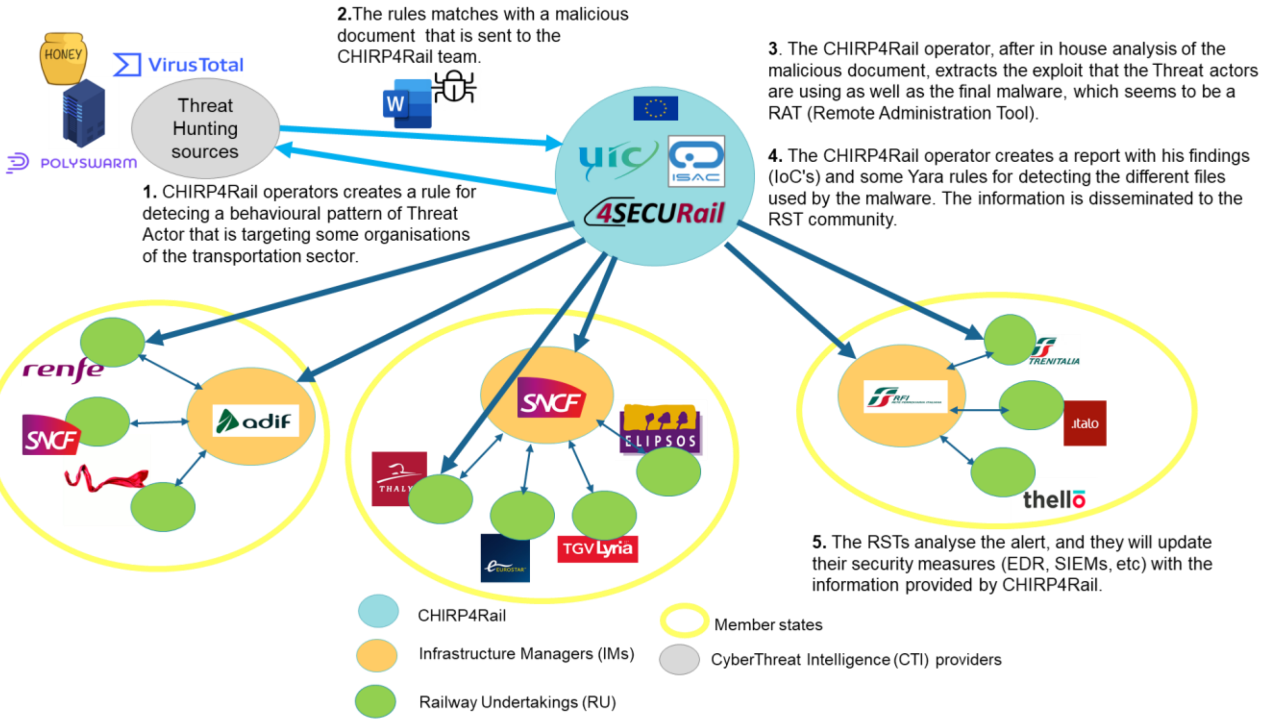
Figure 29: Scenario 5 – ERMTS attack information sharing

10.2.3.6 Scenario 6: Threat Hunting by the CHIRP4Rail team

Threat hunting is the process of proactively and iteratively searching through networks for indicators of abnormal behaviour caused by potential cyber threats, rather than relying on detection tools to flag those threats. In threat hunting, analysts create “assumptions” or “behavioural patterns” that are then automated to quickly search the network for threat indicators.

Security Analysts also use Honeypots or Malware Analysis platforms such as VirusTotal, Hybrid Analysis or PolySwarm that provide Threat Hunting services where the analyst can get malicious samples that match with a specific pattern (e.g. a Yara Rule). Using this approach, they increase the probability of finding new threats before their organisation is attacked.

In this scenario, the CHIRP4Rail operator is proactively looking for malware samples attributed to a notorious Threat Actor that is targeting the transportation sector, or in particular railway. Specifically, some Metro organisations and bus operators have been attacked by this group. The CHIRP4Rail operator has created some behavioural pattern rules for detecting malicious samples of this kind and to perform an analysis of the samples in order to provide Threat Intelligence to the European RST community. Figure 30 below shows an example of the workflow on CHIRP4Rail:



2.The rules matches with a malicious document that is sent to the CHIRP4Rail team.

3. The CHIRP4Rail operator, after in house analysis of the malicious document, extracts the exploit that the Threat actors are using as well as the final malware, which seems to be a RAT (Remote Administration Tool).

1. CHIRP4Rail operators creates a rule for detecing a behavioural pattern of Threat Actor that is targeting some organisations of the transportation sector.

4. The CHIRP4Rail operator creates a report with his findings (IoC's) and some Yara rules for detecting the different files used by the malware. The information is disseminated to the RST community.

5. The RSTs analyse the alert, and they will update their security measures (EDR, SIEMs, etc) with the information provided by CHIRP4Rail.

Figure 30: Scenario 6 – In house threat hunting

11 Conclusions

This section summarises the main conclusions of the CSIRT rail model, highlighted in this report. The CHIRP4Rail concept model and functionality statement concluded that:

- The railway security stakeholders understanding of the **"CSIRT" extends beyond purely response to 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 intelligence building and information sharing 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.

On such basis, the CHIRP4Rail model presented in this report has been designed addressing a threefold perspective:

- The **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); and the CHIRP4Rail Platform Operator (CPO).
    - WHAT (the flows): Cyber Threats relevant for Rail (incidents and/or vulnerabilities) building Actionable Intelligence (bulletins, prevention, response).
    - HOW (the tools): a platform interconnecting RST's tool, enabling voluntary and anonymous sharing of information and guaranteeing cyber secure communications.
- The **organisational model** defines the organisation and process at 3 levels:
    - Roles and functions for each of the actors involved.
    - The management structure.
    - The detailed data and workflows, identifying the inputs (information sources), process (threat analysis and intelligence building), and outputs (results for information sharing).
- The **technical model** defines the data model:
    - Based on the MISP data standard, defining the use of the core event and event attributes for rail.
    - Integrating the use of specific railway taxonomies such as [X2Rail-1 D8.2, 2018], a specific taxonomy for threats in the railway landscape.
    - Enabling access control mechanisms based on the Traffic Light Protocol [TLP], and Threat Intelligence Exchanging protocols at the application level such as [TAXII], [OpenDXL] or [MISP Sync].

Finally, an early outline of the key functional and technical aspects of the CSIRT platform is presented as an anticipation, to be elaborated in further tasks (future deliverable D3.3).

