4SECURail

EU-CSIRT collaborative environment dedicated to rail

A co-designed Model and Platform

Cybersecurity in Railways, ENISA-ERA Conference
16-17 March 2021, Online

Antonio López
alopez@hitrail.com
https://www.hitrail.com
Marcos Sacristán
Marcos.sacristan@treetk.com
https://www.treetk.com/en

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.

Shift2Rail

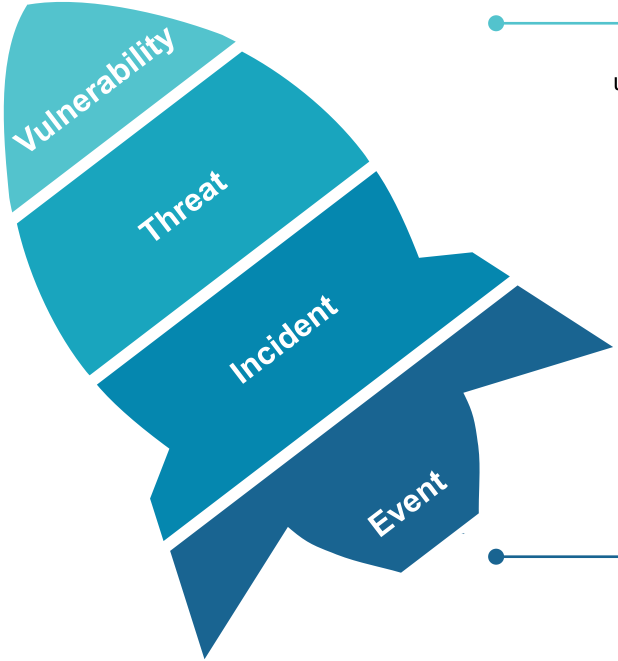
1 Background & context

2 Research, findings & requirements

3 CHIRP4Rail: model & platform

4 Conclusions & Issues for discussion

4SECURail – CSIRT Key definitions (according to ENISA*)



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.

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.

Incident

An **event** that has been assessed as having an actual or potentially **adverse effect on the security** or performance of a system.

Event

Occurrence of a particular set of circumstances (certain or uncertain; single occurrence or a series of occurrences).

* https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary

4SECURail – CSIRT Background, Aim and Objectives

01

Background

The Shitf2Rail programme has called for work on defining a draft **CSIRT organisational framework**, supported by a draft and **demonstrated CSIRT Platform,** and has selected the 4SECURail project to deliver this CSIRT task.

02

Aim

The main aim is to **deliver a pilot CSIRT co-designed by the relevant rail stakeholders** (Rail CISOs + Rail SOCs + Rail IT security teams, etc.) along with a **working pilot platform** (collaborative environment) also co-designed with those stakeholders.

03

Objective 1

To **define stakeholder requirements** for a European Rail CSIRT collaborative activity, and to co-design with them a first draft CSIRT model for open consultation.

04

Objective 2

To **test and validate the draft CSIRT model,** and to obtain sufficient feedback and co-design input to release the final CSIRT model to support organisational collaboration, as well as collaborative platform design.

05

Objective 3

To **identify relevant platforms** to support CSIRT collaboration and, based on requirements and CSIRT model, specify and adapt to meet CSIRT needs.

06

Objective 4

To **test and updated the CSIRT collaborative environment**t to ensure meeting user needs.

4SECURail – CSIRT Context

Single European Railway Area (SERA)

- Railways are a strategic area of European Shared Infrastructure and are one of the **most extensive cross-border and pan-European "essential services".**
- Railway information networks and digital services are interconnected to facilitate the ***SERA concept***.
- All European railway infrastructure, both physical and IT/OT, can be conceived as a **single network.**
- SERA depends on **cross-border inter-organisational collaboration** to ensure effective and safe operation of European railway business.

NIS Directive

- NIS ensures a **European framework for cyber security:**
  - ENISA / National CSIRTs (MS) / Cooperation Group/ European CSIRT Network / ISACs (Sectors).
- European railways are both **Operators of essential services** (OES) and **Critical Infrastructures** (CI).
- Railway OES also depends on **Digital Service Providers** (DSPs) who deploy and manage systems and services.
- Railway OES and DSPs must a) take **appropriate security measures** and b) **notify serious incidents.**
- Within a single rail OES, *identification of threats and response to threats* are coordinated by an **internal security team** (e.g., a CSIRT, SOC, IT-OT security team, etc.)
- At pan-European level, an **intrusion at any point can result in damage at other points** of SERA: collaboration is clearly demanded.
- Therefore, the potential benefit of a **European Railway CSIRT** involving security teams from multiple Rail OES.

4SECURail – CSIRT Context

CSIRT and ISAC

- 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 them and support their constituents to recover from breaches*."
- An ISAC is a "***sectoral member-driven organisation*** *to collect, analyse and disseminate information on cyber-threats, so as to help critical infrastructure owners and operators protect facilities, staff and customers from cyber threats*"
- While the basic difference between a CSIRT and an ISAC is clear (response versus information sharing), it is necessary to highlight the ER-ISAC potential to **capitalise on collaboration and coordination** and to steer the proposed 4SECURail CSIRT Threat Intelligence platform.

Essential Services

ENISA review of rail stakeholders identifies the following rail **essential services:**

- 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

UIC

The UIC **hosting the ER-ISAC initiative** to support and coordinate ER-ISAC activities.

X2RAIL-3

The other Shift2Rail initiative (X2RAIL-3 – CSIRT Concept) will deliver a **feasibility study defining a common criteria** for the implementation and setup of a single European rail CSIRT.

4SECURail – CSIRT Context

Based on the previous analysis, the following general needs can be identified:

These needs identify some general requirements that help to define the potential EU Rail CSIRT Model.

Collaborate in support for **cyber security response**.

Share **threat intelligence** concerning incidents, threats (known and new) and mitigation (strategies and measures).

Build teams for handling **collaborative response** and supporting recovery.

Engage **relevant digital service providers** (DSPs) and **equipment suppliers** in collaborative response.

Ensure all essential services, as defined by ENISA study, **are addressed**.

Define manual or automatic **sharing mechanisms**.

1	Background
2	Research, findings & requirements
3	CHIRP4Rail: model & platform
4	Conclusions & Issues for discussion

4SECURail – CSIRT Desk Research

CSIRT Examples: Significant features of Relevance to EU Rail

CERT-NL

Is a Dutch government model supporting governmental bodies as well as **vital process providers essential** for The Netherlands. In addition to prevention and intrusion-detection solutions, the CERT provides **services to analyse** attempted or real intrusion events.

NATO NCIRC

is an international organisation supporting its various sites and systems, along with its allies and strategic partners. Their focus in on **prevention, including sharing of threat intelligence** and mitigation measures and education activities.

CIRCL-LU

is a government model supporting all communes, private sector, and NGOs. Their primary aim concerns **systematic response** to cyber security incidents and coordination of **communication** between involved stakeholders.

ENISA model

is a very detailed CSIRT model and guidance derived by ENISA offering **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 the strongest preventive capability in the host organisation.

