



D6.1

Project's public website, leaflet, poster

Grant Agreement number:	740723
Project acronym:	CS-AWARE
Project title:	A cybersecurity situational awareness and information sharing solution for local public administrations based on advanced big data analysis
Principal author:	Laurentiu Vasiliu, PERACTON, laurentiu.vasiliu@peracton.com
Document version:	1.0



Table of Contents

Executive Summary	3
1 CS-AWARE website	3
2 Poster	4
3 Leaflet	5
4 Social Media Presence	6

Executive Summary

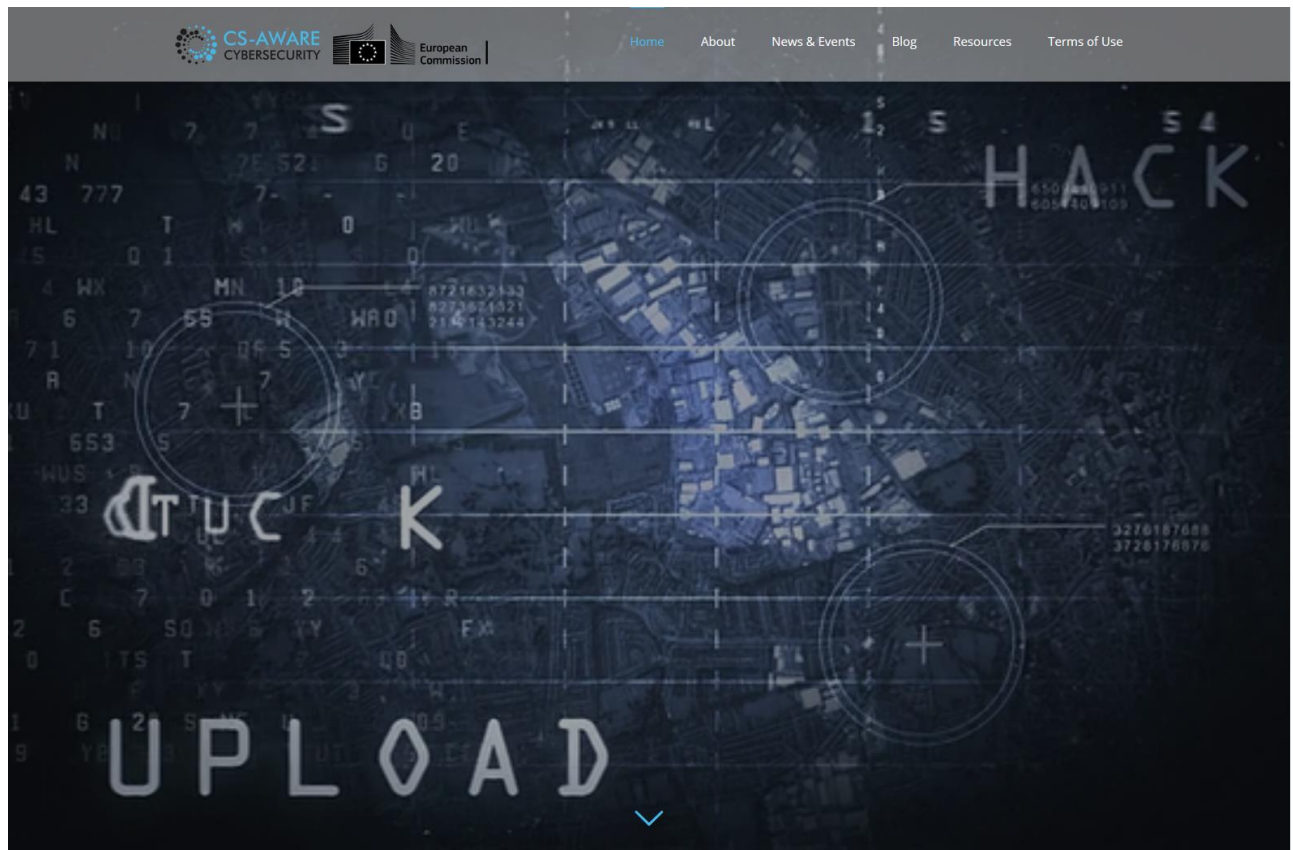
This document describes the CS-AWARE deliverable D6.1, the project's public website, leaflet, poster and our social media handles.

