CYBER-TRUST

Advanced Cyber-Threat Intelligence, Detection, and Mitigation Platform for a Trusted Internet of Things
Grant Agreement: 786698

D9.1 Cyber-Trust Project Website

Work Package 9: Dissemination and exploitation

Document Dissemination Level

P	Public	☒
CO	Confidential, only for members of the Consortium (including the Commission Services)	□

Document Due Date: 31/08/2018
Document Submission Date: 31/08/2018

Co-funded by the Horizon 2020 Framework Programme of the European Union

Document Information

Deliverable number:	D9.1
Deliverable title:	Cyber-Trust Project Website
Deliverable version:	1.0
Work Package number:	WP9
Work Package title:	Dissemination and Exploitation
Due Date of delivery:	31/08/2018
Actual date of delivery:	31/08/2018
Dissemination level:	PU
Editor(s):	Liza Charalambous (ADITESS)
Contributor(s):	
Reviewer(s):	Gohar Sargsyan (CGI) Romain Griffiths (SCORECHAIN)
Project name:	Advanced Cyber-Threat Intelligence, Detection, and Mitigation Platform for a Trusted Internet of Things
Project Acronym	Cyber-Trust
Project starting date:	01/05/2018
Project duration:	36 months
Rights:	Cyber-Trust Consortium

Version History

Version	Date	Beneficiary	Description
0.1	17/08/2018	ADITESS	Proposed outline
0.2	22/08/2018	ADITESS	Deliverable Ready for review
0.3	30/08/2018	SCORECHAIN	Reviewed Document
0.4	30/08/2018	CGI	Reviewed Document
0.5	30/08/2018	ADITESS	Incorporated reviewer's comments
0.6	30/08/2018	ADITESS	Send for Submission
1.0	03/09/2018	ADITESS	Updated Project disclaimers

Acronyms

ACRONYM	EXPLANATION
HTTPS	**Hypertext Transfer Protocol Secure**
SSL	Secure Sockets Layer
TSL	Transport Layer Security
PHP	Hypertext Preprocessor
CMS	Content Management System
CA	Certificate Authority
CAPTCHA	Completely Automated Public Turing test to tell Computers and Humans Apart
RSS	Rich Site Summary
WP	Word Press
DOA	Document of Action

Table of Contents

Table of Figures

Executive summary

The Cyber-Trust website is accessible at the address www.Cyber-Trust.eu and is considered one of the most essential dissemination tools of the project. The website is designed aiming to be simple, functional and intuitive for the project stakeholders' and different types of audience. The content of the website includes information such as a brief description of the Cyber-Trust project including the objectives, information about the consortium, all the research relevant material, documents such as publications, newsletters, etc. News about the project and events are also provided by the website.

Additionally, the social media accounts (a Facebook page and a Twitter account) have been set up with the aim to communicate a simplified presentation of the core activities of Cyber-Trust to the general public. Mailing lists for Cyber-Trust have been created for communication between consortium partners and external stakeholders. The possibility to disseminate project outcomes through newsletters and message digests is also possible in case the need emerges.

In this document we focus on the communication channels of Cyber-Trust for online presence. Our main focus is the design and structure of the dedicated Cyber-Trust website and the created social media accounts.

1. Introduction

As Internet resources are key tools to raise awareness about the project and improve dissemination to specialists and potential users of the security technologies to be developed, a website dedicated to the Cyber-Trust project has been created on which services, such as mailing lists, RSS feeds, discussion forums/blogs, and webcasts/podcasts are hosted. Additionally, the creation of the project Facebook page and a Twitter profile, are expected to spread the Cyber-Trust achievements and activities to the general public.

The development of the Cyber-Trust website is designed with the aim of providing open access (free of charge, online access for any user) to all scientific publications, open-source software, etc., without violating the intellectual property rules established in the initial plan; open access is an efficient way of disseminating knowledge that accelerates scientific and technological progress. The publicity of project website will be promoted putting the address on printed items, press releases, etc. Encouraging linking from all partners' and other websites as well as registering the Cyber-Trust website with appropriate portals will increase the its traffic.

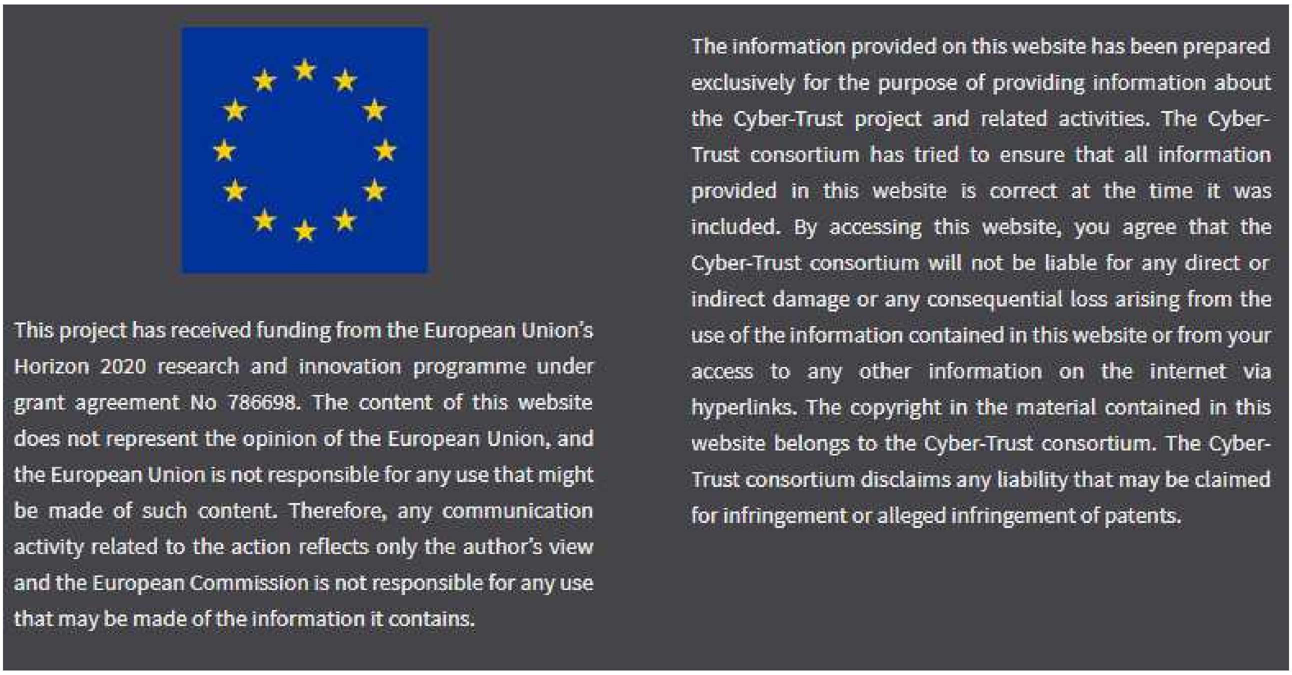
The website hosts blog and news pages where the consortium can share ideas and report technological achievements as they arise in the project; it will be open to individual entities to allow active participation. In this way, new researchers can get acquainted with Cyber-Trust while large industrial entities can support the effort and provide guidelines.

1.1 Project Hashtag

According to the recommendations of the European Commission[1] and in order to establish an audience for the Cyber-Trust project and increase its outreach, the website and social media accounts will promote the published articles and project outcomes under the hashtag ***#CyberTrust***.

1.2 Media Disclaimer

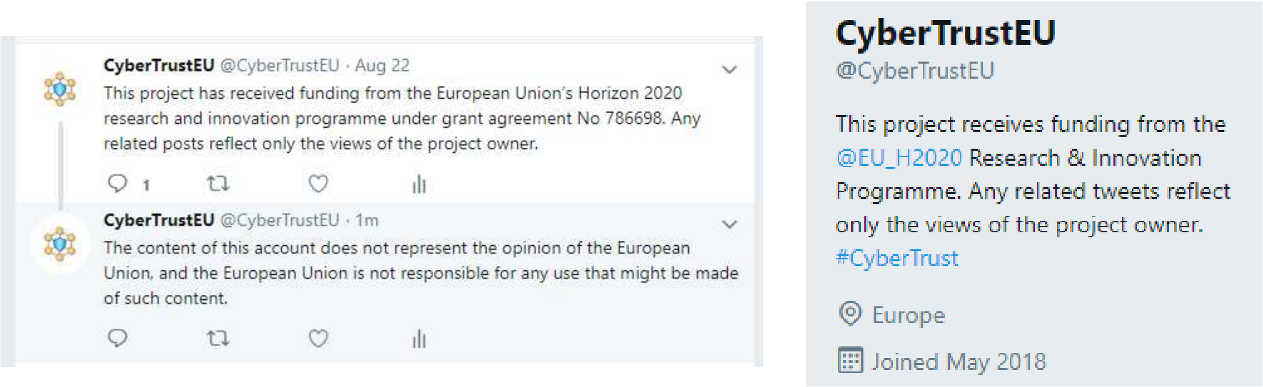
The Cyber Trust project website and social media accounts clearly acknowledge EU Funding (see Figure 1- 1, Figure 1- 2 and Figure 1- 3).



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 786698. The content of this website does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of such content. Therefore, any communication activity related to the action reflects only the author's view and the European Commission is not responsible for any use that may be made of the information it contains.

The information provided on this website has been prepared exclusively for the purpose of providing information about the Cyber-Trust project and related activities. The Cyber-Trust consortium has tried to ensure that all information provided in this website is correct at the time it was included. By accessing this website, you agree that the Cyber-Trust consortium will not be liable for any direct or indirect damage or any consequential loss arising from the use of the information contained in this website or from your access to any other information on the internet via hyperlinks. The copyright in the material contained in this website belongs to the Cyber-Trust consortium. The Cyber-Trust consortium disclaims any liability that may be claimed for infringement or alleged infringement of patents.

