



## D4.8 EU Cybersecurity and Privacy cluster engagement report.

### 4<sup>th</sup> Report

Author(s)	M. Ramirez, AEI CIBERSEGURIDAD
Status	Final
Version	v1.0
Date	28/07/2020

#### Dissemination Level

- |                                     |  |
|-------------------------------------|--|
| <input checked="" type="checkbox"/> | PU: Public   |
| <input type="checkbox"/>            | PP: Restricted to other programme participants (including the Commission)        |
| <input type="checkbox"/>            | RE: Restricted to a group specified by the consortium (including the Commission) |
| <input type="checkbox"/>            | CO: Confidential, only for members of the consortium (including the Commission)  |



The work described in this document has been conducted within the project cyberwatching.eu. This project has received funding from the European Union's Horizon 2020 (H2020) research and innovation programme under the Grant Agreement no 740129. This document does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of its content.

<b>Document identifier: Cyberwatching.eu – WP4 – D4.8</b>	
<b>Deliverable lead</b>	<b>AEI Ciberseguridad</b>
<b>Related work package</b>	<b>WP4</b>
<b>Author(s)</b>	<b>M. Ramirez AEI Ciberseguridad</b>
<b>Contributor(s)</b>	<b>N, Ferguson, Trust-IT &amp; J. Bieliauskaite, DSME</b>
<b>Due date</b>	<b>31/05/2020</b>
<b>Actual submission date</b>	<b>28/07/2021</b>
<b>Reviewed by</b>	<b>N. Ferguson &amp; N. Zazzeri Trust-IT &amp; J. Bieliauskaite, DSME</b>
<b>Start date of Project</b>	<b>01/05/2017</b>
<b>Duration</b>	<b>51 months</b>

### Revision history

Version	Date	Authors	Notes
0.1	16/06/2021	M. Ramírez (AEI)	First version
0.2	06/07/2021	J. Bieliauskaite (DSME)	First internal review
0.3	08/07/2021	N. Ferguson & N. Zazzeri (Trust-IT)	Second internal review
0.4	22/07/2021	M. Ramírez (AEI)	PMB review version
1.0	27/07/2021	N. Ferguson (Trust-IT)	Final version for PMB review & submission

## Executive Summary

Clusters are groups of specialized companies, many SMEs, and other related actors, such as Universities and public administrations that cooperate closely together in a particular sector and geographical location. In D4.2 the first of three EU Cybersecurity and privacy cluster engagement reports<sup>1</sup> published in July 2018 (M27), cyberwatching.eu reported on how it has identified and interacted with clusters actively working in Cybersecurity and Privacy (CS&P) across Europe and a catalogue of these clusters published on the cyberwatching.eu website<sup>2</sup>. In D4.5<sup>3</sup> the second of the reports published in June 2019 (M26), cyberwatching.eu reported on how to consolidate the relationship with a targeted group of clusters to ignite real interaction. Three clusters in particular, were already engaged and very committed to interacting with cyberwatching.eu. In D4.6<sup>4</sup>, the third report published in April 2020 (M36), cyberwatching.eu reported an increased number of engaged clusters covering a wider European geographic area and consolidating the relationships established through the joint development of webinars and the promotion of the tools developed within cyberwatching.

In the following months (M37-M50), efforts have focused on understanding the implications of clusters in the new key figure in the digital transformation of companies and public entities: the European Digital Innovation Hubs (EDIHs).

cyberwatching.eu has extended its positive impact on the clusters and their members by promoting project assets such as the GDPR temperature tool; providing networking opportunities with the R&I community; and raising awareness of emerging technologies and opportunities for businesses, and SME success stories. A key channel for this support is the provision of joint webinars which is being carried out.

cyberwatching.eu has also focused on guaranteeing the sustainability of the project assets. The services offered by cyberwatching.eu have companies as end users, especially SMEs, and clusters and EDIHs are the instrument to reach them. With the leading role of AEI Ciberseguridad offering the assets as part of the services of the new Cybersecurity Innovation Hub, based in Castilla y Leon region, with national focus and European added value, the sustainability of the tools is guaranteed, especially with joint effort from AEI Ciberseguridad and DIGITAL SME in consolidating the relationships with clusters and EDIHs.

