



D9.4

# Final exploitation and dissemination report

## WP9 – Exploitation, Dissemination, Communication and Standardization

**C3ISP**

*Collaborative and Confidential Information Sharing and Analysis for Cyber  
Protection*

Due date of deliverable: <30/09/2019>

Actual submission date: <14/10/2019>

14/10/2019

Version 1.0

*Responsible partner: Digital Catapult*

*Editor: Charles Fox*

*E-mail address:*

*Charles.Fox@Digicatapult.org.uk*



*The C3ISP Project is supported by funding under the Horizon 2020  
Framework Program of the European Commission DS 2015-1, GA #700294*

<b>Project co-funded by the European Commission within the Horizon 2020 Framework Programme</b>		
<b>Dissemination Level</b>		
<b>PU</b>	Public	
<b>PP</b>	Restricted to other programme participants (including the Commission Services)	
<b>RE</b>	Restricted to a group specified by the consortium (including the Commission Services)	
<b>CO</b>	Confidential, only for members of the consortium (including the Commission Services)	



*The C3ISP Project is supported by funding under the Horizon 2020 Framework Program of the European Commission DS 2015-1, GA #700294*

**Authors:**

Charles Fox, Jamie Harrison

**Approved by:**

List of reviewers: Maria Prokopi (DIGICAT),  
 Than Hai Nguyen (CEA), David Chadwick (UNIKENT), Jovan Stevovic (CHINO), Ian Herwono (BT), Selina Wang (BT),

**Revision History**

Version	Date	Name	Partner	Sections Affected / Comments
0.5	2019.07.23	Charles Fox	DIGICAT	Internal D9.4 draft of year 3 updates including the agreed platform exploitation plan,
0.6	2019.08.16	Jamie Harrison	DIGICAT	Updated event calendar, added 2 annex 18/19, letter of support and product deck, added section on client reach out
0.9	2019.08.22	Charles Fox	DIGICAT	Draft for C3ISP partners to provide individual exploitation plan updates.
1.0	2019.09.30	Charles Fox	DIGICAT	Final draft for EU commission – includes updates from Pisa project review in September.



*The C3ISP Project is supported by funding under the Horizon 2020  
 Framework Program of the European Commission DS 2015-1, GA #700294*

## Executive Summary

This is the fourth document related to exploitation and dissemination activities of the C3ISP project. The first document, D9.1, describes the exploitation and dissemination plan of the project, while D9.2 and D9.3 are reports about the activities actually made and also some hints about the future especially related to the exploitation activities. In D9.4 however as well as reporting on dissemination and communication activities we focus more on exploitation and especially on our agreed C3ISP platform exploitation plans.

In particular, this document is the third report about the exploitation and dissemination activities that have been carried on within the third year of the C3ISP project. Indeed, this document extends and updates deliverables D9.3, which reported on the exploitation and dissemination at the end of month 24. The document contains:

- Analysis of the industrial state of the art, business models, the market, and the value proposition of the project results with the aim of describing possible options and scenarios for sustainability plans for the main project results.
- Analysis of the Intellectual Property (IP) associated with the Project.
- The agreed joint C3ISP Platform exploitation plan and progress reports to date
- Individual exploitation plans from each industrial partner focus on innovation aspects.
- C3ISP dissemination and communications activities by listing attended events and scientific publications, related to C3ISP and describes improvements communication means such as webpage analytics, flyer, and brochure.
- Standardization plan and achievements for some C3ISP results.

The content here on the C3ISP platform exploitation plan is also available as a much shorter document restricted to that single topic.



*The C3ISP Project is supported by funding under the Horizon 2020  
Framework Program of the European Commission DS 2015-1, GA #700294*