12 References

[ADIF, 2019] "ADIF's vision for Railways Cybersecurity in Spain.pdf" – presented at ER-ISAC, December 2019.

[Bloomfield et al., 2016] Bloomfield R., Bendele M., Bishop P., Stroud R., Tonks S. (2016). "The Risk Assessment of ERTMS-Based Railway Systems from a Cyber Security Perspective: Methodology and Lessons Learned". In: Lecomte T., Pinger R., Romanovsky A. (eds) Reliability, Safety, and Security of Railway Systems. Modelling, Analysis, Verification, and Certification. RSSRail 2016. Lecture Notes in Computer Science, vol 9707. Springer, Cham. https://doi.org/10.1007/978-3-319-33951-1_1

[BSI Threats Catalogue] The BSI (Bundesamt für Sicherheit in der Informationstechnik; the German Federal Office for Information Security) Threats Catalogue: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/download/threats_catalogue.pdf

[Carnegie Mellon CERT] Carnegie Mellon SEI-CERT: www.sei.cmu.edu/about/divisions/cert/index.cfm

[CERT-CC] http://www.cert.org/

[CERT-NL] https://www.ncsc.nl/

[CIRCL.LU] http://www.circle.lu/

[EC CSIRT Network] https://ec.europa.eu/digital-single-market/en/nis-cooperation-group. Publications: https://www.enisa.europa.eu/publications

[EE-ISAC, 2019] EE-ISAC presentation to ER-ISAC, December 2019: "201910 EE-ISAC Presentation.pdf"

[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] ENISA's Threat Taxonomy, latest version updated in September 2016: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/threat-taxonomy/view

[ENISA] ENISA website: https://www.enisa.europa.eu/

[ENISA_CSIRT, 2006] ENISA CSIRT Setting-up Guide. Deliverable WP2006/5.1(CERT-D1/D2). 22 December, 2006. Available at: https://www.enisa.europa.eu/publications/csirt-setting-up-guide

[ENISA_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_CTI, 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

[EU SURVEY tool] https://ec.europa.eu/eusurvey/

[FIRST] https://www.first.org/. FIRST Information sharing at: https://www.first.org/global/sigs/information-sharing/misp. FIRST security response teams listed at: https://www.first.org/members/teams/

[FIRST_CSIRT] FIRST CSIRT Framework v2.0 2019: https://www.first.org/education/FIRST_CSIRT_Services_Framework_v2.0.pdf

[GDPR] European Parliament and Council of European Union (2016) Regulation (EU) 2016/679. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN.

[ISO 27005:2011] ISO/IEC 27005:2011(en) on Information technology — Security techniques — Information security risk management: https://www.iso.org/obp/ui/#iso:std:iso-iec:27005:ed-2:v1:en

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

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

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

[NATO NCIRC] https://www.ncia.nato.int/

[NIS] The Directive on security of network and information systems (NIS Directive): https://www.enisa.europa.eu/topics/nis-directive

[OpenDXL] OpenDXL initiative to communicate and share information for real-time, accurate security decisions and actions: https://www.opendxl.com/

[SERA] Directive on Single European Railway Area https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32012L0034

[STIX2.1] OASIS, STIX™ Version 2.1, Committee Specification Draft 01, Public Review Draft 01, 26 July 2019: https://docs.oasis-open.org/cti/stix/v2.1/csprd01/stix-v2.1-csprd01.pdf

[TAXII] Trusted Automated Exchange of Intelligence Information: https://oasis-open.github.io/cti-documentation/taxii/intro.html

[TLP] FIRST Standards, Traffic Light Protocol (TLP) Definitions and Usage Guidance — Version 1.0: https://www.first.org/tlp/

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

13 Appendices

13.1 Annex 1 – Summarised CSIRT Examples

CSIRT Example 1: CERT-NL

Organisation/Owner: Netherlands Government NCSC https://www.ncsc.nl + https://www.ncsc.nl/contact/24-uurs-hulp Sits under National Coordinator for Terrorism and Security / Ministry of Interior.
Main Activities / Services Protecting Critical Digital Infrastructures / Information. Dutch National Alerting Service “De Waarschuwingsdienst” (Ministry Economic Affairs). 24-Hour helpline for IT security incidents (Government and Vital Process Providers/OES). Advice on handling cyber security incidents. Analysis of malicious software / threats / intrusions. Estimation of stolen/leaked information/data. Help selecting / installing software for logging / combatting cyber threats. Support for technical staff / showing how to deal with cyber threats / incidents. On-site support where necessary.
Inclusion (departments/partners/etc.) NL-NCSC, ABN AMRO, KPN, NL SURFNET, UPC/CHELLO Government, Banking, Telecoms, Broadband, Email for Business & Citizens, OES.
Team Roles and Tasks General Manager, Technical Team Manager, Technical Specialists (various Cyber topics / services), Communication Team, Support Staff. Tasks are specific to service delivery (see service list*).
Coordination / Management Coordination relies on Ministry level support since different services engage with different constituencies, and relay on different supports (M.Interior, M.Economic.Aff’).
Information Recorded/Exchanged with Stakeholders (& who gets access and how shared) There is an open sharing culture, conjoining all Dutch government departments and key businesses, but it is not yet fully formalised. They intend in future to “…structurally guarantee the exchange of information and at the same time set it up more widely, by promoting cross-sector analyses” etc. Intrusions and identified attempted intrusions are notified.
Platform used National platform: https://www.ncsc.nl
Detection and Prevention tools CERT-NL advises on latest tools (no list available).
Shared Threat Intelligence / Collaboration Tools (e.g. MISP etc.) Threat intelligence is shared with other CERTs, via EU cooperation group, and via ENISA organised events and linkages. A database is implemented, and under development.
Sharing Information with other organisations? – Open sharing via ENISA initiatives.
Other Salient features The Dutch approach is all-inclusive and geared towards a broad view of civil protection, considering all aspects including Citizens, Education, Healthcare, Business, Government, etc. Less successful services are stated in publications, but without full explanation: Knowledge Base; Central Incident Reporting Point; SMS-alerts; Statistics.

CSIRT Example 2: CIRCL.LU Computer Incident Response Centre Luxembourg

Organisation/Owner
Luxembourg Government: CIRCL.LU http://www.circle.lu

Mission:

- provide a systematic response facility to ICT-incidents
- coordinate communication among national and international incident response teams during security emergencies: help prevent future incidents
- support ICT users in Luxembourg to recover quickly and efficiently from security incidents
- minimize ICT incident-based losses, theft of information and disruption of services at a national level
- gather information related to incident handling and security threats to better prepare future incidents management and provide optimized protection for systems and data
- provide a security related alert and warning system for ICT users in Luxembourg
- foster knowledge and awareness exchange in ICT security

Main Activities / Services:
Incident Coordination and Incident Handling.
Reporting of security incidents.
Incident identification, triage, analysis and response.