---

<sup>1</sup> <https://www.cyberwatching.eu/d42-eu-cybersecurity-and-privacy-cluster-engagement-report-1st-report>

<sup>2</sup> <https://www.cyberwatching.eu/clusters>

<sup>3</sup> <https://www.cyberwatching.eu/d45-eu-cybersecurity-and-privacy-cluster-engagement-report-2nd-report>

<sup>4</sup> <https://cyberwatching.eu/d46-eu-cybersecurity-and-privacy-cluster-engagement-report-3rd-report>

## Table of Contents

<b>1</b>	<b>Introduction.....</b>	<b>5</b>
<b>2</b>	<b>From clusters to Digital Innovation Hubs.....</b>	<b>5</b>
<b>3</b>	<b>Work carried out with clusters / DIHs .....</b>	<b>7</b>
3.1	Clusters section on Cyberwatching.eu website .....	7
3.2	Webinar series .....	9
3.3	Other activities .....	11
3.3.1	Communication activities .....	11
3.3.2	AEI Ciberseguridad.....	12
3.3.3	SME success stories .....	12
3.3.4	DIGITAL SME - Coordination Group of European DIH.....	12
3.3.5	'Cybersecurity made in Europe' label by ECSO.....	12
3.3.6	Meetings with EDIH candidates to promote the Cyberwatching.eu tools	13
<b>4</b>	<b>Implications in the cyberwatching sustainability model.....</b>	<b>14</b>
4.1	CyberDIH .....	15
<b>5</b>	<b>Conclusion .....</b>	<b>17</b>

## List of Figures

Figure 1: Engaged clusters section.....	8
Figure 2: Information from the engaged clusters.....	9
Figure 3 Final workshop for BioCyber Project together with Biotecyl and ICTLegal .....	10
Figure 4 Cybersecurity: Use and usefulness of labels for SMEs together with DigitalSME France .....	11
Figure 5 CyberDIH website .....	15
Figure 6 Activities and Services in CyberDIH.....	15
Figure 7 Cyberwatching.eu tools section .....	16

## Glossary

CS&P	Cybersecurity and Privacy
DEP	Digital Europe Programme
DIH	Digital Innovation Hub
EC	European Commission
EDIH	European Digital Innovation Hubs
ECSO	European Cybersecurity Organisation
GDPR	General Data Protection Regulation
HE	Horizon Europe
SME	Small and Medium Enterprise
WG	Working Group

## 1 Introduction

In the first report of the Cluster Engagement strategy, cyberwatching.eu established the motivations and objectives of involving European Cybersecurity and Privacy (CS&P) clusters in the project. In the second report of the Cluster Engagement strategy, cyberwatching.eu focused on a small number of clusters, to consolidate the engagement with the three clusters (CLujIT, CyberWales and GAIA) and to expand this to a further five (AEI Ciberseguridad, The Hague Security Delta, ITSECURITY - Bavarian IT Security & Safety Cluster, DIGITAL SME France and Italian DIGITAL SME Alliance) which also takes into account the geographical distribution, to cover all the European area.

In this deliverable, cyberwatching.eu presents the final report on the performed activities with clusters from M41 to M50 and the analysis of the implications of the achievements in the cyberwatching.eu sustainability model.

## 2 From clusters to Digital Innovation Hubs

In the third report, we already defined a new activity being carried out by the cyberwatching team: “The identification of Digital Innovation Hubs with a strong focus on cybersecurity”.

Support for Digital Innovation Hubs is the key piece in the digitization strategy of European industry. According to EC data, the digitization of products and services will increase annual industrial revenue in the EU by more than €110 billion over five years, which is why it is so important to develop means to streamline this process. The European Network of Digital Innovation Hubs, which aims to provide European industry with advanced digital technologies and skills, is expected to drive Economy 4.0 in Europe.

The call for DIH candidates to be part of the European Network of DIH will open soon, and some of the engaged cybersecurity clusters are involved in DIH candidates.

### ClujIT

- **Country:** Romania
- **Website:** <https://www.clujit.ro/>
- **Related DIH:** [DIH4S](#)
- **Scope:**
  - Main consortium: Cluster Cluj IT, technical university of Cluj Napoca and a chamber of commerce of a nearby county.
  - Covers the geographic area of northwest Romania, which includes 6 counties through agreements with other partners.
  - They specialize in AI and Smart robotics, with cybersecurity as a transversal technology.

- Focus on Manufacturing & Public Authorities.

### **GAIA - Association of Knowledge and Applied Technologies industries in the Basque Country**

- **Country:** Spain
- **Website:** <http://www.gaia.es>
- **Related DIH:** [Cybersecurity Innovation Hub](#) (CyberDIH<sup>5</sup>)
  - They are in the process of signing an agreement to be a regional node of the Cybersecurity Innovation Hub, to join forces and capacities at the service of the digital transformation of SMEs and public administrations.

### **AEI Ciberseguridad**

- **Country:** Spain
- **Website:** <https://www.aeiciberseguridad.es/>
- **Related DIH:** [Cybersecurity Innovation Hub](#) (CyberDIH)
  - AEI is the coordinator of the hub.
  - The hub has a national scope and is strongly focused on cybersecurity.
  - Main consortium: AEI Ciberseguridad, INCIBE (National Institute for Cybersecurity), Regional Government of Castilla y Leon.

### **The Hague Security Delta (HSD)**

- **Country:** Netherlands
- **Website:** <https://www.thehaguesecuritydelta.com/>
- **Related DIH:** [EDIH Zuid-Holland-SMITZH](#)
- **More details:**
  - InnovationQuarter is one of HSD's partners and the coordinator of EDIH Zuid-Holland-SMITZH, which is a regional hub with about 20 partners with the aim of helping front runners and early adopter SMEs in the manufacturing industry with their digital transformation challenges across a wide range of topics.
  - The scope and ambition are still under definition.
  - Main technologies: AI, HPC, Cyber, robotics, 3d printing, AI for maintenance, AR/VR.