4SECURail – CSIRT Desk Research

CSIRT Coordination Examples: Coordinating CSIRTs

CERT-CC Computer Emergency Response Team

- This "Coordination Centre" started in 1988 by the U.S. Department of Defence.
- Provides **CSIRT *coordination***, incident reporting, security audit, sharing threat intelligence, artefact analysis and education of cyber experts.

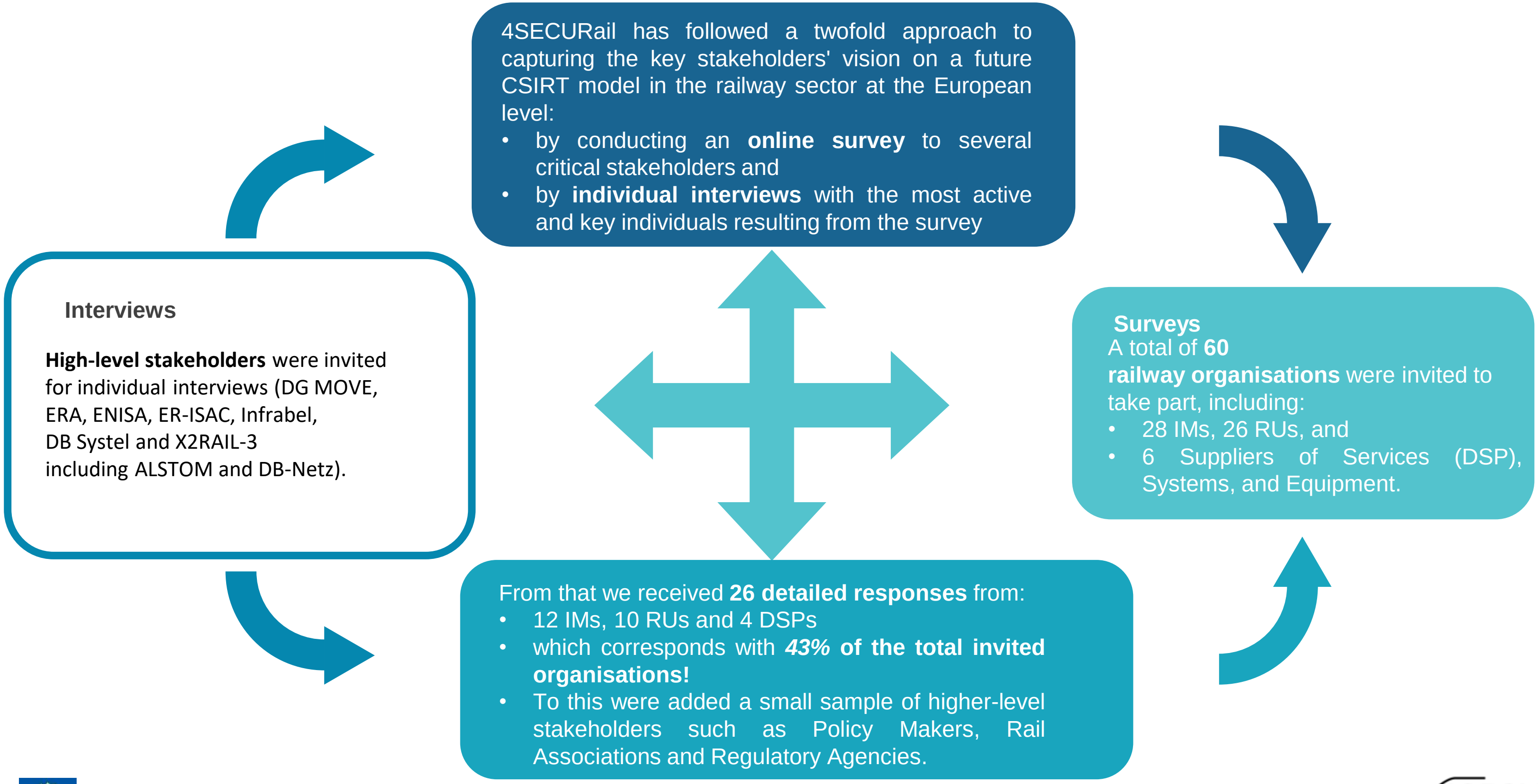
CSIRT Network established under *NIS*

- ensures **strategic cooperation** between EU Member States in ensuring cybersecurity, including exchange of information on threats and incidents.
- 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.

FIRST CSIRT Network

- is a confederation of trusted computer incident *response teams* (not all CSIRTs) who ***cooperate* to support each other in handling security incidents.**
- Members fund FIRST as a **non-profit enterprise** providing security team development and support, training, threat intelligence sharing, coordinating members in supporting each other (best practices + during incident response).

4SECURail – CSIRT Surveys & 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 several critical stakeholders and
- by **individual interviews** with the most active and key individuals resulting from the survey

Surveys

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 that we received **26 detailed responses** from:

- 12 IMs, 10 RUs and 4 DSPs
- which corresponds with ***43%* of the total invited organisations!**
- To this were added a small sample of higher-level stakeholders such as Policy Makers, Rail Associations and Regulatory Agencies.

Interviews

High-level stakeholders were invited for individual interviews (DG MOVE, ERA, ENISA, ER-ISAC, Infrabel, DB Systel and X2RAIL-3 including ALSTOM and DB-Netz).

4SECURail – CSIRT Workshop, Advisory Board and X2RAIL-3

CSIRT Coordination Examples: Coordinating CSIRTs

CSIRT Workshop, June 9th, 2020 online

- Organised by UIC together with Hit Rail and Tree Technology.
- Attended by **25 participants** from several IMs and RUs as well as representatives from ER-ISAC, ENISA, ERA and X2RAIL-3.

CSIRT Advisory Board meetings

- Compounded by a group of **external independent experts** from DG MOVE, Expleo from France, Cervello from Israel and UIFE
- Main discussion and advise was about **sharing experiences on how to build trust** between stakeholders involved in information sharing and cooperation.

Collaboration with Shift2Rail X2RAIL-3

- Several meetings with X2RAIL-3 were organised to **receive feedback and inputs** on the CSIRT model defined by 4SECURail.
- Output of 4SECURail project (model and demonstrator) will be used by X2RAIL-3 to **deliver a feasibility study** on challenges and recommendation for a single European CSIRT dedicated to rail.

4SECURail – CSIRT Functional Requirements

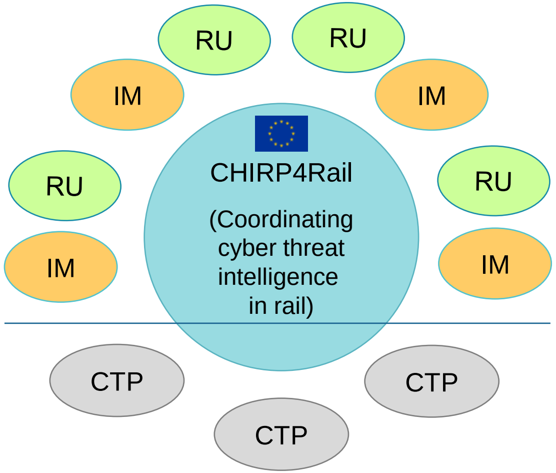
The evident need to coordinate information exchanges between railway security teams for EU-wide cyber security suggests a model that is **data driven, and bottom-up**:

- identifying **what data is to be shared** between rail security teams;
- identifying an **operational strategy to enable exchange**, supported by technical and operational schemes;
- identifying a **suitable management model** to facilitate and ensure 1 and 2.