Technical investigation:

- Incident correlation
- Malware analysis and reverse engineering
- System and network forensic analysis
- Security vulnerability assessment
- Information leak analysis and data mining

International and national CERT/CSIRT cooperation
Vulnerability handling and responsible vulnerability disclosure (on incident).
Awareness / News via CIRCL newsletter
Training and Technical Courses (PDF Catalogue)

Incident Handling Support Tools and Services
URL Abuse to check and review security of URLs
CVE-search + Common Vulnerabilities and Exposures (CVE) web interface and API
IP address to ASN mapping “whois” service including 4 years of historical data
Passive DNS, historical DNS records database (access on request, contact us)
Passive SSL services, historical database of SSL certificate per IP address (access on request, contact us)
Dynamic malware analysis platform (access on request, contact us)
Threat indicators sharing platform for private sector - MISP (access on request, contact us)
Data Feeds and Early Detection Network

Private and public organizations in Luxembourg can benefit from their early detection network by ***hosting a sensor in their unused network spaces***
CIRCL ***provides a contextual feed containing all software vulnerabilities*** including visibility ranking in Luxembourg

Inclusion (departments/partners/etc.)
Supporting all private sector, communes and non-governmental entities in Luxembourg.

Coordination / Management: Team Roles and Tasks
Operational Core Team
Operational Support Team
Development Team
Business and Legal Support Team

Information Recorded/Exchanged with Stakeholders (& who gets access and how shared)

For all clients (see below): Incidents, Malware database, Threat indicators database, etc.
Platforms / Detection Tools / Prevention Tools / Sharing Tools - Dynamic malware analysis platform (access on request). - Threat indicators sharing platform for private sector – MISP (access on request). **Incident Handling Support Tools and Services** URL Abuse to check and review security of URLs CVE-search Common Vulnerabilities and Exposures (CVE) web interface and API https://cve.mitre.org IP address to ASN mapping whois service including 4 years of historical data Passive DNS, historical DNS records database (on request) Passive SSL services, historical database of SSL certificate per IP address (on request) Data Feeds and Early Detection Network **Publications on Cyber Security Issues** http://www.circle.lu/pub/ **Digital First Aid Kit** The Digital First Aid Kit provides preliminary support for people facing the most common types of digital threats. The Kit offers a set of self-diagnostic tools for citizen, human rights defenders, bloggers, activists and journalists facing attacks themselves, as well as providing guidelines for digital first responders to assist a person under threat.
Sharing Information with other orgs Sharing with National authorities and collaborating CSIRTs.
Other Salient features Major trainer in MISP, and active in MISP development.

CSIRT Example 3: EU Rail IM (anonymised example)

Organisation/Owner EU Rail Anonymised Example
Main Activities / Services ***Response***. Lead and coordinate actions in prevention or in reaction to an information system (IS) security incident. Support and resolution of incidents by providing personnel and analysis where needed. Deploy sensitive or secure information (SSI) crisis management (operational) for any major incident. ***Prevention.*** Conduct cyber security monitoring of networks and operational systems. Support examination and analysis of alerts. Define preventive measures for known cyber threats and noted attempted intrusions. Organise defences such as patches and signature databases for all relevant systems. ***Collaboration.*** Collaborate with all security departments, security teams, and other stakeholders to protect the company and its customers, including working with suppliers, brand misuse or other frauds aimed at customers (e.g. phishing and other Internet based frauds).
Inclusion (departments/partners/etc.) All departments or teams managing IT and OT
Team Roles and Tasks (as per above services) Process management. Manage/conduct IT/Network monitoring. Manage and deliver response to security incidents. Periodic survey of systems - updating of preventive measures (new measures / threats). Manage and deliver 24/7 contact for all operational units / systems.
Coordination / Management Coordination of security teams/ actors in operational units.
Information Recorded/Exchanged with Stakeholders (& who gets access and how shared)

Attempted/actual intrusions, irregularities in network activity, phishing & brand fraud.
Platform used Various Intranet platforms for security teams, plus database of threats.
Detection / Prevention tools used 1. Private adaptations to Firewalls, 2. Network Security Solution (Commercial – includes analysis, detection, and forensic analysis tools).
Shared Threat Intelligence / Collaboration Tools (e.g. MISP etc.) MISP with access by all teams, added facility for teams to declare new items for inclusion. Intranet-based "security notices" of events / items of interest for all teams.
Sharing Information with other orgs? Twitter account informs agents / public about cyber threats (e.g. Phishing)

CSIRT Example 4: NATO NCIA NCIRC-TC

Organisation/Owner NATO Computer Incident Response Capability - Technical Centre (NCIRC TC, Brussels) https://www.ncia.nato.int
Main Activities / Services Protection of all NATO sites and critical systems. Centralised and 24-hour cyber defence support to NATO sites and systems. Handling of, and reporting on, any cyber incidents. Disseminating incident-related information to system/security management and users. Deploying Rapid Reaction Teams (RRT) to support the protection of NATO or Allied networks. Sharing cyber intelligence with all sites and strategic partners. Sharing best practices with all sites and strategic partners. Advising technical operations on how to improve cyber incident prevention, resilience and response capabilities. Conducting exercises such as an annual "Cyber Coalition Exercise" to both ***test and demonstrate*** cyber incident prevention and response capabilities.
Inclusion (departments/partners/etc.): All NATO sites, technical & cyber security teams.
Team Roles and Tasks: Central team deliver services as above; local teams deliver on-site support such as logging, monitoring, identifying risks / threats, etc.
Coordination / Management: NCIA coordinates all NATO site teams
Information Recorded/Exchanged with Stakeholders **(& who gets access and how shared)** All known malware / cyber threats are recorded in a database and shared with MISP users. MISP instances linked, e.g. DefCERT NL, BEL MOD.
Platform used: Public and Private web platforms for groups + MISP (see below).
Detection / Prevention tools used: Latest tools advised to teams (list not available)
Shared Threat Intelligence / Collaboration Tools (e.g. MISP etc.): MISP – developed for NCIRC TC. Used by all NATO sites and strategic partners.
Sharing Information with other organisations. NATO NCIA shares with European Union (EU), United Nations (UN), Council of Europe and the Organization for Security and Cooperation in Europe (OSCE) – including a Technical Arrangement on Cyber Defence to better prevent and respond to cyber-attacks (framework for exchanging information and the sharing of best practices between emergency response teams). Partnership with industry uses national CSIRTs/CERTs, and NATO member countries' industry representatives, for information sharing, exercises, education and training.
Other Salient features MISP allows sharing of technical characteristics of malware within a trusted community, ***without having to share information about the context of the incident***. MISP provides mechanisms for automatic import and export of data and interfacing with other systems. The aim is to speed up detection of incidents and production of defence countermeasures, especially for malware that is not yet blocked by protection or is part of sophisticated targeted intrusion attempts.