## **Table of contents**

Executive Summary .....	4
1. Exploitation and Innovation.....	8
1.1. Mission statement.....	8
1.1.1. Market context .....	8
1.2. Market Segments and Opportunities for C3ISP .....	9
1.2.1. Focus on the smart Energy Grid CNI .....	13
1.2.2. Focus on Connected Autonomous Vehicle Transport CNI .....	14
1.2.3. Focus on the Telecommunications CNI .....	15
1.2.4. C3ISP Common Theme for CNI Verticals .....	16
1.2.5. C3ISP Route to Market.....	16
1.3. Innovation Workshops .....	19
1.3.1. Workshop #1 – London March 2018 .....	20
1.3.2. Workshop #2 – Pisa October 2018 .....	26
1.3.3. Workshop #3 – Pisa April 2019.....	34
1.3.4. Promotional activities .....	36
1.4. Industry state of the art.....	36
1.4.1. Threat intelligence market context.....	36
1.4.2. Threat intelligence providers .....	37
1.4.3. Reacting to threat intelligence .....	39
1.4.4. C3ISP Competitive Landscape - Threat Intelligence Sharing platforms.....	45
1.5. Intellectual Property .....	48
1.5.1. Approach.....	48
1.5.2. Components .....	48
1.5.3. IP value assessment.....	49
1.5.4. IP Item prioritization.....	51
1.6. The C3ISP Platform Exploitation Plan .....	52
1.6.1. C3ISP Our Business Model .....	52
1.6.2. C3ISP Platform Exploitation Plan on a page.....	55
1.6.3. Report of C3ISP Platform Exploitation Activities.....	57
1.7. Individual Exploitation Activities and Plan .....	59
1.7.1. CNR .....	59
1.7.2. ISCOM-MISE.....	60



1.7.3.	HPE.....	60
1.7.4.	BT.....	60
1.7.5.	SAP.....	61
1.7.6.	CEA.....	62
1.7.7.	DIGICAT.....	62
1.7.8.	UKENT.....	65
1.7.9.	GPS.....	65
1.7.10.	CHINO.....	66
1.7.11.	3DRepo.....	67
1.8.	Pilot Blogs.....	67
1.8.1.	ISP Pilot Blog.....	68
1.8.2.	CERT Pilot Blog.....	69
1.8.3.	SME Pilot Blog.....	70
1.8.4.	Enterprise Pilot Blog.....	70
2.	Dissemination and Communication.....	72
2.1.	Participation and organization of events.....	72
2.2.	Press Releases.....	77
2.3.	Publications.....	78
2.4.	Communication activities.....	82
2.4.1.	C3ISP WebPage.....	82
2.4.2.	Social Media.....	85
2.4.3.	Other Communication activities.....	87
3.	Standardization.....	88
3.1.	CEA Contribution to Standardization.....	88
3.2.	DigiCat contribution to Standard.....	88
3.3.	Individual Consortium members contribution to Standard Activities.....	89
4.	References.....	92
	ANNEX 1 : Glossary.....	95
	ANNEX 2 - C3ISP “Building a route to market for new cybersecurity technologies”.....	96
	ANNEX 3 - List of Approached Companies.....	97
	ANNEX 4 - List of Attending Companies.....	98
	ANNEX 5 - Workshop 1 Agenda.....	99
	ANNEX 6 - Workshop 1 Table Plan.....	100



ANNEX 7 – Workshop 1 – worksheets.....	101
ANNEX 8 - Workshop 1 - rules of the road.....	104
ANNEX 9 - Workshop 1 - Illustration.....	105
ANNEX 10 - C3ISP Brochure.....	106
ANNEX 11 - Workshop Tweets.....	107
ANNEX 12 – Workshop 1 - Feedback Form Results.....	108
ANNEX 13 - C3ISP Competitor Details.....	111
ANNEX 14: C3ISP Route to Market - Customer Outreach.....	125
ANNEX 15: C3ISPWorkshop 2 – Interviews Report.....	126
ANNEX 16: C3ISPWorkshop 3 – Report.....	132
ANNEX 17: C3ISP Hosted workshop for UK BEIS & NCSC.....	151
ANNEX 18 – C3ISP PRODUCT DECK.....	153
ANNEX 19 - Letter of support Secure Data.....	159
ANNEX 20 – Mutual Non-Disclosure Agreement.....	161
ANNEX 21 – C3ISP Exploitation engagement interview reports.....	168
ANNEX 22 C3ISP Industry Engagement - CyberTech Rome 2019.....	171



*The C3ISP Project is supported by funding under the Horizon 2020  
Framework Program of the European Commission DS 2015-1, GA #700294*