European Digital Innovation Hubs (EDIHs) are selected through a two-step process. First Member and Associated States preselect candidate entities, which will then be eligible to participate to a European call.

<sup>5</sup> <http://cyberdih.eu>

The outcome of the process at country level is available in a [catalogue](#) developed by the Joint Research Centre of the European Commission.

According to EC and the information presented in the event “Leading the Digital Decade”<sup>6</sup>, a two-day online event focused on Europe’s digital transformation towards 2030, there are 334 DIH candidates pre-selected by 27 countries (26 MS and Norway). **137 out of them have a specialization on cybersecurity.**

DIH have been encouraged by EC to cooperate and find synergies for the implementation of the future network. Taking advantage of the knowledge and synergies generated within Cyberwatching.eu, AEI Ciberseguridad and Digital SME have been developing different activities with this aim, as it is described in section 3.3.

### 3 Work carried out with clusters / DIHs

In this section, we look at the work carried out with the clusters since May 2020.

#### 3.1 Clusters section on Cyberwatching.eu website

To make visible the relationships established with the engaged clusters, a dedicated section was created on the Cyberwatching.eu website providing both an overview of each cluster and details the synergies established between with cyberwatching.eu.

---

<sup>6</sup> <https://leading-the-digital-decade.eu/>



Figure 1: Engaged clusters section

The objective is to position these clusters as benchmarks for cybersecurity in Europe, and at the same time strengthen collaboration with cyberwatching.eu both in the organisation of webinars and in the promotion of tools derived from the project that can be useful for companies (GDPR temperature tool<sup>7</sup>, Information Notices tool<sup>8</sup>, Cyber risk temperature tool<sup>9</sup>, Information notice tool and the brand-new Cybersecurity label<sup>10</sup>).

<sup>7</sup> <https://gdprtool.cyberwatching.eu/Pages/Home.aspx>

<sup>8</sup> <https://infonotictool.cyberwatching.eu/Pages/Home.aspx>

<sup>9</sup> <https://cyberrisk.cyberwatching.eu/Pages/Home.aspx>

<sup>10</sup> <http://gtt.cyberwatching.eu/Pages/Home.aspx>



For each engaged cluster the name, website, logo, a short description and the synergies with Cyberwatching.eu during the project duration is provided.









