INTERNATIONAL UNION
OF RAILWAYS

unity, solidarity, universality

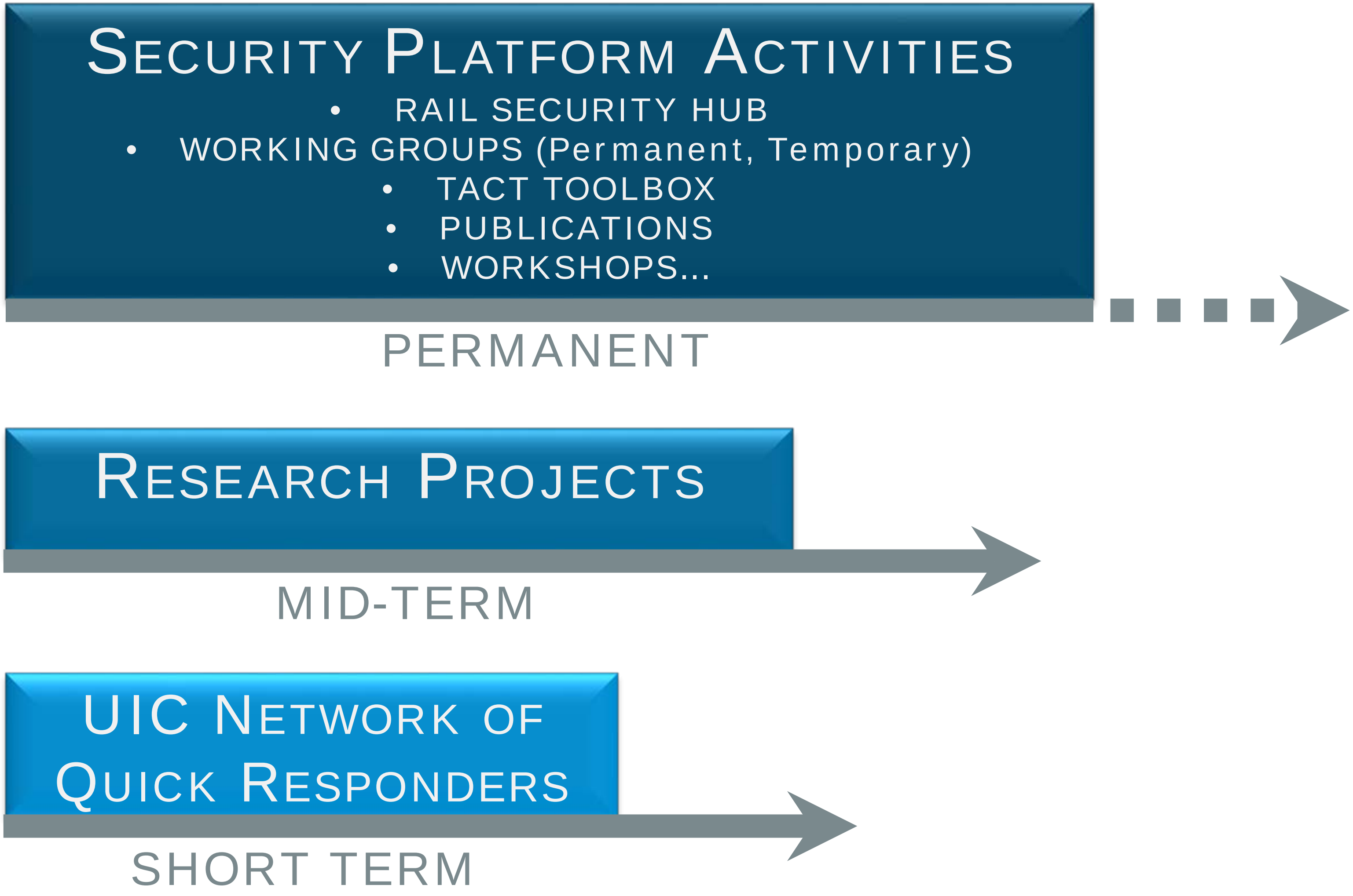
UIC Security Platform

Update on recent activities

UNECE Working Party on Rail Transport (SC.2) 72nd session
Geneva, 21-23.11.2018

Security Division
Bruno De Rosa

UIC Security Activities



Security Platform Activities

- RAIL SECURITY HUB
- WORKING GROUPS (Permanent, Temporary)
- TACT TOOLBOX
- PUBLICATIONS
- WORKSHOPS…

PERMANENT

Research Projects

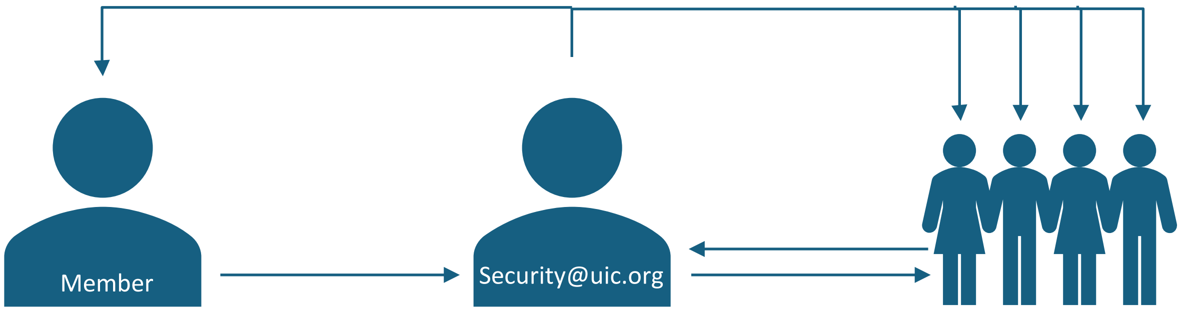
MID-TERM

UIC Network of Quick Responders

SHORT TERM

Network of Quick Responders

- **Goal:** Exchange fast information about arising security questions
- **Process:**



