4SECURail

WS2-CSIRT dedicated to rail

A co-designed Model and Platform

4SECURail Final Event
Paris, 23-24 November 2021

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.

Antonio López
alopez@hitrail.com
https://www.hitrail.com
Javier Gutiérrez
javier.gutierrez@treetk.com
https://www.treetk.com/en

Shift2Rail

1	Background
2	CHIRP4Rail model
3	CHIRP4Rail prototype
4	Lessons learnt
5	Conclusions

4SECURail – CSIRT Background, Aim and Objectives

01

Background

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

02

Aim

The main aim is to **deliver a CSIRT model co-designed by the relevant rail stakeholders** along with a **working prototype** (TRL4) 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

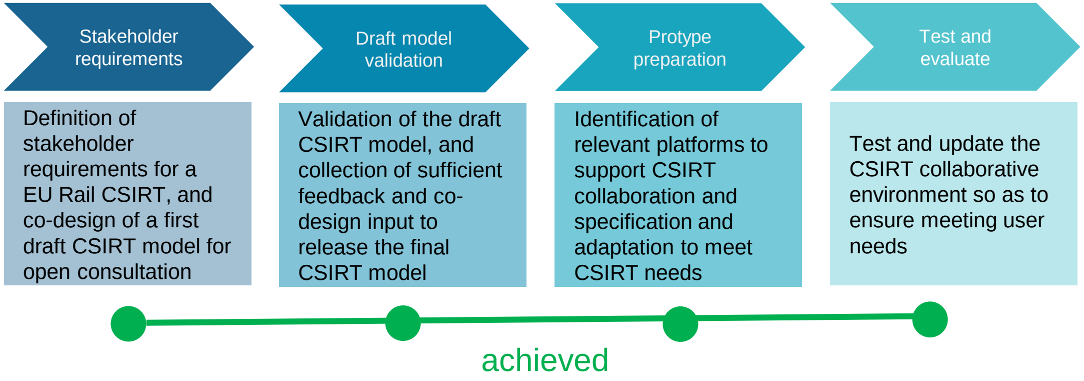
To **identify relevant platforms** to support CSIRT collaboration and, based on requirements and CSIRT model, specify and adapt to meet CSIRT needs.

06

Objective 4

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

4SECURail – CSIRT 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 validation

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

Protype preparation

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

Test and evaluate

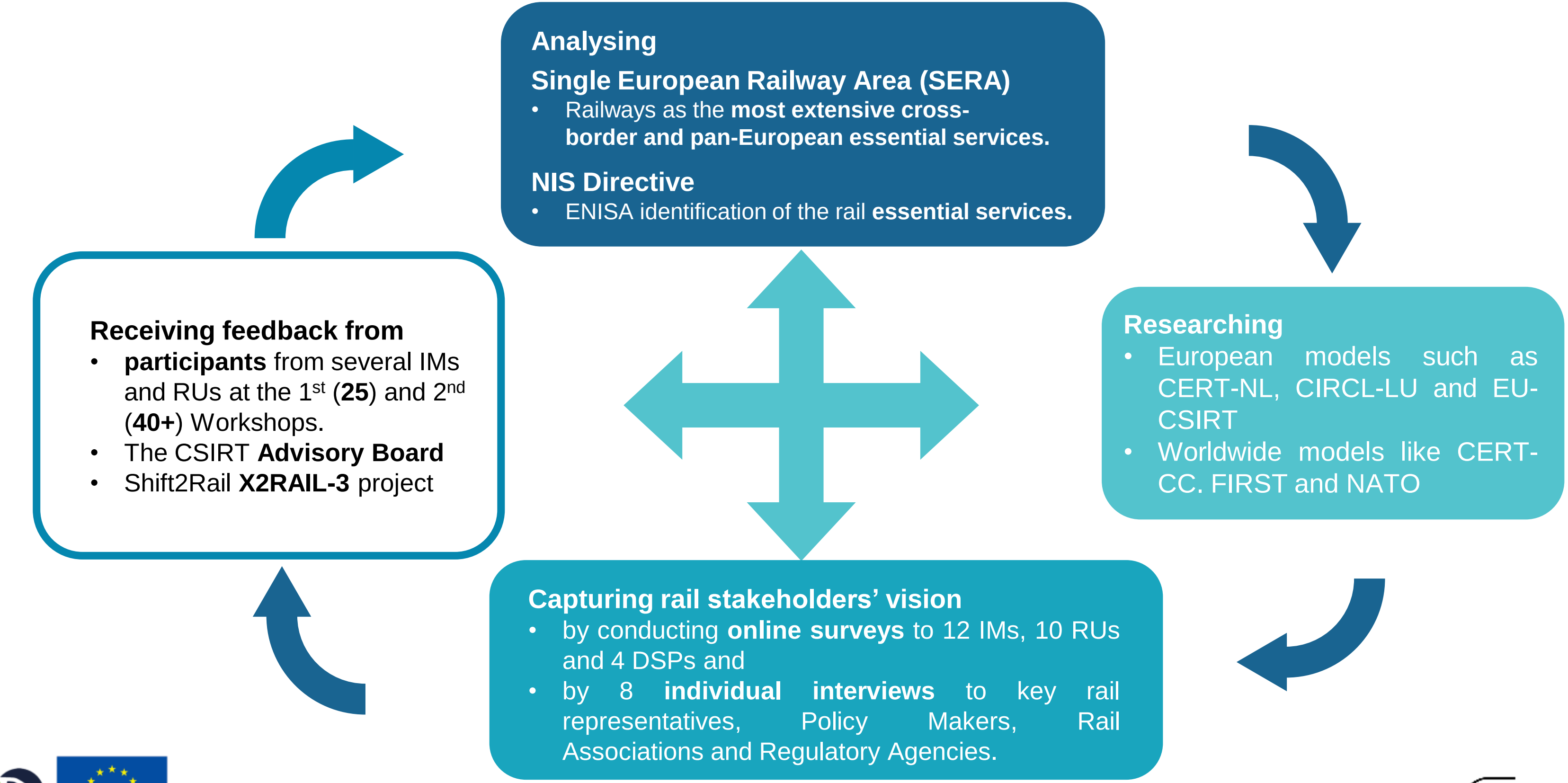
Test and update the CSIRT collaborative environment so as to ensure meeting user needs

CSIRT Workstream

- ● Requirement definition finished
- ● Final CSIRT model released
- ● CSIRT prototype prepared
- ● CSIRT prototype evaluated

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

4SECURail – CSIRT Context, Research and Feedback



Analysing

Single European Railway Area (SERA)

- Railways as the **most extensive cross-border and pan-European essential services.**

NIS Directive

- ENISA identification of the rail **essential services.**

Researching

- European models such as CERT-NL, CIRCL-LU and EU-CSIRT
- Worldwide models like CERT-CC. FIRST and NATO

Capturing rail stakeholders' vision

- by conducting **online surveys** to 12 IMs, 10 RUs and 4 DSPs and
- by 8 **individual interviews** to key rail representatives, Policy Makers, Rail Associations and Regulatory Agencies.

Receiving feedback from

- **participants** from several IMs and RUs at the 1st (**25**) and 2nd (**40+**) Workshops.
- The CSIRT **Advisory Board**
- Shift2Rail **X2RAIL-3** project

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 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 Feedback main findings

Sharing Security Intelligence Between Organisations

- **Point of contact** for sharing between organisations must be a local choice (not just CISO).
- Choice of **anonymity** is context-dependent.
- A **trusted network** must be organised around trusted parties.

