CyberKit4SME
Democratizing a Cyber Security Toolkit for SMEs and MEs
Project Nº 883188

Deliverable 6.3 -
1st Report on Dissemination Actions and Preliminary Results

Responsible: Erisa Karafili (University of Southampton)
Document Reference: Deliverable
Dissemination Level: Public
Version: 1
Date: 23/11/2021

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 883188.
Executive Summary

In this deliverable, we provide the first results of the CyberKit4SME dissemination activities. We present the various actions performed in the first 18 months of the project, where a special attention was put on the creation of the brand identity which was used for almost all of the performed activities. The list of published academic papers and work in progress is provided, as well as industrial and academic activities. A list of the achieved and target KPIs is provided, and in general we can state that the project is on a good track and has in place strategies to improve the work towards the KPIs that were partially achieved for month 18. A section on cross-project collaboration is provided detailing mainly collaborations with other EU funded projects, in particular projects from the same call as the CyberKit4SME project. Overall, during the first 18 months of the project, 5 scientific papers were published, the project partners gave 5 scientific talks in workshops/conferences/seminars, 9 blog posts were published by the consortium, the partners were part of 4 industrial events and organized 3 industrial events, there were two press releases. Furthermore, the paper promotional material (brochure) was designed and delivered, and social media interactions have been active. In terms of cross-project collaboration, discussions and plans are in place with 5 EU funded projects.
### Contributors Table

<table>
<thead>
<tr>
<th>DOCUMENT SECTION</th>
<th>AUTHOR(S)</th>
<th>REVIEWER(S)</th>
</tr>
</thead>
<tbody>
<tr>
<td>All</td>
<td>Erisa Karafili (UoS Cyber), All (contributors)</td>
<td>Tiberiu Cocias (EB), Aurelien Lecamus (Inetum), Stephen C Phillips (UoS ITInnov)</td>
</tr>
<tr>
<td>III</td>
<td>Yosef Moatti (IBM), Tiberiu Cocias (EB), Erisa Karafili (UoS Cyber)</td>
<td></td>
</tr>
</tbody>
</table>
Table of Contents

I. INTRODUCTION ............................................................................................................ 6

II. DISSEMINATION AND COMMUNICATION ACTIONS ............................................. 8
II.1. Creation of the Brand Identity .................................................................................. 8
II.2. Project Website ........................................................................................................ 8
   II.2.1. Blogs on the project website and other websites ............................................. 10
   II.2.2. Statistics on the CyberKit4SME website ....................................................... 12
II.3. Social Media Activities ............................................................................................ 13
II.4. Press Releases ......................................................................................................... 15
II.5. Brochure - Paper Promotional Material .................................................................. 16
II.6. Industrial Activities .................................................................................................. 18
II.7. Academic Events, Publications, and Education Activities ................................... 19
   II.7.1. Scientific publications .................................................................................... 19
   II.7.2. Academic activities ....................................................................................... 20
   II.7.3. Educational activities .................................................................................... 20
II.8. Actions Mapped to the Dissemination and Communication Strategy ..................... 20

III. CROSS-PROJECT COLLABORATIONS ................................................................... 23
III.1. Cross-project Collaborations with EU Projects ..................................................... 24
III.2. Next Steps .............................................................................................................. 28

IV. CONCLUSIONS .......................................................................................................... 29

Table of Figures

Figure 1 – CyberKit4SME website main page 1.............................................................. 8
Figure 2 – CyberKit4SME website main page 2.............................................................. 9
Figure 3 – CyberKit4SME website main page 3.............................................................. 9
Figure 4 – CyberKit4SME website main page 4............................................................. 10
Figure 5 – Users distribution for the Cyberkit4SME website (period 08-10/2021) .............. 12
Figure 6 – Average session duration for the website accesses (period 08-10/2021) .......... 12
Figure 7 – Twitter activity analytics for October 2021 .................................................. 14
Figure 8 – LinkedIn analytics of the visitor metrics for the last 6 months (M12-M16) .... 15
Figure 9- LinkedIn analytics of the update metrics for the last 6 months (M12-M16) ... 15
Figure 10 – JRC press release ....................................................................................... 16
Figure 11 – Informative brochure for the project (page 1) .............................................. 17
Figure 12 – Informative brochure for the project (page 2) .............................................. 17
Figure 13 – cyberwatching.eu page that describes our project ..................................... 23
Figure 14 – Screenshot of the tweet about the first meeting with Geiger ...........................................24
Figure 15 – Screenshot of the tweets about the meeting with Protego .................................................26
Figure 16 – Another screenshot of the tweets about the meeting with Protego.................................26
Figure 17 - Screenshot of the tweets about the meeting with Energy Shield.................................27
Figure 18 – Another screenshot of the tweets about the meeting with Energy Shield .................27
Figure 19 – Screenshot of Curex post on the first meeting with CyberKit4SME project ...........28

List of Tables

Table 1 – Published blog posts.................................................................................................................10
Table 2 – Users CyberKit4SME website users for the period August-October 2021....................12
Table 3 – Impressions and clicks on the CyberKit4SME website (period 08-10/2021).............13
Table 4 – A list of the social media interactions .......................................................................................13
Table 5 – Organized industry-community activities .............................................................................18
Table 6 – Participation in third-party industrial events ........................................................................18
Table 7 – Current and targeted dissemination key performance indicators ....................................21

Table of Acronyms and Definitions

<table>
<thead>
<tr>
<th>Acronym/Definition</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>WP</td>
<td>Work Package</td>
</tr>
<tr>
<td>WPL</td>
<td>Work Package Leader</td>
</tr>
</tbody>
</table>
I. INTRODUCTION

This report has been produced in the framework of the CyberKit4SME project “Democratizing a Cyber Security Toolkit for SMEs and MEs” and in particular it is related to WP6 Dissemination and Impact as Deliverable D6.3 – “1st Report on Dissemination Actions and Preliminary Results”, a public report, produced by the end of month 18 (November 2021). This is the 1st Report on the conducted dissemination actions including cross-project collaboration and results.