Figure 1- 1 Disclaimer on Project Website



CyberTrustEU @CyberTrustEU · Aug 22

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 786698. Any related posts reflect only the views of the project owner.

CyberTrustEU @CyberTrustEU · 1m

The content of this account does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of such content.

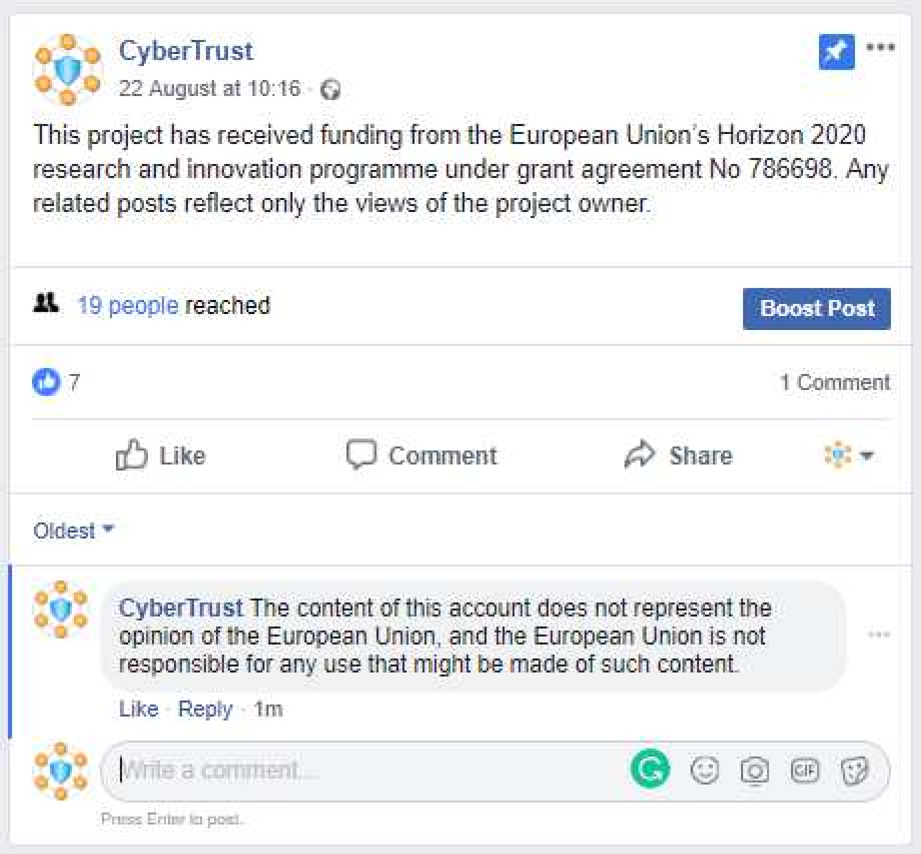
CyberTrustEU
@CyberTrustEU

This project receives funding from the @EU_H2020 Research & Innovation Programme. Any related tweets reflect only the views of the project owner. #CyberTrust

Europe

Joined May 2018

Figure 1- 2 Disclaimer on Twitter account



CyberTrust
22 August at 10:16 ·

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 786698. Any related posts reflect only the views of the project owner.

CyberTrust The content of this account does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of such content.

Figure 1- 3 Disclaimer on Facebook Page

The rest of this deliverable discusses aspects concerning the Cyber-Trust official website and social media accounts.

2. Cyber-Trust Website Design

2.1 Hosting and Domain

The Cyber-Trust website is hosted on a dedicated server owned by ADITESS Ltd. The registered domain name (Cyber-Trust.eu) used for hosting the website has been registered and purchased for 10 years; period that can also be extended if needed. The Cyber-Trust website can be accessed at www.Cyber-Trust.eu.

2.2 Web-Design Tools and Methods

For the design and development of the Cyber-Trust website, the WordPress[2] platform has been used. WordPress is a free and open source blogging tool and CMS based on PHP and MySQL, featuring a plugin architecture and a template system. WordPress users may install and switch between themes. Themes allow users to change the look and functionality of a WordPress website or installation without altering the information content or structure of the site. WordPress's plugin architecture allows users to extend its features. Customizations range from search engine optimization, to client portals used to display private information to logged in users, to content displaying features, such as the addition of widgets and navigation bars. WordPress also features integrated link management; a search engine–friendly, clean permalink structure; the ability to assign multiple categories to articles; and support for tagging of posts and articles. Automatic filters are also included, providing standardized formatting and styling of text in articles (for example, converting regular quotes to smart quotes). WordPress also supports the Trackback and Pingback standards for displaying links to other sites that have themselves linked to a post or an article.

Cyber-Trust uses the proprietary template Allegiant Pro[3], a visually striking multipurpose WordPress theme packed with features and widgets with its one-page layout and dedicated homepage sections making it especially suited as a business theme.

2.3 Browser Compatibility

To maximise visibility, the Cyber-Trust website was designed to render appropriately in all common web browsers on all common operating systems. These included various versions of Firefox, Internet Explorer, Google Chrome and Safari browsers on Apple MAC OS X, IOS and Microsoft Windows operating systems. Furthermore, due to the responsive theme the website is accessible from all the devices including tablets and smartphones.

2.4 HTTPS (SSL/TLS) Certificates

The Cyber-Trust website supports HTTPS access through the Let’s Encrypt service for a more secure and privacy-respecting Web. Let’s Encrypt is a free, automated, and open certificate authority (CA), run for the public’s benefit. It is a service provided by the Internet Security Research Group (ISRG)[1]. Let’s Encrypt provides digital certificates in order to enable HTTPS (SSL/TLS) for websites.

3. Cyber-Trust Website Content

The design of this website is one of the key dissemination tasks for the project. The website provides an overview of the project and will be continuously updated when this is necessary with actual information regarding Cyber-Trust activity and results (news, events, deliverables, newsletters, etc.).

The Cyber-Trust website (https://www.Cyber-Trust.eu) aims to:

- Establish an online dissemination and communication channel between the project consortium and target audiences;
- Inform the target audience for the project’s progress and latest news, and attract various users;
- Be a reference point to the forthcoming newsletters, leaflets and link to online communication channels, such as Facebook and Twitter.

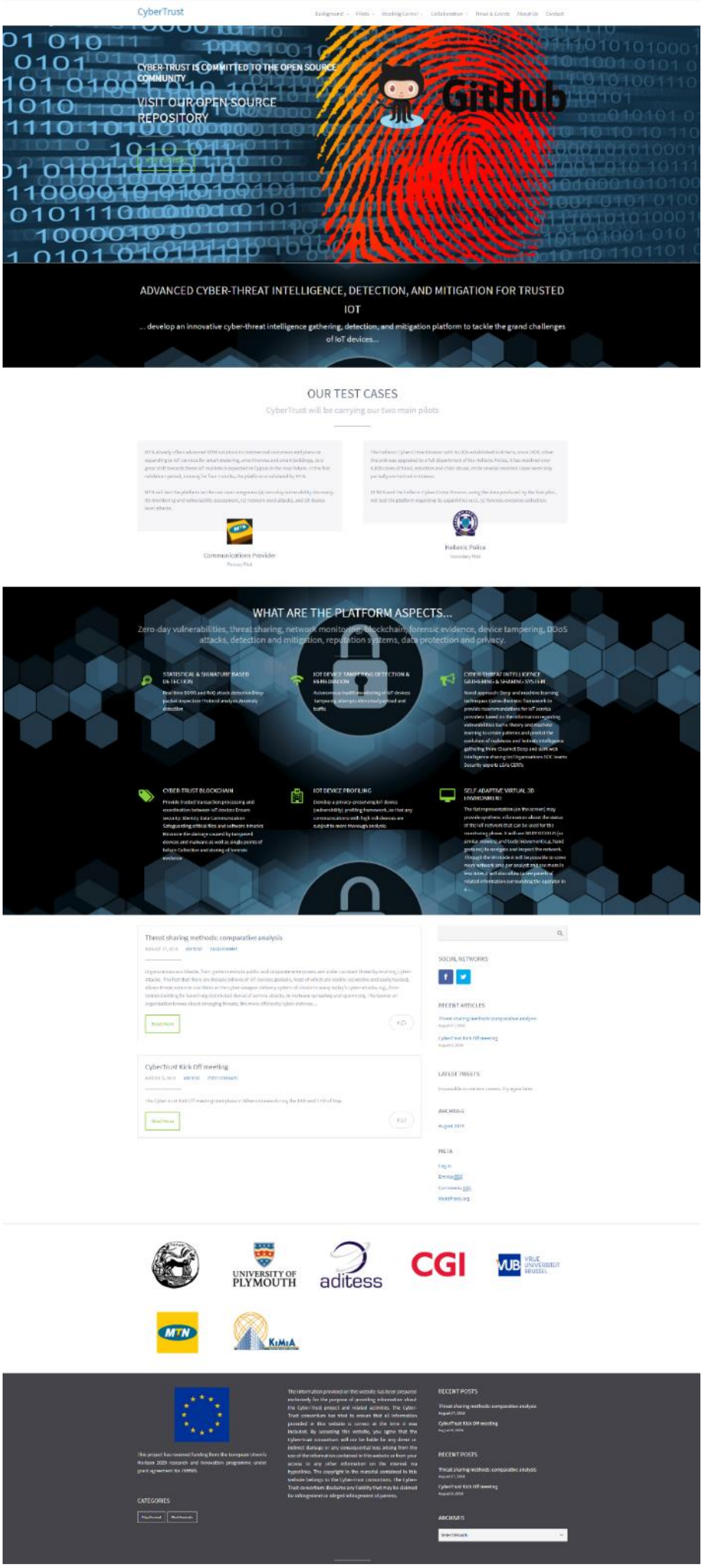
The Cyber-Trust website is developed by ADITESS responsible for its administration. The content of the website consists of static information about the project and relevant activities planned to address its objectives. The maintenance of the content of the website will be managed mainly by ADITESS with contributions provided by all partners. If partners wish to submit information to be published on the website, they should submit it to ADITESS who will then check its appropriateness together with CSCAN (WP leader) before publishing.