Suggested Platform Facilities

- Inter-organisational sharing of threat intelligence should include a **platform** with:
  - **Library** of threat intelligence (up-to-date library of threats + defensive measures).
  - **Communication facilities** for rapid alerts, awareness bulletins, etc.
  - **Analytics module** (threats experienced by different users / locations / times etc.).

Relationship with UIC/ER-ISAC and NIS Directive

- The 4SECURail CSIRT collaboration initiative should be **linked to UIC/ER-ISAC.**
- Governance will be a key issue: 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 improve intelligence.

Respondent Advice to Remainder of Study

- Exploit **platforms** already in use for exchange and collaboration.
- A **4SECURail demonstrator** will convince people through experience.

4SECURail – CSIRT Requirements: Actors

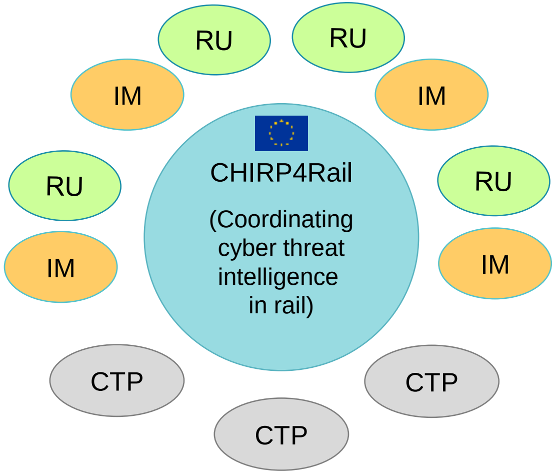
The evident need to coordinate information exchanges between railway security teams for EU-wide cyber security suggests a model that is **data driven, and bottom-up**:

1. identifying **what data is to be shared** between rail security teams;
2. identifying an **operational strategy to enable exchange**, supported by technical and operational schemes;
3. 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:

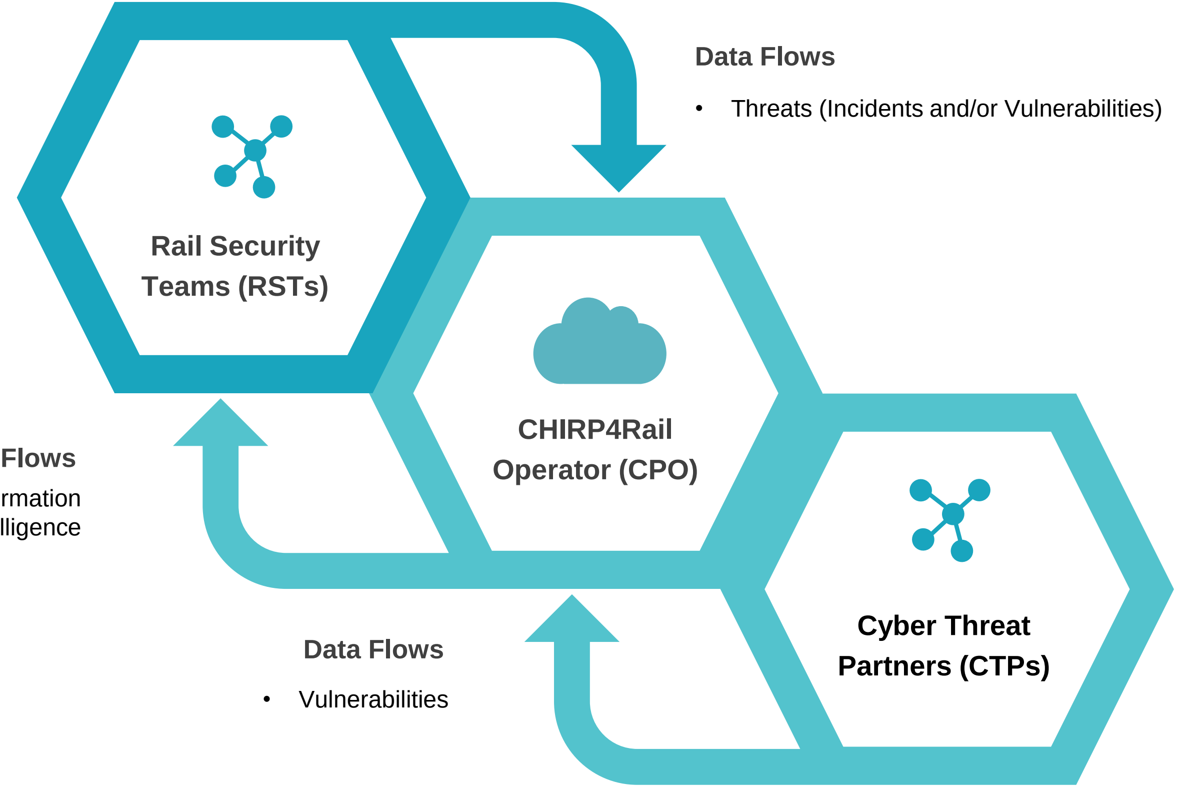
- **IM / RU Rail Security Teams** (RSTs):
  - Formed as a CSIRT, CERT, SOC or any other operational form.
  - Operational at national level.
- **CHIRP4Rail:**
  - EU level Rail CSIRTs THreat Intelligence coordination - **CHIRP4Rail Platform Operator (CPO)**.
  - Operational at EU level; intelligence 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 Requirements: Flows (1)



Rail Security Teams (RSTs)
CHIRP4Rail Operator (CPO)
Cyber Threat Partners (CTPs)

Data Flows

- Threats (Incidents and/or Vulnerabilities)

Data Flows

- Aggregated Information
- Actionable Intelligence

Data Flows

- Vulnerabilities

4SECURail – CSIRT Requirements: Flows (2)

From information sharing to intelligence: a value-adding process

Information sharing

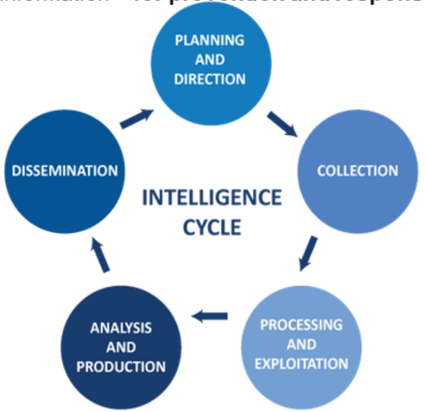
(threats, incidents, vulnerabilities)
+
Availability of expertise