CSIRT Example 5: ENISA Essential Model

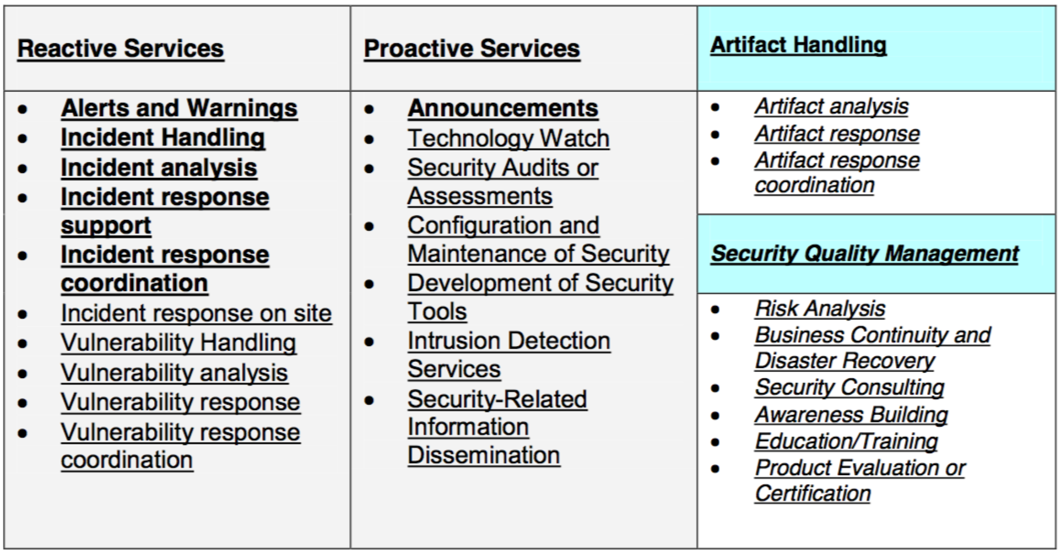
Organisation/Owner

ENISA – based on ENISA guidance and reflections on EU status (typical elements) https://www.enisa.europa.eu/publications/csirt-setting-up-guide

Main Activities

Deploy a team of security experts to respond to computer security incidents.
Ensure 24/7 support since events can happen any time.
Monitor systems to detect intrusions /attempts.
Monitor cyber threat intelligence landscape to identify all/new risks and remedies.
Identify intrusions / attempted intrusions and deploy response.
Receive alerts from stakeholders regarding risks/threats/events and react/support.
Deploy forensic tools / IDS / threats databases etc. to support all activities.
Deploy communication facilities for receiving alerts / sending alerts / guidance.
Provide preventative and educational services for the constituency to mitigate risks and minimise the number of required responses.
Collaborate with relevant related CSIRTs to ensure shared benefit in security.

Specific Services (From ENISA report - adapted from CERT-CC – core services in bold)



Reactive Services	Proactive Services	Artifact Handling
Alerts and Warnings **Incident Handling** **Incident analysis** **Incident response support** **Incident response coordination** Incident response on site Vulnerability Handling Vulnerability analysis Vulnerability response Vulnerability response coordination	**Announcements** Technology Watch Security Audits or Assessments Configuration and Maintenance of Security Development of Security Tools Intrusion Detection Services Security-Related Information Dissemination	*Artifact analysis* *Artifact response* *Artifact response coordination*
		Security Quality Management
		Risk Analysis *Business Continuity and Disaster Recovery* *Security Consulting* *Awareness Building* *Education/Training* *Product Evaluation or Certification*

Inclusion (departments/partners/etc.)

All organisational technical teams / security teams (can be multiple sites).

Team Roles and Tasks

Roles and tasks are defined by the selected services from the set above. See ENISA guide for low-level detail on specific services and their tasks / data flows / etc.

Coordination / Management (adapted from ENISA model).

Define the Mission Statement / Objectives / Key aims /Info Security Policy.
Define the CSIRT services to deliver the stated Objectives.
Define an organisational structure / management to deliver the services.
Allocate staff to deliver the services.
Define the communication approach to the constituents.
Design the financial model to support the above elements (cost / revenue).
Organise cooperation with other relevant CSIRTs and initiatives.

Management / Support Team / Roles:- General manager.
- Office manager.-
Accountant.- Communication
consultant.- Legal consultant.

Operational Technical Team / Roles:

- Technical team leader.- Technical CSIRT technicians, delivering the CSIRT services.- Researchers. - External experts as needed. **Business Model:** - Independent entity - Embedded entity - Campus model (set of collaborating CSIRTs) - Virtual team (spread across a set of organisations – not from ENISA document*)
Information Recorded/Exchanged with Stakeholders Threat intelligence – known risks, mitigation, remedies (database). Cyber events – intrusions, attempts, logged irregularities, etc. Access by all stakeholders in principle, plus suppliers whose products are unsafe, and collaborating CSIRTs.
Platforms used: Not addressed since it is a general guide.
Shared Threat Intelligence / Collaboration Tools (e.g. MISP etc.) : Not addressed
Sharing Information with other organisations: addressed as a potential action if relevant related CSIRTs can be identified.
Other Salient features This is based on a guide, which in turn is derived from practical experience.

13.2 Annex 2 – Summarised CSIRT Coordination Examples

CSIRT Coordination Example 1: CERT-CC http://www.cert.org/

Organisation/Owner http://www.cert.org/
Carnegie Mellon CERT Coordination Centre (CERT CC) via Software Engineering Institute

Main Activities

- Coordinate a set of CERTs (what we call CSIRTs).
- Focal point for reporting security vulnerabilities / facilitating correction.
- Analysing threat info. to develop and share countermeasures / prevention tech.
- Provide model for others to develop incident response teams (CERT).
- Raise awareness and understanding of security trends and issues.