The deliverable presents the dissemination and awareness actions for the outcomes of the CyberKit4SME project until month 18. It presents the overall approach used to disseminate and communicate the set of project results and activities. Furthermore, it presents the actions for cross-project collaborations and the steps forward to establish new collaborations. This deliverable includes also the main achieved results of the project.

This dissemination report was anticipated by the Dissemination and Communication Plan (D6.1) delivered on M3 and will be followed by another periodic report that will be produced on M36, describing the dissemination and communication activities performed during the period analysed. The remaining deliverable is identified with the code and D6.6.

The key achievements that will be presented are the following:

- Academic Publications: The results of CyberKit4SME were published in academic conferences and journals. Specifically, 5 papers were accepted and are published or are in the process of being published.
- Social Media activities: The consortium has increased the social media engagement using social media like LinkedIn and Twitter. A strategy is in place to increase the social media interactions.
- Website and Blog Posts: The website was updated in order to create a brand identity for the CyberKit4SMe project. Currently, 9 blog posts have been published by the consortium.
- Industry activities: Despite the Covid-19 pandemic the consortium has been active in participating in industrial activities and disseminating the results of the project with members from the industry and has participated in 4 industrial activities organized by third parties.
- Workshops and Presentations: The members of the consortium have organized 4 in-house workshop and has given presentation in 4 industrial and academic events.
- Cross-project collaborations: Currently the cross-project collaboration has started with 5 projects. These collaborations for now have included social media dissemination of each other’s results, one joint paper. Activities like workshops organizations, presentations, and possible applications of the results between projects are being discussed.

The current dissemination activities and results are in line with the key elements presented in the Dissemination and Communication Plan.

- Creating a community: Through the cross-project collaborations, the participations, and interactions in industrial and academic events, as well as workshop organisations and social media interaction, CyberKit4SME is working towards establishing a community of scientists and industrial partners working on security as well as SMEs and MEs.
- EU Networks: The current cross-projects collaborations activities with other EU projects are helping to establish connections with EU networks working on similar areas.
- Industry-community building activities: The CyberKit4SME consortium will participate in the strengthening of the cybersecurity community. Furthermore, it will take part of industrial events and exhibitions to spread the project progress among the industrial stakeholders. Seminars and training sessions will be built and delivered into industrial activities with SMEs.
- **Academic events, publication activities, and synergies**: The consortium has participated at third party events and has presented and published scientific publications.
II. **DISSEMINATION AND COMMUNICATION ACTIONS**

In this section we will present the main dissemination and communication actions performed.

II.1. **Creation of the Brand Identity**

The brand identity for the CyberKit4SME has been designed, following the project logo and similar colours. The same colours are used for the project website, documents, social media accounts and produced paper promotional material.

The hashtag #cyberkit4sme is associated to the project and has been used while posting on social media.

We have booked the CyberKit4SME.eu domain for our project and there is an email info@cyberkit4sme.eu that can be used by the general public to get in contact with the project.

II.2. **Project Website**

The project website [https://cyberkit4sme.eu/](https://cyberkit4sme.eu/) is fully operational. This is the second version of the website, and it incorporates in it the logo of the project as well as the brand identity, where the logo’s colours have been used in the design of the website. The main page of the website is shown in Figure 1, where the project brand identity is used. In order to improve the users’ experience the front page has dynamic elements in it.

![Figure 1 – CyberKit4SME website main page 1](image)

One the same page, just by scrolling, we show the main news for the project, in order to immediately provide information about what is going on with the project (Figure 2). Furthermore, down on the first page, we provide further information on the project, recalling again the similar designs of the project logo and leaflets, see Figure 3. Finally, the link to the latest publication is provided, as well as contact information, see Figure 4.

The “Blog” page that can be accessed from the top menu provides direct access to the news and publications of the projects. The user can learn more about the project by clicking on “The Project” tab on the top menu and about the project partners at the “Project Partners” link.

We are currently updating the project website to also include a “Cross-Project Collaboration” page, where we will provide information about the projects we are collaborating with and the various performed activities. Another page that will appear on the top menu will be a “Get in Contact” page, where we will have a form for the public to directly get in contact with the project.
Depending on the need, further pages will be added, in order to improve the users' experience and to provide clear and prompt information to the public.

**Figure 2 – CyberKit4SME website main page 2**

The website was developed taking into consideration simple navigation and access to services and content of research. The developed website is based on a distributed management, where each of the project partners can update the information, add news, blogs and other information. This was done to provide the information to the public as promptly as possible without dealing with the bottleneck of the website administrator. The website has an administrator that mainly deals with further development, maintenance, and security maintenance. The project website has been developed and is maintained by UoS Cyber, in accordance with the project proposal.

**Figure 3 – CyberKit4SME website main page 3**

The website respects the EU privacy policy requirements and a page with privacy information is provided on the website.
The website incorporates the main requirements established on D6.1:

- a short description of the project and its objectives;
- blog to announce and disseminate information;
- featured content on the front page (e.g., latest news, comments, additions, press releases, etc.);
- possibility to embed video, documents, presentations, and/or photos;
- relevant contacts (including an ad-hoc mailbox);
- links and publicly available documentation supporting the project achievements;
- links to Twitter or LinkedIn posts.

