D9.1 Cyber-Trust Project Website

Work Package 9: Dissemination and exploitation

Document Dissemination Level

<table>
<thead>
<tr>
<th></th>
<th>Public</th>
<th>□</th>
</tr>
</thead>
<tbody>
<tr>
<td>CO</td>
<td>Confidential, only for members of the Consortium (including the Commission Services)</td>
<td>☒</td>
</tr>
</tbody>
</table>

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

Co-funded by the Horizon 2020 Framework Programme of the European Union
<table>
<thead>
<tr>
<th>Document Information</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Deliverable number:</td>
<td>D9.1</td>
</tr>
<tr>
<td>Deliverable title:</td>
<td>Cyber-Trust Project Website</td>
</tr>
<tr>
<td>Deliverable version:</td>
<td>1.0</td>
</tr>
<tr>
<td>Work Package number:</td>
<td>WP9</td>
</tr>
<tr>
<td>Work Package title:</td>
<td>Dissemination and Exploitation</td>
</tr>
<tr>
<td>Due Date of delivery:</td>
<td>31/08/2018</td>
</tr>
<tr>
<td>Actual date of delivery:</td>
<td>31/08/2018</td>
</tr>
<tr>
<td>Dissemination level:</td>
<td>PU</td>
</tr>
<tr>
<td>Editor(s):</td>
<td>Liza Charalambous (ADITESS)</td>
</tr>
<tr>
<td>Contributor(s):</td>
<td>Gohar Sargsyan (CGI) Romain Griffiths (SCORECHAIN)</td>
</tr>
<tr>
<td>Reviewer(s):</td>
<td></td>
</tr>
<tr>
<td>Project name:</td>
<td>Advanced Cyber-Threat Intelligence, Detection, and Mitigation Platform for a Trusted Internet of Things</td>
</tr>
<tr>
<td>Project Acronym</td>
<td>Cyber-Trust</td>
</tr>
<tr>
<td>Project starting date:</td>
<td>01/05/2018</td>
</tr>
<tr>
<td>Project duration:</td>
<td>36 months</td>
</tr>
<tr>
<td>Rights:</td>
<td>Cyber-Trust Consortium</td>
</tr>
</tbody>
</table>
# Version History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Beneficiary</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>17/08/2018</td>
<td>ADITESS</td>
<td>Proposed outline</td>
</tr>
<tr>
<td>0.2</td>
<td>22/08/2018</td>
<td>ADITESS</td>
<td>Deliverable Ready for review</td>
</tr>
<tr>
<td>0.3</td>
<td>30/08/2018</td>
<td>SCORECHAIN</td>
<td>Reviewed Document</td>
</tr>
<tr>
<td>0.4</td>
<td>30/08/2018</td>
<td>CGI</td>
<td>Reviewed Document</td>
</tr>
<tr>
<td>0.5</td>
<td>30/08/2018</td>
<td>ADITESS</td>
<td>Incorporated reviewer’s comments</td>
</tr>
<tr>
<td>0.6</td>
<td>30/08/2018</td>
<td>ADITESS</td>
<td>Send for Submission</td>
</tr>
<tr>
<td>1.0</td>
<td>03/09/2018</td>
<td>ADITESS</td>
<td>Updated Project disclaimers</td>
</tr>
</tbody>
</table>
## Acronyms

<table>
<thead>
<tr>
<th>ACRONYM</th>
<th>EXPLANATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTPS</td>
<td>Hypertext Transfer Protocol Secure</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer</td>
</tr>
<tr>
<td>TSL</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>PHP</td>
<td>Hypertext Preprocessor</td>
</tr>
<tr>
<td>CMS</td>
<td>Content Management System</td>
</tr>
<tr>
<td>CA</td>
<td>Certificate Authority</td>
</tr>
<tr>
<td>CAPTCHA</td>
<td>Completely Automated Public Turing test to tell Computers and Humans Apart</td>
</tr>
<tr>
<td>RSS</td>
<td>Rich Site Summary</td>
</tr>
<tr>
<td>WP</td>
<td>Word Press</td>
</tr>
<tr>
<td>DOA</td>
<td>Document of Action</td>
</tr>
</tbody>
</table>
# Table of Contents