3.1 Homepage

The Cyber-Trust Homepage is split into a number of rows (see Figure 3- 1):

[1] https://letsencrypt.org/isrg/

- Header which is in the form of a spinner links to articles or sources the consortium would like to promote;
- Tagline disclosing the extended name of the project as well as its target;
- Our Test Cases section containing short descriptions of each of the two pilots;
- What are the platform aspects section, listing key aspects of the project;
- List of the most recent News & Events items;
- List of partner logos;
- Footer with the project disclaimer, the EU emblem, the post categories, outline of recent posts and access to monthly archives;



CYBER-TRUST IS COMMITTED TO THE OPEN SOURCE COMMUNITY

VISIT OUR OPEN SOURCE REPOSITORY

ADVANCED CYBER-THREAT INTELLIGENCE, DETECTION, AND MITIGATION FOR TRUSTED IOT

... develop an innovative cyber-threat intelligence gathering, detection, and mitigation platform to tackle the grand challenges of IoT devices...

OUR TEST CASES

CyberTrust will be carrying our two main pilots

[illegible]

Communications Provider

Primary Pilot

[illegible]

Hellenic Police

Secondary Pilot

WHAT ARE THE PLATFORM ASPECTS...

Zero-day vulnerabilities, threat sharing, network monitoring, blockchain, forensic evidence, device tampering, DDoS attacks, detection and mitigation, reputation systems, data protection and privacy.

STATISTICAL & SIGNATURE BASED DETECTION

Real time DDOS and RoQ attack detection Deep packet inspection Protocol analysis Anomaly detection

IOT DEVICE TAMPERING DETECTION & REMEDIATION

Autonomous health monitoring of IoT devices tampering attempts Abnormal payload and traffic

CYBER-THREAT INTELLIGENCE GATHERING & SHARING SYSTEM

Novel approach: Deep and machine learning techniques Game-theoretic framework to provide recommendations for IoT service providers based on the information regarding vulnerabilities Game theory and machine learning to create patterns and predict the evolution of malware and botnets Intelligence gathering from Clearnet Deep and dark web Intelligence sharing to Organisations SOC teams Security experts LEAs CERTs

CYBER-TRUST BLOCKCHAIN

Provide trusted transaction processing and coordination between IoT devices Ensure security: Identity Data Communication Safeguarding critical files and software binaries Minimize the damage caused by tampered devices and malware as well as single points of failure Collection and storing of forensic evidence

IOT DEVICE PROFILING

Develop a privacy-preserving IoT device (vulnerability) profiling framework, so that any communications with high risk devices are subject to more thorough analysis.

SELF ADAPTIVE VIRTUAL 3D ENVIRONMENT

The 3d representation (on the screen) may provide synthetic information about the status of the IoT network that can be used for the monitoring phase. It will use INDEX OCULUS (or similar devices) and body movements (e.g. hand gestures) to navigate and inspect the network. Through the VR mode it will be possible to cover more network area per analyst and see more in less time; it will also allow to see panels of related information surrounding the operator in a...

Threat sharing methods: comparative analysis

AUGUST 17, 2018 [illegible]

[illegible]

Read More

CyberTrust Kick Off meeting

AUGUST 6, 2018 [illegible]

[illegible]

Read More

SOCIAL NETWORKS

RECENT ARTICLES

Threat sharing methods: comparative analysis
August 17, 2018

CyberTrust Kick Off meeting
August 6, 2018

LATEST TWEETS

[illegible]

ARCHIVES

August 2018

META

Log in
Entries RSS
Comments RSS
WordPress.org

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 786698.

CATEGORIES

[illegible]

The information provided on this website has been prepared exclusively for the purpose of providing information about the Cyber-Trust project and related activities. The Cyber-Trust consortium has tried to ensure that all information provided in this website is correct at the time it was included. By accessing this website, you agree that the Cyber-Trust consortium will not be liable for any direct or indirect damage or any consequential loss arising from the use of the information contained in this website or from your access to any other information on the internet via hyperlinks. The copyright in the material contained in this website belongs to the Cyber-Trust consortium. The Cyber-Trust consortium disclaims any liability that may be claimed for infringement or alleged infringement of patents.

RECENT POSTS

Threat sharing methods: comparative analysis
August 17, 2018

CyberTrust Kick Off meeting
August 6, 2018

RECENT POSTS

Threat sharing methods: comparative analysis
August 17, 2018

CyberTrust Kick Off meeting
August 6, 2018

ARCHIVES

Select Month

Figure 3- 1 Website Homepage

3.2 Cyber-Trust Website Main Pages

The sticky main menu (see Figure 3- 2) always displayed at the top of the page as well as the sitemap (see Figure 3- 3) presented in the footer of the page allow access to all website pages. The menu options cover the different aspects of the project with additional sections for communication aspects.

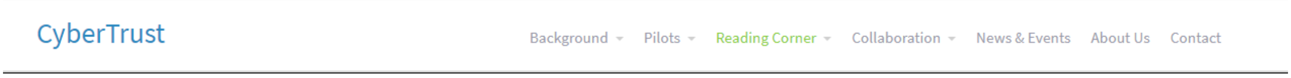


Figure 3- 2 Project Main Menu

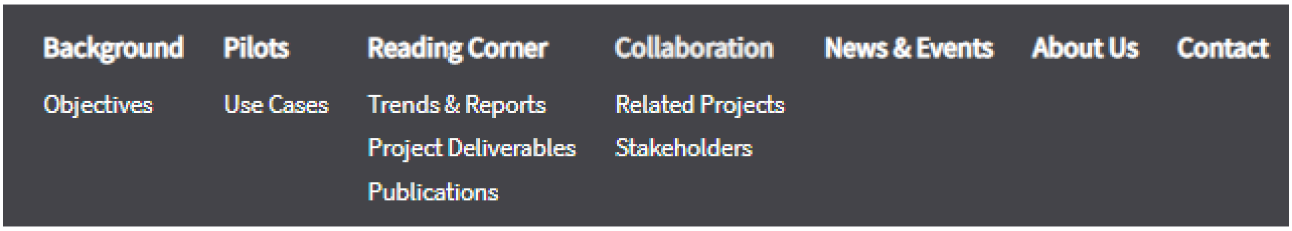
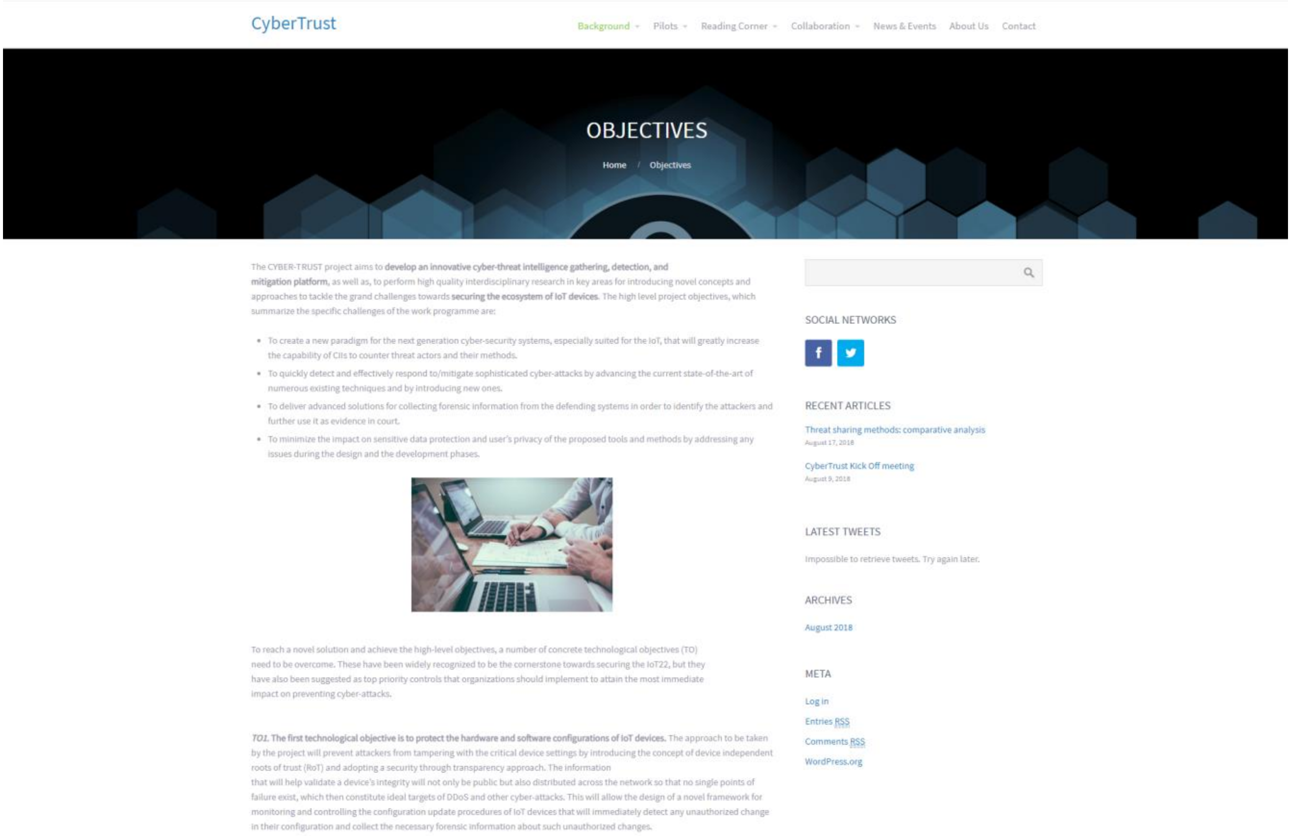


Figure 3- 3 Project Sitemap

A description of the content in each Menu section will be disclosed below.

3.2.1 Background

The background menu option contains static information related to the project's objective, ambition and impact (see Figure 3- 4).