Based on the requirements collected in the previously reported activities, we have identified the need for exchanges of different kinds of data and information flows among the key actors.

Key Actors:

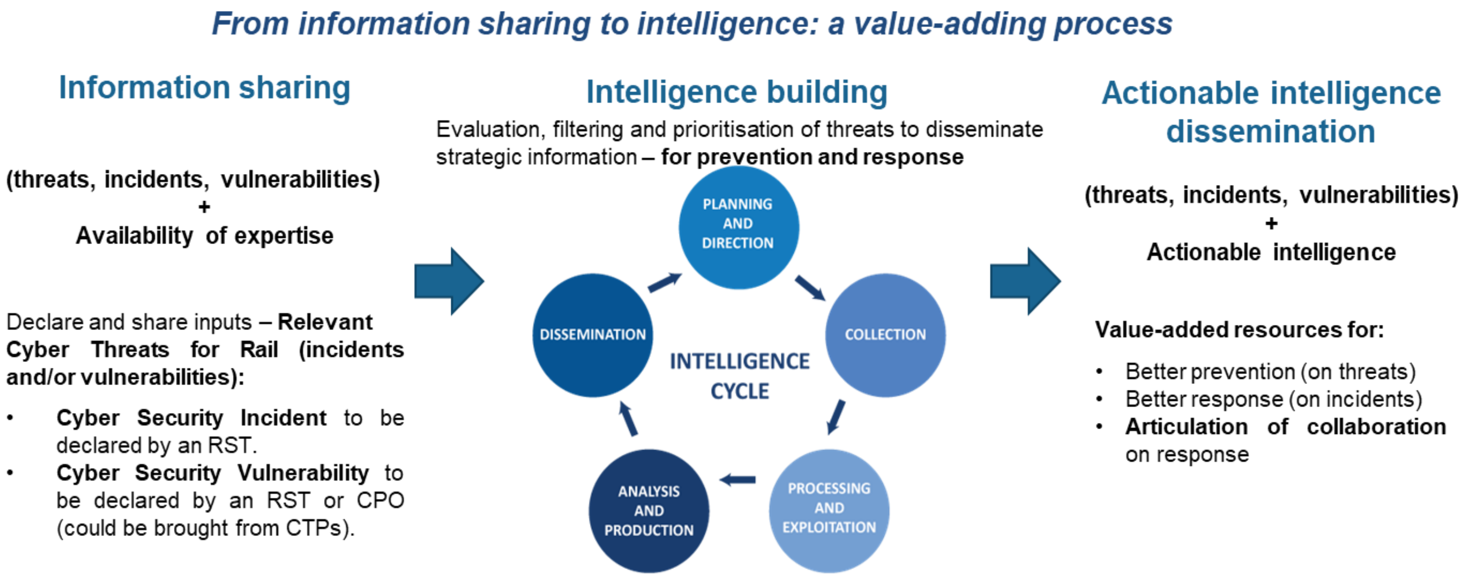
- **IM / RU Rail Security Teams** (RSTs):
  - Formed as a CSIRT, CERT, SOC or any other operational form.
  - Operational at national level.
- **CHIRP4Rail:**
  - EU level Rail CSIRTs Threat Intelligence coordination - **CHIRP4Rail Platform Operator (CPO)**.
  - Operational at EU level; intelligence coordination role.



Cyber Threat trusted Partners (CTPs)

- Public bodies (e.g., National CERTs, European CSIRT Network –ECN–)
- Rail DSPs and equipment suppliers
- Commercial rail threat intelligence providers (e.g., cybersecurity industry)

4SECURail – CSIRT Functional Requirements



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

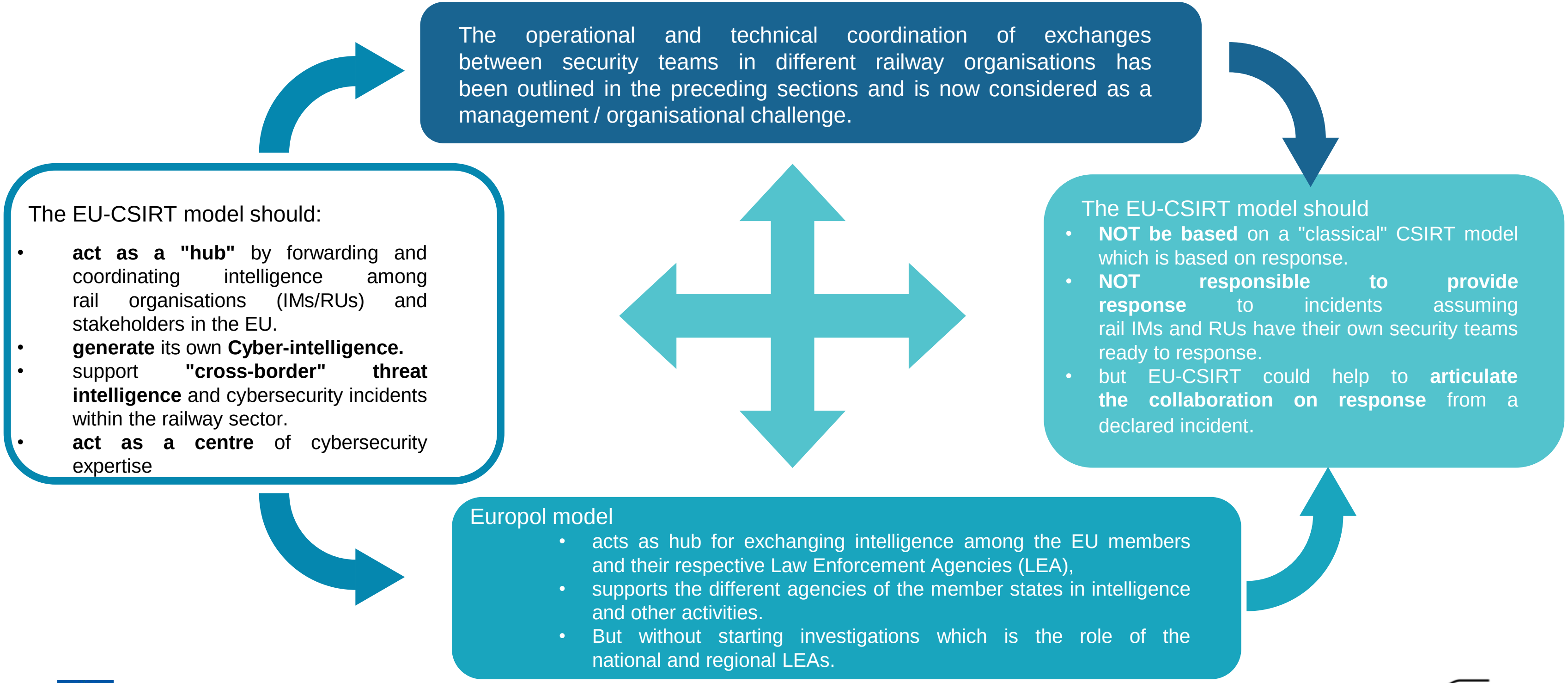
(threats, incidents, vulnerabilities)
+
Actionable intelligence

Value-added resources for:

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

- These data sharing and information flow will determine the **functional model** and the necessary operational and **organisational features** required to support such exchanges.
- The data and information to be exchanged between railway security teams may **need to be anonymised depending on the content** and the trust relations established among the security teams.