# 1. Exploitation and Innovation

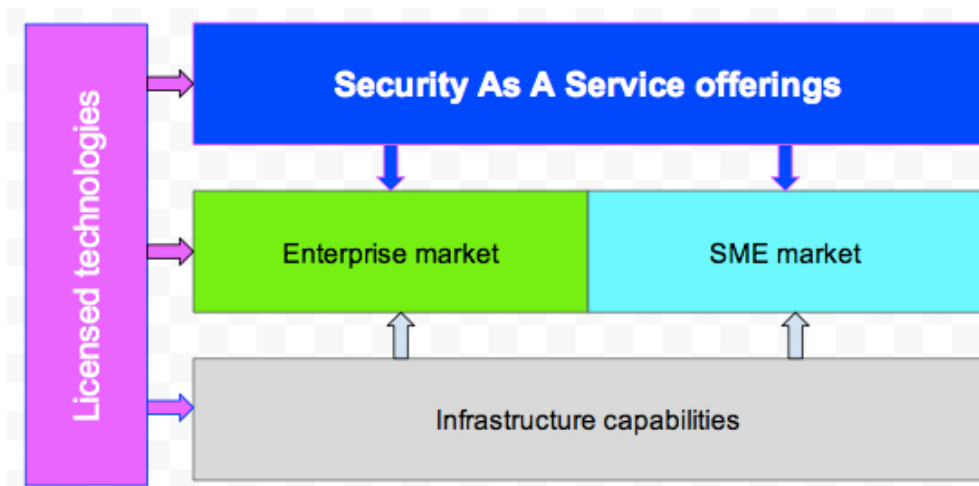
## 1.1. Mission statement

The mission of the C3ISP project is to define an exploitable collaborative and confidential information sharing, analysis and protection framework-as-a-service for cyber security management, regulated by Data Sharing Agreements (DSAs) that are computer interpretable and multi-stakeholder. The framework can share information inside a collaborative multi-domain environment to improve detection of cyber threats and response capabilities, while appropriately preserving the confidentiality of the shared information.

### 1.1.1. Market context

The C3ISP technology innovations have the potential to impact industrial security markets, which span enterprise and SMEs, as well as infrastructure capabilities, such as Community Emergency Response Teams (CERTs), Cloud Service Providers (CSPs) and Internet service Providers Community Emergency Response Team (ISPs).

As shown schematically in Figure 1 C3ISP technologies could be licensed to providers of infrastructure capabilities that serve the Enterprise and SME markets (and potentially more widely). They could also be licensed directly into the enterprise market (or those who supply products to that market), and to those offering Security-as-a-Service (SaaS) into the enterprise and SME markets.



**Figure 1. Schematic of C3ISP market context.**

In addition, the C3ISP Consortium includes both CSP and Managed Security Service (MSS) providers, who could leverage C3ISP technologies directly into products and services that they offer or will offer.

The key areas where C3ISP has (and plans to) innovate technology concern Cyber Security Sharing and Analytics (CSSA), including:

- Data sharing mechanisms that define and dynamically control access rights, notably Data Sharing Agreement (DSA).





- Privacy Enhancing Technologies (PETs) and their application to Cyber Threat Intelligence (CTI).
- Combinations of visualization and analysis technologies with PETs in the context of CTI
- Distributed architectures for CSSA.

## 1.2. *Market Segments and Opportunities for C3ISP*

The market for Threat Intelligence sharing Platforms (TIPs) is one distinct component of the wider Threat Intelligence market. According to a recent 2019 report by Global Market Insights (Ref 1) the overall global Threat Intelligence Market size was over USD 4 billion in 2018 and is set to grow at 14% CAGR from 2019 to 2025.

According to this report North America dominates the threat intelligence market landscape with a 40% share of the total market in 2018. The rise in the number of connected devices and the government support along with the increasing use of remote monitoring & tracking devices are encouraging companies to adopt advanced security solutions. The presence of several large threat intelligence vendors such as IBM, Symantec, and Palo Alto Networks and the widespread awareness regarding the security solutions will help in market growth.

The European threat intelligence market will grow at a CAGR of 14% over the projected timeline. This is attributed to the introduction of stringent compliance regulations (such as NIS) mandating the companies to incorporate advanced security solutions into their network infrastructure. The early adoption of various next-generation technologies such as IoT and cloud computing across various businesses sectors has further added to market growth.