- **Timeline:**
  - app. 2 weeks – Responds from the network
  - app. 2 months – 1st technical position paper
  - If needed, further actions

Network of Quick Responders

Topic	Survey	Follow-up activities
1. Awareness of radicalized employees	03/2017	06/2017: Dedicate Workshop during the Security Week
2. Use of Air Drones	05/2017	12/2017: Main focus of the WG Security Technologies with authorities and provider
3. Inspire Magazine	09/2017	On-going: Thematized within the WG SIA & single exchange
4. Attacks against maintenance staff	09/2017	11/2017: Hand over to the Safety Unit for further actions
5. Anti-smoking policy at railway stations	10/2017	No further actions requested by the responders
6. Security of women in railway transport	02/2018	06/2018: Dedicated topic during the 2nd Awareness Day
7. Use of FFCCTV	04-05/2018	09/2018: Dedicated Workshop on the 12 September 2018, next planned in 02/2019
8. Aggression against ticket inspectors	06-07/2018	Integration in WG Human Factor under the umbrella “Security feeling in public transport” (focus customer and employees)
9. Mystery Customer	07/2018	Currently no further actions requested by the responders (topic memory)
10. Use of AED’s	09/2018	First half 2019: Organization of a dedicate workshop together with the safety unit
11. Use of body cameras	10-11/2018	In evaluation
12. Security Organization	11/2018	On-going
13. CBRN	11-12/2018	In preparation

FFCCTV – follow up activities

- **Date:** 12 September 2018 (Paris, France)
- **Contents:**
  - Test area setting
  - Purpose
  - Technical aspects
  - Fleet
  - Cooperation with law enforcements
  - Trade unions
  - Public reaction
  - Experience
  - Drawbacks / difficulties

- **Outlook:** next meeting in February/March 2019

4th UIC Security Week
18 – 21 June in Paris, France

- Seminar on CBRNE terrorism
- Workshop on Cybersecurity
- 2nd UIC Security Awareness Day
- Workshop on BCM
- Interactive Session Security Hub

- Conclusions available at: https://events.uic.org/uic-security-week-2018

14th UIC World Security Congress
16 – 18 October in Bled, Slovenia

- **15th October: Tunnel Safety and Security Workshop**
- **16th October**: Official opening session
- Technical sessions:
  - 1st session: Blackout Situation in Slovenia 2014
  - 2nd session: Ice storm and impact on railways
  - 3rd session: Blackout Situations. Railway experiences and challenges.
  - 4th session: Crisis Management
- Official closing session incl. UIC security actions, conclusion and next steps
- Conclusion: https://events.uic.org/14th-uic-world-security-congress-crisis-management-and-resilience

Storm, cease and restart of train operations in the Netherlands (2018)

Crisis Management - Member request 2018

- Recommendations for the external and internal communication incl. key words, reaction times, design of websites, preparation of communication channels like a special hotline, use of social media
- Date: 13 – 14.02.2018 in Paris

Crisis Communication

- Recommendations for the framework of BCM and the close connection to CM incl. devising plans and strategies to continue business operations and recovering quickly and efficiently from different types of disruption
- Date: 21.06.2018 in Paris

Business Continuity Management

Analysis
Design
Implementation
Validation
Embedding Business Continuity
Policy and Programme Management

- Example: 12 May 2017 Cyberattack WannaCry – over 150 countries involved
- Recommendations for the handling of (partially) blackout situations
- Date: 16.-18.10.2018 in Slovenia

Blackout Situations

By the end of 2018 / beginning 2019, publication of recommendations for each topic in cooperation with UITP and COLPOFER.

CYRAIL CYbersecurity in the RAILway sector

This project has received funding from the Shift2Rail Joint Undertaking under the European Union's Horizon 2020 research and innovation programme under grant agreement No 730843 addressing the topic "Threat detection and profile protection definition for cybersecurity assessment".

- **Duration**: 1 Oct. 2016 - 30 Sept. 2018
- **Budget**: 1,5 M
- **Coordinator**: Evoleo Technologies
- **Consortium**: 6 Partners from 5 countries