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

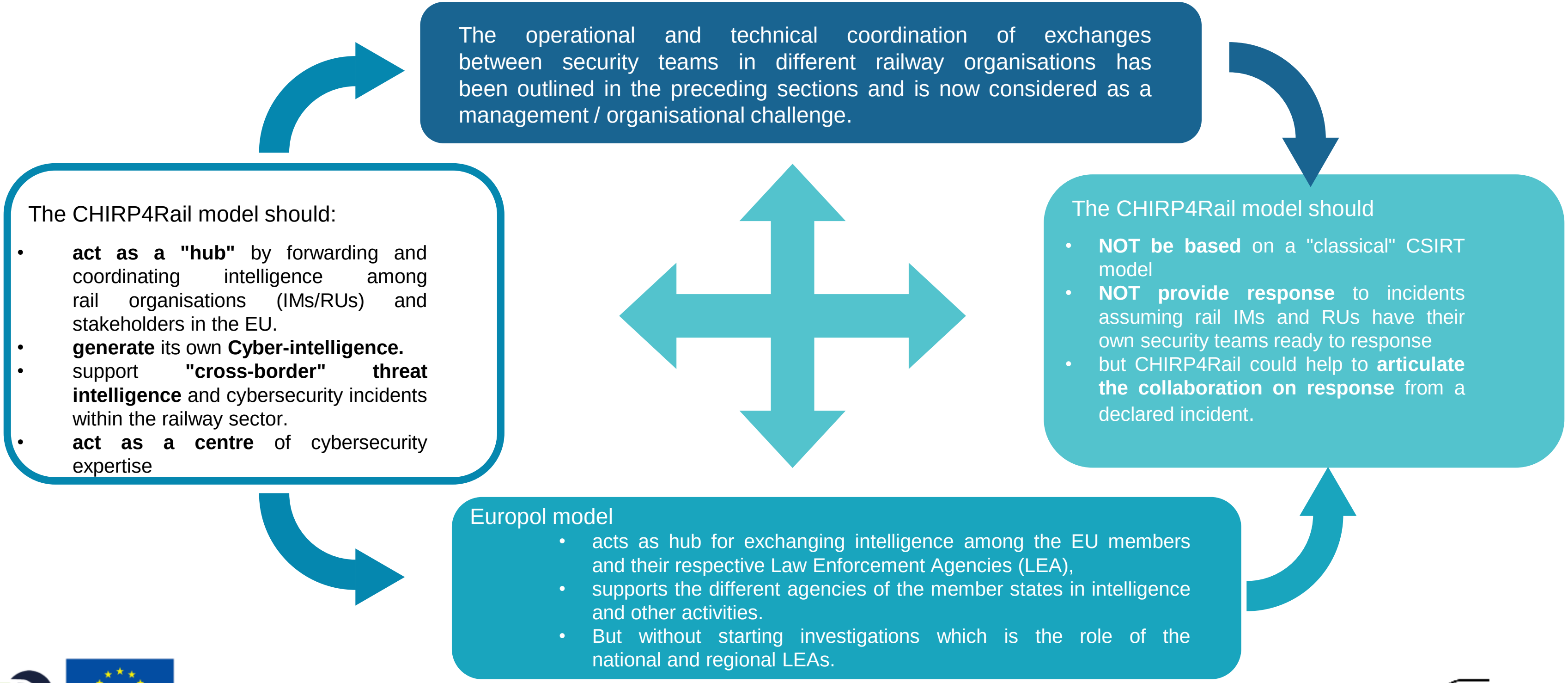
(threats, incidents, vulnerabilities)
+
Actionable intelligence

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 CHIRP4Rail model should

- **NOT be based** on a "classical" CSIRT model
- **NOT provide response** to incidents assuming rail IMs and RUs have their own security teams ready to response
- but CHIRP4Rail 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.

The CHIRP4Rail 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

1. Background
2. CHIRP4Rail model
3. CHIRP4Rail prototype
4. Lessons learnt
5. Conclusions

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

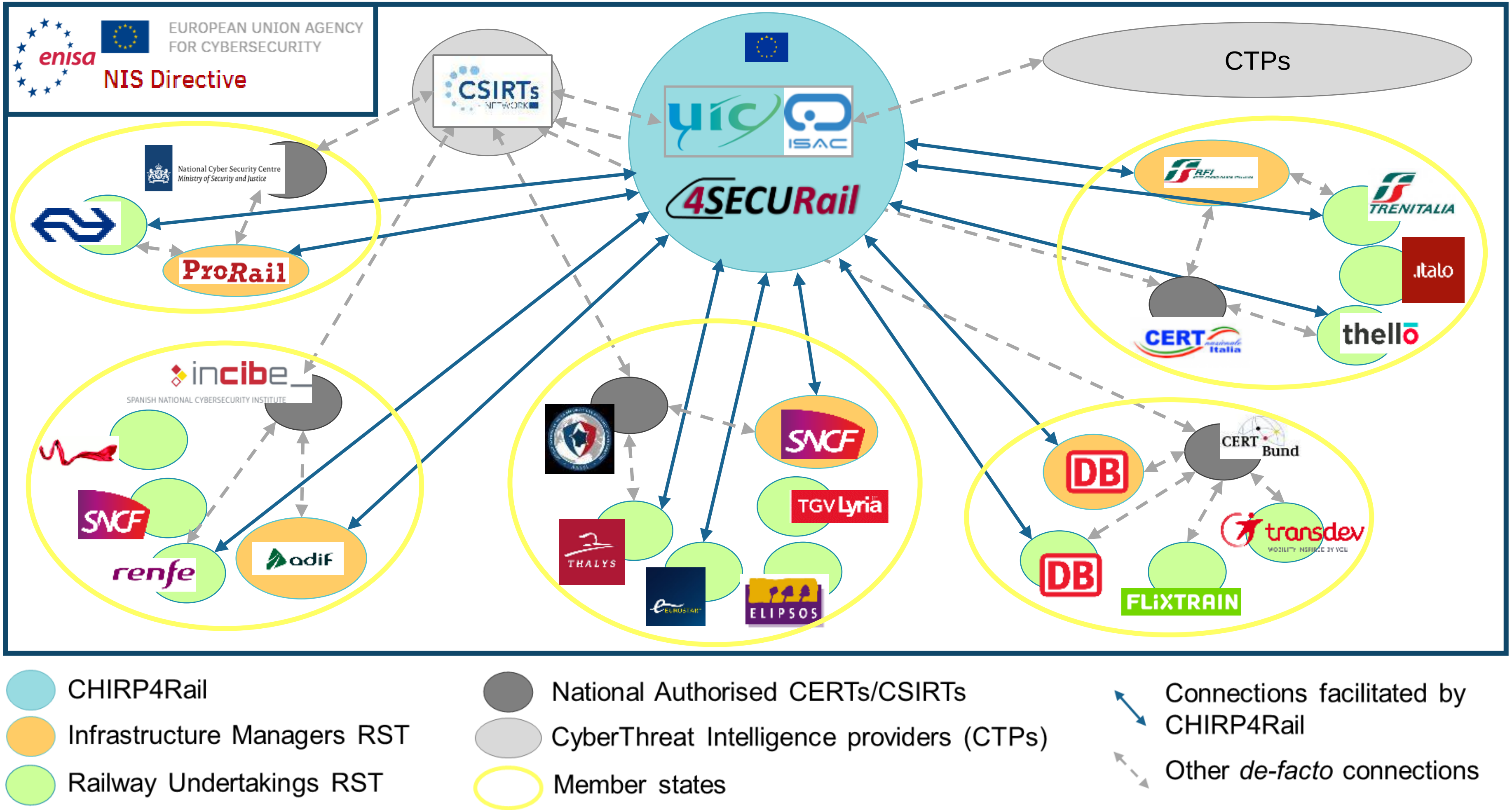
The opportunity:

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

4SECURail

The CHIRP4Rail approach:

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


enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY
NIS Directive
CSIRTs NETWORK
CTPs
UIC
ISAC
4SECURail
National Cyber Security Centre
Ministry of Security and Justice
ProRail
RFI
TRENITALIA
italo
CERT nazionale 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

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 info, community 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