1 CS-AWARE website

Our website is live at the following address:

<http://cs-aware.eu/>

It contains a high-level project description, news about the project, a public deliverables section, regular updated blog posts as well as a resources section that will contain materials and information related to the goals and results of the project. As of November 2017, we have uploaded 8 blog posts and continuously update the webpage. The further described leaflet and poster are also part of the website and can be found in the resources/documentation section



2 Poster

The poster informs about the problem tackled, our project goals, methods and solutions presented in more detail, lists the project partners and guides the reader to relevant contact points.

CS-AWARE CYBERSECURITY

A 2017-2020 EU H2020 Project. Funding received under the EU 3.7.4 Innovation Action # 740723

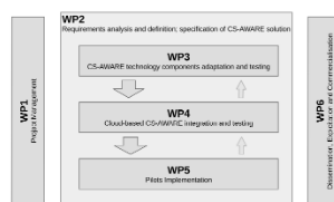
Problem

Cybersecurity is one of today's most challenging societal security problems, affecting large commercial companies, SMEs, NGOs or governmental institutions. Deliberate or accidental threats and attacks threaten digitally administered data and digitally handled processes.

Project objectives

- Objective 1: Provide a cybersecurity situational awareness solution for local public administrations.
- Objective 2: Advance the automation of cyber incident detection, classification and visualisation to provide situational awareness.
- Objective 3: Include a cybersecurity information exchange framework that embraces the collaboration and cooperation initiatives of EU.
- Objective 4: Illustrate that cyber situational awareness is a key technology in cybersecurity by building advanced features like system self-healing on top of the situational awareness capabilities.
- Objective 5: Evaluate and validate the user needs through end-user involvement and pilot testing.

Work Packages



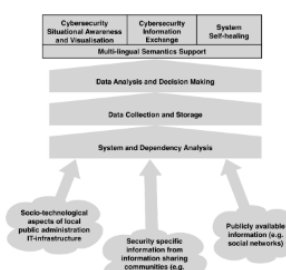
Main Goal

- The main goal of the CS-AWARE project is to provide a cybersecurity situational awareness solution for small to medium sized IT infrastructures.

Project Overview

- CS-AWARE approach will be a big step towards automation of cyber incident detection, classification and visualisation, and will be based on mature big data analysis tools and methodologies provided by consortium partners.
- This solution enables detect, classify and visualise cybersecurity incidents in real-time, supporting the prevention or mitigation of cyber attacks.
- However, cyber situational awareness will never be a fully automatic process that only requires to install a tool that, without any configuration, will be able to monitor the different setups and configurations of different organisational IT infrastructures.

CS-AWARE Concept



Expected Impacts

- Increased competitiveness of European ICT security products and services catering to the needs of SMEs, local public administrations and individuals.
- Increased resilience against widespread cybersecurity threats facing SMEs, local public administrations and individuals.
- Increased effectiveness of cybersecurity solutions through usability advancements and increased automation.

Proposed Solution

Situational Awareness

- Enables the end user to counteract cybersecurity incidents. Full control is retained by the user over his / her actions and receives recommendations for counter actions if available.


Information Sharing

- While providing automated mechanisms for information sharing, the user stays in control over which data will be shared, especially when confidentiality or privacy matters have to be taken into account.

Self-healing




- While providing cybersecurity strategies that can be invoked automatically to mitigate incidents or attacks, the user should retain the control about which strategies will be invoked in which situation, and/or if they should be invoked without user interaction.



Consortium Partners



Contact us

cs-aware.eu
 Prof. Juha Rönkä
Juha.Ronka@oulu.fi
 tel: +358294482612

3 Leaflet

The leaflet serves as an attention grabber at public events in which we present CS-AWARE. It contains key points in a concise and condensed version.



AWARENESS

•

DETECTION

•

PROTECTION



The problem

Cybersecurity is one of the most challenging security problems of today. Large and small organizations, as well as public administrations face various growing threats on a daily basis having limited resources and expertise to handle it.

CS-AWARE Solution:

- Automatic incident detection, classification & visualization
- Information exchange with relevant authorities
- System self-healing
- Multi-lingual semantic support

Contact Us

cs-aware.eu

[Twitter](#)

[Facebook](#)

Prof. Juha Roning

Juha.Roning@oulu.fi

tel:+358294482612



4 Social Media Presence

The social media presence it is an interlinked part of our dissemination program. In this respect we have created CS-AWARE dedicated pages on Twitter, Facebook and You-Tube that will become more and more lively as the project progresses. The links are the followings:

Twitter: https://twitter.com/H2020EU_CSWARE

Facebook: <https://www.facebook.com/H2020.CSAWARE.CyberS3curity.Situational.Awareness/>

YouTube: https://www.youtube.com/channel/UCQbnu8tb4zIW9u4_bKYAyMg/featured?