The CYBER-TRUST project aims to **develop an innovative cyber-threat intelligence gathering, detection, and mitigation platform**, as well as, to perform high quality interdisciplinary research in key areas for introducing novel concepts and approaches to tackle the grand challenges towards **securing the ecosystem of IoT devices.** The high level project objectives, which summarize the specific challenges of the work programme are:

- To create a new paradigm for the next generation cyber-security systems, especially suited for the IoT, that will greatly increase the capability of CIIs to counter threat actors and their methods.
- To quickly detect and effectively respond to/mitigate sophisticated cyber-attacks by advancing the current state-of-the-art of numerous existing techniques and by introducing new ones.
- To deliver advanced solutions for collecting forensic information from the defending systems in order to identify the attackers and further use it as evidence in court.
- To minimize the impact on sensitive data protection and user's privacy of the proposed tools and methods by addressing any issues during the design and the development phases.

To reach a novel solution and achieve the high-level objectives, a number of concrete technological objectives (TO) need to be overcome. These have been widely recognized to be the cornerstone towards securing the IoT22, but they have also been suggested as top priority controls that organizations should implement to attain the most immediate impact on preventing cyber-attacks.

TO1. **The first technological objective is to protect the hardware and software configurations of IoT devices.** The approach to be taken by the project will prevent attackers from tampering with the critical device settings by introducing the concept of device independent roots of trust (RoT) and adopting a security through transparency approach. The information that will help validate a device's integrity will not only be public but also distributed across the network so that no single points of failure exist, which then constitute ideal targets of DDoS and other cyber-attacks. This will allow the design of a novel framework for monitoring and controlling the configuration update procedures of IoT devices that will immediately detect any unauthorized change in their configuration and collect the necessary forensic information about such unauthorized changes.

Impossible to retrieve tweets. Try again later.

Figure 3- 4 Project Objectives Page

3.2.2 Pilots

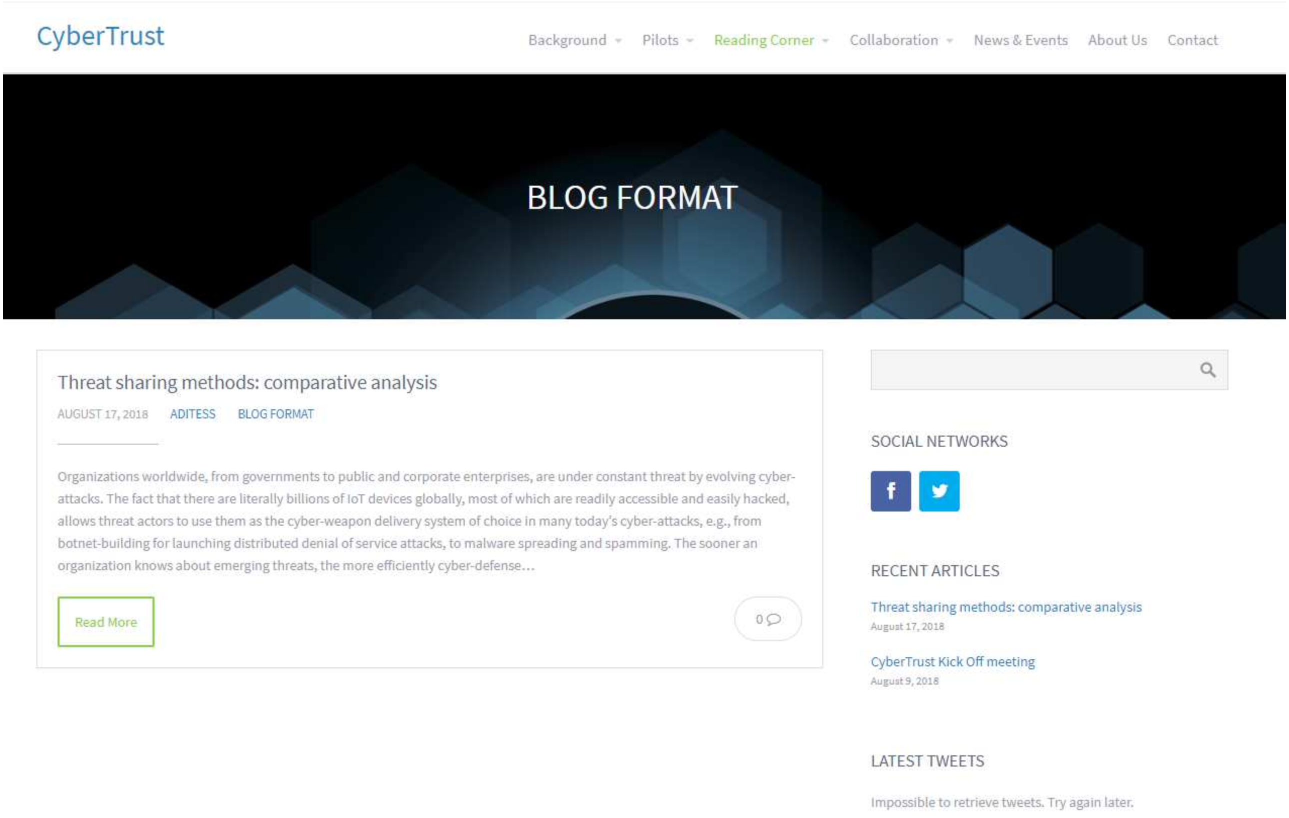
The Pilots menu option will hold information related to the preparation and execution of pilots as well as the defined Cyber-Trust use cases. Information will be updated as soon as new information and project activities are planned. This page will hold a comprehensive article regarding each pilot, its specified objectives and progress.

3.2.3 Reading Corner

In order to retain an audience, the Cyber-Trust will be continuously updated with articles of different types, available under the Reading Corner menu option. Articles in this section will involve, trends on cyber-security, news about emerging threats and vulnerabilities as well as project research outcomes.

3.2.3.1 Trends & Reports

This section is a blog-based section in which the consortium will be sharing interesting outcomes of our research as well as articles on trends and reports related to cyber security and attacks (see Figure 3- 5). By clicking on the read more button the reader is presented with the full article and the option to leave a comment initiating a discussion. Content from new commenters goes through moderation with the user required to provide their name and email; additionally, to avoid spamming a CAPTCHA also needs to be filled. Once a user's comment is approved by the page moderators, the user is free to comment without the need to undergo moderation again; making their experience more pleasant.



Threat sharing methods: comparative analysis

AUGUST 17, 2018 ADITESS BLOG FORMAT

Organizations worldwide, from governments to public and corporate enterprises, are under constant threat by evolving cyber-attacks. The fact that there are literally billions of IoT devices globally, most of which are readily accessible and easily hacked, allows threat actors to use them as the cyber-weapon delivery system of choice in many today's cyber-attacks, e.g., from botnet-building for launching distributed denial of service attacks, to malware spreading and spamming. The sooner an organization knows about emerging threats, the more efficiently cyber-defense…

Threat sharing methods: comparative analysis
August 17, 2018

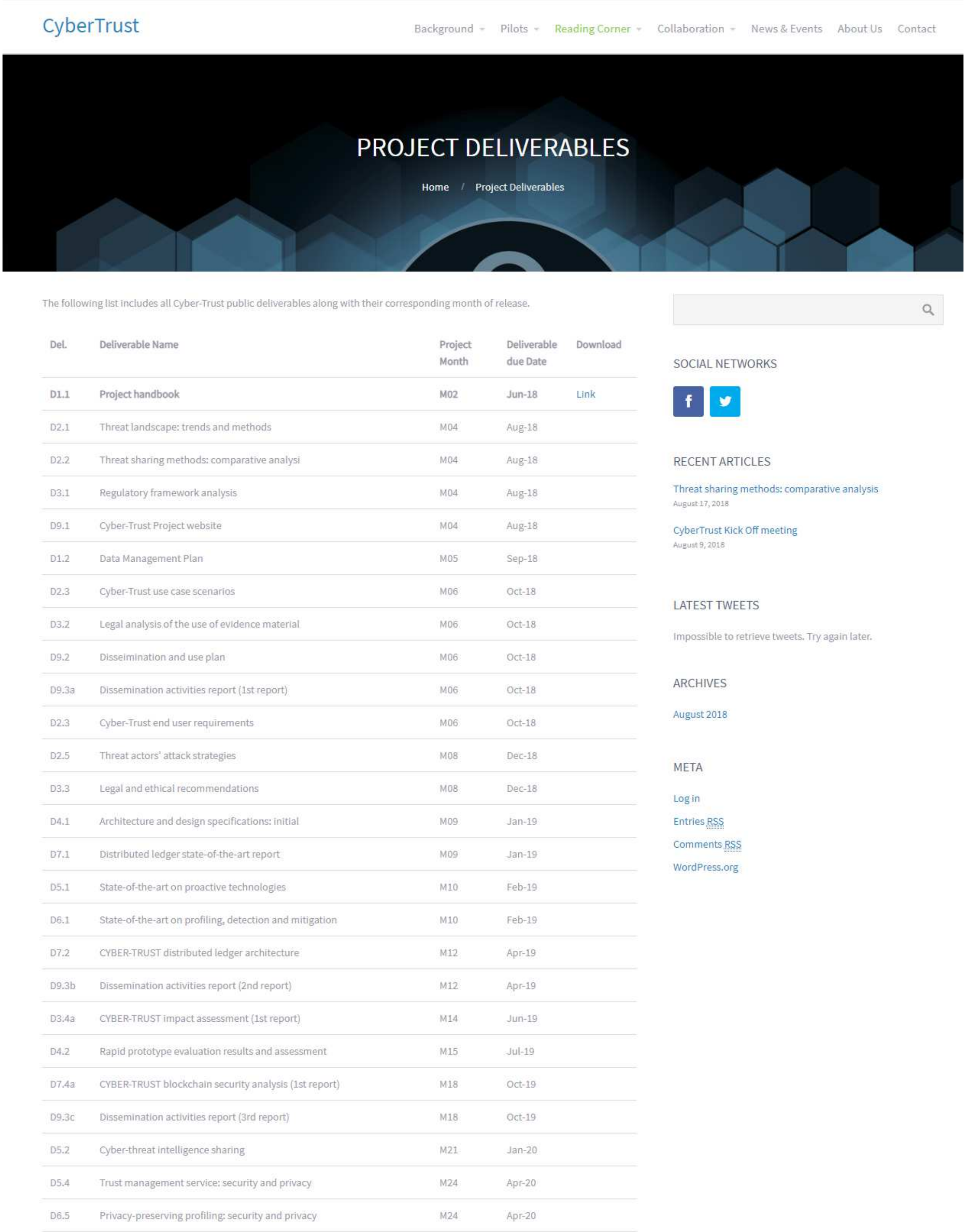
CyberTrust Kick Off meeting
August 9, 2018

Impossible to retrieve tweets. Try again later.