4SECURail – CSIRT Organisational Requirements



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

The EU-CSIRT model should:

- **act as a "hub"** by forwarding and coordinating intelligence among rail organisations (IMs/RUs) and stakeholders in the EU.
- **generate** its own **Cyber-intelligence.**
- support **"cross-border" threat intelligence** and cybersecurity incidents within the railway sector.
- **act as a centre** of cybersecurity expertise

The EU-CSIRT model should

- **NOT be based** on a "classical" CSIRT model which is based on response.
- **NOT responsible to provide response** to incidents assuming rail IMs and RUs have their own security teams ready to response.
- but EU-CSIRT could help to **articulate the collaboration on response** from a declared incident.

Europol model

- acts as hub for exchanging intelligence among the EU members and their respective Law Enforcement Agencies (LEA),
- supports the different agencies of the member states in intelligence and other activities.
- But without starting investigations which is the role of the national and regional LEAs.

1 Background

2 Research, findings & requirements

3 CHIRP4Rail: model & platform

4 Conclusions & Issues for discussion

4SECURail – CSIRT - CHIRP4Rail Concept and Rationale

The need:

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

The context:

enisa NIS Directive CSIRTs NETWORK ISAC Shift2Rail X2RAIL 3

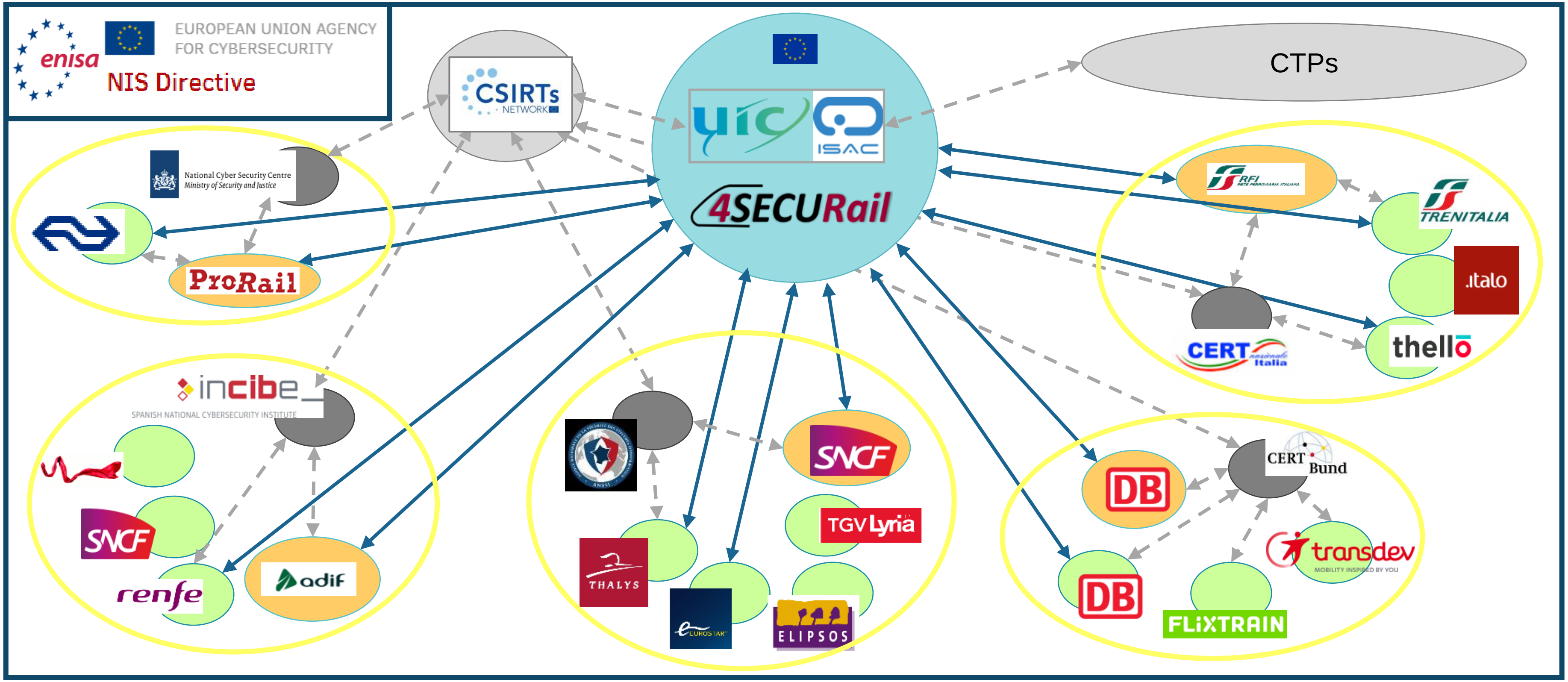
The opportunity:

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

4SECURail

The CHIRP4Rail approach:

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



● CHIRP4Rail platform

● Infrastructure Managers RST

● Railway Undertakings RST

● National Authorised CERTs/CSIRTs

● CyberThreat Intelligence providers (CTPs)

○ Member states

4SECURail –CHIRP4Rail Mission and Objectives

Mission

Support information sharing and threat intelligence generation among the rail cybersecurity teams.

☑ Objective

Structure a bottom-up dialogue among European rail cybersecurity teams

☑ Objective

Provide effective means for information sharing among rail stakeholders

☑ Objective

Build community and trust among rail cybersecurity stakeholders

☑ Objective

Leverage information and expertise to produce rail-specific cybersecurity intelligence

4SECURail – CHIRP4Rail Functional Model – 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