<p><b>ClujT, Romania, 82 members</b></p> <p>Website: <a href="https://www.clujt.ro">https://www.clujt.ro</a></p>  <p>About: ClujT with the ultimate goal to become a key supplier from Central and Eastern Europe on promotion of the Romanian IT market, aims to become competitive on national and international in providing innovative IT services, products and organizational support systems. ClujT supports local public-private partnerships for the mutual benefit of the cluster's members and of the society is act towards the creation of a partnership culture based on trust and dependability. The promotion of its in processes, design of products and services to increase competitiveness on an international level the vision of its working groups and interests. Dataintelligence, Learning and Development of SMEs Marketing and internationalization.</p> <p><b>Synergies with Cyberwatching.eu</b> - Presentation at a number of events including:</p> <ul style="list-style-type: none"> <li>• Concertation meeting April 2018 Webinar "Cybersecurity as an opportunity in a changing market" 2018</li> <li>• Webinar "Teleworking and cyber security in times of Covid-19: challenges and risks for SMEs" 2020</li> </ul>	<p><b>AEI Ciberseguridad, 71 members, Spain</b></p> <p>Website: <a href="http://www.aeiciberseguridad.es/">www.aeiciberseguridad.es/</a></p>  <p>About: AEI Ciberseguridad aims to provide an operational structure to all companies interested in IT promotion and development of a Business Technological Pole linked to INCIBE's mandate. With its members, their main interest relies on International Cybersecurity Seal.</p> <p><b>Synergies with Cyberwatching.eu:</b></p> <ul style="list-style-type: none"> <li>• AEI is a partner in the cyberwatching.eu project leading the engagement with other SME cluster the analysis of market and technology readiness levels of R&amp;D projects.</li> </ul>	<p><b>DIGITAL SME, 5 members, France</b></p> <p>Website: <a href="http://www.digitalisme.eu/digital-sme-france-membership">www.digitalisme.eu/digital-sme-france-membership</a></p>  <p>About: DIGITAL SME France as a member of the European DIGITAL SME Alliance promotes a Euro-oriented approach towards the development of French SMEs active in Information and Communication Technologies (ICT).</p> <p><b>Synergies with Cyberwatching.eu:</b></p> <ul style="list-style-type: none"> <li>• On 25 May 2020, Cyberwatching.eu, in collaboration with DIGITAL SME France, organised an online workshop to raise SMEs' awareness about the cybersecurity issues when teleworking. The workshop was held in French and allowed to reach the target audience of French-speaking SMEs mainly located in Eastern France and Luxembourg. Besides being informed about the Cyberwatching.eu and its key offers for the SMEs, the participants got an introduction to cyber and cyber-attacks. The experts then raised the risk awareness of the participants, describing IT specific risks and cyber threats related to teleworking: phishing, ransomware, data theft, Business Email Compromise (BEC) scam, etc. and explaining what kind of vulnerabilities might be exploited by cyber criminals. Finally, the participants got security recommendations from the experts.</li> <li>• On 22 July 2020, Cyberwatching.eu and DSME France signed a Memorandum of Understanding based on their common goals with some commitments from both parties.</li> </ul>
<p><b>GAIA - Association of Knowledge and Applied Technologies Industries in the Basque Country, 255 members, Spain</b></p> <p>Website: <a href="http://www.gaia.es">www.gaia.es</a></p>  <p>About: GAIA aims to become a benchmarking for collaborative innovation for the creation and implementation of globally competitive solutions based on their own Knowledge and Technology. The creation of alliances on knowledge and technology at the international level reflects the vision of its groups and interests: Consulting, Engineering, Electronics, Computing, Telecommunications and Gamification.</p> <p><b>Synergies with Cyberwatching.eu</b> - Speaker at:</p> <ul style="list-style-type: none"> <li>• Concertation meeting April 2018</li> <li>• Webinar "Cybersecurity as an opportunity in a changing market" June 2018.</li> </ul>	<p><b>The Hague Security Delta (HSD), 299 members, the Netherlands</b></p> <p>Website: <a href="http://www.thehagensecuritydelta.com/">www.thehagensecuritydelta.com/</a></p>  <p>About: The Hague Security Delta aims to form partnerships and create knowledge bridges with the global security clusters in the USA, Canada, Singapore and South Africa. Besides, it has strong ties with main European security regions and Brussels, making the Netherlands the secure gateway to Europe. HSD took the initiative in 2016 to collaborate with other relevant security clusters in Europe (France: SA Cluster, Denmark: CensSec, Finland: Safety and Security Cluster, Germany: KIT, Germany: Security so we considered them a relevant cluster to collaborate with. Their working groups and main interest on cybersecurity awareness, Dataintelligence, Data Dioder, Data traffic that can only go one way, CRI infrastructures, Talent and training, Artificial intelligence (their research institutions were focused on do in AI from the stakeholder view).</p> <p><b>Synergies with Cyberwatching.eu</b></p> <ul style="list-style-type: none"> <li>• In November 2019, we had a virtual meeting with Bert Fiskens, from HSD, and they were keen to collaborate with us, especially interested in SMEs, because their two main goals, as a cluster, developing cybersecurity solutions and increasing economic development.</li> <li>• In December 2019, we had a virtual meeting with Herman Hartgers, from SME Connect (help HSD). Interested in fraud and cybercrime and Digital SME, presented the Twint/2x event and opportunities that it brings to SMEs; HSD promoted GDPR Temperature Tool, and other useful Cyberwatching.eu resources for SMEs (like SMEs guides).</li> </ul>	<p><b>Italian DIGITAL SME Alliance, 16 members, Italy</b></p> <p>Website: <a href="https://www.digitalisme.eu/digital-sme-italy-membership">https://www.digitalisme.eu/digital-sme-italy-membership</a></p>  <p>About: Italian DIGITAL SME Alliance aims to represent the interests of Italian SMEs in the ICT sector at national and European level, by becoming a direct channel of communication with the European institutions through bilateral meetings. Keeping track of information and news release on European policies and regulatory updates, it promotes the exchange of know-how and expands possible working collaborations between members in Europe. In addition, dissemination activities and support to members for projects funded by the European Union is one of the activities aiming to enhance its members' skills by participating to European training and workshops.</p>
<p><b>CyberWales, +2000 members, United Kingdom</b></p> <p>Website: <a href="http://cyberwales.net">cyberwales.net</a></p>  <p>About: Cyber Wales is a representative body with the aim of being the Heart and the Voice of the Communities in Wales. Being a network of cyber-related clusters it helps companies to grow by communicating initiatives &amp; trade opportunities, providing a networking platform to share ideas &amp; best practice, encouraging collaboration and identifying partnership opportunities. With a mission to help businesses more resilient to cyber-attacks by building cybersecurity knowledge and skills.</p> <p>Main interests and working groups focus on: Women in Cyber, Capture the Flag, Critical National Infrastructure, Data Privacy, South Wales Cluster, North Wales Cluster and IP Wales Cluster.</p> <p><b>Synergies with Cyberwatching.eu</b> - Speaker at:</p> <ul style="list-style-type: none"> <li>• Webinar "Cybersecurity as an opportunity in a changing market" June 2018</li> <li>• Annual Workshop October 2018 Webinar "Cyber risk management from the SME point of view" October 2018</li> <li>• Webinar "Teleworking and cyber security in times of Covid-19: challenges and risks for SMEs" 2020.</li> </ul>	<p><b>Bavarian IT Security &amp; Safety Cluster, 134 members Germany</b></p> <p>Website: <a href="http://www.it-sicherheitscluster.de">www.it-sicherheitscluster.de</a></p>  <p>About: ITSECURITY aims to initiate and promote collaborations, particularly between the scientific economic community to further the development of IT security research and training, while providing information about security risks and their technical and organisational solutions. Also, they want to leverage the Cluster's member security expertise and launch and mentor company start-ups. Main interests, working groups? ITSECURITY includes all issues of IT or information security (which are concerned in broader sense with protection against intelligent, strategic attack), Data protection, Cloud Security, Industrial IT Security, Information security management, IT Safety applies to the technical functions issues of information security and is primarily concerned with protection against harmful influences.</p> <p><b>Synergies with Cyberwatching.eu:</b></p> <ul style="list-style-type: none"> <li>• On 8-10 October 2020, organised the SME workshop and had a chance to meet the Bavarians and they were informed about the Cyberwatching.eu project. A follow-up call identified that the is interested in participating in H2020 projects and were using Cyberwatching.eu as a reference.</li> </ul>	