In determining the C3ISP platform market opportunities in this context we first need to view the Threat Intelligence services market in terms of the five stages of the Threat Intelligence Life cycle as shown in Figure 2 below.

### The Threat Intelligence Life Cycle



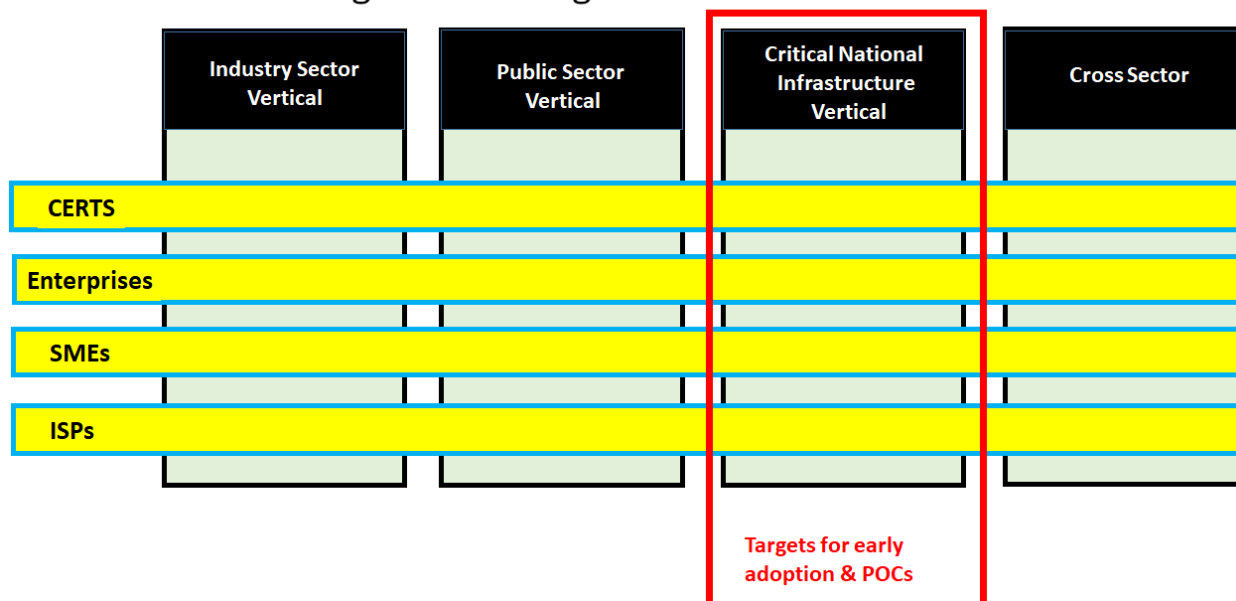
*The C3ISP Project is supported by funding under the Horizon 2020 Framework Program of the European Commission DS 2015-1, GA #700294*

**Figure 2 – The Threat Intelligence Life Cycle**

Although the Collection stage of the life cycle is already saturated with providers of pure threat data feeds there are current market opportunities for C3ISP since the latter stages of the threat intelligence life cycle are less mature and feature a smaller number of competitors as we shall show in section 3. The C3ISP CTI platform capabilities span all five stages with varying degrees of maturity.

From the C3ISP perspective we further structure the market using the simple target segmentation model shown in Figure 3.

**C3ISP Threat Intelligence Sharing - Market Structure**



**Figure 3 – C3ISP Threat Intelligence Platform Market Structure**

The provision of a Cyber Threat Information (CTI) sharing platform and or service can support collaboration across industry sectors both nationally and internationally. However, such platforms and services can also be targeted at individual industry verticals, bringing together an often fragmented ecosystem of stakeholders. This is particularly important in Critical National Infrastructure (CNI) sectors, where the rapid emergence of new vulnerabilities and a fast-changing threat landscape is leading to a drive to improve cyber resilience through better collaboration. State and commercially motivated threat actors are most likely to target businesses within the Critical National Infrastructure area and we also know the CNI is one of the largest spending segments of the market on cyber security solutions at all levels.