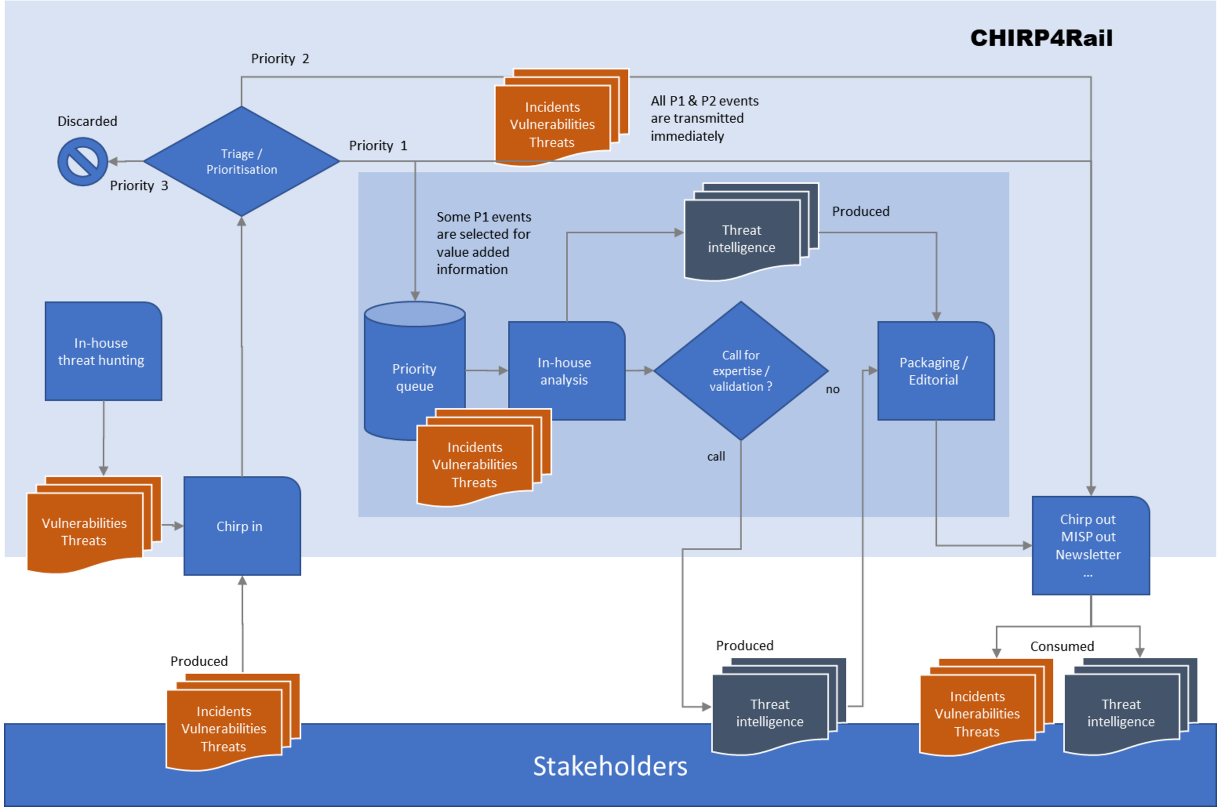
Collaborative prioritisation and analysis of threats

- 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**

4SECURail – CHIRP4Rail Functional Model – Workflow


CHIRP4Rail
Priority 2
Incidents Vulnerabilities Threats
All P1 & P2 events are transmitted immediately
Discarded
Triage / Prioritisation
Priority 1
Priority 3
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
Threat intelligence
Consumed
Produced
Incidents Vulnerabilities Threats
Incidents Vulnerabilities Threats
Threat intelligence
Stakeholders

4SECURail – CHIRP4Rail Organisational Model

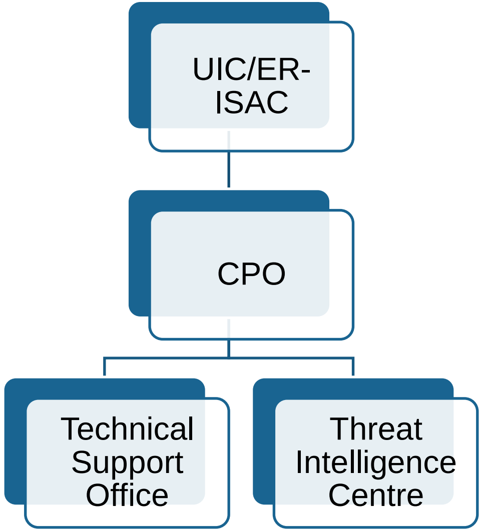
The proposed functional model shall be expressed as an organisational form among the key actors, based on key role and main functions:

Actors	UIC/ER-ISAC	IM/RU RSTs	CTPs	CPO
Role	• **Steer** the CHIRP4Rail Model	• Be a **Member**	• Be a **Trusted Partner**	• **Manage** 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	• Provide a **secure communication** platform • Provide **actionable intelligence** • Provide **technical support** to RSTs and CTPs

4SECURail – CHIRP4Rail Management Model

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

- The UIC/ER-ISAC bodies should:
  - **Select** the trusted CPO,
  - **Manage** on a day-to-day basis the CPO,
  - **Coordinate** activities with the ECN.
- The CPO should provide:
  - **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.



4SECURail – CHIRP4Rail Technical Model

Data Model

Modelling Cyber-Incident, Threats or Vulnerabilites relevant within the Rail sector

- Based on **MISP**
- **Event** as the high-level entity

Control of sensitive information

- Traffic Light Protocol (TLP)
- Information flow confirfguration (local, all the organisations, custom group)