EVOLEO TECHNOLOGIES

euskoiker

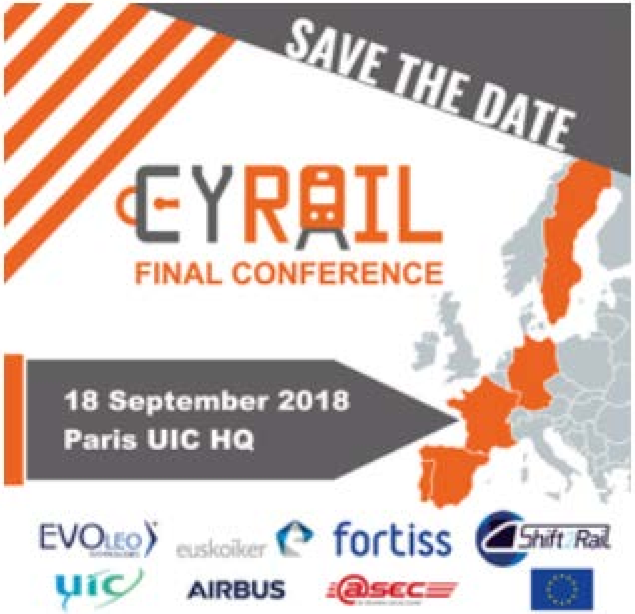
UIC INTERNATIONAL UNION OF RAILWAYS

fortiss

AIRBUS DEFENCE & SPACE

@SEC the information security provider

CYRAIL CYbersecurity in the RAILway sector



SAVE THE DATE

CYRAIL

FINAL CONFERENCE

18 September 2018

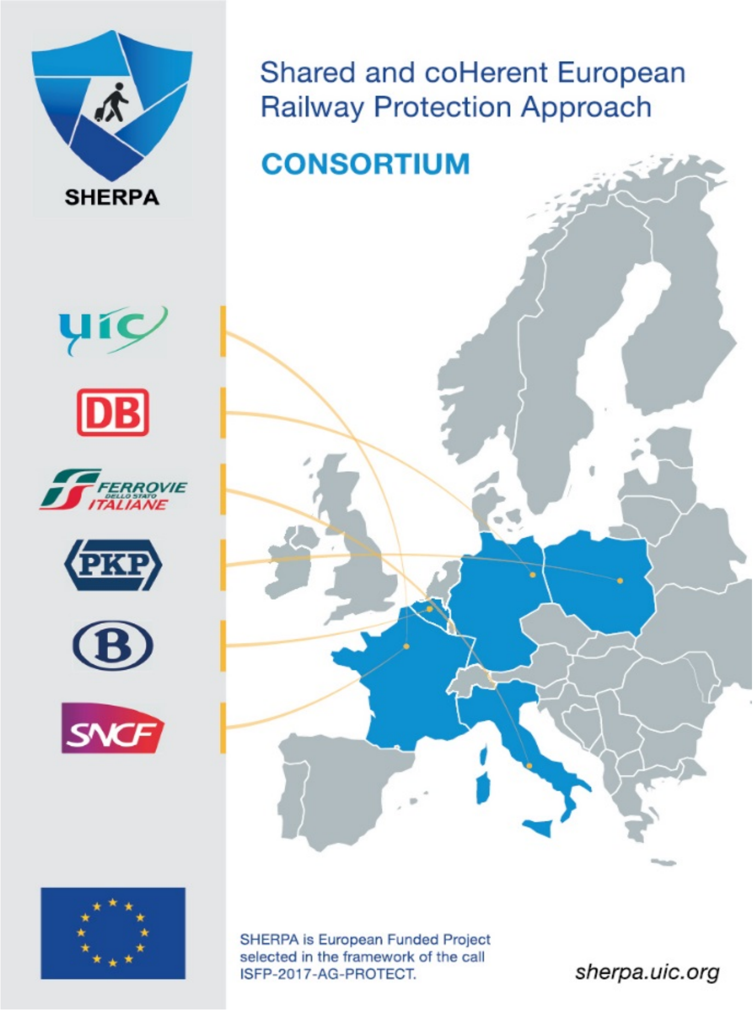
Paris UIC HQ

Final Conference held in Paris at UIC Headquarters on September 18th, 2018

Project brochure publicly available online at: **www.cyrail.eu**

SHERPA - Shared and coHerent European Railway Protection Approach

- **Framework:** DG HOME call for proposal
- **Planning:**
  - 31/01/2018 : submission of the proposal
  - June 2018 – October 2018 : Signature of the GA
  - 13 November 2018: Kick off meeting in Paris



Shared and coHerent European Railway Protection Approach

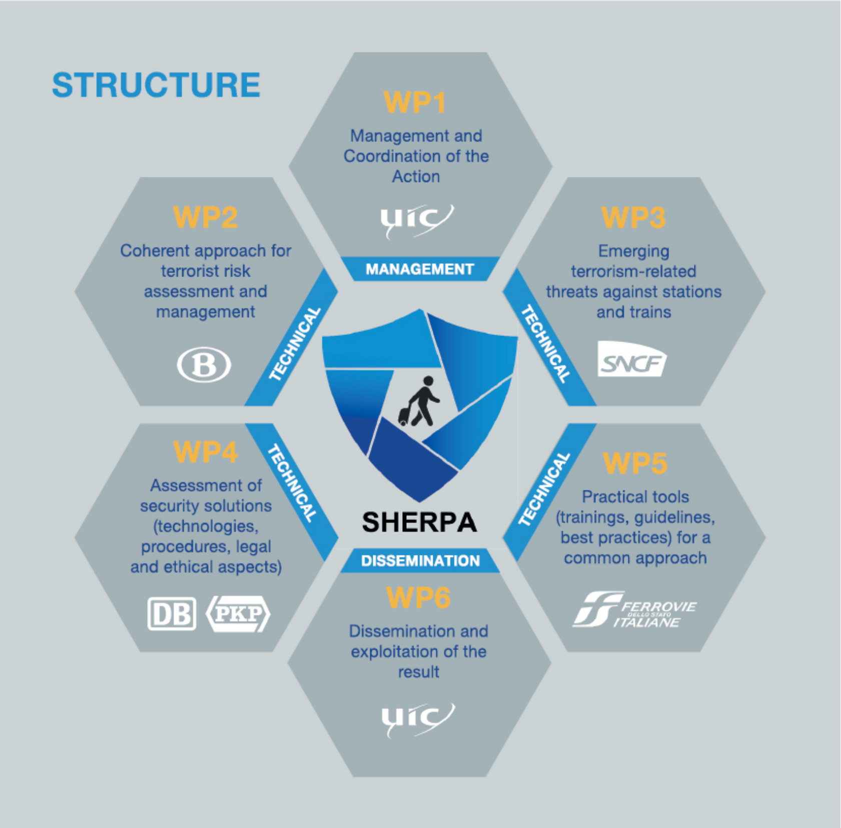
CONSORTIUM

SHERPA is European Funded Project selected in the framework of the call ISFP-2017-AG-PROTECT.