In the next period, the website will be upgraded to accommodate a more disseminative structure which includes better transparency with regards to objectives, vision and challenges of the project, concrete description of the tools comprising the toolkit. The new structure was discussed and approved by the project consortium and it is now in the graphical design phase.

II.2.1. Blogs on the project website and other websites

The project website is used as a tool to communicate the project activities, news and results. For this reason, various blog posts were published on the website. In Table 1 we list all of these blog posts as well as blog posts made on the partners websites.

Table 1 – Published blog posts

<table>
<thead>
<tr>
<th>Blog Post</th>
<th>Objective</th>
<th>Partner</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>SINTEF launched an anonymous survey about cybersecurity: <a href="https://survey.quenchtec.net/c?rspid=f5b69d0f-b924-4bb7-a530-e1924be9d30f&amp;qsid=887e43bb-2da6-42d2-988a-efdf36b3afe2d">https://survey.quenchtec.net/c?rspid=f5b69d0f-b924-4bb7-a530-e1924be9d30f&amp;qsid=887e43bb-2da6-42d2-988a-efdf36b3afe2d</a></td>
<td>An anonymous survey was created via quenchTec (see URL) to ask people in SMEs/MEs and in other companies about their understanding and current practices in cybersecurity. The results were also used in two publications SINTEF was involved in as reported in Section II.7.</td>
<td>SINTEF</td>
<td>21/10/20</td>
</tr>
<tr>
<td>Project website blog</td>
<td>Publicising and disseminating the project results.</td>
<td>UoS ITInnov</td>
<td>25/06/21</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------</td>
<td>-------------</td>
<td>----------</td>
</tr>
<tr>
<td>Project website blog</td>
<td>Publicising and disseminating the project results.</td>
<td>SINTEF</td>
<td>09/08/21</td>
</tr>
<tr>
<td><strong>Publicising and disseminating the project results.</strong></td>
<td>Paper [3] It’s Not My Problem: How Healthcare Models relate to SME Cybersecurity Awareness. Accepted at HCI for Cybersecurity, Privacy and Trust.</td>
<td>SINTEF</td>
<td>09/08/21</td>
</tr>
<tr>
<td>SINTEF’s website project blog. Norwegian blog:</td>
<td>Publicising the CyberKit4SME project. Two blogs were published in English and Norwegian on SINTEF’s webpages to spread awareness about CyberKit4SME to local SMEs and MEs.</td>
<td>SINTEF</td>
<td>09/08/21</td>
</tr>
<tr>
<td><strong>Publicising and disseminating the project results.</strong></td>
<td>The blog &quot;Parquet Modular Encryption: The New Open Standard for Big Data Security Reaches a Milestone&quot; published with use cases based on CyberKit4SME use cases.</td>
<td>IBM</td>
<td>20/08/21</td>
</tr>
<tr>
<td>Project website blog</td>
<td>Publicising the CyberKit4SME project Brochure.</td>
<td>EB</td>
<td>06/10/21</td>
</tr>
<tr>
<td><strong>Publicising and disseminating the project results.</strong></td>
<td>One blog was published in English webpage to spread the news about the availability of the project brochure</td>
<td>EB</td>
<td>06/10/21</td>
</tr>
<tr>
<td>Project website blog</td>
<td>Publicising and disseminating the project results.</td>
<td>SINTEF</td>
<td>01/11/21</td>
</tr>
<tr>
<td><strong>Publicising and disseminating the project results.</strong></td>
<td>Paper [2] Cybersecurity for SMEs: Introducing the Human Element into Socio-Technical Cybersecurity Risk Assessment’</td>
<td>SINTEF</td>
<td>01/11/21</td>
</tr>
<tr>
<td>Project website blog</td>
<td>Publicising and disseminating the project results</td>
<td>UoS Cyber</td>
<td>11/11/21</td>
</tr>
</tbody>
</table>
II.2.2. Statistics on the CyberKit4SME website

We now provide some statistics on the CyberKit4SME website. In particular, the collected statistics are for the months of August/September/October 2021 (M15-17). In Table 2 we present the number of users of the website in this period, where we distinguish between the users and new users. We calculated an average monthly usage of 52 users per month.

Table 2 – Users CyberKit4SME website users for the period August-October 2021

<table>
<thead>
<tr>
<th>Date</th>
<th>Sum of Users</th>
<th>Sum of new Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>August 2021</td>
<td>39</td>
<td>33</td>
</tr>
<tr>
<td>September 2021</td>
<td>70</td>
<td>40</td>
</tr>
<tr>
<td>October 2021</td>
<td>47</td>
<td>31</td>
</tr>
<tr>
<td>Total</td>
<td>156</td>
<td>104</td>
</tr>
</tbody>
</table>

We provide in Figure 5 below the distribution of the users on the website. We also collected the average session duration for such accesses and the graphical distribution is provided in Figure 6.

For this period, we also checked the interactions with the main website and the other pages of our website and found the overall number of impressions and clicks, provided in Table 3.
Generally, we noticed a good interaction with the website not just the main landing page but also the other pages, e.g., the blog posts. We plan to continue with adding you blog posts and publicising them through our social media accounts in order to increase the interactions with our website.

II.3. Social Media Activities

The project has been active with its social media presence. We created a LinkedIn and a Twitter profile that are used to communicate with the general audience the project aims, information about the partners and project activities as well as news about the latest activities. During the social media interactions, the hashtag #cyberkit4sme has been constantly used. Furthermore, the partners have shared information about the project using their own accounts.

We had an average of at least 2 tweets/posts per month on between LinkedIn and Twitter posts. The interaction levels for the social media activities have been satisfactory but we aim in the future to increase our social media presence. To achieve this, we have prepared we are identifying in the consortium a social media manager and have establish a plan to engage all partners during these activities.