Specific Services*

- Security Alerts / Announcements
- Vulnerability Analysis / Risk Analysis for Clients
- Artifact Analysis for Clients
- Auditing and Penetration Testing
- CSIRT guidance / Education and Training
- Incident tracing
- Open sharing of risks knowledge - https://twitter.com/certcc?lang=en

Inclusion (departments/partners/etc.)
US Government, Education and Business CERTs / other Security Teams

Coordination Roles and their Tasks

- Engage stakeholders and organise ***stakeholder membership***
- Identify educational needs and ***organise education***
- Organise and manage ***Specific Services*** (see list items *)
- Operate Specific Services (as above *)
- Implement / Manage Content / Operate ***Threats Database***
- Facilitate communication between CERTs (incidents, etc.)

Information Recorded/Exchanged with Stakeholders

- Threat library (risks and remedies)
- New threats / new remedies (shared with stakeholders)

Tools used for Recording / Sharing Threat Intelligence

- CERT-CC Vulnerabilities Database : https://www.kb.cert.org/vuls/
- National Vulnerabilities Database : https://nvd.nist.gov
- Vulnerability Archive : https://github.com/CERTCC/Vulnerability-Data-Archive

Other Salient features

- Method for quick notification (speed reduces damage to others).
- Common policies and procedures.
- Automation of incident handling tasks (speed reduces damage to others).
- Methods to collaborate and share information with others.
- Easy and efficient way to sort through incoming information.

Overview: CERT CC is short for the Computer Emergency Response Team Coordination Centre. CERT was started in December 1988 by the Defence Advanced Research Projects Agency (DARPA), a part of the U.S. Department of Defence, after the Morris Worm disabled about 10% of all computers connected to the Internet. CERT/CC is located at the Software Engineering Institute (SEI), a federally funded research centre operated by Carnegie Mellon University.
CERT CC studies Internet security vulnerabilities, publishes security alerts, and provides services to organisations that have been attacked. CERT CC research activities include WAN computing and developing improved Internet security. The organization also provides training to incident response professionals.

CSIRT Coordination Example 2: FIRST - Forum of Incident Response and Security Teams

Organisation/Owner

FIRST https://www.first.org

Main Activities

- Support 500+ CSIRTs in 80+ countries world-wide.
- Education, technical support, database provision.

Specific Services

- Promote development of quality security products, policies and services.
- Identify/develop and share best computer security practices.
- Promote creation and development of Incident Response teams.
- Facilitate members in using and sharing their combined knowledge, skills and experience to ensure safer and more secure electronic environments.
- Courses, Conferences, Training programmes.
- Support to cyber security standards.

Inclusion (departments/partners/etc.)

FIRST is a membership organisation that both helps to create effective CSIRTs, and then coordinates and facilitates their collaboration, and their development.

Coordination Roles and their Tasks

- Roles are as per services above
- Training and Education (used by ITU for capacity building).
- Conferences.
- Organising and supporting Special Interest Groups (SIGs).

Information Recorded/Exchanged with Stakeholders

- Contacts information for other CSIRTs in the network.
- Threat intelligence and incidents via database.
- Supporting information (cases, reports, etc.).

Tools used for Recording / Sharing Threat Intelligence

- MISP database is used and made accessible to all members.

https://www.first.org/global/sigs/information-sharing/misp

Other Salient features

- FIRST was formed to support “normalisation” and “collaboration” as CSIRTs/CERTs rapidly emerged.
- FIRST is non-profit, being only for charitable and educational purposes.
- Members are “Response Teams”.

Overview: FIRST is an international confederation of trusted computer incident response teams who cooperatively handle computer security incidents and promote incident prevention programs. FIRST members develop and share technical information, tools, methodologies, processes and best practices. (Source: FIRST web site, February 2020)

CSIRT Coordination Example 3: EC NIS CSIRT Network (European) https://ec.europa.eu/digital-single-market/en/nis-cooperation-group

Organisation/Owner: EU-ENISA (n.b. report here combines ENISA/DG/ECG actions)

Main Activities

- Support understanding of NIS Directive and Cyber Security Act + Conformance.
- Coordinate a set of CSIRTs (Governmental and non-Governmental).
- Support CSIRT formation + models for consideration.
- Contact points for reporting security incidents, vulnerabilities, correction.
- Raise awareness and understanding of CSIRT developments.
- Raise awareness of security trends and issues.

Specific Services (main examples – see web site for further details)

- Creation and support of active CSIRT Network.
- Coordinate response to large scale / cross-border cyber security incidents.
- Security Alerts / Announcements (shared between Country CSIRTS via ECN).
- Guide how To Set Up A CSIRT (advice and assistance from ENISA).
- Analysis and reporting of CSIRT maturity.

• Analysing threat information to advise CSIRTs (info notes) • Provide and manage content for *online cyber security information resource* (e.g. see https://www.enisa.europa.eu/publications for both above) • CSIRT guidance / Education and Training / Hands-on Support for Cyber Security. • Pan-European Exercises. • Support for National Cyber Security Strategies. • Support CSIRT Capacity Building. • Studies on relevant security topics to benefit stakeholders. • Recommendations / advice on cyber security (all areas). • Support for policy development / Cyber Security certification schemes.
Inclusion: European country governments and links to their Operators of Essential Services.
Coordination Roles and their Tasks • Engage stakeholders and organise ***stakeholder networks (Gov, OES)*** • Facilitate communication between CSIRTs in networks (incidents, etc.) • Identify awareness/educational needs and ***organise awareness/education*** • Organise and manage ***Specific Services*** (see list items) • Operate Specific Services (as above)
Information Recorded/Exchanged with Stakeholders • Threat news and advice. • Incidents reported via NCP to NIS CSIRT Network.
Tools used for Recording / Sharing Threat Intelligence • Library of news / reports as above.
Other Salient features • Publications https://www.enisa.europa.eu/publications ○ Reports on Cyber Security topics ○ Info notes (e.g. threats and mitigation) ○ Opinion papers (e.g. on ISAC cooperation)

13.3 Annex 3 – Attributes type in the MISP format

The list of attribute types is based on the MISP format:

- AS: Autonomous system
- aba-rtn: ABA routing transit number
- anonymised: Anonymised value - described with the anonymisation object via a relationship
- attachment: Attachment with external information
- authentihash: Authenticode executable signature hash
- bank-account-nr: Bank account number without any routing number
- bic: Bank Identifier Code Number also known as SWIFT-BIC, SWIFT code or ISO 9362 code
- bin: Bank Identification Number
- boolean: Boolean value - to be used in objects
- bro: An NIDS rule in the Bro rule-format
- btc: Bitcoin Address
- campaign-id: Associated campaign ID
- campaign-name: Associated campaign name
- cc-number: Credit-Card Number
- cdhash: An Apple Code Directory Hash, identifying a code-signed Mach-O executable file
- chrome-extension-id: Chrome extension id
- comment: Comment or description in a human language
- community-id: a community ID flow hashing algorithm to map multiple traffic monitors into common flow id
- cookie: HTTP cookie as often stored on the user web client. This can include authentication cookie or session cookie.
- cortex: Cortex analysis result
- counter: An integer counter, generally to be used in objects
- country-of-residence: The country of residence of a natural person
- cpe: Common platform enumeration
- dash: Dash Address
- date-of-birth: Date of birth of a natural person (in YYYY-MM-DD format)
- datetime: Datetime in the ISO 8601 format
- dns-soa-email: RFC1035 mandates that DNS zones should have a SOA (Statement Of Authority) record that contains an email address where a PoC for the domain could be contacted. This can sometimes be used for attribution/linkage between different domains even if protected by whois privacy
- domain: A domain name used in the malware
- domain|ip: A domain name and its IP address (as found in DNS lookup) separated by a |
- email: An e-mail address
- email-attachment: File name of the email attachment.
- email-body: Email body
- email-dst: The destination email address. Used to describe the recipient when describing an e-mail.
- email-dst-display-name: Email destination display name
- email-header: Email header
- email-message-id: The email message ID
- email-mime-boundary: The email mime boundary separating parts in a multipart email
- email-reply-to: Email reply to header
- email-src: The source email address. Used to describe the sender when describing an e-mail.
- email-src-display-name: Email source display name

- email-subject: The subject of the email
- email-thread-index: The email thread index header
- email-x-mailer: Email x-mailer header
- eppn: eduPersonPrincipalName - eppn - the NetId of the person for the purposes of inter-institutional authentication. Should be stored in the form of user@univ.edu, where univ.edu is the name of the local security domain.
- filename: Filename
- filename|authentihash: A checksum in md5 format
- filename|impfuzzy: Import fuzzy hash - a fuzzy hash created based on the imports in the sample.
- filename|imphash: Import hash - a hash created based on the imports in the sample.
- filename|md5: A filename and an md5 hash separated by a |
- filename|pehash: A filename and a PEhash separated by a |
- filename|sha1: A filename and an sha1 hash separated by a |
- filename|sha224: A filename and a sha-224 hash separated by a |
- filename|sha256: A filename and an sha256 hash separated by a |
- filename|sha3-224: A filename and an sha3-224 hash separated by a |
- filename|sha3-256: A filename and an sha3-256 hash separated by a |
- filename|sha3-384: A filename and an sha3-384 hash separated by a |
- filename|sha3-512: A filename and an sha3-512 hash separated by a |
- filename|sha384: A filename and a sha-384 hash separated by a |
- filename|sha512: A filename and a sha-512 hash separated by a |
- filename|sha512/224: A filename and a sha-512/224 hash separated by a |
- filename|sha512/256: A filename and a sha-512/256 hash separated by a |
- filename|ssdeep: A checksum in ssdeep format
- filename|tlsh: A filename and a Trend Micro Locality Sensitive Hash separated by a |
- filename|vhash: A filename and a VirusTotal hash separated by a |
- first-name: First name of a natural person
- float: A floating point value.
- frequent-flyer-number: The frequent flyer number of a passenger
- gender: The gender of a natural person (Male, Female, Other, Prefer not to say)
- gene: GENE - Go Evtx sigNature Engine
- git-commit-id: A git commit ID.
- github-organisation: A github organisation
- github-repository: A github repository
- github-username: A github user name
- hassh-md5: hassh is a network fingerprinting standard which can be used to identify specific Client SSH implementations. The fingerprints can be easily stored, searched and shared in the form of an MD5 fingerprint.
- hasshserver-md5: hasshServer is a network fingerprinting standard which can be used to identify specific Server SSH implementations. The fingerprints can be easily stored, searched and shared in the form of an MD5 fingerprint.
- hex: A value in hexadecimal format
- hostname: A full host/dnsname of an attacker
- hostname|port: Hostname and port number separated by a |
- http-method: HTTP method used by the malware (e.g. POST, GET, …).
- iban: International Bank Account Number
- identity-card-number: Identity card number

- impfuzzy: A fuzzy hash of import table of Portable Executable format
- imphash: Import hash - a hash created based on the imports in the sample.
- ip-dst: A destination IP address of the attacker or C&C server
- ip-dst|port: IP destination and port number separated by a |
- ip-src: A source IP address of the attacker
- ip-src|port: IP source and port number separated by a |
- issue-date-of-the-visa: The date on which the visa was issued
- ja3-fingerprint-md5: JA3 is a method for creating SSL/TLS client fingerprints that should be easy to produce on any platform and can be easily shared for threat intelligence.
- jabber-id: Jabber ID
- kusto-query: Kusto query - Kusto from Microsoft Azure is a service for storing and running interactive analytics over Big Data.
- last-name: Last name of a natural person
- link: Link to an external information
- mac-address: Mac address
- mac-eui-64: Mac EUI-64 address
- malware-sample: Attachment containing encrypted malware sample
- malware-type:
- md5: A checksum in md5 format
- middle-name: Middle name of a natural person
- mime-type: A media type (also MIME type and content type) is a two-part identifier for file formats and format contents transmitted on the Internet
- mobile-application-id: The application id of a mobile application
- mutex: Mutex, use the format \BaseNamedObjects<Mutex>
- named pipe: Named pipe, use the format .\pipe<PipeName>
- nationality: The nationality of a natural person
- other: Other attribute
- passenger-name-record-locator-number: The Passenger Name Record Locator is a key under which the reservation for a trip is stored in the system. The PNR contains, among other data, the name, flight segments and address of the passenger. It is defined by a combination of five or six letters and numbers.
- passport-country: The country in which the passport was issued
- passport-expiration: The expiration date of a passport
- passport-number: The passport number of a natural person
- pattern-in-file: Pattern in file that identifies the malware
- pattern-in-memory: Pattern in memory dump that identifies the malware
- pattern-in-traffic: Pattern in network traffic that identifies the malware
- payment-details: Payment details
- pdb: Microsoft Program database (PDB) path information
- pehash: PEhash - a hash calculated based of certain pieces of a PE executable file
- pgp-private-key: A PGP private key
- pgp-public-key: A PGP public key
- phone-number: Telephone Number
- place-of-birth: Place of birth of a natural person
- place-port-of-clearance: The port of clearance
- place-port-of-onward-foreign-destination: A Port where the passenger is transiting to
- place-port-of-original-embarkation: The orignal port of embarkation