1. **Introduction** ........................................................................................................................ 8
   1.1 Project Hashtag ..................................................................................................................... 8
   1.2 Media Disclaimer ................................................................................................................... 8
2. **Cyber-Trust Website Design** ............................................................................................... 10
   2.1 Hosting and Domain ............................................................................................................ 10
   2.2 Web-Design Tools and Methods ......................................................................................... 10
   2.3 Browser Compatibility ......................................................................................................... 11
   2.4 HTTPS (SSL/TLS) Certificates ........................................................................................... 11
3. **Cyber-Trust Website Content** ............................................................................................. 11
   3.1 Homepage ........................................................................................................................... 11
   3.2 Cyber-Trust Website Main Pages ........................................................................................ 14
      3.2.1 Background .................................................................................................................. 14
      3.2.2 Pilots ............................................................................................................................. 15
      3.2.3 Reading Corner .......................................................................................................... 15
         3.2.3.1 Trends & Reports .................................................................................................. 15
         3.2.3.2 Project Deliverables .............................................................................................. 16
         3.2.3.3 Publications ........................................................................................................... 17
      3.2.4 Collaboration .............................................................................................................. 17
      3.2.5 News & Events ............................................................................................................. 17
      3.2.6 About Us ..................................................................................................................... 17
      3.2.7 Contact ......................................................................................................................... 18
   3.3 Plugins ................................................................................................................................. 19
      3.3.1 Google reCAPTCHA .................................................................................................. 19
      3.3.2 Google Analytics ........................................................................................................... 20
      3.3.3 RSS feeds ...................................................................................................................... 22
      3.3.4 Sharing to Social Media platforms ............................................................................... 22
4. **Cyber-Trust Social Media** ................................................................................................... 22
5. **Conclusion** .......................................................................................................................... 24
6. **References** .......................................................................................................................... 24
## Table of Figures

| Figure 1-1 | Disclaimer on Project Website | 9 |
| Figure 1-2 | Disclaimer on Twitter account | 9 |
| Figure 1-3 | Disclaimer on Facebook Page | 10 |
| Figure 3-1 | Website Homepage | 13 |
| Figure 3-2 | Project Main Menu | 14 |
| Figure 3-3 | Project Sitemap | 14 |
| Figure 3-4 | Project Objectives Page | 14 |
| Figure 3-5 | The Trends & Reports page | 15 |
| Figure 3-6 | List of Public Deliverables | 16 |
| Figure 3-7 | News & Events Page | 17 |
| Figure 3-8 | The About Us page | 18 |
| Figure 3-9 | Website Contact Form | 19 |
| Figure 3-10 | Website Activated Plugins | 19 |
| Figure 3-11 | reCAPTCHA widget for website forms and comment sections | 20 |
| Figure 3-12 | Google Analytics Dashboard on WordPress | 20 |
| Figure 3-13 | Real Time Monitoring Google Analytics Dashboard | 21 |
| Figure 3-14 | Fresh Integration of Cyber-Trust with the Google Analytics Dashboard | 21 |
| Figure 3-15 | External Social Media buttons | 22 |
| Figure 4-1 | Screenshot of the Facebook Page | 23 |
| Figure 4-2 | Screenshot of Twitter Account | 23 |
| Figure 4-3 | Links to Cyber-Trust social media accounts | 23 |
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

Figure 1-2 Disclaimer on Twitter account
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;
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](image)

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).

![Figure 3-4 Project Objectives Page](image)
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.

Figure 3-5 The Trends & Reports page
3.2.3.2 Project Deliverables

CyberTrust is committed 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 deliverables 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). For confidential and therefore restricted deliverables a publishable executive summary will be made available.

---

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 as 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.

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.
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- 9Error! 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.
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.

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.

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

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 3-14 show snapshots of the google analytics dashboard.
Figure 3- 13 Real Time Monitoring Google Analytics Dashboard

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 quite 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](image)

4. Cyber-Trust Social Media
Communication of Cyber-Trust activities and outcomes to the social media will be performed 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 page² and Twitter account³ respectively.

---
² https://www.facebook.com/cybertrust/
³ https://twitter.com/CyberTrustEU
Figure 4-1 Screenshot of the Facebook Page

Figure 4-2 Screenshot of Twitter Account

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