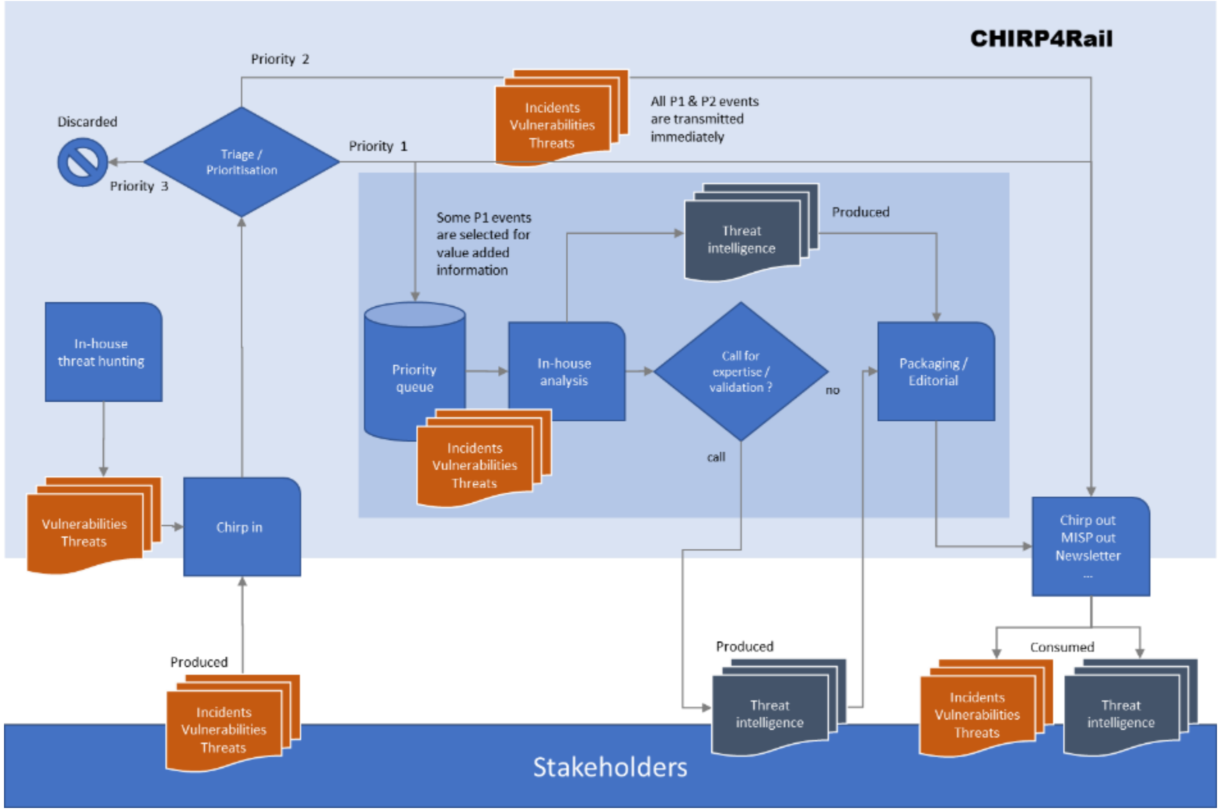
Collaborative prioritisation and analysis of threats

- 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



1. Background
2. CHIRP4Rail model
3. CHIRP4Rail prototype
4. Lessons learnt
5. Conclusions

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 configuration (local, all the organisations, custom group)

Taxonomy

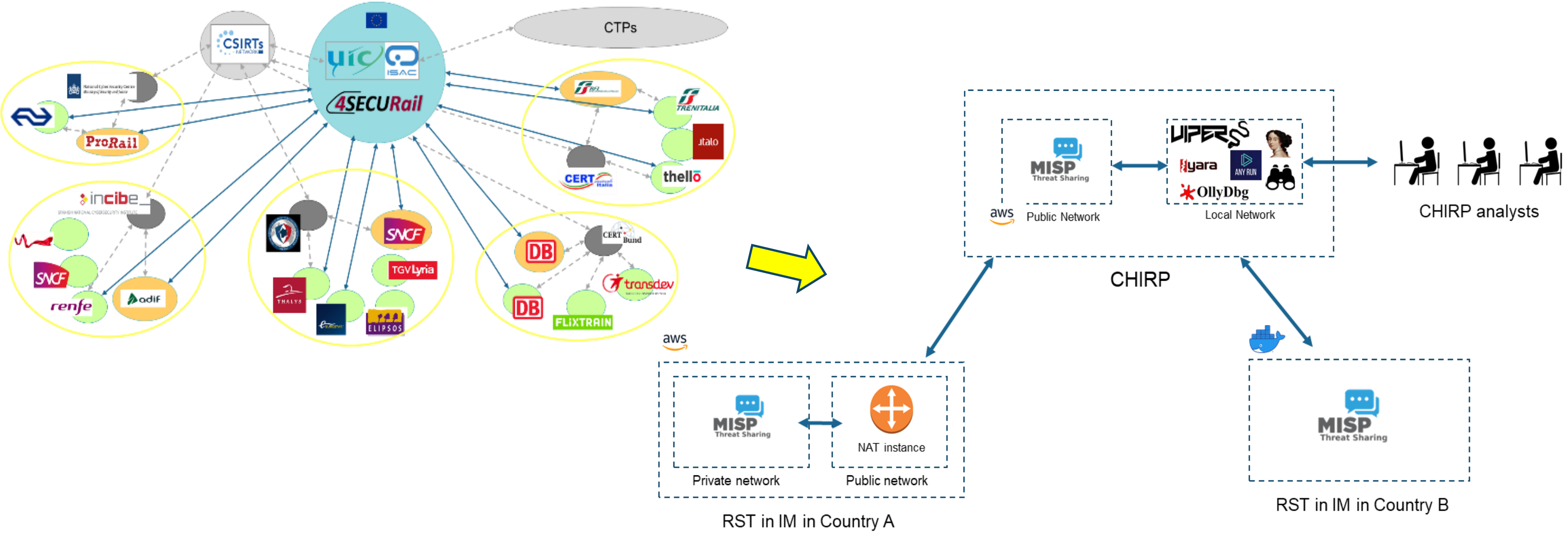
Classify and organise Events

- 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 in use (use case examples)



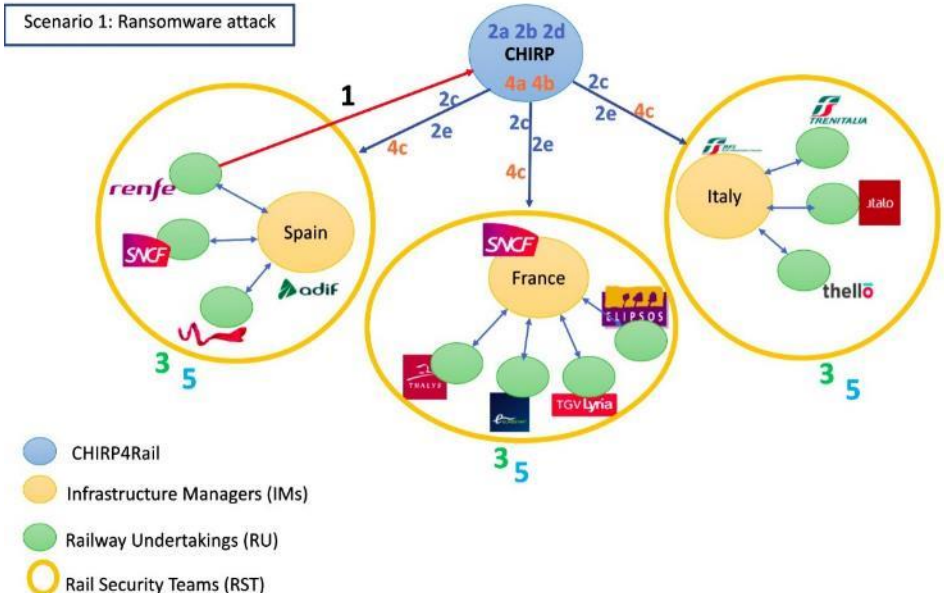
Recreation of Threat Intelligence information sharing in the RST community. We will use 2 scenarios as examples:

Example 1: Ransomware case

Example 2: Critical vulnerability

4SECURail – CHIRP4Rail in use (use case examples)