Figure 2: Information from the engaged clusters

### 3.2 Webinar series

The webinar series has proved popular with SMEs with consistent participation at webinars focussing on technical topics and vertical sectors. To leverage this and the **DIGITAL SME** network, 10 SME workshops have been organised. They are all described in detail in the D5.3 Early validation & end-users' club final report. In this section, we focus two workshops, co-organised also with DIGITAL SME France, one of the business organisations closely collaborating with cyberwatching.eu.

The first online SME workshop with DIGITAL SME France was organised on 25 May, as described in D4.6<sup>11</sup>. In addition, SME guidebook '10 cybersecurity tips for teleworking'<sup>12</sup> was produced in English as an additional outcome of the workshop, allowing all other SMEs to get informed about the main steps.

<sup>11</sup> <https://cyberwatching.eu/d46-eu-cybersecurity-and-privacy-cluster-engagement-report-3rd-report>

<sup>12</sup> <https://www.cyberwatching.eu/news-events/news/additional-cybersecurity-tips-teleworking-during-covid-19>

## Webinar 1: FINAL WORKSHOP FOR BIOCYBER PROJECT<sup>13</sup> - 9 NOVEMBER 2020



### Jornada Final del Proyecto:



**Lunes, 9 noviembre de 2020, de 12h00 a 13h30 | Online**

Figure 3 Final workshop for BioCyber Project together with Biotecyl and ICTLegal

As part of BioCyber, a project developed by AEI Ciberseguridad with regional funds, a final event was held on 9 November 2020 to present the results to companies in the health sector in Castilla y León, with the collaboration of the regional health cluster, Biotecyl.

The general objective of the BioCyber project was to increase the competitiveness of companies in the health sector of Castilla y León and in particular, of those that are part of the AEI BIOTECYL, allowing them to improve their positioning through a specialized service of evaluation and advice in cybersecurity matter.

ICTLegal was one of the invited speakers to present: "A Novice's Guide to build a solid GDPR Data Protection Compliance Framework: a focus on the healthcare sector", where the RGPD tool and the Information notice tool, developed in Cyberwatching.eu, were promoted.

<sup>13</sup> <https://www.youtube.com/watch?v=xhpRv5Qn6zc>

## Webinar 2: CYBERSECURITY: USE AND USEFULNESS OF LABELS FOR SMES<sup>14</sup> - 29 April 2021



Figure 4 Cybersecurity: Use and usefulness of labels for SMEs together with DigitalSME France

In collaboration with DIGITAL SME France, Cyberwatching.eu, organised this webinar to discuss the establishment of labels in the cybersecurity sector following the example of two complementary labels:

- The French “ExpertCyber” label, which certifies and promotes a company's expertise in cybersecurity.
- The European label "Cybersecurity made in Europe", which distinguishes companies developing digital security solutions in Europe.

After introducing these two labels as well as their complementarity, the discussion focused on the advantages provided by these labels, especially for SMEs, for example in terms of visibility, promotion of their activity and image of reliability with their customers.

The webinar also focused on the cost issues that SMEs may encounter when acquiring labels. A representative of the municipality of Metz gave the perspective of public procurement with regard to the value of labels during public procurement and contract award procedures. The webinar also presented the strategic vision of these labels, which are part of a political will for digital sovereignty.

It was concluded with a teaser for the upcoming cyberwatching.eu label, informing French companies of what is coming up. The French authorities also expressed their interest in using this label and offering the translated version to the French SMEs.

### 3.3 Other activities

#### 3.3.1 Communication activities

We have maintained communication with the engaged clusters over time to inform them of the updates related to cyberwatching.eu: the tools, the marketplace and the webinars.