In Table 4 we provide a summary of our Social Media activities.

<table>
<thead>
<tr>
<th>Item</th>
<th>Partner/s</th>
<th>Language</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sharing the CyberKit4SME Website on LinkedIn</td>
<td>INETUM</td>
<td>English</td>
<td>08-09/20</td>
</tr>
<tr>
<td>Disseminating and publicising the Scientific article published at MDPI [1] via LinkedIn</td>
<td>INETUM</td>
<td>English</td>
<td>09/20</td>
</tr>
<tr>
<td>Participant recruiting for the survey about cybersecurity awareness and practices via SINTEF's main Twitter profile: <a href="https://twitter.com/SINTEFdigital/status/1319268276996870147?s=20">https://twitter.com/SINTEFdigital/status/1319268276996870147?s=20</a></td>
<td>SINTEF</td>
<td>English</td>
<td>10/20</td>
</tr>
<tr>
<td>Participant recruiting for the survey about cybersecurity awareness and practices via SINTEF's main LinkedIn profile: <a href="https://www.linkedin.com/posts/sintef-digital_quenchtec-data-collection-activity-6725035512970674176-iaCc">https://www.linkedin.com/posts/sintef-digital_quenchtec-data-collection-activity-6725035512970674176-iaCc</a></td>
<td>SINTEF</td>
<td>English</td>
<td>10/20</td>
</tr>
<tr>
<td>Participant recruiting for the survey about cybersecurity awareness and practices via SINTEF's HCI-group LinkedIn profile: <a href="https://twitter.com/SINTEF_HCI/status/1319170529526468608">https://twitter.com/SINTEF_HCI/status/1319170529526468608</a></td>
<td>SINTEF</td>
<td>English</td>
<td>10/20</td>
</tr>
<tr>
<td>Sharing the CyberKit4SME Survey via LinkedIn</td>
<td>INETUM</td>
<td>English</td>
<td>10-11/20</td>
</tr>
<tr>
<td>Tweets via the Project Twitter Account</td>
<td>UoS Cyber and ITInnov</td>
<td>English</td>
<td>02-04/21</td>
</tr>
<tr>
<td>Tweets via the Project Twitter Account</td>
<td>EB</td>
<td>English</td>
<td>02-04/21</td>
</tr>
<tr>
<td>Post on the LinkedIn Account</td>
<td>UoS Cyber and ITInnov</td>
<td>English</td>
<td>02-04/21</td>
</tr>
<tr>
<td>Post on the LinkedIn Account</td>
<td>EB</td>
<td>English</td>
<td>02-04/21</td>
</tr>
<tr>
<td>Re-tweets from the CyberKIT4SME account</td>
<td>JRC</td>
<td>English</td>
<td>04/21</td>
</tr>
<tr>
<td>Twitter Post</td>
<td>JRC</td>
<td>English</td>
<td>05/21</td>
</tr>
</tbody>
</table>

Table 3 – Impressions and clicks on the CyberKit4SME website (period 08-10/2021)

<table>
<thead>
<tr>
<th>Visited pages at CyberKit4SME website</th>
<th>Sum of Impressions</th>
<th>Sum of Clicks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Main landing page</td>
<td>3509</td>
<td>93</td>
</tr>
<tr>
<td>Other pages</td>
<td>1884</td>
<td>13</td>
</tr>
<tr>
<td>Total</td>
<td>5393</td>
<td>106</td>
</tr>
<tr>
<td>LinkedIn Post</td>
<td>JRC</td>
<td>Language</td>
</tr>
<tr>
<td>------------------------------------------------------------------------------</td>
<td>---------</td>
<td>----------------</td>
</tr>
<tr>
<td>Tweet about the published paper (Cybersecurity for SMEs: Introducing the Human Element into Socio-technical Cybersecurity Risk Assessment). <a href="https://twitter.com/cyberkit4sme/status/1404347878231973889">https://twitter.com/cyberkit4sme/status/1404347878231973889</a></td>
<td>SINTEF</td>
<td>English</td>
</tr>
<tr>
<td>Twitter and LinkedIn posts publicising SINTEF’s article published in the magazine &quot;Norwegian SciTech News&quot; <a href="https://gemini.no/2021/06/dette-ma-du-ma-vite-om-cybersikkerhet/">https://gemini.no/2021/06/dette-ma-du-ma-vite-om-cybersikkerhet/</a></td>
<td>SINTEF</td>
<td>English and Norwegian</td>
</tr>
<tr>
<td>Tweet on SINTEF’s Twitter profile (with over 1300 followers): <a href="https://twitter.com/SINTEFdigital/status/1392426842041241600">https://twitter.com/SINTEFdigital/status/1392426842041241600</a></td>
<td>SINTEF</td>
<td>English</td>
</tr>
<tr>
<td>Post on SINTEF’s LinkedIn profile (with about 4700 followers): <a href="https://www.linkedin.com/posts/sintef-digital_dette-m%C3%A5-du-vite-om-cybersikkerhet-activity-6798163871354908672-1O3u">https://www.linkedin.com/posts/sintef-digital_dette-m%C3%A5-du-vite-om-cybersikkerhet-activity-6798163871354908672-1O3u</a></td>
<td>SINTEF</td>
<td>English</td>
</tr>
<tr>
<td>LinkedIn reports from the CyberKIT4SME account</td>
<td>JRC</td>
<td>English</td>
</tr>
<tr>
<td>Re-tweets from CyberKIT4SME account</td>
<td>JRC</td>
<td>English</td>
</tr>
<tr>
<td>Posts on JRC LinkedIn and Xing about the project</td>
<td>JRC</td>
<td>English</td>
</tr>
<tr>
<td>Re-tweets from CyberKIT4SME account</td>
<td>JRC</td>
<td>English</td>
</tr>
<tr>
<td>Re-tweets and Reposts from the CyberKit4SME accounts</td>
<td>UoS Cyber</td>
<td>English</td>
</tr>
<tr>
<td>LinkedIn and Twitter Post from personal accounts to disseminate the project’s results</td>
<td>UoS Cyber</td>
<td>English</td>
</tr>
<tr>
<td>Twitter and Linkedin posts about Cross-Projects collaborations</td>
<td>EB, INETUM</td>
<td>English</td>
</tr>
<tr>
<td>LinkedIn reports on CyberKIT4SME’s account about Inetum’s participation (among whom CyberKit4SME’s project coordinator) to Less Assises industrial event</td>
<td>Inetum</td>
<td>French</td>
</tr>
<tr>
<td>LinkedIn posts on Inetum’s Cybersecurity account about Inetum’s participation (among whom CyberKit4SME’s project coordinator) to Less Assises industrial event, mentioning CyberKit4SME</td>
<td>Inetum</td>
<td>French</td>
</tr>
<tr>
<td>LinkedIn reports on CyberKIT4SME’s account about Inetum’s participation (among whom CyberKit4SME’s project coordinator) to Less Assises industrial event</td>
<td>Inetum</td>
<td>English</td>
</tr>
<tr>
<td>LinkedIn posts on Inetum’s Cybersecurity account about Inetum’s participation (among whom CyberKit4SME’s project coordinator) to Less Assises industrial event, mentioning CyberKit4SME</td>
<td>Inetum</td>
<td>French</td>
</tr>
</tbody>
</table>