sherpa.uic.org

Structure of the project

Shared and coHerent European Railway Protection Approach


STRUCTURE
WP1
Management and Coordination of the Action
UIC
MANAGEMENT
WP2
Coherent approach for terrorist risk assessment and management
B
TECHNICAL
WP3
Emerging terrorism-related threats against stations and trains
SNCF
TECHNICAL
WP4
Assessment of security solutions (technologies, procedures, legal and ethical aspects)
DB
PKP
TECHNICAL
SHERPA
DISSEMINATION
WP5
Practical tools (trainings, guidelines, best practices) for a common approach
FERROVIE DELLO STATO ITALIANE
TECHNICAL
WP6
Dissemination and exploitation of the result
UIC

SHERPA is European Funded Project selected in the framework of the call ISFP-2017-AG-PROTECT.

sherpa.uic.org

- **WP2 – Coherent approach for terrorist risk assessment and management - Lead:** SNCB

  Objectives: to achieve a comprehensive and consistent understanding of terrorism-related threats against railway stations and trains and thus to elaborate a coherent approach for terrorist risk assessment and management in the railway sector.

- **WP3 – Analysis of emerging terrorism-related threats against stations and trains - Lead:** SNCF

  Objectives: to identify and assess emerging threats -e.g. insider threats, misuse of commercial UAVs- potentially affecting stations and trains; to define and share an updated knowledge base on the matter; to identify requirements and priorities for industry, research and policy making bodies.

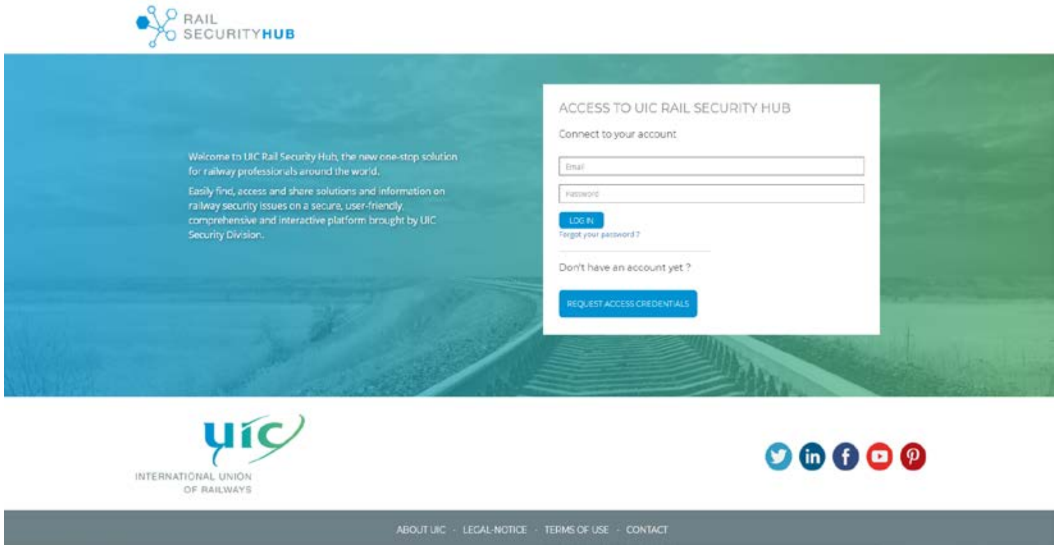
- **WP4 – Assessment of security solutions: technologies, procedures, legal and ethical aspects -Lead:** PKP S.A. and DB AG

  Objectives: building a common knowledge base -validated by users and external experts- featuring the most efficient solutions for protecting trains and stations; identifying the gaps to be fulfilled and the future needs for better securing stations and trains in accordance with business constraints.

- **WP5 – Practical tools for a common approach on raising awareness and improving security of stations and trains- Lead:** FS Italiane

  Objectives: designing and delivering practical tools aimed at fostering a common, effective approach to the protection of stations and trains from both already experienced and emerging security threats.

UIC Rail Security Hub



RAIL SECURITYHUB

Welcome to UIC Rail Security Hub, the new one-stop solution for railway professionals around the world.

Easily find, access and share solutions and information on railway security issues on a secure, user-friendly, comprehensive and interactive platform brought by UIC Security Division.

ACCESS TO UIC RAIL SECURITY HUB

Connect to your account

Email

Password

LOG IN

Forgot your password ?

Don't have an account yet ?