Example 1: Ransomware case



CHIRP Flow overview

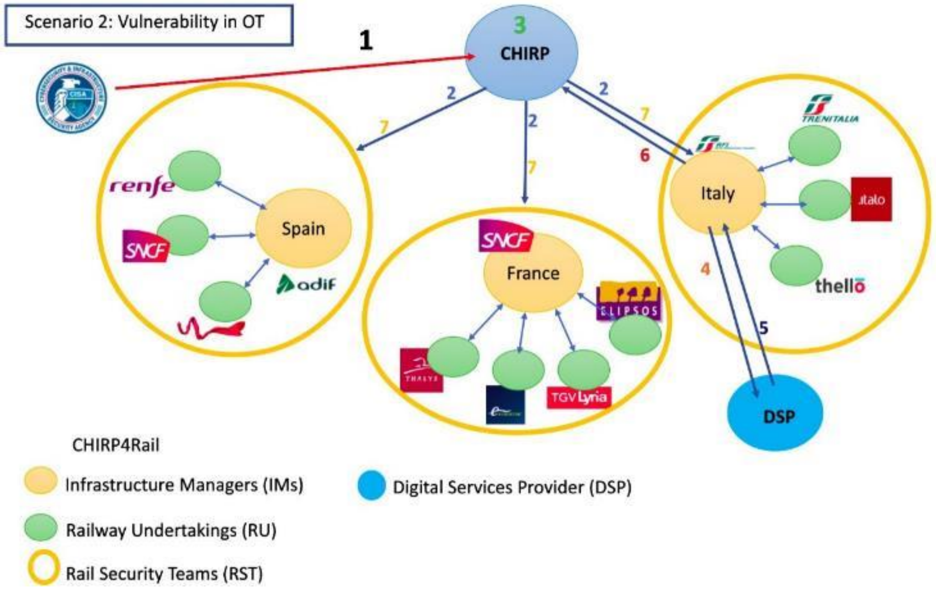
1. **Spear phishing notification**: A RST discovered an attempt of attack, and reported to CHIRP
2. **Early in-house analysis:** CHIRP analysts perform “in-house analysis” to expand information about this threat:
   a. Technical details of the malware (family, goal, IoCs).
   b. Event update with findings (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 in use (use case examples)

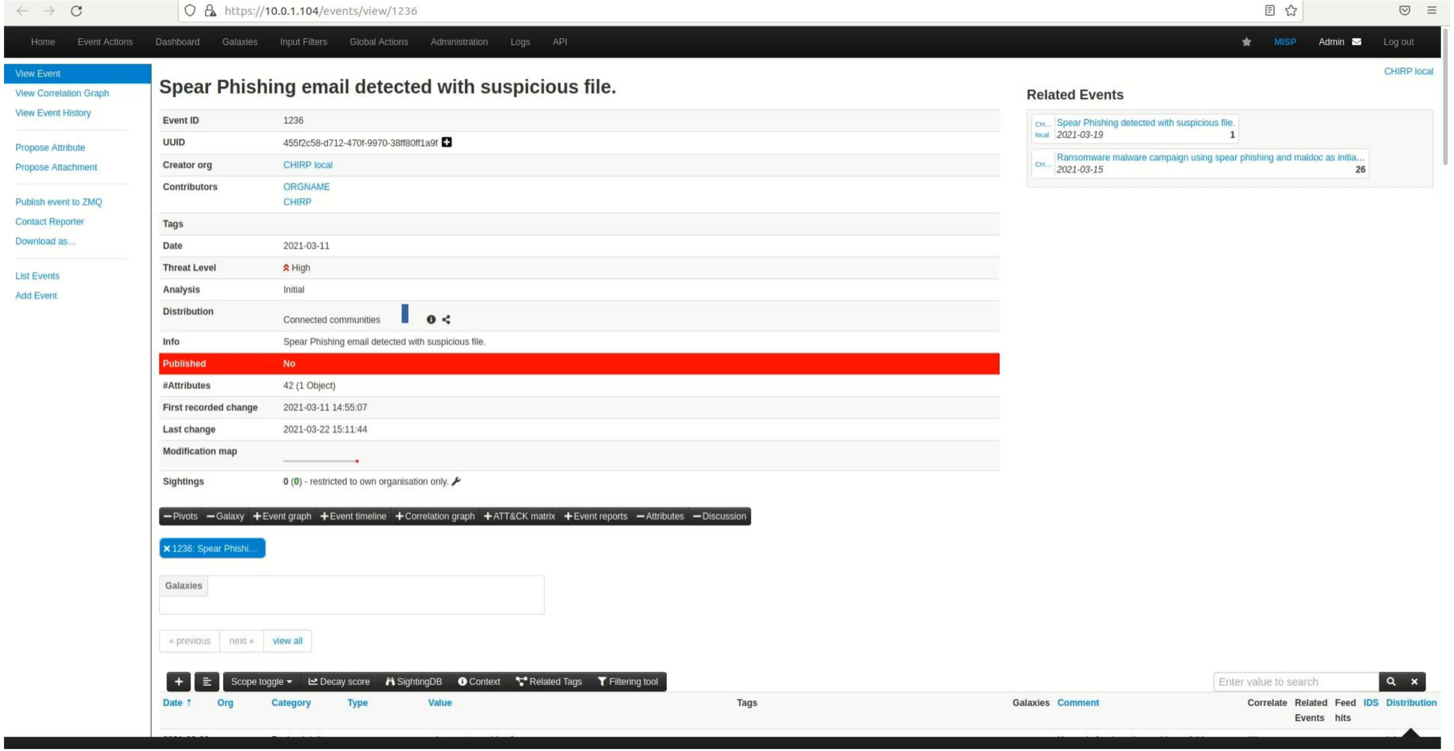
Example 2: Critical vulnerability report

CHIRP Flow overview

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 (CTP) 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
renfe
SNCF
adif
Spain
SNCF
France
ELIPSOS
THALYS
TGV Lyria
TRENITALIA
Italy
italo
thello
DSP
CHIRP4Rail
Infrastructure Managers (IMs)
Digital Services Provider (DSP)
Railway Undertakings (RU)
Rail Security Teams (RST)

4SECURail – CHIRP4Rail in action



Spear Phishing email detected with suspicious file.

Event ID	1236
UUID	455f2c58-d712-470f-9970-38ff80ff1a9f
Creator org	CHIRP local
Contributors	ORGNAME CHIRP
Tags	
Date	2021-03-11
Threat Level	High
Analysis	Initial
Distribution	Connected communities
Info	Spear Phishing email detected with suspicious file.
Published	No
#Attributes	42 (1 Object)
First recorded change	2021-03-11 14:55:07
Last change	2021-03-22 15:11:44
Modification map	
Sightings	0 (0) - restricted to own organisation only.