Our tweets on Twitter have an average of 700 visualisations per tweet, and lately we have seen more active interactions with them with likes and retweets. In Figure 7, we show the graph of the Twitter analytics for October 2021 (month 17 of the project).

![Figure 7 – Twitter activity analytics for October 2021](image)

In regard to our other social media account, LinkedIn we present in Figure 8 and Figure 9 the analytics of the visitors and updates on our account. An increasing trend is visible and this due...
to the strategic measures we have taken and we are currently undertaking to improved our visibility.

To increase the social media presence, the project consortium decided to empower each project partner and appoint each one to communication activities for a 2 week period in turns during the remaining project timeline. To properly frame this activity, solid planning, KPIs and publishing guidelines were defined.

II.4. Press Releases

Through the press releases we aim to disseminate and communicate our findings, achievements and to promote events or initiatives to local SMEs and MEs. The following were the press releases made so far.

- JRC had a press release to present the project to local SMEs, MEs and other industrial partners. The press release was made in German, see Figure 10 for details.

- SINTEF published a popular science article including 12 things companies should be aware of and need to know about cybersecurity and hacking to protect the companies and their employees. The main audience was the general public, especially SINTEF’s users, clients and local SMEs and MEs. The article was “The risk of cyber-attacks on SMEs/MEs and companies in general has increased during the COVID pandemic”. The
article is in Norwegian and was also published (10/06/21) in the magazine "Norwegian SciTech News" which is a magazine that frequently publishes popular science articles and news in Norway: https://gemini.no/2021/06/dette-du-ma-vite-om-cybersikkerhet/

II.5. Brochure - Paper Promotional Material

UoS Cyber has produced a leaflet to promote the project, its objectives, and the main partners, in March 2021. The brochure was designed by professional graphical designers at the UoS Printing Centre Office and the material was first approved and reviewed by all the project’s partners. This informative brochure was aimed at disseminating the project to all the main actors (it represents the initial communication tool that will show the project framework, the timetable, the methodology to be carried out, to whom the project is addressed to). The leaflet has not yet been printed in large quantities, given also the only “online” activities but it will be printed and the hard copies will be delivered to the partners when required. Inetum has distributed around 20 printed copies of the leaflet during their face-to-face dissemination activities (see Industrial Activities for more detail). The online leaflet has been distributed to the partners who has distributed the leaflet in different occasions to possible stakeholders, SMEs and MEs, and through mass e-mailing to all relevant contacts. The brochure has also been distributed through the project social media accounts.

The brochure presented in Figure 11 and Figure 12 uses the CyberKit4SME logo as well as similar colours and images that are used also on the website. All the logos of the partners are presented, as well as general information about the project, contact information and the timeline. The leaflet was designed to be foldable when printed in order to improve the usability.
CyberKit4SME Partners:

- inetum
- Elektrotīt
- Southampton
- IBM
- TIANI
- Energis
- 3SOFT
- SINTEF
- Sogefi

CyberKit4SME EU Horizon 2020 Call
SU-DI03-2019-2020
Digital Security and privacy for citizens, Small, Medium and Micro Enterprises
Budget: €4,890,725
EU Contribution: €3,913,052.38
Contact:
cyberkit4sme.eu
info@cyberkit4sme.eu

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 883188.

democratizing a Cyber Security Toolkit for SMEs and MEs
cyberkit4sme.eu

Figure 11 – Informative brochure for the project (page 1)

CyberKit4SME: Making SMEs more cyber-resilient

The EU-funded CyberKit4SME project aims to enhance small businesses’ autonomy in dealing with cyber security thanks to a simplified, though affordable toolkit. The project will help small businesses become more aware of their risks and enable them to monitor, forecast and manage such risks. CyberKit4SME will also provide to small and medium businesses the capabilities to protect their information system from the identified risks and to share intelligence without exposing commercially-sensitive data.