REQUEST ACCESS CREDENTIALS

INTERNATIONAL UNION OF RAILWAYS

ABOUT UIC · LEGAL-NOTICE · TERMS OF USE · CONTACT

SECURE *web platform, accessible to UIC Members and other eligible stakeholders with differentiated access levels.*

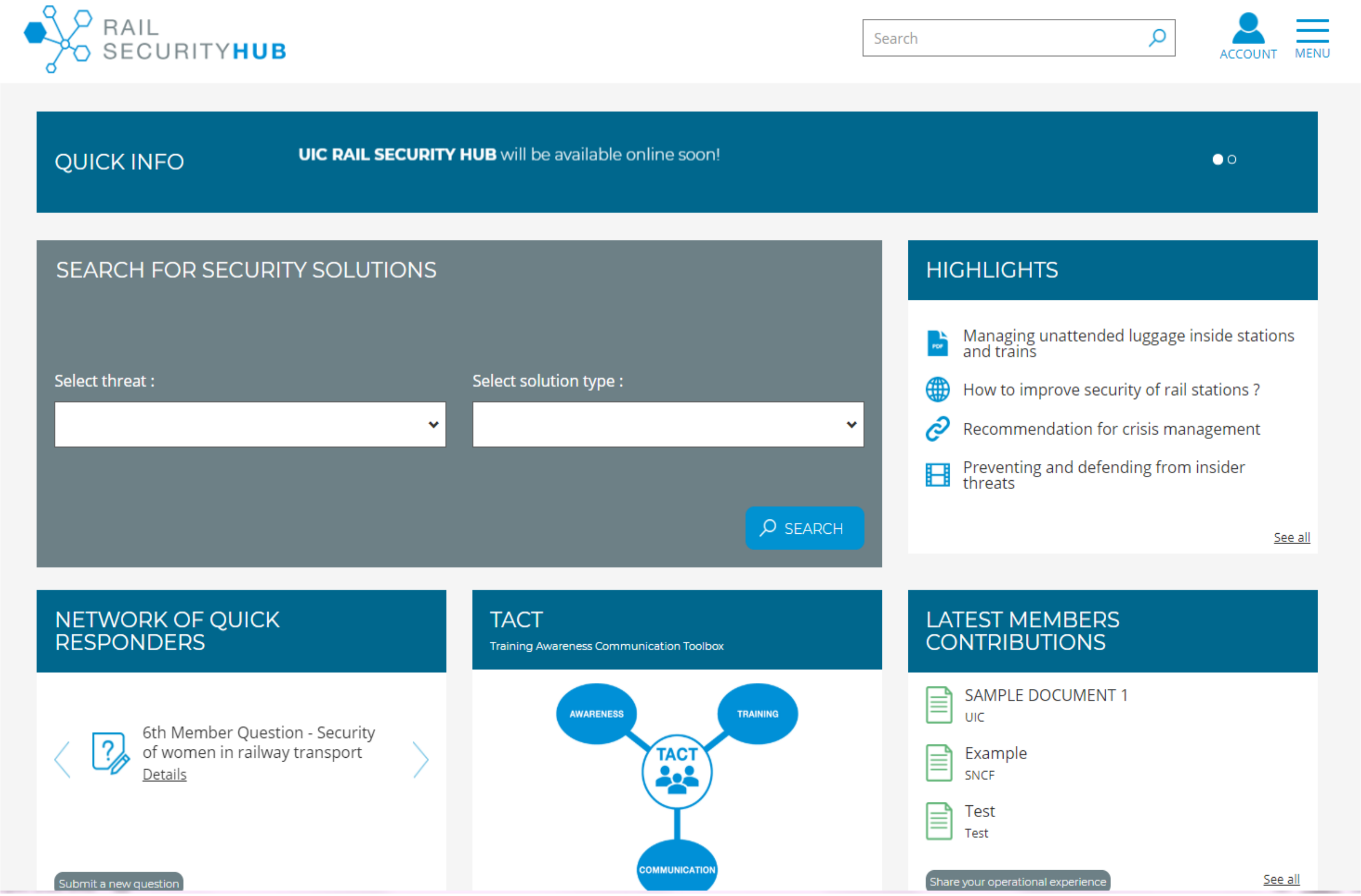
USER-FRIENDLY *content search and navigation with a clear browsing interface.*

COMPREHENSIVE *catalogue of hundreds of security solutions addressing both daily crime issues and emerging threats to the railway environment.*

INTEGRATED *with all the UIC Security Division projects and tools such as the Network of Quick Responders and Training Awareness Communication Toolbox.*

OPEN *to interaction with and between users through comments, ratings and information sharing.*

UPDATED *permanently by UIC Security Division.*



RAIL SECURITYHUB

QUICK INFO

UIC RAIL SECURITY HUB will be available online soon!

SEARCH FOR SECURITY SOLUTIONS

Select threat :

Select solution type :

HIGHLIGHTS

- Managing unattended luggage inside stations and trains
- How to improve security of rail stations ?
- Recommendation for crisis management
- Preventing and defending from insider threats