<sup>14</sup> <https://www.cyberwatching.eu/news-events/events/cybersecurity-use-and-usefulness-labels-smes>

### 3.3.2 AEI Ciberseguridad

Through the AEI Ciberseguridad, as a European cybersecurity cluster, we have promoted the cyberwatching.eu assets, as well as the different surveys that have been launched from the consortium, in addition to communicating the progress of the project through monthly newsletters, as well as in the meetings of the Board of Directors.

### 3.3.3 SME success stories

To emphasise Cyberwatching.eu's commitment to the pan-European SME community, the consortium compiled a series of cases where SMEs have successfully used cybersecurity solutions stemming from the research results of European projects.

We invited the engaged clusters to identify among their members companies that would like to promote themselves as a success story after developing a product or service based on the R&D results of CD&P projects.

Although the current SME success stories published in Cyberwatching.eu are from SMEs that don't belong to the engaged clusters, the section<sup>15</sup> the section is open to attract new success stories from clusters or DIH, to gain visibility in the European Cybersecurity Ecosystem.

### 3.3.4 DIGITAL SME - Coordination Group of European DIH

In October 2020, DIGITAL SME organised the event "Making European DIHs work for SMEs<sup>16</sup>" in order to answer two fundamental questions for the success of European DIH: What makes a Digital Innovation Hub truly European? And what should be the role of existing industrial ecosystems within EDIH?

After the success of the event, DIGITAL SME considered creating and energizing a Coordination Group of European DIH, within its WG DIGITALISATION, with the aim of providing more opportunities for its members to connect with other DIH in Europe, share experiences, discuss services and create your own network and collaborations across the EU.

Although this activity is not a specific cyberwatching.eu activity, it was led by DIGITAL SME and clusters such as Cluj IT or AEI Ciberseguridad participated within this group.

### 3.3.5 'Cybersecurity made in Europe' label by ECSO

In March 2021 ECSO launched the CYBERSECURITY MADE IN EUROPE label, an industry-driven marketing tool aimed at supporting the role of European cybersecurity companies and increasing their visibility in the European and global markets, not only among potential business partners, but also among end users and investors in the cybersecurity industry.

All companies applying for the label must meet a number of general requirements and only 16 ECSO organisations can issue the label, among which are DIGITAL SME, Cybasque (GAIA group), CINI (belonging to MicroCyber DIH) and Cyber Wales.

<sup>15</sup> <https://cyberwatching.eu/sme-success-stories>

<sup>16</sup> <https://www.digitalsme.eu/making-european-digital-innovation-hubs-work-for-smes/>

The label was promoted in the webinar “Cybersecurity: Use and usefulness of labels for SMEs” organised by Cyberwatching.eu and DIGITAL SME France mentioned in section 3.2.

### 3.3.6 Meetings with EDIH candidates to promote the Cyberwatching.eu tools

During this period, the AEI Ciberseguridad held meetings with different EDIHs with the intention of knowing their objectives and activities, as well as to establish possible ways of collaboration in the future network of EDIHs. An important part of the meetings was to promote the cyberwatching.eu tools developed for SMEs.

As a result of these meetings, a Memorandum of Understanding has been signed to reflect the desire to find synergies that can benefit companies in the regions involved in their digital transformation, and particularly in relation to cybersecurity.

This type of meeting will continue beyond the lifetime of cyberwatching.eu and will be reinforced if CyberDIH becomes part of the European network of DIHs. This is because there is a specific tool, the Digital Transformation Accelerator, created by the European Commission to favour the exchange of experiences and good practices among DIHs.

The following is a list of the first meetings of rapprochement between the AEI Ciberseguridad and other DIH candidates.



#### **Cybersecurity Innovation Hub (Czech Republic):**

Coordinated by the National centre of competence for cybersecurity, the consortium is completed with 2 universities, a chamber of commerce, two industrial clusters and the National Cyber and Information Security Agency. Within this DIH, Kypa was developed

(the Cyber Range Infrastructure of SPARTA).



#### **Mycrocyber (Italy):**

Coordinated by the Ente Nazionale per il Microcredito, the consortium is completed with CINI (National Interuniversity Consortium for Informatics, with 48 universities), Università Luigi Vamvitelli and Deloitte.

They have a national scope and a strong focus on cybersecurity for microenterprises.



#### **DIH4Sm@rtRegions (Portugal):**

Coordinated by Morecolab, a technology transfer office, the consortium is completed with 12 entities including clusters, collaborative labs, higher education institutes, municipalities, etc. They have a focus on regions of low population density and cross-border with other regions of Spain and Europe.



#### **DIH4Society (Romania):**

Coordinated by Cluj IT cluster, the consortium is completed with the technical university of Cluj Napoca and a chamber of commerce of a

nearby county. They cover the geographic area of northwest Romania, which includes 6 counties through agreements with other partners. They specialize in AI and Smart robotics, with cybersecurity as a transversal technology, with strong focus on Manufacturing & Public Authorities.