Related Events

CH… local — Spear Phishing detected with suspicious file. — *2021-03-19* — 1

CH… — Ransomware malware campaign using spear phishing and maldoc as initia… — *2021-03-15* — 26

Date ↑	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution

1 Background

2 CHIRP4Rail model

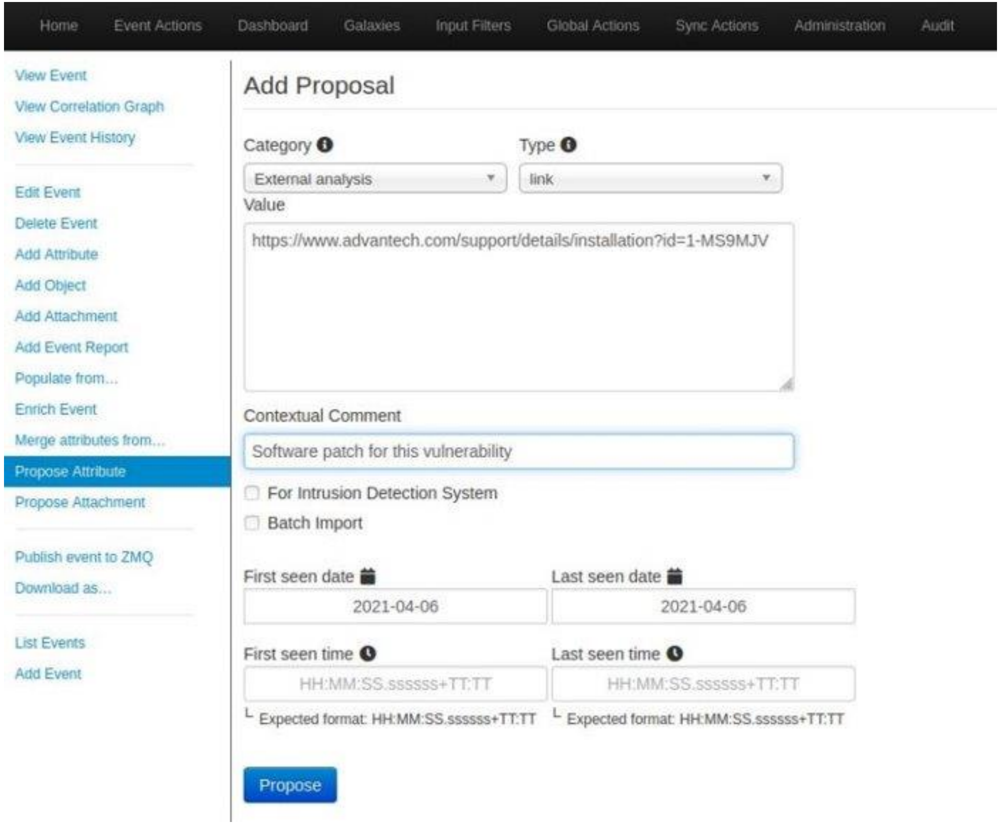
3 CHIRP4Rail prototype

4 Lessons learnt

5 Conclusions

4SECURail – Lessons learnt 1

CHIRP becomes a trusted sharing platform among RSTs



Add Proposal

Category: External analysis

Type: link

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

Contextual Comment: Software patch for this vulnerability

□ For Intrusion Detection System

□ Batch Import

First seen date: 2021-04-06

Last seen date: 2021-04-06

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

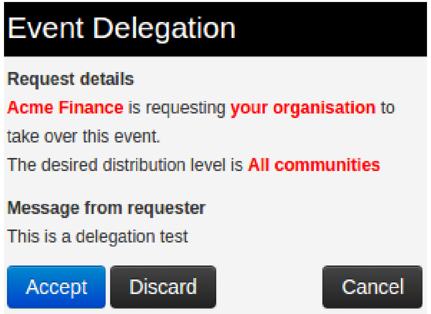
Expected format: HH:MM:SS.ssssss+TT:TT

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

Expected format: HH:MM:SS.ssssss+TT:TT

4SECURail – Lessons learnt 2

Pseudo-anonymisation may be required by victims and/or contributors



Event Delegation

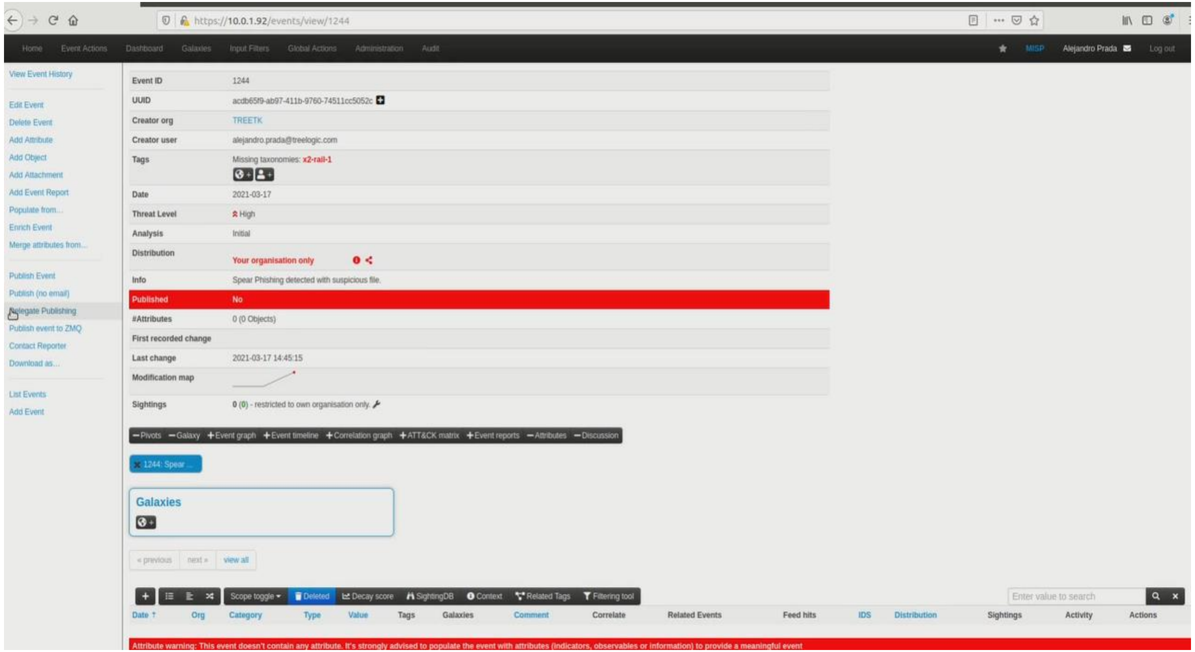
Request details

Acme Finance is requesting your organisation to take over this event.