Taxonomy

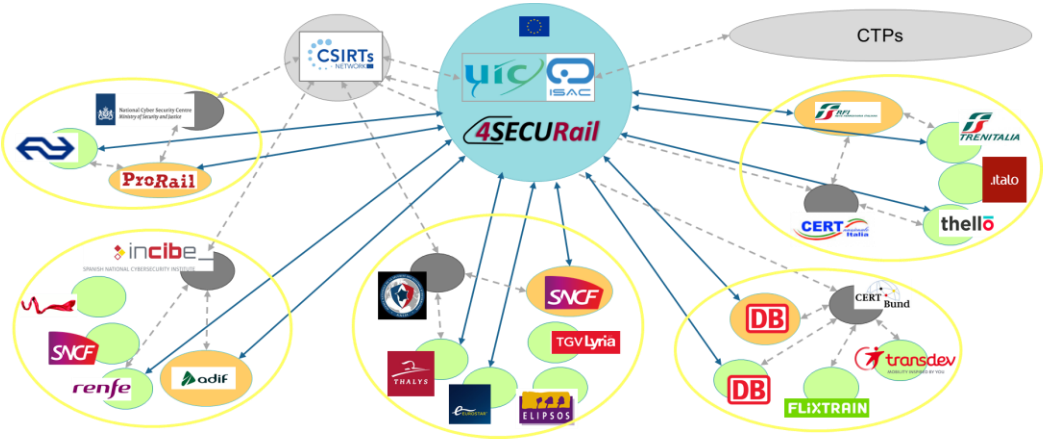
Classify and organise Events

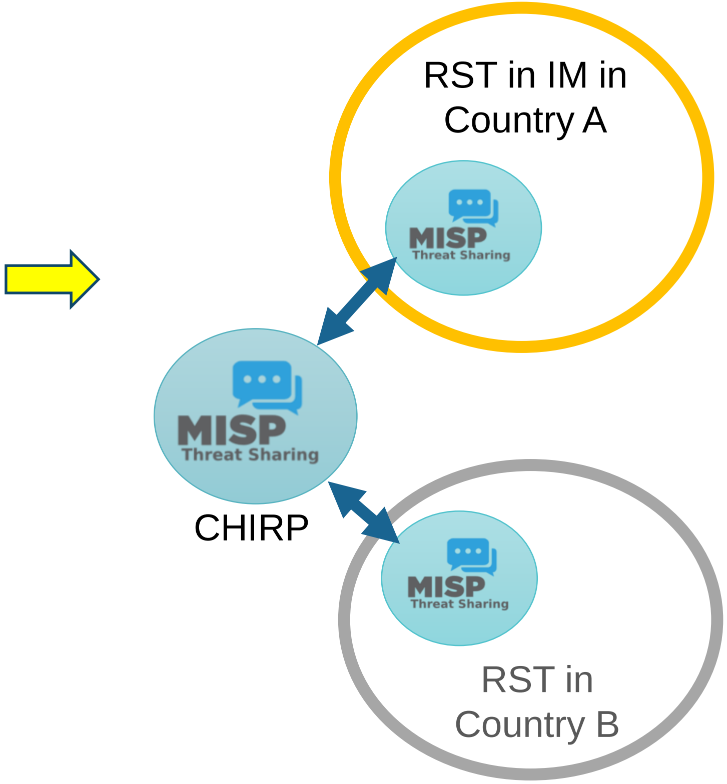
- A **common vocabulary** among different organisations.
- **Better and quicker understanding**, high-level category

X2-Rail-1 Taxonomy

- **Threats in the railway landscape.**
- Deliverable 8.2 "Security Assessment"
- "Name of Taxonomy: Category": "Threat"

4SECURail – CHIRP4Rail Platform (protoype)



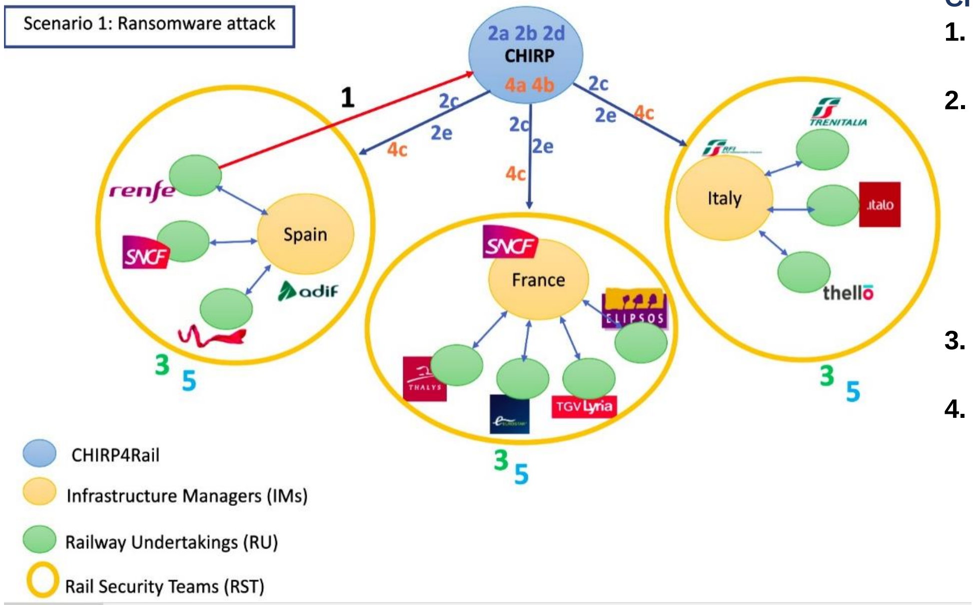


Recreation of Threat Intelligence information sharing in the RST community:

- **Threat / Incident report**
- **Detection of malware campaigns**
- **Identification and correction of IT/OT vulnerabilities**
- **…**

4SECURail – CHIRP4Rail un use (use case examples)

Example 1: Ransomware case

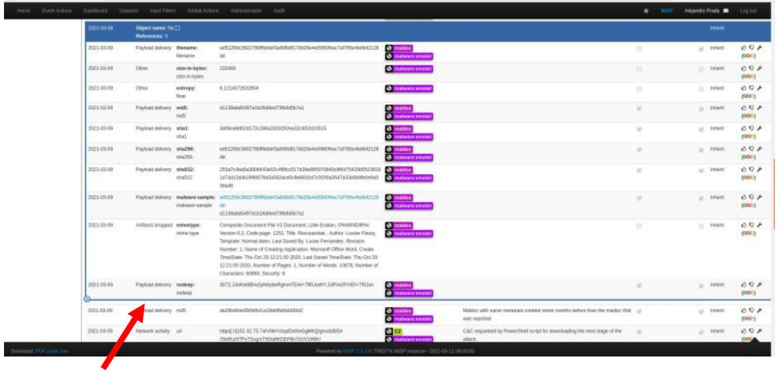


CHIRP flow

1. **Spear phishing notification**: An RST discovered an attempt of attack, and reported to CHIRP
2. **Early in-house analysis:** CHIRP analysts perform "in-house analysis" to expand information about this threat:
   a. Technical details of the malware (family, goal, IoCs).
   b. Event update with findings (URLs, Yara rule).
   c. Share finding with RST community.
   d. Further analysis with OSINT reveals context.
   e. CHIRP analysts update info with new URLs.
3. **RST Notification (1):** RST community get feedback; they can update their systems with information provided by the CHIRP.
4. **Further malware analysis**: CHIRP continue analysing malicious files in-depth for understanding the malware behaviour:
   a. Static and dynamic analysis reveals lateral network move.
   b. Threat Hunting reveals malware variants (samples).
   c. Notification updated with TTPs (Tactics, Techniques and Procedures) used by attackers.
5. **RST notification (2)**: The RST community can update their defence and detection mechanisms based on the TTPs reported by the CHIRP

4SECURail – CHIRP4Rail un use (use case examples)