#### **Health Hub (Greece):**

Coordinated by the Institute of Entrepreneurship Development, it brings together a team of experts with extensive experience in the areas of Artificial Intelligence (AI) combined with advanced research in the fields of health and pharma, drug design and re-purposing, digital technologies providers (software and hardware), training and lifelong learning as well as business and innovation.

## **4 Implications in the cyberwatching sustainability model**

As part of the sustainability strategy of cyberwatching.eu, an agreement has been reached within the consortium to transfer the exploitation rights of the four tools developed for SMEs (GDPR temperature tool, Cyber Risk temperature tool, Information Notice tool and the Cybersecurity Label) to the AEI Ciberseguridad, with a plan for their integration as part of the services offered by the AEI within the CyberDIH.

In this way, the AEI Ciberseguridad, as coordinator of the CyberDIH, will ensure that the tools are promoted correctly among SMEs and public entities so that their use proliferates, and that the functionalities of the tools are expanded with complementary payment services that support their sustainability. This cost of the new services associated with the tools will not necessarily have to be covered by the end users (SMEs and public entities), since in case of being chosen as EDIH in the European call, the EC will co-finance the services offered by EDIH with 50% of its cost.

This implies taking advantage of the project results, together with the generation of new services, but also implies the projection and collaboration of the partners in the medium-long term.

The relationship established not only with the cybersecurity clusters, but also with the DIH candidates to be part of the European Network of DIH allow us to position the tools developed within cyberwatching.eu as support elements for the digital transformation of SMEs and public administrations. The EDIHs will not be watertight compartments that offer their services only at the regional level, but the network will promote the provision of cross-border services.

In addition, DIGITAL SME will integrate the permanent links to the resources hosted by CyberDIH in its members' platform (currently under development), which will lead DIGITAL SME member DIHs, clusters and their SMEs to further exploit the assets, and, at the same time, continue collaboration with the CyberDIH. In addition, the work carried out by DIGITAL SME as a facilitator of a specific working group for DIHs (where AEI Ciberseguridad is also participating) positions them as a quality partner in the promotion of the tools as part of the CyberDIH services.

In this way, the tools developed will be integrated into the CyberDIH services, and therefore, will become available to any European SME or public entity that needs them. By signing collaboration agreements, the promotion of DIH services is



encouraged among entities from other countries that can complement the services offered by their local DIH, and therefore, the tools developed within cyberwatching are enhanced, thus contributing to its sustainability, serving as the basis for the development of new related services.

#### 4.1 CyberDIH

The Cybersecurity Innovation Hub (CyberDIH)<sup>17</sup> is a digital ecosystem around cybersecurity and advanced technologies, which has INCIBE (the Spanish Institute of Cybersecurity) as a reference center and has been promoted by the Regional Government of Castilla y León (ICE) and the AEI (the national cybersecurity cluster), to bring the benefits of digitalization to companies, and help them accelerate their adoption of digital technologies, especially designed to improve an industry 4.0.



Figure 5 CyberDIH website

Through the website, activities and services around six big areas are promoted for companies (specially SMEs) and public entities.

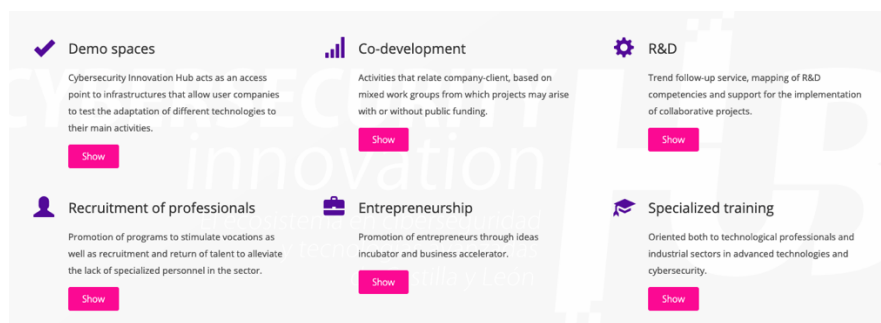


Figure 6 Activities and Services in CyberDIH

New services are under development, other services are in the process of being defined, and the CyberDIH will be the entry point to access these services.

The new services have to preferably fit into one of the four main groups that EDIHs are supposed to offer: Test before invest, Skills and training, Support to find investments and Innovation ecosystem and networking. The group of services enabling **test before invest** may include: **awareness raising**, **digital maturity assessment**, demonstration activities, visioning for digital transformation, fostering the integration, adaptation and customisation of various technologies, testing and

<sup>17</sup> <https://www.cyberdih.com/en/>

experimentation with digital technologies (software and hardware), knowledge and technology transfer. Special focus will be on the key technologies promoted in Digital Europe Programme: HPC, AI, and Cybersecurity.

The four tools developed within cyberwatching.eu that will be transferred to the AEI and the CyberDIH focus on raising awareness and assessing cybersecurity and privacy maturity and therefore belong to this group.