As also shown in Figure 2.2 each of these target market segments is comprised of an ecosystem of stakeholders which in our model are classified in line with the C3ISP Pilot groups i.e. ISPs, SMEs, Enterprises and CERTs. C3ISP will be most impactful when organisations in all stakeholder groups are participating, this will increase the chance of a threat being identified at the earliest opportunity, especially relevant to those threats designed to target systems within a dedicated vertical market.



Although the C3ISP core platform will be made available as an open source resource that can be exploited by all these market segments the opportunity to provide the C3ISP CTI platforms full range of intelligence life cycle capabilities will involve a more targeted approach in order to gain early adopters of the proprietary modules and associated commercial services.

As we describe in section 3 of this document there is already some significant competition from existing companies offering both open source and commercial full life cycle CTI sharing platforms / services. Consequently the C3ISP exploitation plan focuses on specific market segments that our knowledge and research suggest are most likely to be early adopters of our platform.

Although we do not restrict in any way the market for the C3ISP platform we focus here on the industry verticals that feature the strongest market drivers for exploiting the services that the C3ISP platform has to offer.

As part of this market analysis we consider the most attractive vertical industry sectors to focus on for the exploitation of the C3ISP platform.

Each of the target market segments but especially the CNI verticals require:

- Trusted and controlled threat intelligence sharing to counter advanced attacks
- Growing demand for integrating security operations with threat intelligence (e.g. through analytics capabilities)

These CNI targeted sectors are just one of the potential routes to market for C3ISP. However in line with the conclusions of the C3ISP WP 9 workshop 3 report this industry vertical focus takes precedence over the productised approach to ensure we produce solutions with specific customers in mind. It also narrows our focus on specific organisations and subsectors.

We use the UK CNI as an example for bringing this analysis to life however the following UK CNI sectors are typical of most EU and major Nation states. In the UK, there are 13 national infrastructure sectors these being:

Chemicals	Civil Nuclear
Communications	Defense
Emergency Services	Energy
Finance	Food
Government	Health
Space	Transport
Water	



*The C3ISP Project is supported by funding under the Horizon 2020 Framework Program of the European Commission DS 2015-1, GA #700294*

Each sector has one or more Lead Government Department(s) (LGD) responsible for the sector, and ensuring protective security is in place for critical asset. In table 1 below we show the results of our initial analysis of each of these CNI vertical sectors from the C3ISP perspective.

	Threat Sharing	openness to share generally	Wealth	Cyber Certification and regulation	Threat Landscape (size)	Attractiveness to attackers	TOTAL	Blockers
Chemicals		2	4	2	2	1	11	Low score
Civil Nuclear	4	5	5	5	3	5	27	Regulatory complexity
Communications	3	2	4	4	5	5	23	
Defence	5	2	5	5	5	5	27	Regulatory complexity
Emergency Services	2	3	2	4	3	2	16	Low score
Energy	3	4	4	3	5	5	24	
Finance	4	3	5	4	5	5	26	Already mature market
Food	2	2	3	2	3	1	13	
Central Government	3	4	2	4	4	5	22	
Health	4	4	2	3	5	2	20	Low score
Space	3	5	4	3	2	4	21	Low score
Transport	3	3	4	3	5	4	22	
Water	3	3	3	3	2	1	15	Low score

**Table 1 – Prioritising CNI vertical sectors that will benefit most from exploiting the C3ISP threat sharing capabilities**

We have considered both the market drivers and market inhibitors (blockers). The market drivers here include the attractiveness of each particular CNI sector to threat actors which will typically involve Nation States and their proxies in the case of CNI targets. The attractiveness of the CNI in each case will be a function of its criticality to the host (target) nation, e.g. the national power supply is a highly attractive target since taking that out for a prolonged period takes out pretty much everything else!

Other market drivers for threat sharing services include the size of the threat surface and the level of interdependencies across the member stakeholders comprising the cyber ecosystem of each CNI. As we shall show rapidly evolving CNI verticals such as the UK smart grid cyber ecosystem and the UK connected autonomous vehicle cyber ecosystem feature explosive growth in the size of the threat surface and in a similar growth in the number of and diversity of stakeholder types and interconnectedness.