See all

NETWORK OF QUICK RESPONDERS

6th Member Question - Security of women in railway transport
Details

TACT

Training Awareness Communication Toolbox

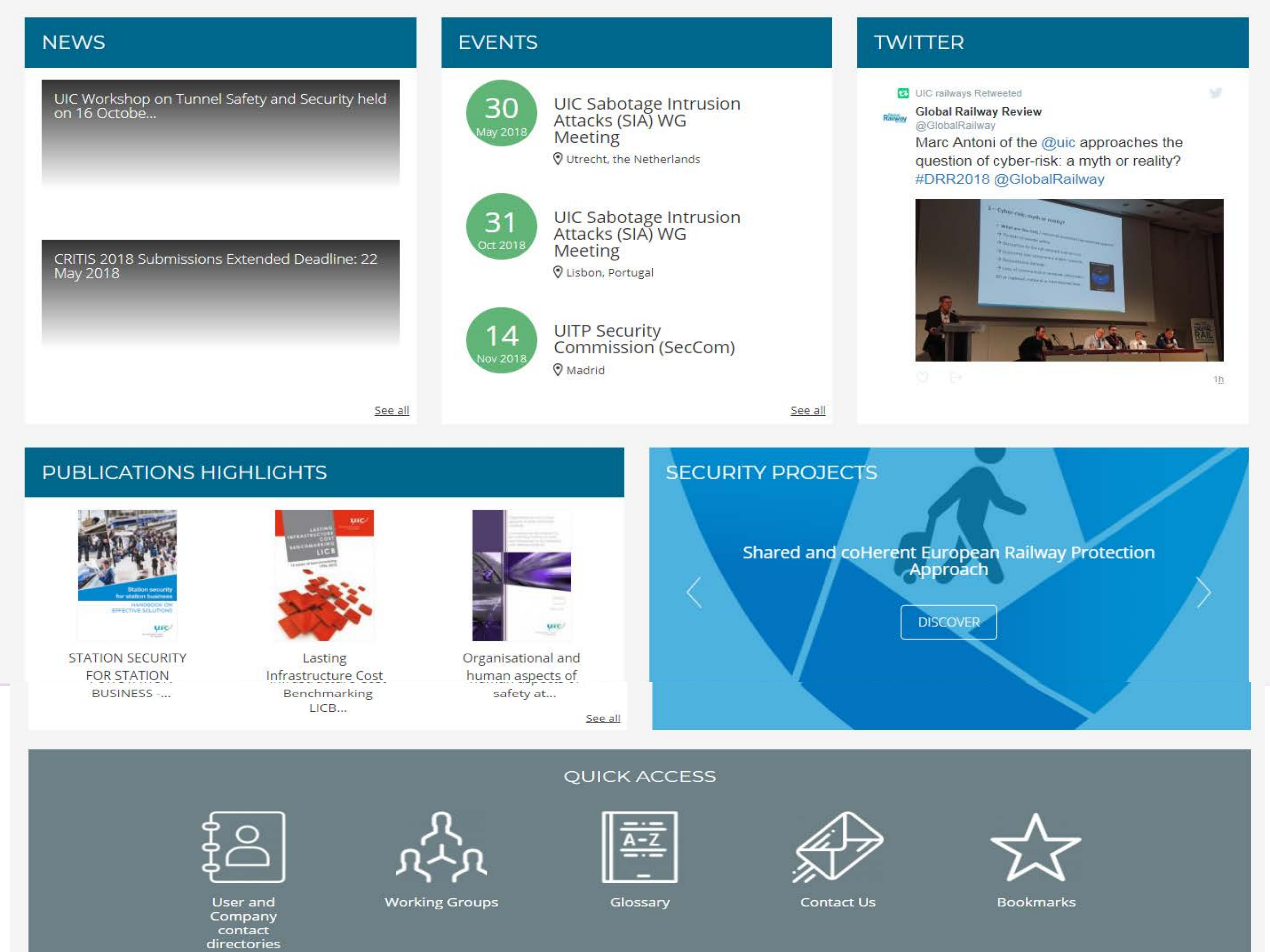
LATEST MEMBERS CONTRIBUTIONS

SAMPLE DOCUMENT 1
UIC

Example
SNCF

Test
Test

See all



NEWS

UIC Workshop on Tunnel Safety and Security held on 16 Octobe...

CRITIS 2018 Submissions Extended Deadline: 22 May 2018

See all

EVENTS

30 May 2018 — UIC Sabotage Intrusion Attacks (SIA) WG Meeting
Utrecht, the Netherlands

31 Oct 2018 — UIC Sabotage Intrusion Attacks (SIA) WG Meeting
Lisbon, Portugal

14 Nov 2018 — UITP Security Commission (SecCom)
Madrid

See all

TWITTER

UIC railways Retweeted

Global Railway Review
@GlobalRailway

Marc Antoni of the @uic approaches the question of cyber-risk: a myth or reality? #DRR2018 @GlobalRailway

1h

PUBLICATIONS HIGHLIGHTS

STATION SECURITY FOR STATION BUSINESS -...

Lasting Infrastructure Cost Benchmarking LICB...

Organisational and human aspects of safety at...