Figure 3- 5 The Trends & Reports page

3.2.3.2 *Project Deliverables*

CyberTrust is commited to public and open source content and as a result a large percentage of its deliverables will be released after their submission as public content. Submitted, approved by the EC and released deliveralbes will be published in the Project Deliverables page. The page currently displays the list of all public deliverables along with their expected day of submission to the EC. Once clearance is being released for the publication of a deliverable a link will be produced for saving the document in PDF form (see Figure 3- 6**Error! Reference source not found.**). For confidential and therefore restricted deliveralbed a publishable executive summary will be made available.



The following list includes all Cyber-Trust public deliverables along with their corresponding month of release.

Del.	Deliverable Name	Project Month	Deliverable due Date	Download
D1.1	**Project handbook**	**M02**	**Jun-18**	Link
D2.1	Threat landscape: trends and methods	M04	Aug-18	
D2.2	Threat sharing methods: comparative analysi	M04	Aug-18	
D3.1	Regulatory framework analysis	M04	Aug-18	
D9.1	Cyber-Trust Project website	M04	Aug-18	
D1.2	Data Management Plan	M05	Sep-18	
D2.3	Cyber-Trust use case scenarios	M06	Oct-18	
D3.2	Legal analysis of the use of evidence material	M06	Oct-18	
D9.2	Disseimination and use plan	M06	Oct-18	
D9.3a	Dissemination activities report (1st report)	M06	Oct-18	
D2.3	Cyber-Trust end user requirements	M06	Oct-18	
D2.5	Threat actors' attack strategies	M08	Dec-18	
D3.3	Legal and ethical recommendations	M08	Dec-18	
D4.1	Architecture and design specifications: initial	M09	Jan-19	
D7.1	Distributed ledger state-of-the-art report	M09	Jan-19	
D5.1	State-of-the-art on proactive technologies	M10	Feb-19	
D6.1	State-of-the-art on profiling, detection and mitigation	M10	Feb-19	
D7.2	CYBER-TRUST distributed ledger architecture	M12	Apr-19	
D9.3b	Dissemination activities report (2nd report)	M12	Apr-19	
D3.4a	CYBER-TRUST impact assessment (1st report)	M14	Jun-19	
D4.2	Rapid prototype evaluation results and assessment	M15	Jul-19	
D7.4a	CYBER-TRUST blockchain security analysis (1st report)	M18	Oct-19	
D9.3c	Dissemination activities report (3rd report)	M18	Oct-19	
D5.2	Cyber-threat intelligence sharing	M21	Jan-20	
D5.4	Trust management service: security and privacy	M24	Apr-20	
D6.5	Privacy-preserving profiling: security and privacy	M24	Apr-20	

SOCIAL NETWORKS

RECENT ARTICLES

Threat sharing methods: comparative analysis
August 17, 2018

CyberTrust Kick Off meeting
August 9, 2018

LATEST TWEETS

Impossible to retrieve tweets. Try again later.

ARCHIVES

August 2018

META

Log in
Entries RSS
Comments RSS
WordPress.org

Figure 3- 6 List of Public Deliverables

3.2.3.3 Publications

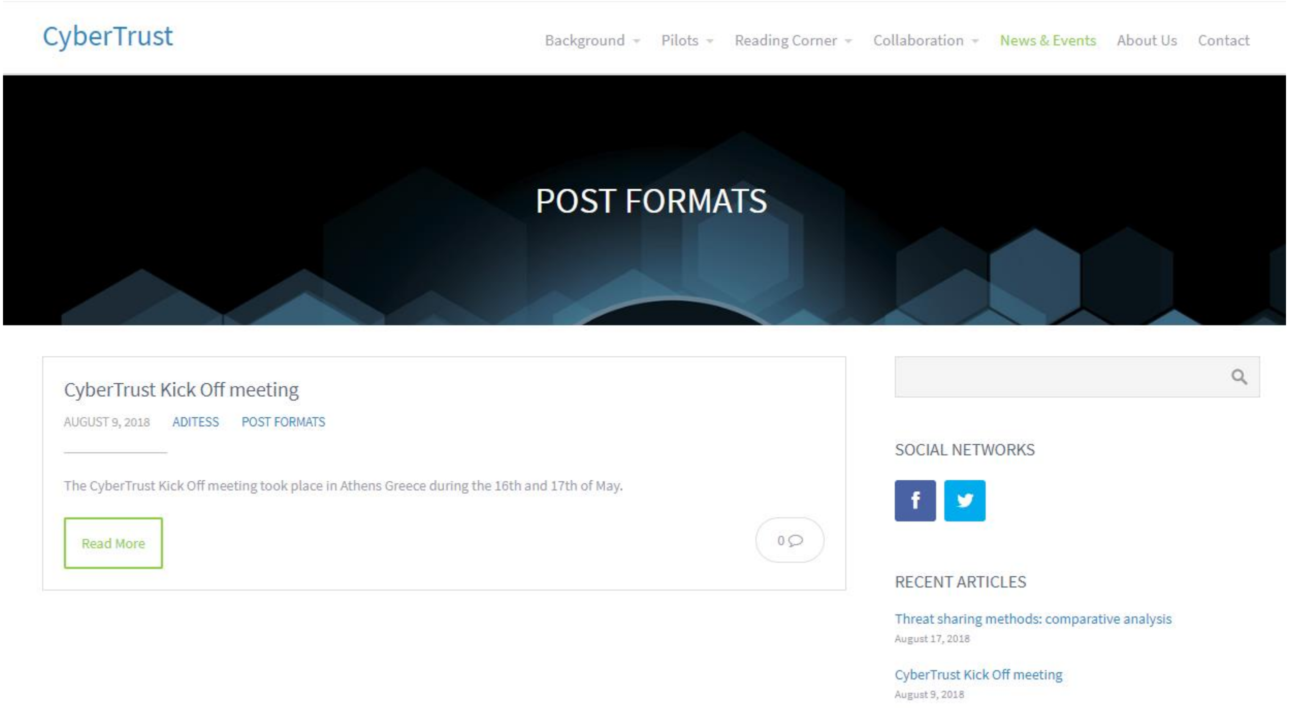
Finally, in the last submenu option of the Reading Corner category is called publications. This page will hold references and links to the pdf files of Cyber-Trust publications.

3.2.4 Collaboration

The collaboration menu holds the options to view Cyber-Trust collaborations with external bodies and other H2020 projects as well ad the Related Projects page which holds information with regards to other EU research projects funded under the same, or related, topic.

3.2.5 News & Events

This section is another blog-based section in which the consortium will be communicating interesting outcomes of our research, key events in which consortium partners will be participating as well as planned project meetings (plenary meetings and progress, technical sessions and pilot trials) (see Figure 3- 7). Additionally, this page will provide links to webcasts or webinars produced by the consortium for the end users. By clicking on the read more button the reader is presented with the full article and the option to leave a comment initiating a discussion.



CyberTrust Kick Off meeting

AUGUST 9, 2018 ADITESS POST FORMATS

The CyberTrust Kick Off meeting took place in Athens Greece during the 16th and 17th of May.

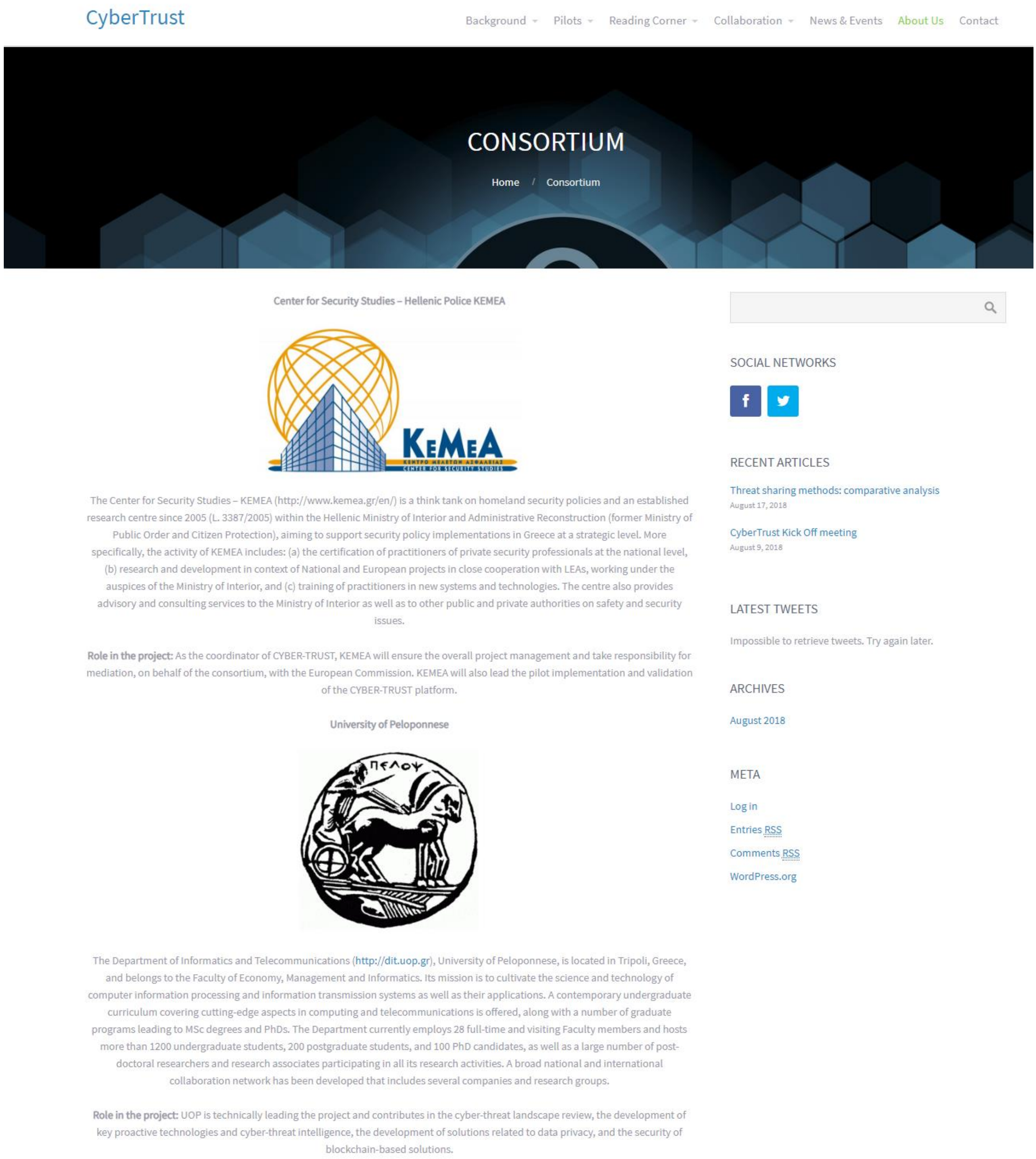
Threat sharing methods: comparative analysis
August 17, 2018