In a first stage, the four tools will be promoted through a specific section included in the website, to better promote the tools as a package and also to promote the Cyberwatching.eu project.

In a second stage, the tools can be included within the 4 mentioned groups of services, and further services derived from these tools could be developed. The new services could be free of charge or can be offered at a reduced price, if they are approved by the European Commission and therefore 50% funded.

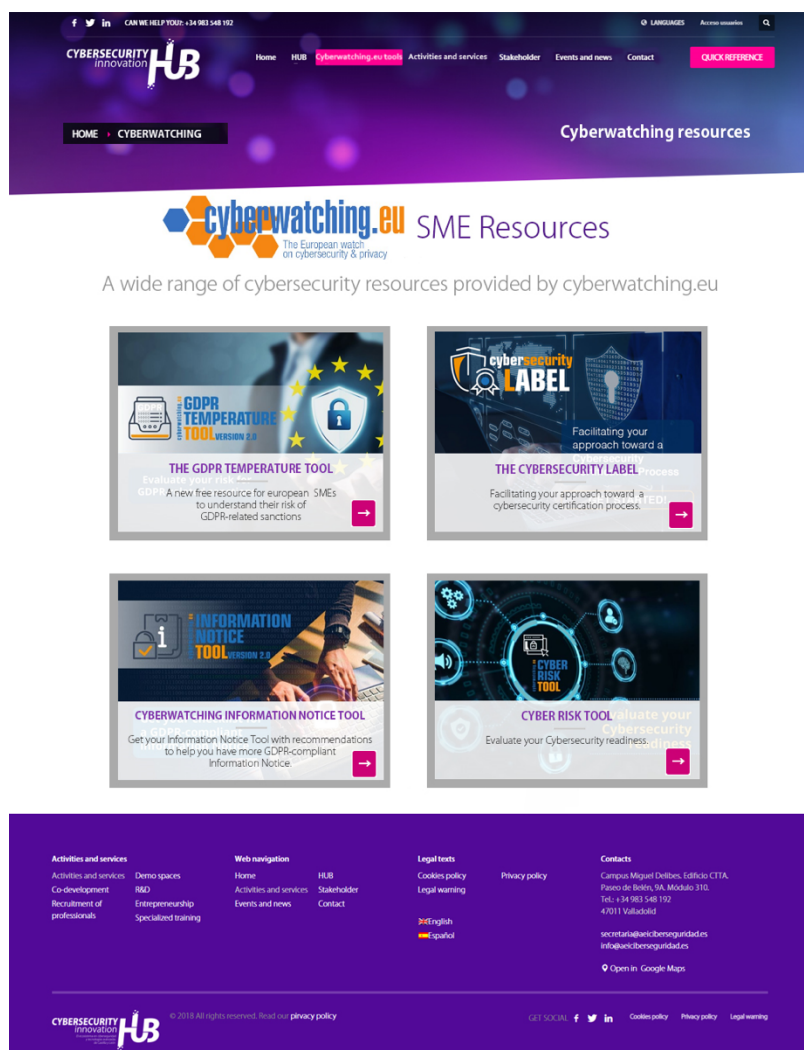


Figure 7 Cyberwatching.eu tools section



## 5 Conclusion

During the last 14 months, the project has worked to try to consolidate relationships with European cybersecurity clusters and DIH, publicising the results of the projects for the benefit of SMEs and encouraging them to participate as marketplace providers.

But the main focus has been on trying to understand the new key figure in digital transformation, the European Digital Innovation Hubs, and how European cybersecurity clusters relate to them.

EDIHs are ecosystems that must integrate academia, public administration and industry (clusters), to transfer knowledge and facilitate the secure digital transformation of SMEs and public entities, giving rise to a sovereign and more sustainable Europe. Cybersecurity is one of the three pillars that the European Commission establishes as keys to the success of digital transformation.

The knowledge acquired on the European cybersecurity R&D landscape during the 4-year duration of the project, as well as the tools developed for SMEs, are important assets that provide great value for the definition of services that EDIHs can offer to companies. SMEs, services that will be innovative as they are based on the results of projects financed with European funds.

The CS&P projects analysed and supported by Cyberwatching.eu integrate all emerging technologies that can and should be applied to different sectors to facilitate digital transformation.

It is clear that the digital maturity of SMEs is not the same throughout Europe, and that depending on the region, the services to be defined will be different. However, the EDIHs project is a long-term project (3 years with the possibility of an extension for 4 more years), so that although in the first place the EDIHs will be able to offer services adapted to the maturity of regional companies, It is also necessary that they include more advanced services, based on emerging technologies, to avoid that no region is left behind, and that evolution occurs in an egalitarian way.

Continuing to share the knowledge acquired and promoting the tools developed with other clusters and EDIHs is a task that must be continued by the partners once the project is finished, especially by the partners whose goals are to increase the competitiveness of SMEs, such as DIGITAL SME and AEI Ciberseguridad.