The desired distribution level is All communities

Message from requester

This is a delegation test



https://10.0.1.92/events/view/1244

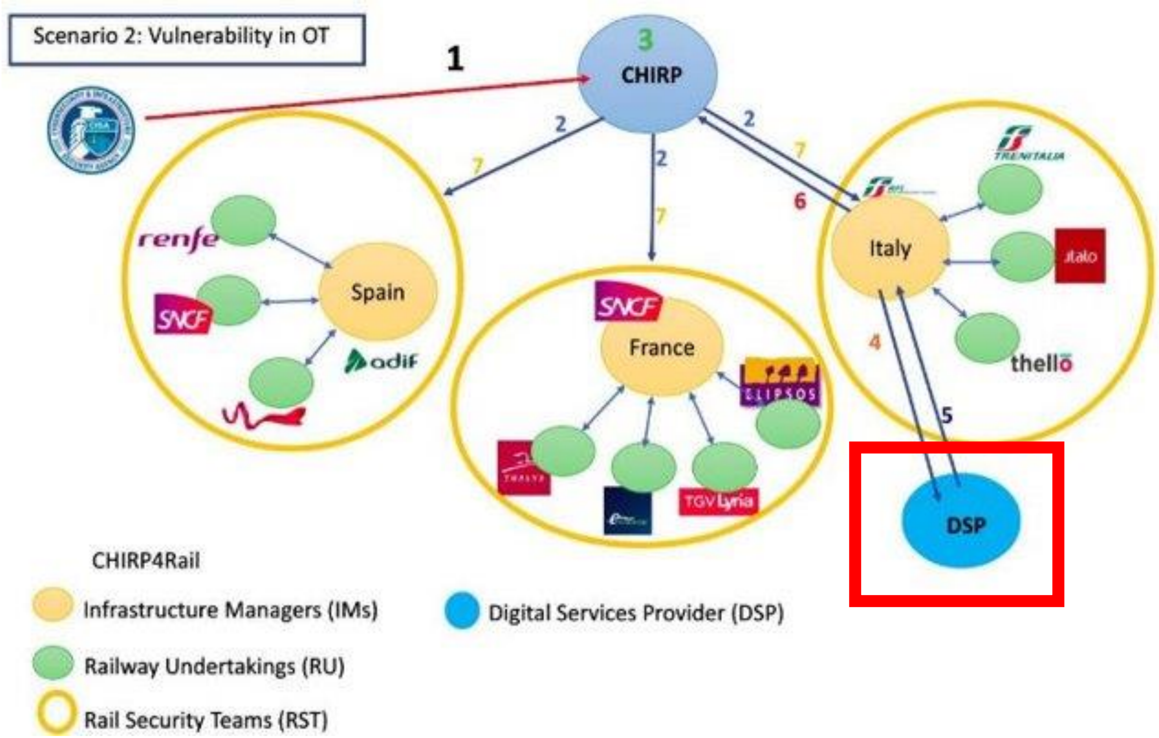
Event ID	1244
UUID	acdb65f9-ab97-411b-9760-74511cc5052c
Creator org	TREETK
Creator user	alejandro.prada@treelogic.com
Tags	Missing taxonomies: x2-rail-1
Date	2021-03-17
Threat Level	High
Analysis	Initial
Distribution	Your organisation only
Info	Spear Phishing detected with suspicious file.
Published	No
#Attributes	0 (0 Objects)
First recorded change	
Last change	2021-03-17 14:45:15
Modification map	
Sightings	0 (0) - restricted to own organisation only.

Date ↑	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings	Activity	Actions

Attribute warning: This event doesn't contain any attribute. It's strongly advised to populate the event with attributes (indicators, observables or information) to provide a meaningful event

4SECURail – Lessons learnt 3

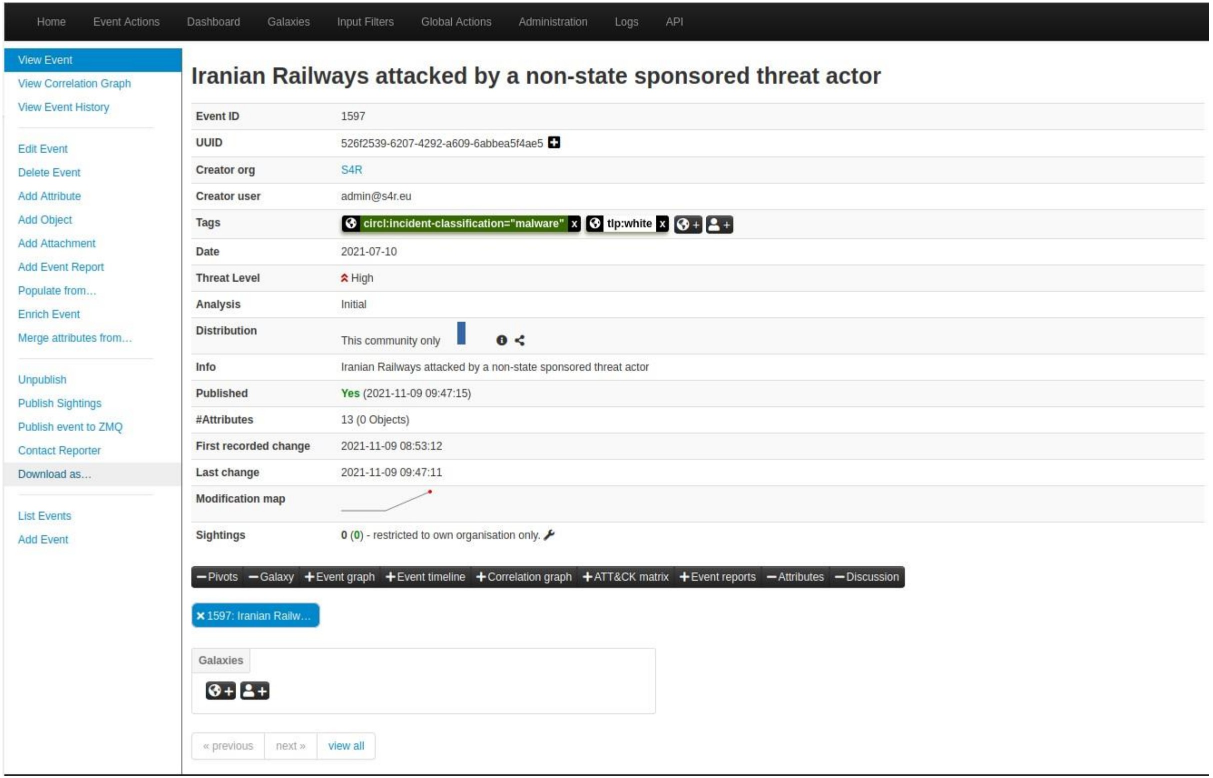
Importance of the involvement of suppliers and DSPs