CyberTrust Kick Off meeting
August 9, 2018

Figure 3- 7 News & Events Page

3.2.6 About Us

The web page of the consortium presents the nine participating organizations of the project (see Figure 3- 8). For each partner its logo is presented along with their organisation name, their short profile and role in the Cyber-Trust project. A link to the official webpage of each partner is also provided through the logo and the organization name.



Center for Security Studies – Hellenic Police KEMEA

The Center for Security Studies – KEMEA (http://www.kemea.gr/en/) is a think tank on homeland security policies and an established research centre since 2005 (L. 3387/2005) within the Hellenic Ministry of Interior and Administrative Reconstruction (former Ministry of Public Order and Citizen Protection), aiming to support security policy implementations in Greece at a strategic level. More specifically, the activity of KEMEA includes: (a) the certification of practitioners of private security professionals at the national level, (b) research and development in context of National and European projects in close cooperation with LEAs, working under the auspices of the Ministry of Interior, and (c) training of practitioners in new systems and technologies. The centre also provides advisory and consulting services to the Ministry of Interior as well as to other public and private authorities on safety and security issues.

Role in the project: As the coordinator of CYBER-TRUST, KEMEA will ensure the overall project management and take responsibility for mediation, on behalf of the consortium, with the European Commission. KEMEA will also lead the pilot implementation and validation of the CYBER-TRUST platform.

University of Peloponnese

The Department of Informatics and Telecommunications (http://dit.uop.gr), University of Peloponnese, is located in Tripoli, Greece, and belongs to the Faculty of Economy, Management and Informatics. Its mission is to cultivate the science and technology of computer information processing and information transmission systems as well as their applications. A contemporary undergraduate curriculum covering cutting-edge aspects in computing and telecommunications is offered, along with a number of graduate programs leading to MSc degrees and PhDs. The Department currently employs 28 full-time and visiting Faculty members and hosts more than 1200 undergraduate students, 200 postgraduate students, and 100 PhD candidates, as well as a large number of post-doctoral researchers and research associates participating in all its research activities. A broad national and international collaboration network has been developed that includes several companies and research groups.

Role in the project: UOP is technically leading the project and contributes in the cyber-threat landscape review, the development of key proactive technologies and cyber-threat intelligence, the development of solutions related to data privacy, and the security of blockchain-based solutions.

RECENT ARTICLES

Threat sharing methods: comparative analysis
August 17, 2018

CyberTrust Kick Off meeting
August 9, 2018

LATEST TWEETS

Impossible to retrieve tweets. Try again later.

ARCHIVES

August 2018

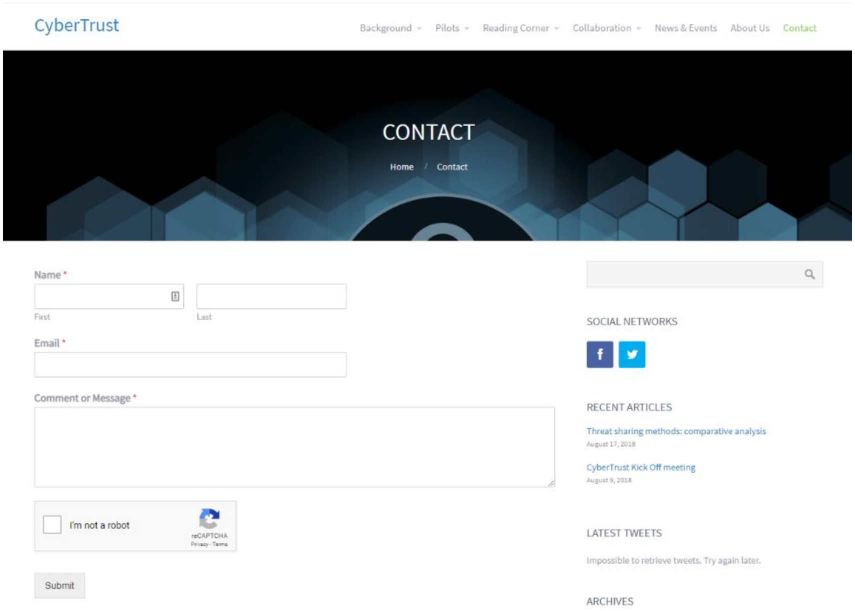
META

Log in
Entries RSS
Comments RSS
WordPress.org

Figure 3- 8 The About Us page

3.2.7 Contact

The last main menu option is the contact page through which a user may send a message or request to the moderator of the website (see Figure 3- 9**Error! Reference source not found.**). The content of the query will then be shared to the relevant partner in the consortium for resolution. This page also required the user to fill in a CAPTCHA to avoid spamming.



Name *

First Last

Email *

Comment or Message *

SOCIAL NETWORKS

RECENT ARTICLES

Threat sharing methods: comparative analysis
August 17, 2018

CyberTrust Kick Off meeting
August 9, 2018

LATEST TWEETS

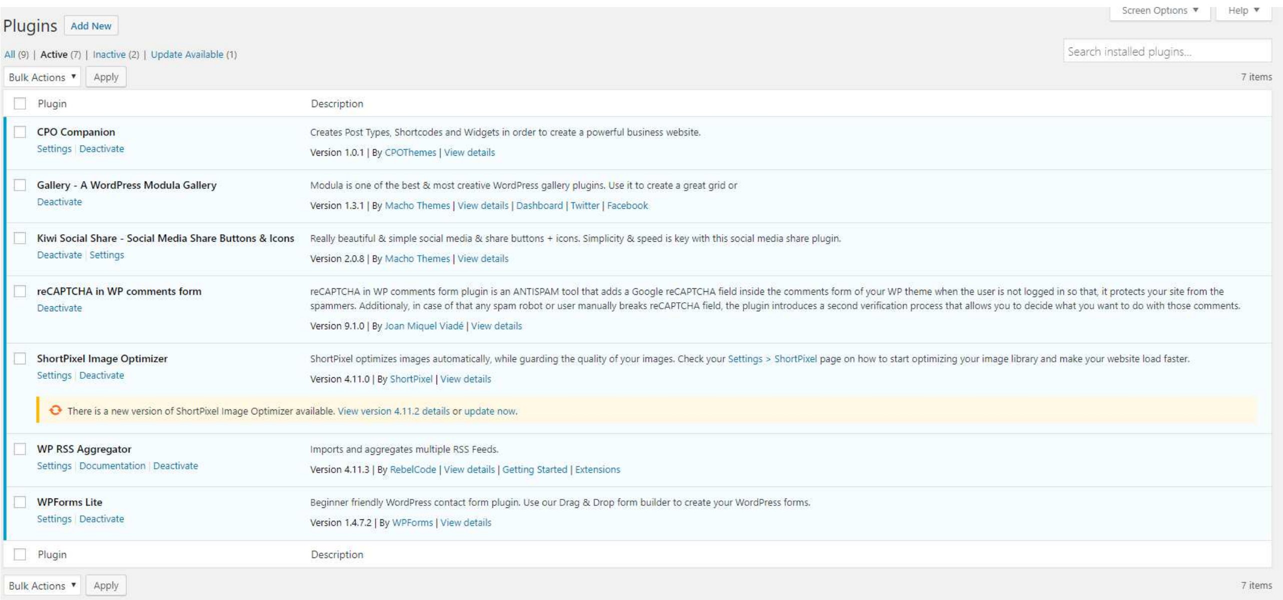
Impossible to retrieve tweets. Try again later.

ARCHIVES

Figure 3- 9 Website Contact Form

3.3 Plugins

The operation of the Cyber-Trust website is supported by a number of plugins which can be seen in Figure 3- 10. The main plugins are discussed in the rest of this section.