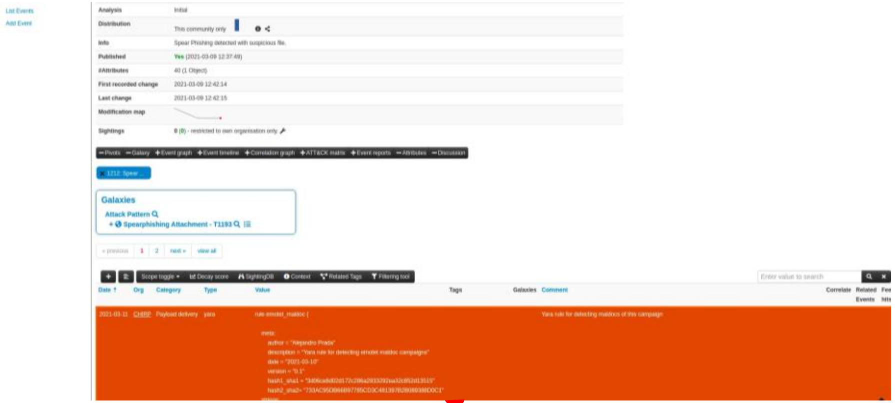
Example 1: Ransomware case



2021-03-09	Object name: file References: 0					Inherit
2021-03-09	Payload delivery	filename: filename	ed51269c3602786f6dde f3a808d8178d26e4e5960f4ac7af765e4bd642128 dd	maldoc malware:emotet		Inherit
2021-03-09	Other	size-in-bytes: size-in-bytes	233466	malware:emotet		Inherit
2021-03-09	Other	entropy: float	6.1214072632604	malware:emotet		Inherit
2021-03-09	Payload delivery	md5: md5	d1138abd5467e1b26d6ed73fb9d5b7a1	maldoc malware:emotet		Inherit
2021-03-09	Payload delivery	sha1: sha1	3d06ce8d02d172c286a2833292ea32c852d13515	maldoc malware:emotet		Inherit
2021-03-09	Payload delivery	sha256: sha256	ed51269c3602786f6dde f3a808d8178d26e4e5960f4ac7af765e4bd642128 dd	maldoc malware:emotet		Inherit
2021-03-09	Payload delivery	sha512: sha512	[illegible]	maldoc malware:emotet		Inherit
2021-03-09	Payload delivery	malware-sample: malware-sample	ed51269c3602786f6dde f3a808d8178d26e4e5960f4ac7af765e4bd642128 dd d1138abd5467e1b26d6ed73fb9d5b7a1	maldoc malware:emotet		Inherit
2021-03-09	Artifacts dropped	mimetype: mime-type	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Title: Recusandae., Author: Louise Fleury, Template: Normal.dotm, Last Saved By: Lucas Fernandez, Revision Number: 1, Name of Creating Application: Microsoft Office Word, Create Time/Date: Thu Oct 29 12:21:00 2020, Last Saved Time/Date: Thu Oct 29 12:21:00 2020, Number of Pages: 1, Number of Words: 10676, Number of Characters: 60888, Security: 8	maldoc malware:emotet		Inherit
2021-03-09	Payload delivery	ssdeep: ssdeep	[illegible]	maldoc malware:emotet		Inherit
2021-03-09	Payload delivery	md5	[illegible]	maldoc malware:emotet	Maldoc with same metadata created some months before than the maldoc that was reported	Inherit
2021-03-09	Network activity	url	[illegible]	C2 malware:emotet	C&C requested by PowerShell script for downloading the next stage of the attack	Inherit

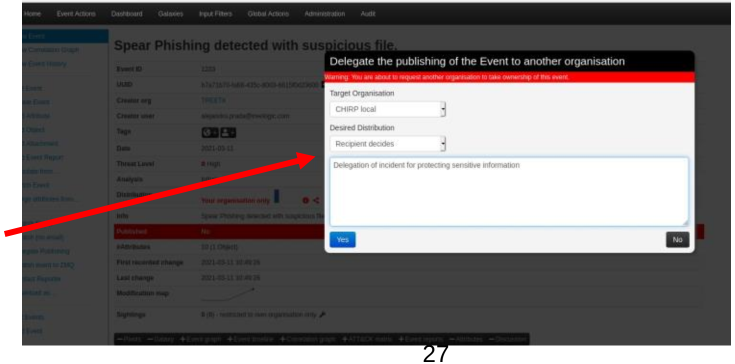
Download: PGP public key — Powered by MISP 2.4.140 TREETK MISP instance - 2021-03-11 08:03:00

Malicious doc reported by IM's RST.



Analysis	Initial
Distribution	This community only
Info	Spear Phishing detected with suspicious file.
Published	Yes (2021-03-09 12:37:49)
#Attributes	40 (1 Object)
First recorded change	2021-03-09 12:42:14
Last change	2021-03-09 12:42:15
Modification map	
Sightings	0 (0) - restricted to own organisation only

Date	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events
2021-03-11	CHIRP	Payload delivery	yara	rule emotet_maldoc { meta: author = "Alejandro Prada" description = "Yara rule for detecting emotet maldoc campaigne" date = "2021-03-10" version = "0.1" hash1_sha1 = "3d06ca8d02d172c286a2833292ea32c852d13515" hash2_sha2= "733AC95D866B977B5CD3C481397B2808938DC1"			Yara rule for detecting maldocs of this campaign		



Spear Phishing detected with suspicious file.

Event ID	1233
UUID	b7a71b70-fa68-435c-8009-6615f0d23600
Creator org	TREETK
Creator user	alejandro.prada@treetk.com
Tags	
Date	2021-03-11
Threat Level	High
Analysis	Initial
Distribution	Your organisation only
Info	Spear Phishing detected with suspicious file
Published	No
#Attributes	10 (1 Object)
First recorded change	2021-03-11 10:49:26
Last change	2021-03-11 10:49:26
Modification map	
Sightings	0 (0) - restricted to own organisation only

Delegate the publishing of the Event to another organisation

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

Target Organisation: CHIRP local

Desired Distribution: Recipient decides

Delegation of incident for protecting sensitive information

Attribute (Yara rule) proposed (orange) by the CHIRP.

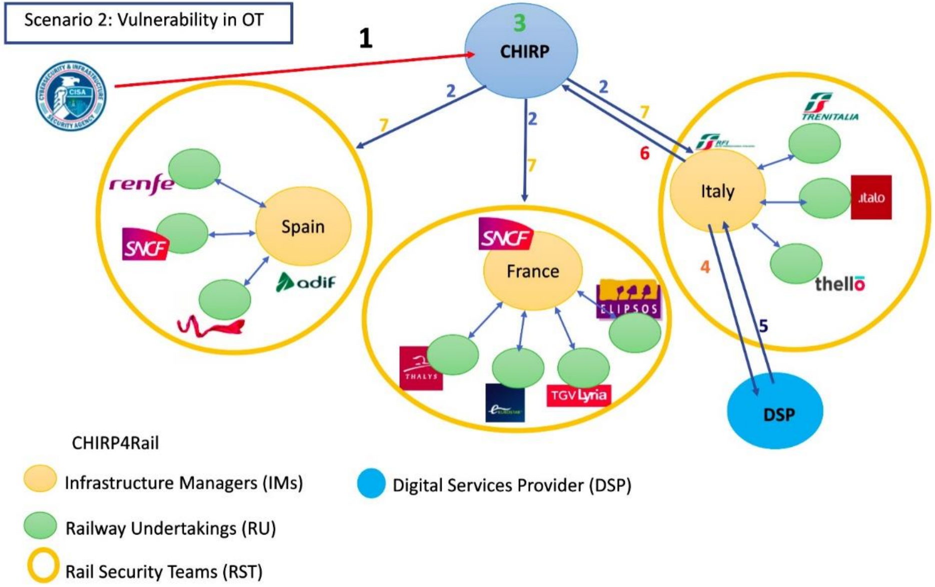
Delegation of event publication to CHIRP (pseudo-anonymisation)

4SECURail – CHIRP4Rail un use (use case examples)

Example 2: Ransomware case

CHIRP flow

1. **Vulnerability report**: CISA published a public vulnerability on a specific device, together with mitigation recommendations. An automatic alert at CHIRP has identified this as relevant for rail. After analysis, triage has been rankled high as it impacts a critical component in railway, in particular in high-speed tunnels.
2. **RST Notification (1)**: CHIRP alerts RSTs at IMs. They can manage internally how to mitigate, considering recommendations.
3. **In-house analysis**: CHIRP analysts have been monitoring the Internet and discovered a public exploit. They update the information about the exploit, and effective countermeasures – RST Notification (2).
4. **Supplier's involvement**: RST has discovered the vulnerability would impact other components. The OT supplier in involved in fixing.
5. **Supplier's update**: A firmware update is published. This will protect infrastructure without compromising other components.
6. **Event update notification**: The RST updates the event on the CHIRP with info about the new firmware version fixing vulnerability.
7. **RST Notification (3)**: The RST community update their information, and check updates for their devices.