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

4SECURail – Lessons learnt 4

CHIRP must be a Threat Intelligence and Vulnerability triage provider

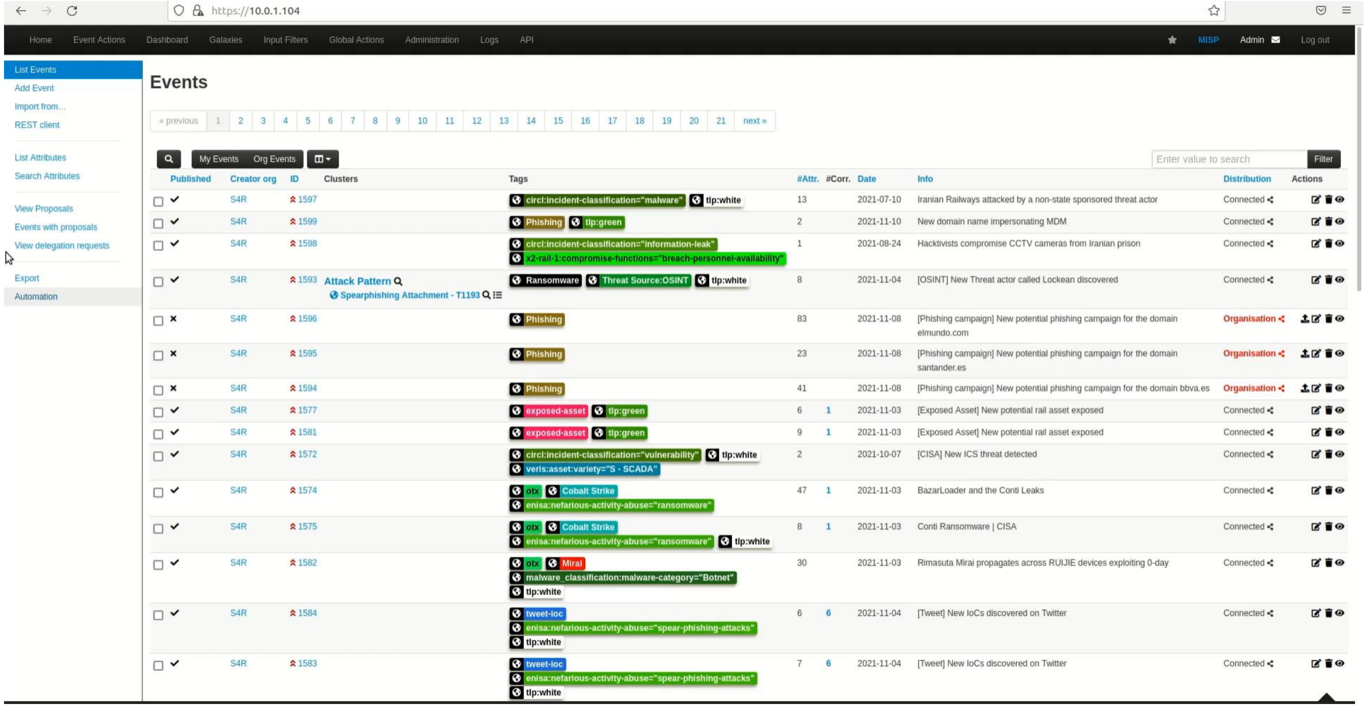


Iranian Railways attacked by a non-state sponsored threat actor

Event ID	1597
UUID	526f2539-6207-4292-a609-6abbea5f4ae5
Creator org	S4R
Creator user	admin@s4r.eu
Tags	circl:incident-classification="malware" x tlp:white x
Date	2021-07-10
Threat Level	High
Analysis	Initial
Distribution	This community only
Info	Iranian Railways attacked by a non-state sponsored threat actor
Published	Yes (2021-11-09 09:47:15)
#Attributes	13 (0 Objects)
First recorded change	2021-11-09 08:53:12
Last change	2021-11-09 09:47:11
Modification map	
Sightings	0 (0) - restricted to own organisation only.

4SECURail – Lessons learnt 5

Taxonomies are useful



Events

	Published	Creator org	ID	Clusters	Tags	#Attr.	#Corr.	Date	Info	Distribution	Actions
□	✓	S4R	1597		circl:incident-classification="malware" tlp:white	13		2021-07-10	Iranian Railways attacked by a non-state sponsored threat actor	Connected	
□	✓	S4R	1599		Phishing tlp:green	2		2021-11-10	New domain name impersonating MDM	Connected	
□	✓	S4R	1598		circl:incident-classification="information-leak" x2-rail-1:compromise-functions="breach-personnel-availability"	1		2021-08-24	Hacktivists compromise CCTV cameras from Iranian prison	Connected	
□	✓	S4R	1593	Attack Pattern Spearphishing Attachment - T1193	Ransomware Threat Source:OSINT tlp:white	8		2021-11-04	[OSINT] New Threat actor called Lockean discovered	Connected	
□	✗	S4R	1596		Phishing	83		2021-11-08	[Phishing campaign] New potential phishing campaign for the domain elmundo.com	Organisation	
□	✗	S4R	1595		Phishing	23		2021-11-08	[Phishing campaign] New potential phishing campaign for the domain santander.es	Organisation	
□	✗	S4R	1594		Phishing	41		2021-11-08	[Phishing campaign] New potential phishing campaign for the domain bbva.es	Organisation	
□	✓	S4R	1577		exposed-asset tlp:green	6	1	2021-11-03	[Exposed Asset] New potential rail asset exposed	Connected	
□	✓	S4R	1581		exposed-asset tlp:green	9	1	2021-11-03	[Exposed Asset] New potential rail asset exposed	Connected	
□	✓	S4R	1572		circl:incident-classification="vulnerability" tlp:white veris:asset:variety="S - SCADA"	2		2021-10-07	[CISA] New ICS threat detected	Connected	
□	✓	S4R	1574		otx Cobalt Strike enisa:nefarious-activity-abuse="ransomware"	47	1	2021-11-03	BazarLoader and the Conti Leaks	Connected	
□	✓	S4R	1575		otx Cobalt Strike enisa:nefarious-activity-abuse="ransomware" tlp:white	8	1	2021-11-03	Conti Ransomware | CISA	Connected	
□	✓	S4R	1582		otx Mirai malware_classification:malware-category="Botnet" tlp:white	30		2021-11-03	Rimasuta Mirai propagates across RUIJIE devices exploiting 0-day	Connected	
□	✓	S4R	1584		tweet-ioc enisa:nefarious-activity-abuse="spear-phishing-attacks" tlp:white	6	6	2021-11-04	[Tweet] New IoCs discovered on Twitter	Connected	
□	✓	S4R	1583		tweet-ioc enisa:nefarious-activity-abuse="spear-phishing-attacks" tlp:white	7	6	2021-11-04	[Tweet] New IoCs discovered on Twitter	Connected	

1 Background

2 CHIRP4Rail model

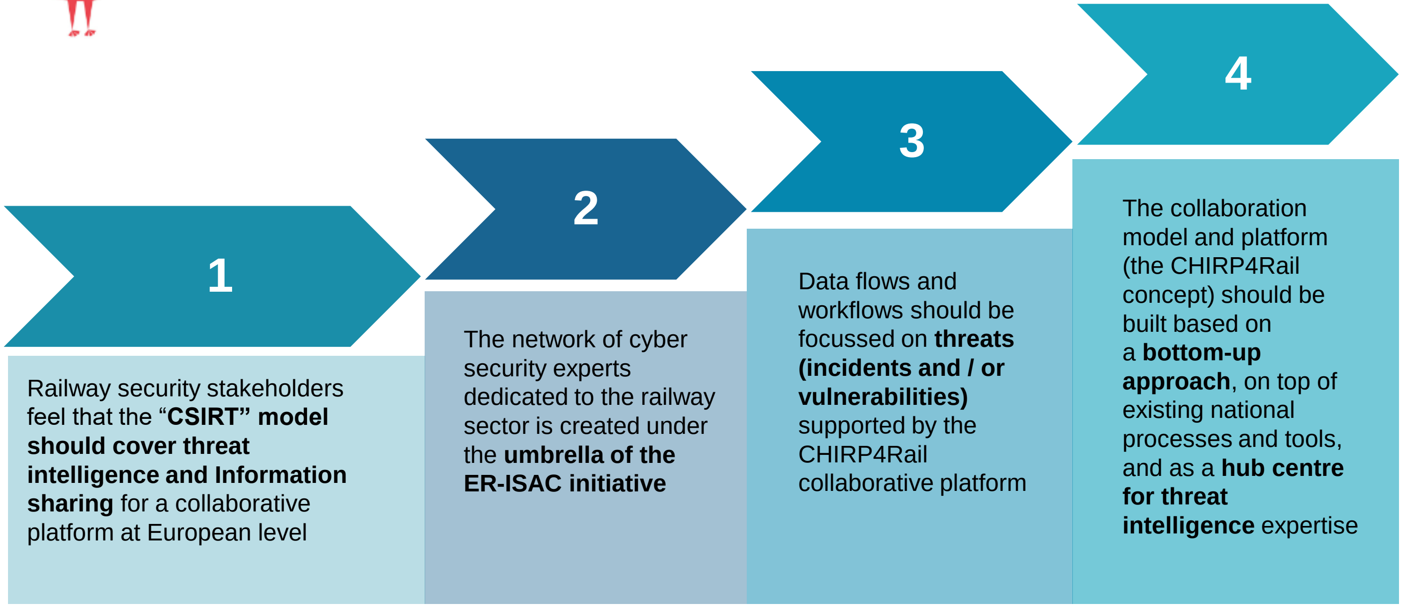
3 CHIRP4Rail prototype

4 Lessons learnt

5 Conclusions

4SECURail – 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 initiative**

3

Data flows and workflows should be 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 national processes and tools, and as a **hub centre for threat intelligence** expertise

4SECURail

Thank you for your attention

Antonio López
alopez@hitrail.com
https://www.hitrail.com
Javier Gutiérrez
javier.gutierrez@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