See all

SECURITY PROJECTS

Shared and coHerent European Railway Protection Approach

DISCOVER

QUICK ACCESS

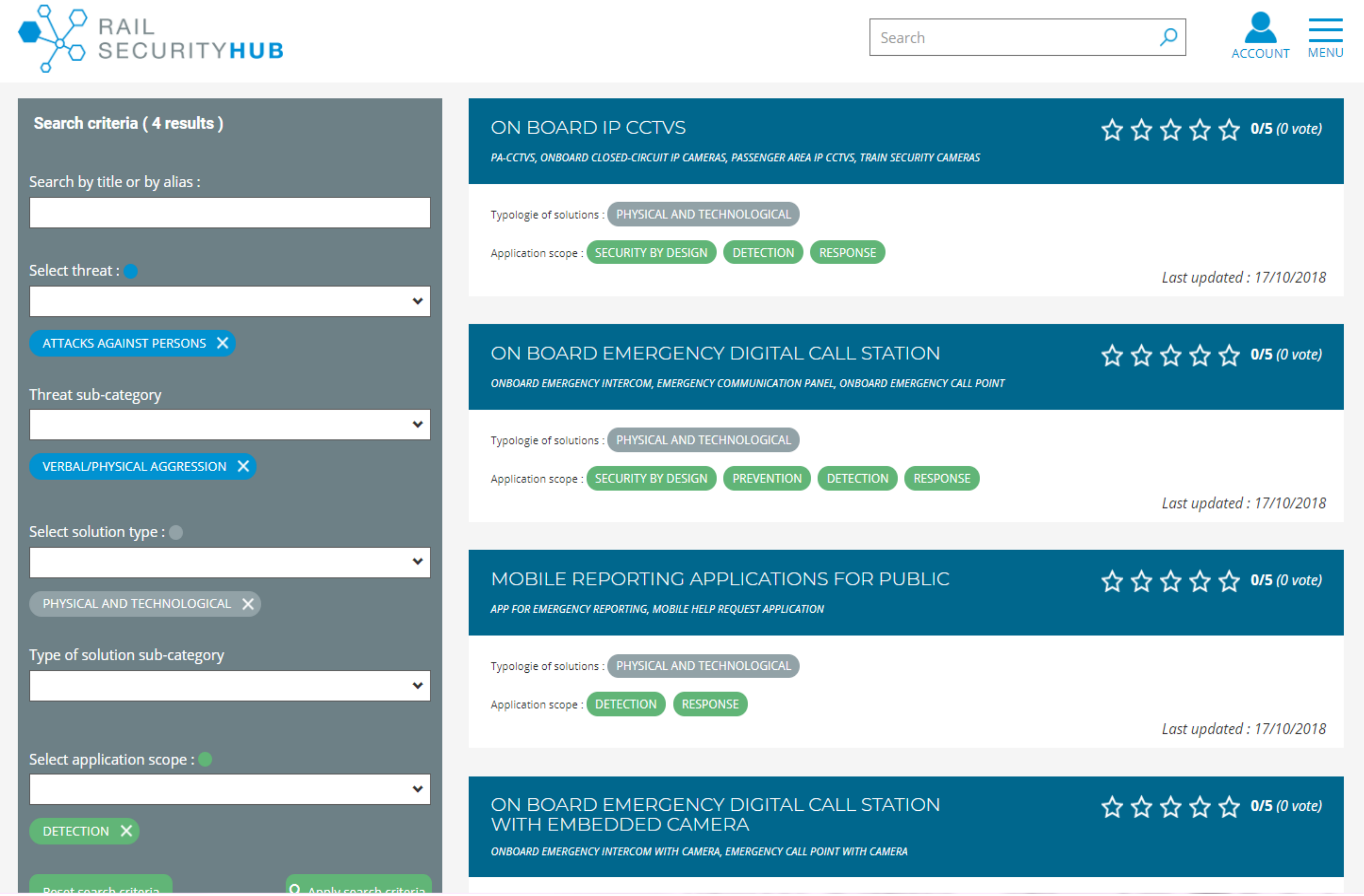
User and Company contact directories

Working Groups

Glossary

Contact Us

Bookmarks



Search criteria (4 results)

Search by title or by alias :