Scope and objectives

CyberKit4SME aims to deliver a toolkit of cyber security tools and methods enabling SMEs/MEs to:
- Increase awareness of cyber security risks, vulnerabilities and attacks;
- Monitor and forecast risks;
- Manage risks using organisational, human and technical security measures with greater confidence;
- Collaborate and share information in a collective security and data protection effort.

Methodology and innovation

The developed toolkit will consist of:
- Offline risk modelling tools to support ISO 2700x risk analyser, and privacy and data protection by design;
- Online cyber security risk monitoring based on collaborative security intelligence and event management (SIEM) tool;
- Affordable and easy-to-use services to guarantee the security and integrity of data;
- Cyber security incident reporting and security intelligence sharing support by a secure, privacy-aware blockchain framework, allowing SMEs to collaborate with CERTs, supply chain partners and other SMEs.

The project will use its tools and cyber range demos to train SMEs/MEs to identify their top threats and recognize and address them with greater confidence. Results will be validated by SME/ME in four critical sectors.

Impact

CyberKit4SME will contribute to create a trustworthy EU digital environment benefiting all economic and social actors by:
- Helping SMEs and MEs to become stronger in the cyber security chain underpinning the EU digital environment;
- Improving the security of SME/ME services, data and infrastructures;
- Strengthening security, privacy and personal data protection;
- Reducing the damage caused by cyber attacks and data protection breaches.

CyberKit4SME aims to help SMEs and MEs demonstrate compliance with any regulation that imposes requirements for cyber security or data protection.

Figure 12 – Informative brochure for the project (page 2)
II.6. Industrial Activities

The CyberKit4SME consortium has actively participated in the strengthening of the cybersecurity community in clustering and liaison events and is promoting awareness through engagement with their local SME organisations. We present in Table 5 the main activities performed by the project consortium during this first 18 Months.

Table 5 – Organized industry-community activities

<table>
<thead>
<tr>
<th>Activities</th>
<th>Communication Tools</th>
<th>Audience</th>
<th>Partner/s</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>In-house workshops. Objective: Raise awareness about the project and collect feedback from staff.</td>
<td>Internal workshop</td>
<td>JRC Staff and Stakeholders</td>
<td>JRC</td>
<td>29/05/20</td>
</tr>
<tr>
<td>High Level Presentation from INETUM to Prospects about the CyberKit4SME project</td>
<td>Presentation (Face-to-Face and Virtual)</td>
<td>Prospects</td>
<td>INETUM</td>
<td>08/20</td>
</tr>
<tr>
<td>High Level presentation of the project</td>
<td>Meetings and Presentations</td>
<td>Prospects and Clients</td>
<td>INETUM</td>
<td>10-11/20</td>
</tr>
<tr>
<td>In-house workshop</td>
<td>Face-to-Face Meeting and Presentation</td>
<td>JRC users and clients</td>
<td>JRC</td>
<td>05/21</td>
</tr>
</tbody>
</table>

The consortium also participated in third-party industrial events where the CyberKit4SME project was presented or further information were provided about the projects objectives, first results and to spread awareness. We present in Table 6 the main third-party industrial events participated in during the first 18 months.

Table 6 – Participation in third-party industrial events

<table>
<thead>
<tr>
<th>Event</th>
<th>Participation/Presentation</th>
<th>Audience</th>
<th>Partner</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Annual Cybersecurity Industrial Event. Location: Monaco</td>
<td>Participation and presentation of the project. Presentation title “Assises de la sécurité”</td>
<td>Event Audience. 818 participants, where 26% of them were from small to medium size companies (1-500 employees)</td>
<td>INETUM</td>
<td>14-16/10/20</td>
</tr>
<tr>
<td>European Robotics Forum¹</td>
<td>Participation</td>
<td>The forum audience and participants: Researchers and experts in Robotics More than 500 participants.</td>
<td>EB</td>
<td>13-15/04/21</td>
</tr>
<tr>
<td>CyberUK Online 2021</td>
<td>Participation</td>
<td>Event audience: Cybersecurity experts and researchers from the UK. This is the biggest Cybersecurity event in the UK with participants from the industry, academia and public sector.</td>
<td>UoS ITInnov</td>
<td>11-12/05/21</td>
</tr>
</tbody>
</table>

¹ [https://www.eu-robotics.net/robotics_forum/programme/index.html](https://www.eu-robotics.net/robotics_forum/programme/index.html)
### II.7. Academic Events, Publications, and Education Activities

#### II.7.1. Scientific publications

An important channel for disseminating and communicating the CyberKit4SME project results to the academic community is by publishing and presenting scientific publications. The project consortium has successfully published 5 research papers. We provide below the list of the accepted and published papers, together with information about the journal, conference or workshop where it was published and a link to these publications.


The following paper/s are work in progress or under review to an academic conference/journal and we are waiting for the outcome.
II.7.2. Academic activities

The CyberKit4SME consortium has presented the project results and research papers in various academic venues. We present below a list of the third-party events where the partners participated and presented the project results.


2) "HCI for Cybersecurity, Privacy and Trust 2021" (HCII 2021). Presentation of the paper "It’s Not My Problem: How Healthcare Models relate to SME Cybersecurity Awareness" by Brian Pickering (UoS ITInnov).


II.7.3. Educational activities

The project partners were involved in Educational activities. In particular, SINTEF has two master students working on topics related to the CyberKit4SME project (since October 2020). The students at SINTEF will continue their work in 2022 until they complete their MSc thesis. UoS Cyber is offering students final projects (undergraduate and Masters) and is incorporating some of the project aims and problems tackled in lectures, for example Foundations of Cyber Security (Comp6224) 2021-2022.