All (9) | Active (7) | Inactive (2) | Update Available (1)

7 items

Plugin	Description
CPO Companion Settings | Deactivate	Creates Post Types, Shortcodes and Widgets in order to create a powerful business website. Version 1.0.1 | By CPOThemes | View details
Gallery - A WordPress Modula Gallery Deactivate	Modula is one of the best & most creative WordPress gallery plugins. Use it to create a great grid or Version 1.3.1 | By Macho Themes | View details | Dashboard | Twitter | Facebook
Kiwi Social Share - Social Media Share Buttons & Icons Deactivate | Settings	Really beautiful & simple social media & share buttons + icons. Simplicity & speed is key with this social media share plugin. Version 2.0.8 | By Macho Themes | View details
reCAPTCHA in WP comments form Deactivate	reCAPTCHA in WP comments form plugin is an ANTISPAM tool that adds a Google reCAPTCHA field inside the comments form of your WP theme when the user is not logged in so that, it protects your site from the spammers. Additionaly, in case of that any spam robot or user manually breaks reCAPTCHA field, the plugin introduces a second verification process that allows you to decide what you want to do with those comments. Version 9.1.0 | By Joan Miquel Viadé | View details
ShortPixel Image Optimizer Settings | Deactivate	ShortPixel optimizes images automatically, while guarding the quality of your images. Check your Settings > ShortPixel page on how to start optimizing your image library and make your website load faster. Version 4.11.0 | By ShortPixel | View details There is a new version of ShortPixel Image Optimizer available. View version 4.11.2 details or update now.
WP RSS Aggregator Settings | Documentation | Deactivate	Imports and aggregates multiple RSS Feeds. Version 4.11.3 | By RebelCode | View details | Getting Started | Extensions
WPForms Lite Settings | Deactivate	Beginner friendly WordPress contact form plugin. Use our Drag & Drop form builder to create your WordPress forms. Version 1.4.7.2 | By WPForms | View details
Plugin	Description

7 items

Figure 3- 10 Website Activated Plugins

3.3.1 Google reCAPTCHA

Google reCAPTCHA [4] is a free service that protects your site from spam and abuse. It uses advanced risk analysis techniques to tell humans and bots apart. With the new API, a significant number of your valid human users will pass the reCAPTCHA challenge without having to solve a CAPTCHA. reCAPTCHA comes in the form of a widget (see Figure 3- 11) that you can easily add to your blog, forum, registration form, etc. Additionally, in case of that any spam robot or user manually breaks reCAPTCHA field, the plugin introduces a second verification process that allows you to decide what you want to do with those comments.

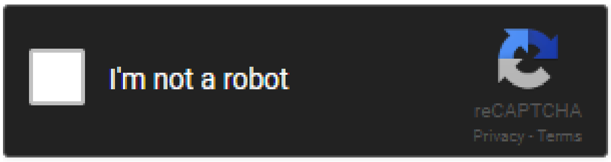


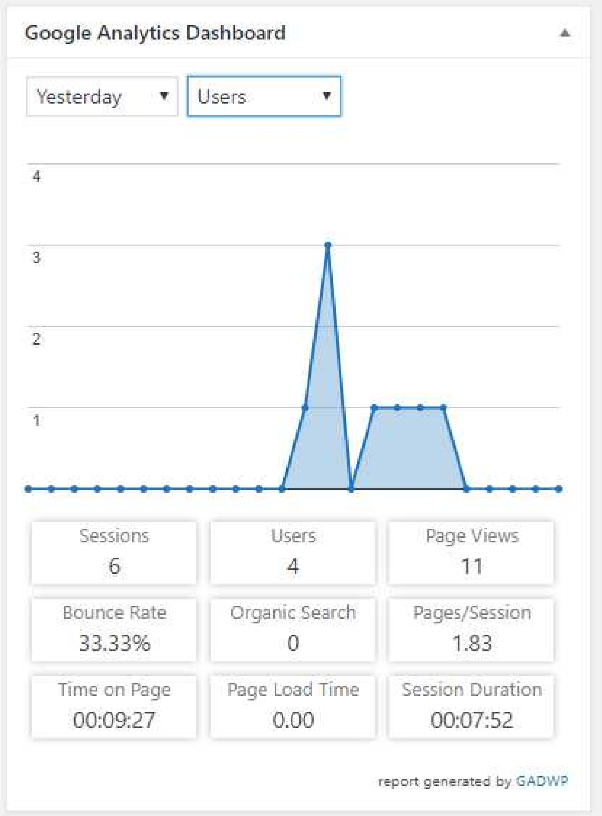
Figure 3- 11 reCAPTCHA widget for website forms and comment sections

The reCAPTCHA tool for WordPress acts as an ANTISPAM tool adding a reCAPTCHA field inside the comments form when the user is not logged in so that, protecting the site from spammers.

3.3.2 Google Analytics

In order to help the monitoring and analysing the usage of our website, we have registered the site with the free Google Analytics service. Using this service, reports about the usage and accessing of public data (webpages) will be created providing the site administration with helpful information on:

- How many users are visiting the site
- The number of the returning visitors
- How long users are spending on the site
- Which pages are most popular
- How users where informed about the site
- Countries from which users are accessing the site
- The number of downloads of specific publicly available files on the site
- The kind of the devices that interacting with the website

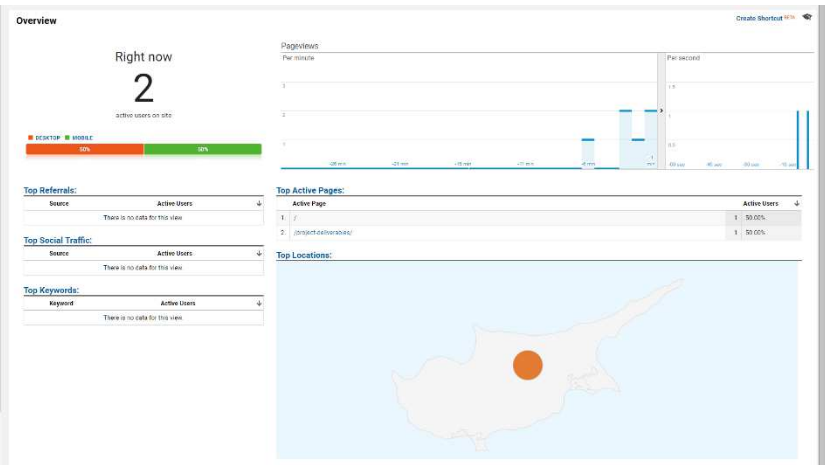


Yesterday ▾ Users ▾

Sessions	Users	Page Views
6	4	11
Bounce Rate	Organic Search	Pages/Session
33.33%	0	1.83
Time on Page	Page Load Time	Session Duration
00:09:27	0.00	00:07:52

Figure 3- 12 Google Analytics Dashboard on WordPress

The google analytics data are accessible through the Google Analytics official website and mobile application as well an installed plugin to our website administration panel which provides all the available reports. Figure 3- 12, Figure 3- 13 and Figure 3- 14show snapshots of the google analytics dashboard.



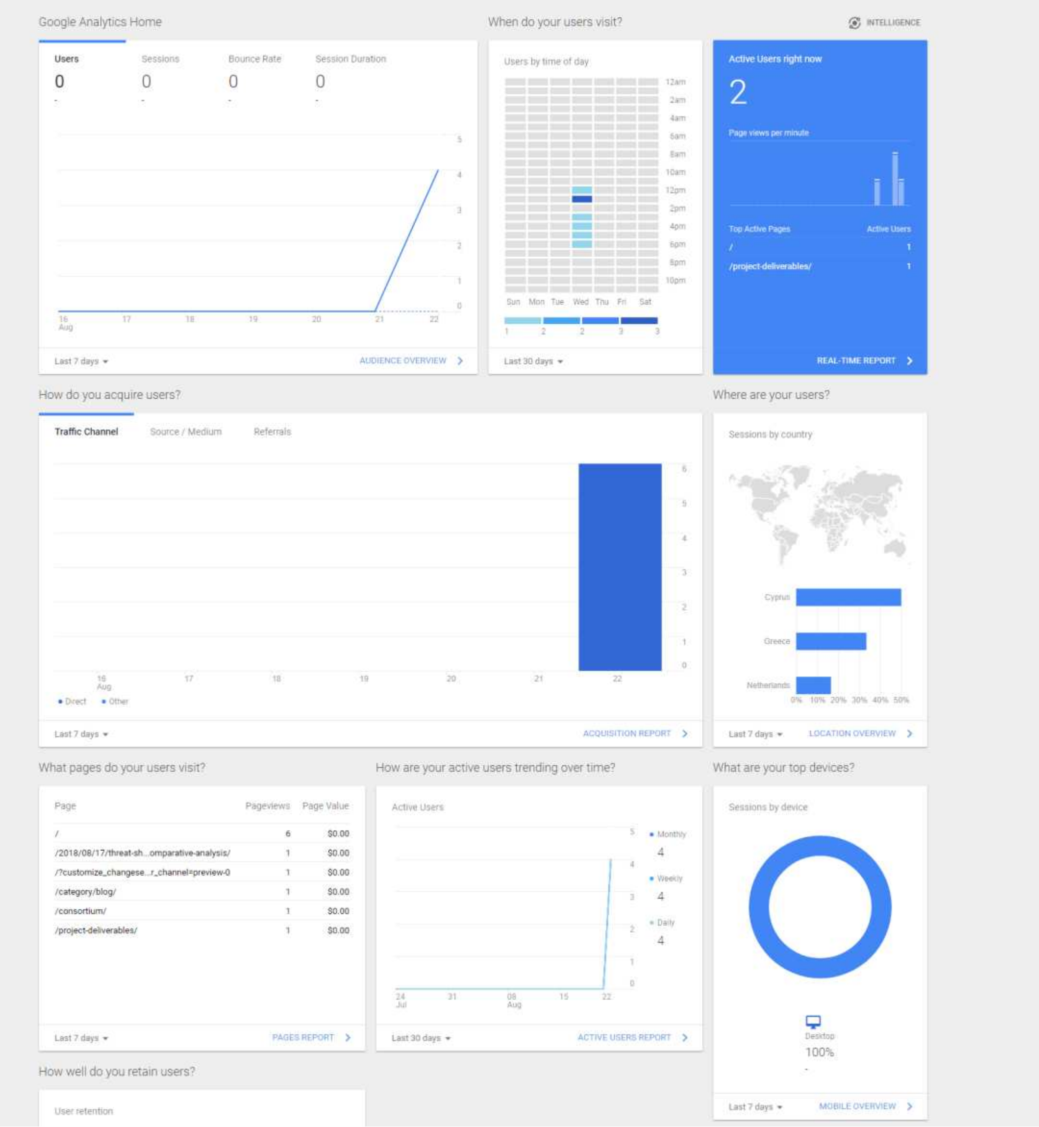
Source	Active Users
There is no data for this view	