- port: Port number
- primary-residence: The primary residence of a natural person
- prtn: Premium-Rate Telephone Number
- redress-number: The Redress Control Number is the record identifier for people who apply for redress through the DHS Travel Redress Inquiry Program (DHS TRIP). DHS TRIP is for travelers who have been repeatedly identified for additional screening and who want to file an inquiry to have erroneous information corrected in DHS systems
- regkey: Registry key or value
- regkey|value: Registry value + data separated by |
- sha1: A checksum in sha1 format
- sha224: A checksum in sha-224 format
- sha256: A checksum in sha256 format
- sha3-224: A checksum in sha3-224 format
- sha3-256: A checksum in sha3-256 format
- sha3-384: A checksum in sha3-384 format
- sha3-512: A checksum in sha3-512 format
- sha384: A checksum in sha-384 format
- sha512: A checksum in sha-512 format
- sha512/224: A checksum in the sha-512/224 format
- sha512/256: A checksum in the sha-512/256 format
- sigma: Sigma - Generic Signature Format for SIEM Systems
- size-in-bytes: Size expressed in bytes
- snort: An IDS rule in Snort rule-format
- special-service-request: A Special Service Request is a function to an airline to provide a particular facility for A Passenger or passengers.
- ssdeep: A checksum in ssdeep format
- stix2-pattern: STIX 2 pattern
- target-email: Attack Targets Email(s)
- target-external: External Target Organizations Affected by this Attack
- target-location: Attack Targets Physical Location(s)
- target-machine: Attack Targets Machine Name(s)
- target-org: Attack Targets Department or Organization(s)
- target-user: Attack Targets Username(s)
- text: Name, ID or a reference
- threat-actor: A string identifying the threat actor
- tlsh: A checksum in the Trend Micro Locality Sensitive Hash format
- travel-details: Travel details
- twitter-id: Twitter ID
- uri: Uniform Resource Identifier
- url: url
- user-agent: The user-agent used by the malware in the HTTP request.
- vhash: A VirusTotal checksum
- visa-number: Visa number
- vulnerability: A reference to the vulnerability used in the exploit
- weakness: A reference to the weakness used in the exploit
- whois-creation-date: The date of domain's creation, obtained from the WHOIS information.
- whois-registrant-email: The e-mail of a domain's registrant, obtained from the WHOIS information.

- whois-registrant-name: The name of a domain's registrant, obtained from the WHOIS information.
- whois-registrant-org: The org of a domain's registrant, obtained from the WHOIS information.
- whois-registrant-phone: The phone number of a domain's registrant, obtained from the WHOIS information.
- whois-registrar: The registrar of the domain, obtained from the WHOIS information.
- windows-scheduled-task: A scheduled task in windows
- windows-service-displayname: A windows service's displayname, not to be confused with the windows-service-name. This is the name that applications will generally display as the service's name in applications.
- windows-service-name: A windows service name. This is the name used internally by windows. Not to be confused with the windows-service-displayname.
- x509-fingerprint-md5: X509 fingerprint in MD5 format
- x509-fingerprint-sha1: X509 fingerprint in SHA-1 format
- x509-fingerprint-sha256: X509 fingerprint in SHA-256 format
- xmr: Monero Address
- yara: Yara signature
- zeek: An NIDS rule in the Zeek rule-format

13.4 Annex 4 – Good practices in Threat Intelligence

13.4.1 Introduction

This guide describes a set of best practices in threat intelligence analysis, based on the experience of the MISP project described in an article "Best Practices in Threat Intelligence" and well-known practises described by Information Sharing communities (ISAC or CSIRT).

13.4.2 Best practices

13.4.2.1 Improving analysis

Improvements on an existing Threat Intelligence analysis process may range from a notification of a false positive or a typographic error to a counter analysis of the original analysis.

According to the MISP project, there is a common challenge or question when an analyst is trying to improve an existing analysis: "**What will be the target audience of the improved analysis and the objective thereof?**" And three possible answers or scenarios:

- Informing the original analyst/author (e.g. a security vendor or a CSIRT) about a specific mistake or error which needs to be corrected.
- Improving an existing analysis by performing a complementary analysis or review which will be shared to and used by another group (e.g. a specific constituent, or a team within your organisation or a member of an ISAC, etc).
- The end-consumer will be an automaton.

In the first case, the Threat Intelligence platform (e.g. MISP), provides a way for proposing to the author of the analysis a correction or improvement. This functionality or mechanism is called "**proposals**". The proposal will be evaluated by the original author of the analysis, who can decide to accept or discard it. The proposal mechanism is a simple and fast way that avoids the need of creating a new event for improving or correcting an existing one.

In the second scenario, the analyst provides additional details to an existing analysis or an alternate point of view. The MISP platform provides a functionality for "**Extended events**" which allows to add additional information to an existing event that references the original analysis. The extended event can be shared back with the original author of the event or kept within a limited distribution scope such as a specific sector (e.g. Rail), a trusted group or as internal intelligence for the organisation providing the additional information.

The third scenario is about processing Threat Intelligence information in an **automated way**, such as processing an event using the PyMISP library and applying rules to the IDS or other security component automatically. This process can be potentially unreliable and it is key to fully understand the attributes of an event related with automation (e.g. IDS flag) as well as to understand the source of the data, the destination and how it can be used and the impact of using the data (e.g. using an attribute such a domain name in the firewall for blocking access).

13.4.2.2 Sharing valuable information

Valuable information might depend on the goal of the users sharing and/or using the information. There are different ways of contributing to share information that can be useful or valuable for a community:

- Analysis of a specific threat.
- Enhanced analysis of an existing report (such as data qualification, competitive or counter analysis).
- A post-mortem analysis of an incident.
- Additional information about existing or known threats (such as adversary techniques, new malware samples or complementary discoveries).
- False-positive or false-negative reporting.
- Asking for contribution or support from the community. This is also a way of warning others about a new threat. To address this approach, MISP platform provides the "collaborative intelligence" tag which allows to express the needs of the user/organisation asking for help.

13.4.2.3 Intelligence Tagging

The MISP platform provides a feature for classifying and tagging events using "taxonomies". There are more than 60 different taxonomies available, each of them with their tag associated. However, a large number of taxonomies may lead to two different concerns: "over-tagging" and "miss-tagging".

Over-tagging may lead to an overwhelming visual appearance and to confuse the audience. Miss-tagging, however, may lead to a misuse of shared data, which can be potentially harmful (e.g. to share with other groups information that is confidential).