II.8. Actions Mapped to the Dissemination and Communication Strategy

The performed dissemination and communication activities are in line with the developed strategy as they fulfil the main strategy objectives provided in D6.1:

- Create awareness and understanding of the benefits of the initiative;
  - Through the social media, blog posts, industrial, academics, in-house and third-party events we have raise the awareness about the CyberKit4SME project, especially in the SMEs, MEs and industrial community.
- Provide assistance and collect feedback from stakeholders and clients;
  - The main feedback has been collected through in-house workshops organized by the project partners.
- Create active interaction with stakeholders and receive feedback and reactions about the project that will be used in media relations and in updating the dissemination and communication plan;
Through in-house workshops, surveys, social media interactions the project is working towards this project. Further workshops and interactions with stakeholders are planned in the coming months.

- Establish and maintain a favourable reputation of the project;
  - This is achieved through the very good publishing track record of this project and workshop and industrial events participation.
- Define the exploitable knowledge and its use.
  - Through the various industrial and workshop activities, as well as cross-projects meetings an exploitation plan is being developed.

We present in Table 7 the main KPIs of our project and what has been achieved so far. Generally, our KPIs have been achieved for this period (see publications, academic and industrial events) by taking into consideration also the fact that there have been both travel and face-to-face meetings restrictions in many of the countries where the partners are located. We are currently working on achieving the remaining KPIs as well as putting strategy in place for the underperformed KPIs, e.g., social media interactions and blog posts.

### Table 7 – Current and targeted dissemination key performance indicators

<table>
<thead>
<tr>
<th>KPI</th>
<th>Specification</th>
<th>Target Groups</th>
<th>Achieved M18</th>
<th>Target Value M36</th>
</tr>
</thead>
<tbody>
<tr>
<td>D-KPI#1</td>
<td>Number of events in which brochures and/or leaflets will be distributed</td>
<td>All TGs</td>
<td>2</td>
<td>At least 10</td>
</tr>
<tr>
<td>D-KPI#2</td>
<td>Number of scientific publications in conferences, events and journals (prioritizing quality and promoting joint publications)</td>
<td>TG-E</td>
<td>5</td>
<td>At least 10</td>
</tr>
<tr>
<td>D-KPI#3</td>
<td>Number of white papers published (scientific and/or industrial)</td>
<td>TG-A, TG-B, TG-C, TG-D, TG-E</td>
<td>0</td>
<td>At least 4</td>
</tr>
<tr>
<td>D-KPI#4</td>
<td>Number of events where CyberKit4SME will show a poster or present a paper</td>
<td>All TGs</td>
<td>5</td>
<td>At least 10</td>
</tr>
<tr>
<td>D-KPI#5</td>
<td>Number of industry-oriented events, workshops and conferences (w/o scientific publication) in which CyberKit4SME partners will participate and actively present the project</td>
<td>TG-A, TG-B, TG-C</td>
<td>4</td>
<td>At least 10</td>
</tr>
<tr>
<td>D-KPI#6</td>
<td>Number of workshops organized by CyberKit4SME (including cross-project workshops)</td>
<td>All TGs</td>
<td>4</td>
<td>At least 4</td>
</tr>
<tr>
<td>D-KPI#7</td>
<td>Number of seminars and technical session organized by CyberKit4SME partners (including cross-project events)</td>
<td>TG-B, TG-C</td>
<td>0</td>
<td>At least 3</td>
</tr>
<tr>
<td>D-KPI#8</td>
<td>Number of press releases published</td>
<td>All TGs</td>
<td>2</td>
<td>At least 8</td>
</tr>
<tr>
<td>D-KPI#9</td>
<td>Number of produced videos introducing the project and its results</td>
<td>All TGs</td>
<td>0</td>
<td>At least 2 videos</td>
</tr>
<tr>
<td>D-KPI#10</td>
<td>Social media channels for community building</td>
<td>TG-C, TG-D, TG-F</td>
<td>1.4</td>
<td>At least 2 posts per month per network</td>
</tr>
<tr>
<td>D-KPI#11</td>
<td>Frequency of blog posts (e.g. via medium.com) and short news feed on CyberKit4SME website on topics treated during the project</td>
<td>All TGs</td>
<td>0.5</td>
<td>1 post per month</td>
</tr>
</tbody>
</table>

We now provide information related to the **Target Groups** used in the above table.

- TG-A: Industrial stakeholders consisting of several actors in the cybersecurity market
- TG-B: IT systems experts and technical decision makers in the SME context
- TG-C: End-users that are consuming ICT services from SMEs
- TG-D1: Policy related stakeholders including national and European SME associations and regulators
- TG-D2: Cluster initiatives
- TG-E: Scientific community
- TG-F: General public
III. CROSS-PROJECT COLLABORATIONS

In this section we present the main cross-project activities performed, the identified collaborators and the planned actions.

Our main goal for the cross-projects collaborations is creating and exploiting opportunities to increase the impact of CyberKit4SME and other related projects through joint activities.

The two main areas for joint action are:

- disseminating CyberKit4SME research with other relevant digital security projects sponsored by the Horizon2020 work programme;
- looking for ways to take the results of other projects into account in CyberKit4SME, e.g. by identifying where tools are complementary and could be used together by an SME/ME.

The main mechanisms for joint action is through jointly sponsored cluster events, coordinated cross-project dissemination activities (including cross-referencing project websites), teleconferences and webinars, or jointly sponsored workshops or similar events.