Source	Active Users
There is no data for this view	

Keyword	Active Users
There is no data for this view	

	Active Page	Active Users	
1.	/	1	50.00%
2.	/project-deliverables/	1	50.00%

Figure 3- 13 Real Time Monitoring Google Analytics Dashboard



Top Active Pages	Active Users
/	1
/project-deliverables/	1

Page	Pageviews	Page Value
/	6	$0.00
/2018/08/17/threat-sh...omparative-analysis/	1	$0.00
/?customize_changese...r_channel=preview-0	1	$0.00
/category/blog/	1	$0.00
/consortium/	1	$0.00
/project-deliverables/	1	$0.00

Figure 3- 14 Fresh Integration of Cyber-Trust with the Google Analytics Dashboard

3.3.3 RSS feeds

Support for RSS feeds is also added to the website through the WP RSS aggregator[5] for easily importing, merging and displaying RSS and Atom feeds. The RSS aggregator offers a quite comprehensive and elegant RSS feed solution, allowing the aggregation of unlimited RSS feeds, with the ability to stagger the update process for better performance.

3.3.4 Sharing to Social Media platforms

The Kiwi Social Share plugin [6] adds buttons for sharing content to external social media platforms at the bottom of each page (see Figure 3- 15). This plugin supports a quire extensive number of social media platforms, however we have enabled sharing to Facebook, Twitter and LinkedIn, as these are the most relevant social media platforms to CyberTrust.

Figure 3- 15 External Social Media buttons

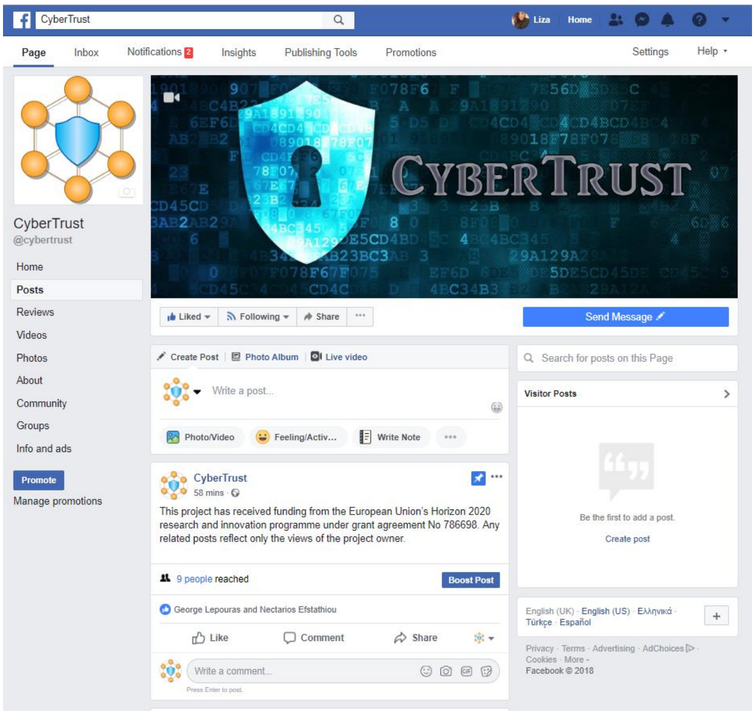
4. Cyber-Trust Social Media

Communication of Cyber-Trust activities and outcomes to the social media will be preformed through its Facebook Page (see **Error! Reference source not found.**) and Twitter account (see **Error! Reference source not found.**). These accounts have been set up with the aim to communicate a simplified presentation of the core activities of Cyber-Trust to the general public.

In order to link the project website with the social media accounts, the website's sidebar (visible on the right of all paged) contains buttons leading to the Cyber-Trust social media accounts (see **Error! Reference source not found.**). Clicking each of these will lead the user to our Facebook page[2] and Twitter account[3] respectively.

[2] https://www.facebook.com/cybertrust/

[3] https://twitter.com/CyberTrustEU



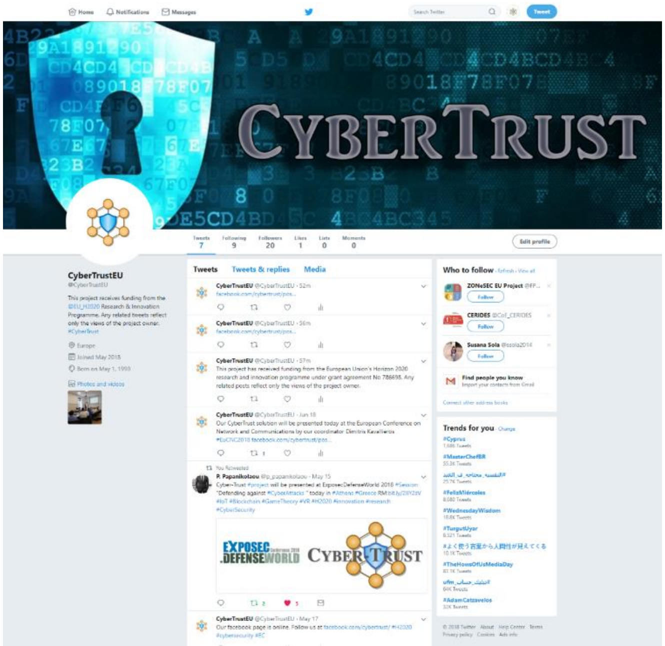
CyberTrust
58 mins

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 786698. Any related posts reflect only the views of the project owner.

9 people reached

George Lepouras and Nectarios Efstathiou

Figure 4- 1 Screenshot of the Facebook Page



CyberTrustEU
@CyberTrustEU

This project receives funding from the @EU_H2020 Research & Innovation Programme. Any related tweets reflect only the views of the project owner. #CyberTrust

Europe
Joined May 2018
Born on May 1, 1990
Photos and videos

CyberTrustEU @CyberTrustEU · 52m
facebook.com/cybertrust/pos...

CyberTrustEU @CyberTrustEU · 56m
facebook.com/cybertrust/pos...

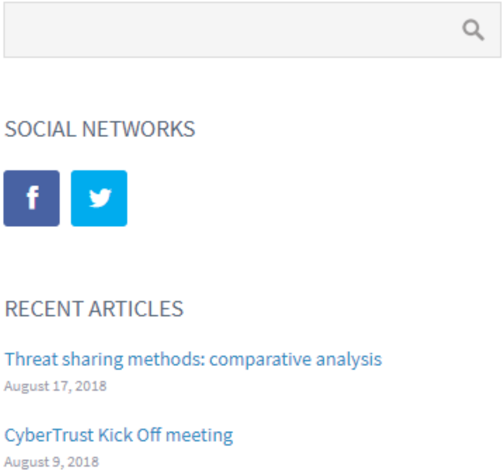
CyberTrustEU @CyberTrustEU · 57m
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 786698. Any related posts reflect only the views of the project owner.

CyberTrustEU @CyberTrustEU · Jun 18
Our CyberTrust solution will be presented today at the European Conference on Network and Communications by our coordinator Dimitris Kavallieros #EuCNC2018 facebook.com/cybertrust/pos...

You Retweeted
P. Papanikolaou @p_papanikolaou · May 15
Cyber-Trust #project will be presented at ExposecDefenseWorld 2018 #Session "Defending against #CyberAttacks " today in #Athens #Greece RM bit.ly/2IlY2sV #IoT #Blockchain #GameTheory #VR #H2020 #innovation #research #CyberSecurity

CyberTrustEU @CyberTrustEU · May 17
Our facebook page is online. Follow us at facebook.com/cybertrust/ #H2020 #cybersecurity #EC

Figure 4- 2 Screenshot of Twitter Account



Threat sharing methods: comparative analysis
August 17, 2018

CyberTrust Kick Off meeting
August 9, 2018

Figure 4- 3 Links to Cyber-Trust social media accounts

5. Conclusion

In a nutshell, in this document, a detailed approach for the Cyber-Trust website has been presented. Description of the methods used to build it, the hosting features and its structure were presented along with information regarding the project's social media accounts. The Cyber-Trust website is designed with the aim of providing open access (free of charge, online access for any user) to all scientific publications, open-source software, etc., without violating the intellectual property rules established in the initial plan. The website hosts blog and news pages where the consortium can share ideas and report technological achievements as they arise in the project; it will be open to individual entities to allow active participation. In this way, new researchers can get acquainted with Cyber-Trust while large industrial entities can support the effort and provide guidelines.

6. References

[1] "H2020 Programme Guidance Social media guide for EU funded R&amp;I projects," 2018.

[2] "Blog Tool, Publishing Platform, and CMS — WordPress." [Online]. Available: https://wordpress.org/. [Accessed: 23-Aug-2018].

[3] "Allegiant – Free Multipurpose WordPress Theme." [Online]. Available: https://cpothemes.com/theme/allegiant. [Accessed: 23-Aug-2018].

[4] "reCAPTCHA | Google Developers." [Online]. Available: https://developers.google.com/recaptcha/. [Accessed: 23-Aug-2018].

[5] RebelCode, "WP RSS Aggregator | WordPress.org." [Online]. Available: https://wordpress.org/plugins/wp-rss-aggregator/. [Accessed: 23-Aug-2018].

[6] Macho Themes, "Kiwi Social Share – Social Media Share Buttons &amp; Icons | WordPress.org." [Online]. Available: https://wordpress.org/plugins/kiwi-social-share/. [Accessed: 23-Aug-2018].