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

1 Background

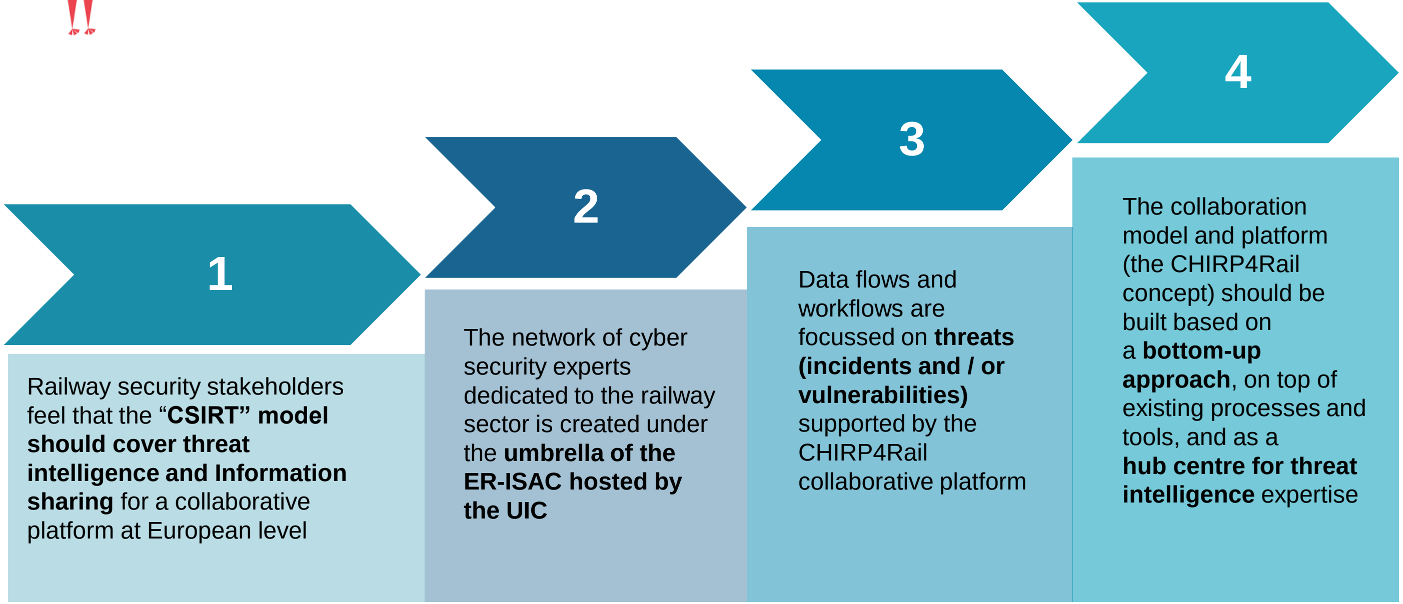
2 Research, findings & requirements

3 CHIRP4Rail: model & platform

4 Conclusions & Issues for discussion

4SECURail – CHIRP4Rail – Conclusions

CHIRP: “***Sharp sound made by small birds***”



1

Railway security stakeholders feel that the **“CSIRT” model should cover threat intelligence and Information sharing** for a collaborative platform at European level

2

The network of cyber security experts dedicated to the railway sector is created under the **umbrella of the ER-ISAC hosted by the UIC**

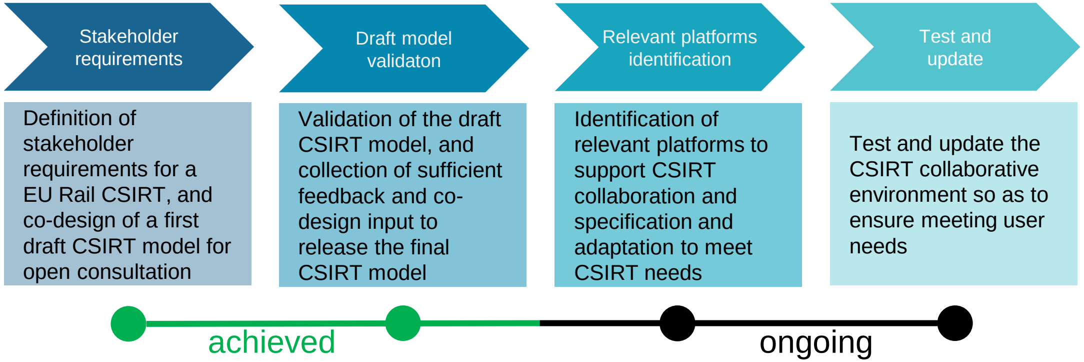
3

Data flows and workflows are focussed on **threats (incidents and / or vulnerabilities)** supported by the CHIRP4Rail collaborative platform

4

The collaboration model and platform (the CHIRP4Rail concept) 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

4SECURail – CSIRT Project Status



Stakeholder requirements

Definition of stakeholder requirements for a EU Rail CSIRT, and co-design of a first draft CSIRT model for open consultation

Draft model validaton

Validation of the draft CSIRT model, and collection of sufficient feedback and co-design input to release the final CSIRT model

Relevant platforms identification

Identification of relevant platforms to support CSIRT collaboration and specification and adaptation to meet CSIRT needs

Test and update

Test and update the CSIRT collaborative environment so as to ensure meeting user needs

CSIRT Workstream

- 🟢 Requirement definition finished
- 🟢 Final CSIRT model released
- ⚫ Currently working on the CSIRT platform

https://www.4securail.eu/Documents.html

4SECURail – CHIRP4Rail platform: trust building?

What could be the community engagement mechanisms to encourage contributions?

Initiative 1

Get fully support from ER-ISAC, the UIC and the rail national CISOs.

Initiative 2

Get early adopters capable of leading the implementation of the CHIRP4Rail platform.

Initiative 3

Get valuable and relevant information, avoid noise and information overload.

Initiative 4

Deliver actionable intelligence to prevent real threats relevant to rail.

Information Sharing and Cooperation: How to build trust?

Initiative 5

Deliver an easy-to-use and highly secure platform.

Initiative 6

Guarantee voluntary and anonymous sharing of threat intelligence information.

Initiative 7

Provide suitable and useful training to the users.

Initiative 8

Provide additional community tools such as a Technical Forum.

4SECURail

Thank you for your attention

Antonio López
alopez@hitrail.com
https://www.hitrail.com
Marcos Sacristán
Marcos.sacristan@treetk.com
https://www.treetk.com/en

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

Call identifier: H2020-S2RJU-2019
Topic: S2R-OC-IP2-01-2019 - Demonstrator development for the use of Formal Methods in railway environment and Support to implementation of CSIRT to the railway sector