To achieve our goals in cross-project collaborations, Cyberkit4SME has joined the cyberwatching.eu hub (https://cyberwatching.eu/), see in the page Figure 13 created for our project. This permits to publicise the CyberKit4SME project and also enables us to discover interesting projects in our segment.
III.1. Cross-project Collaborations with EU Projects

We are currently collaborating with the following partners:

- GEIGER (https://project.cyber-geiger.eu);
- ProTego (https://protego-project.eu);
- Panacea (https://panace-h2020.eu);
- Energy Shield (https://energy-shield.eu);
- Curex (https://curex-project.eu).

Specifically, with the GEIGER project, we had a collaboration kick-off meeting (Sept. 30th 2021) which was announced as detailed in the image presented in Figure 14. In addition, we have the following actions on the pipeline and planned:

- Continue our discussions on different fronts;
- We have a technical collaboration meeting scheduled for the end of November, to discuss further possibilities on collaborating on the research side of the projects;
- We have scheduled a meeting for the end of November about the educational activities that Geiger has developed and how we can use their know-how;
- We are discussing possible public engagement activities like joint-workshops for SMEs and MEs and in participating at the workshops organized by Geiger;
- Share training materials such as GEIGER videos and other training materials (assuming no IP issue);
- Collaborate on the Beta Launch party planned for end of May - beginning of July 2022 and supported by ENISA;
- Share our research on SME types.

Figure 14 – Screenshot of the tweet about the first meeting with Geiger

With the ProTego project, we had a collaboration kick-off meeting and we have submitted a joint paper (paper [6]) “Protecting Sensitive Tabular Data in Hybrid Clouds”, Maya Anderson (IBM Research), Gidon Gershinsky (IBM Research), Eliot Salant (IBM Research), Salvador Garcia (Marina Salud Hospital) at Middleware 2021. The paper was rejected and we are currently improving the paper and will resubmit to an appropriate venue as soon as possible. We also announced the meeting on Twitter and LinkedIn as shown in the images in Figure 15 and Figure 16.
In addition, we plan to:

- Re-use or adapt the training material of ProTego available at the ProTego website: https://protego-project.eu/cybersecurity/. This assumes agreement of the ProTego consortium.

With the Panacea project, we are in the process of planning the kick-off meeting.

With the Energy Shield project, we had a collaborative kick-off meeting which was followed by a follow-up meeting (Oct. 5th 2021). We show in Figure 17 and Figure 18 some images of the tweets we posted about the cross-project meeting. We are currently working on the followings:

- Continue our discussions and identify ways to collaborate with each other;
- Strengthen our social media interaction, with re-tweets and re-posts;
- Exploring the possibility of a common workshop;
- Join forces on contributing on public policies and standardisation;
- Write a common white research paper on tools and developed technologies;
- Participate at the Energy Shield final project event, in order to disseminate our results and expand the network of further SMEs and MEs interested on CyberKit4SME;
- Working on possible ways to exploit the CyberKit4SME results by the project partners of Energy Shield.

With the Curex project we had a collaborative kick-off meeting which was announced on the Facebook page of Curex, see Figure 19. Our next steps in terms of cross-project collaboration with this project are the following:

- Continue our discussions and plan further meetings to define possible collaborations;
- Create news post with the meetings and publicise them;
- Create post on LinkedIn/Twitter and join forces for a more impactful social media presence.
We're excited to announce the beginning of a new cross-project collaborative journey with the @protego_project. This relationship is strengthened by multiple synergies, and we are convinced that we will achieve excellent outcomes together.

Figure 15 – Screenshot of the tweets about the meeting with Protego

We're excited to announce the beginning of a new cross-project collaborative journey with the #protego_project. This relationship is strengthened by multiple synergies, and we are convinced that we will achieve excellent outcomes together.

Figure 16 – Another screenshot of the tweets about the meeting with Protego
We'd like to express our gratitude to the @EnergyShield project for the very positive and fruitful conversations that took place on September 22nd during our first cross-project collaboration meeting.

The @cyberkit4sme project is eager to work with you in the near future.

Figure 17 - Screenshot of the tweets about the meeting with Energy Shield

To learn more about the @cyberkit4sme project, check out our new brochure.

Scope, objectives, motivations and impact, are all there.

Please do not hesitate to contact us for further information or to collaborate.

Figure 18 – Another screenshot of the tweets about the meeting with Energy Shield
III.2. Next Steps

Our next steps are to continue and accomplish the tasks planned with the already-contacted projects and to widen our network of projects collaborations by getting in contact with the remaining projects that were funded from the same call as the CyberKit4SME projects as well as others that are related.

Our main goals for the existing and coming cross-projects collaborations are the following:

- Join forces on the dissemination and exploitation activities;
- Technical and research collaborations, with papers, technical reports and policy proposal writings;
- Organize joined workshops and educational activities;
- Share and disseminate the project results;
- Other activities.

Furthermore, we are currently identifying projects that are part of other types of funding from the EC as well as national funding bodies (see Innovate UK funding, etc.).
IV. CONCLUSIONS

In this deliverable, we provide the project dissemination actions and some of the preliminary results. In particular, in the first 18 months of the project: 5 scientific papers were published, another paper is work in progress and will soon be submitted. The consortium was very active in scientific talks, overall, 5 scientific presentations were given by the members of the consortium in workshops, conferences, and seminars. In terms of industrial activities, 3 industrial activities were organized by the CyberKit4SME partners, and the partners participated in 5 industrial activities organized by third parties. The paper promotional material was produced and is being used. The consortium is actively using the social media accounts to disseminate and advertised the results of the project and has currently in place a plan to increase these frequency and impact of these activities. In terms of cross-project collaborations, the consortium is actively discussing with other 5 EU funded research projects and has planned activities to intensify these collaborations. In this report, we also provide a mapping of performed dissemination activities to the dissemination and communication strategy and the next steps for the cross-project collaborations.