Select threat : ●

ATTACKS AGAINST PERSONS ✕

Threat sub-category

VERBAL/PHYSICAL AGGRESSION ✕

Select solution type : ●

PHYSICAL AND TECHNOLOGICAL ✕

Type of solution sub-category

Select application scope : ●

DETECTION ✕

Reset search criteria

Apply search criteria

ON BOARD IP CCTVS ☆☆☆☆☆ 0/5 *(0 vote)*

PA-CCTVS, ONBOARD CLOSED-CIRCUIT IP CAMERAS, PASSENGER AREA IP CCTVS, TRAIN SECURITY CAMERAS

Typologie of solutions : PHYSICAL AND TECHNOLOGICAL

Application scope : SECURITY BY DESIGN DETECTION RESPONSE

Last updated : 17/10/2018

ON BOARD EMERGENCY DIGITAL CALL STATION ☆☆☆☆☆ 0/5 *(0 vote)*

ONBOARD EMERGENCY INTERCOM, EMERGENCY COMMUNICATION PANEL, ONBOARD EMERGENCY CALL POINT

Typologie of solutions : PHYSICAL AND TECHNOLOGICAL

Application scope : SECURITY BY DESIGN PREVENTION DETECTION RESPONSE

Last updated : 17/10/2018

MOBILE REPORTING APPLICATIONS FOR PUBLIC ☆☆☆☆☆ 0/5 *(0 vote)*

APP FOR EMERGENCY REPORTING, MOBILE HELP REQUEST APPLICATION

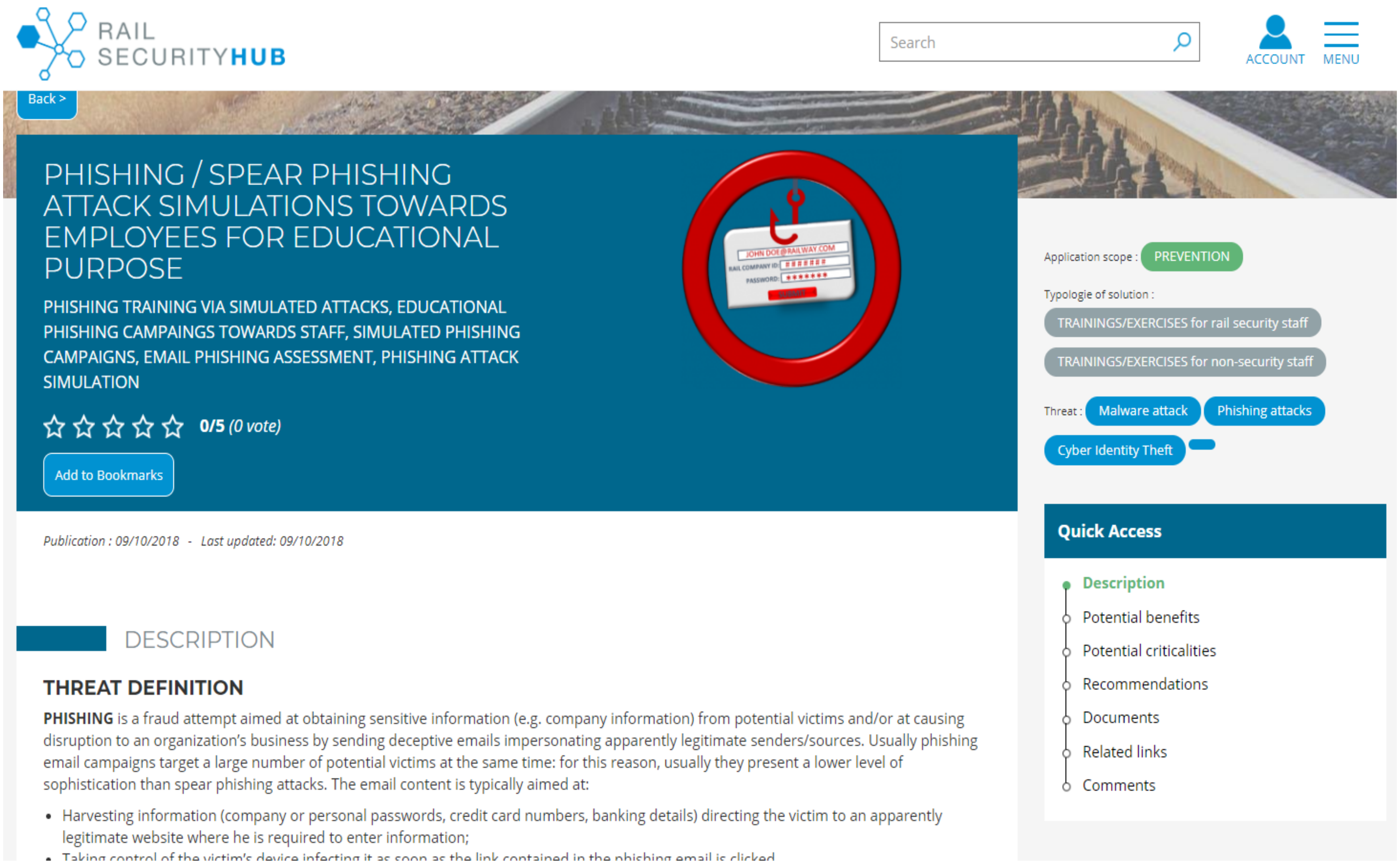
Typologie of solutions : PHYSICAL AND TECHNOLOGICAL

Application scope : DETECTION RESPONSE

Last updated : 17/10/2018

ON BOARD EMERGENCY DIGITAL CALL STATION WITH EMBEDDED CAMERA ☆☆☆☆☆ 0/5 *(0 vote)*

ONBOARD EMERGENCY INTERCOM WITH CAMERA, EMERGENCY CALL POINT WITH CAMERA



PHISHING / SPEAR PHISHING ATTACK SIMULATIONS TOWARDS EMPLOYEES FOR EDUCATIONAL PURPOSE

PHISHING TRAINING VIA SIMULATED ATTACKS, EDUCATIONAL PHISHING CAMPAINGS TOWARDS STAFF, SIMULATED PHISHING CAMPAIGNS, EMAIL PHISHING ASSESSMENT, PHISHING ATTACK SIMULATION

☆☆☆☆☆ **0/5** *(0 vote)*

Publication : 09/10/2018 - Last updated: 09/10/2018

Application scope : PREVENTION

Typologie of solution : TRAININGS/EXERCISES for rail security staff; TRAININGS/EXERCISES for non-security staff

Threat : Malware attack; Phishing attacks; Cyber Identity Theft

Quick Access

- Description
- Potential benefits
- Potential criticalities
- Recommendations
- Documents
- Related links
- Comments

DESCRIPTION

THREAT DEFINITION

PHISHING is a fraud attempt aimed at obtaining sensitive information (e.g. company information) from potential victims and/or at causing disruption to an organization's business by sending deceptive emails impersonating apparently legitimate senders/sources. Usually phishing email campaigns target a large number of potential victims at the same time: for this reason, usually they present a lower level of sophistication than spear phishing attacks. The email content is typically aimed at:

- Harvesting information (company or personal passwords, credit card numbers, banking details) directing the victim to an apparently legitimate website where he is required to enter information;
- Taking control of the victim's device infecting it as soon as the link contained in the phishing email is clicked

Thank you for your kind attention!

UIC website (Security):	http://www.uic.org/security
Rail Security HUB: *Online from January 2019*	http://www.railsecurityhub.org
Contact:	security@uic.org