To address the problem of data misusing, MISP proposes a set of tags that should be at the creation stage of any event such as:

- **TLP-Tags**: TLP uses a simple four colour schema for indicating how intelligence can be shared.
- **Confidence-Tags/Vetting State**: there are huge differences in the quality of data, whether it was careful exanimated before sharing. As this means that the author was confident that the shared data is or at least was a good indicator of compromise.
- **Origin-Tags**: describes where the information came from, and whether it was in an automated fashion or in a manual investigation. This should give an impression how reliable and valuable this intelligence is, as manual investigation should have more added value than an automatic generation of data.
- **PAP-Tags**: a more advanced approach of data classification is using the Permissible Actions Protocol. It indicates how the received data can be used to search for compromises within the individual company or constituency.

13.4.2.4 Express confidence or probability in an analysis

Threat Intelligence analysis or reports are often shared together with technical details and it is a good practise to add to this information a confidence level using some existing options that MISP provides such as the MISP taxonomies admiralty-scale or the estimative-language.

Generally, it is a good practice to use this kind of taxonomies, as this will enhance the trust/value. Adding confidence or estimative probability has multiple advantages such as allowing organisations to filter, classify and score the information in an automated way based on related tags (e.g. prioritise events with high confidence).

13.4.2.5 Track and keep the state of an analysis

Keeping track of the advancement of an analysis, tracing the progress and what actions have been done or what are the next steps is something useful for the analyst as well as for other people or organisations reding or relying on the analysis.

The MISP platform provides a taxonomy for this propose called workflow, which allows the analyst to express the state of the analysis as well as what actions have to be performed.

13.4.2.6 Classify information

Classifying information helps assessing the main information quickly. Besides, it can help build correlations between events or attributes, allowing analysts to better understand threats and to connect the dots.

MISP provides several mechanisms or features for classifying information such as tags and taxonomies:

- Tags can be used to describe how the information can be shared, using the TLP (Traffic Light Protocol) taxonomy, in order to prevent information leaks. They can also be used to describe the source where information came from.
- Taxonomies allow the user to further explain the kind of threat or make relations
- The analyst can also to add their own custom taxonomy or galaxy as well as to use comments to complete or clarify the information of the event.

13.4.3 Glossary

ISAC
Information Sharing and Analysis Center

MISP
MISP - Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing

MISP Modules
MISP modules are autonomous modules that can be used for expansion and other services in MISP. MISP modules GitHub Repository

MISP warninglists

MISP warninglists are lists of well-known indicators that can be associated to potential false positives, errors or mistakes. MISP warninglists GitHub Repository

MISP noticelists

Notice lists to inform MISP users of the legal, privacy, policy or even technical implications of using specific attributes, categories or objects. MISP noticelist GitHub Repository

MISP Taxonomies

Taxonomy is the practice and science of classification. The word is also used as a count noun: a taxonomy, or taxonomic scheme, is a particular classification. The word finds its roots in the Greek language τάξις, taxis (meaning 'order', 'arrangement') and νόμος, nomos ('law' or 'science'). For more details on taxonomies and classification the documentation. Partial source "Taxonomy_(general)" - CCBYSA. There is a Python module available to work with Taxonomies in a Pythonic way called PyTaxonomies. MISP taxonomies GitHub Repository

MISP Sightings

Basically, sighting is a system allowing people to react on attributes on an event. It was originally designed to provide an easy method for user to tell when they see a given attribute, giving it more credibility.

MISP Objects

MISP objects are used in MISP (starting from version 2.4.80) system and can be used by other information sharing tool. MISP objects are in addition to MISP attributes to allow advanced combinations of attributes. The creation of these objects and their associated attributes are based on real cyber security use-cases and existing practices in information sharing. The objects are just shared like any other attributes in MISP even if the other MISP instances don’t have the template of the object. The following document is generated from the machine-readable JSON describing the MISP objects. MISP objects GitHub Repository More

API

MISP makes extensive use of its RESTful API (Application programming interface) both internally and provides an external API for automation, synchronisation or any other tasks requiring a machine to machine interface. In general terms, it is a set of clearly defined methods of communication between various software components. A good API makes it easier to develop a computer program by providing all the building blocks, which are then put together by the programmer. An API may be for a web-based system, operating system, database system, computer hardware or software library. The de-facto standard for talking to MISP via an API is PyMISP. Partial source "API" - CCBYSA.

RESTful

Representational state transfer (REST) or RESTful web services are a way of providing interoperability between computer systems on the Internet. REST-compliant Web services allow requesting systems to access and manipulate textual representations of Web resources using a uniform and predefined set of stateless operations. Other forms of Web services exist which expose their own arbitrary sets of operations such as WSDL and SOAP. Source "REST" - CCBYSA.

PyMISP
PyMISP is a Python library to access MISP platforms via their REST API. PyMISP allows you to fetch events, add or update events/attributes, add or update samples or search for attributes.

IDS
An IDS flag on an attribute allows to determine if an attribute can be automated (such as being exported as an IDS ruleset or used for detection). If the IDS flag is not present, the attribute can be useful for contextualisation only.

IOC
Indicator of compromise (IOC or IoC) is an artefact observed on a network or in an operating system or information channel that could reference an intrusion or a reference to a technique used by an attacker. IoCs are a subset of indicators.

Attribute
Attributes in MISP can be network indicators (e.g. IP address), system indicators (e.g. a string in memory) or even bank account details.

Observable
Observables are essentially the same as (MISP) attributes.

Site Admin
As an admin (not to be confused with Org Admin), you can set up new accounts for users, edit user profiles, delete them, or just have a look at all the viewers' profiles. Site admins have access to every administrator feature for all the data located on the system including global features such as the creation and modification of user roles and instance links. You will also see all other organisations connected or setup in the instance. The site admin can be considered as a super-user of a MISP instance.

Org Admin
Organisation admins (Org Admin) are restricted to executing site-admin actions exclusively within their own organisation’s users only. They can administer users, events and logs of their own respective organisations.

OSINT
Open-source intelligence (OSINT) is data collected from publicly available sources to be used in an intelligence context. In the intelligence community, the term "open" refers to overt, publicly available sources (as opposed to covert or clandestine sources). It is not related to open-source software or public intelligence. OSINT under one name or another has been around for hundreds of years. With the advent of instant communications and rapid information transfer, a great deal of actionable and predictive intelligence can now be obtained from public, unclassified sources. Source "Open-source intelligence" - CCBYSA.