The wealth i.e. economic growth potential associated with each CNI is also an indicator of the appetite for investing in threat sharing services across those ecosystems. In essence it points to potentially positive business cases for C3ISP to mitigate the risk of economic loss associated with any successful systemic attacks on those CNI.

As we stated earlier we have also considered in our analysis the market inhibitors / blockers these include regulatory constraints and security classifications which typically introduce levels of complexity (cost) in for example the Defence and Nuclear CNI verticals.

As highlighted in table 1 this initial analysis has enabled us to prioritise the CNI verticals to focus on for exploiting C3ISP services. The three we have chosen at this initial stage being:

- **Energy** – supporting its cyber resilient evolution to the smart grid
- **Transport** – supporting its cyber resilient evolution of the Connected Autonomous Vehicle
- **Communications** – supporting the cyber resilient evolution to 5G

Further justification for the selection of these three CNI areas is the inherent interdependencies of the sectors which in relation to the C3ISP platform would create cross-vertical benefits. The energy sector underpins both transport and telecoms and the growth of connected vehicles is heavily dependent on the telecommunications industry. Many near future scenarios, such as intelligent energy distribution and the impact of autonomous delivery systems further enhance the need for connectivity between these sectors. These areas of cross over will be stipulated alongside vertical justification.

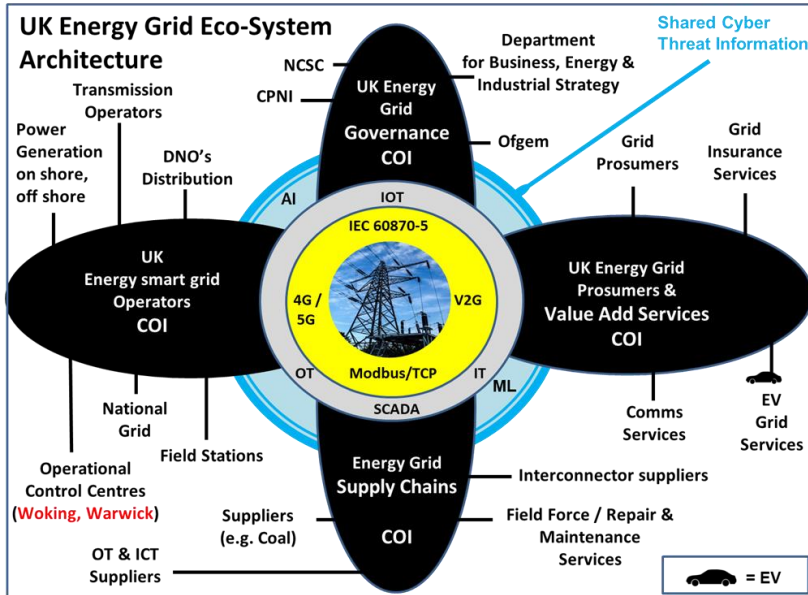
Although Central Government is highlighted as an area of interest within CNI the cyber security agenda across most of Europe and developed Nations with regard to government is heavily guided by a single governmental department. In the UK this is the National Cyber Security Centre (NCSC) which is heavily associated with the Government Communication Headquarters (GCHQ) and is responsible for the UK CERT. The CERT has heavy influence across all of the CNI areas and the associated government departments therefore we did not feel it was necessary to provide additional evidence to justify our engagement with CERTs/Central Government.

### **1.2.1. Focus on the smart Energy Grid CNI**

The evolution of the UK energy grid from analogue to smart is being driven by the increasing adoption of diverse energy sources, including wind and solar, together with a fundamental shift from being a monopoly of grid operators and utilities generating power to a system where prosumers play a key role. At the technological heart of the convergence between operational technology (OT) and information technology (IT) is the internet of things (IoT). The UK energy ecosystem is embedded in the wider global energy ecosystem and is subject to global political, economic, social, technical and legal (PESTL) influences. Our conceptual architecture model for this CNI vertical highlighting the shared threat information services is shown below in Figure 4

## The UK Energy Grid ecosystem – Mitigation through sharing CTI

In our complex VL4 systems of systems the scale and dynamic nature of the threat landscape coupled with the motivation of Threat Actors to focus on Cyber ecosystems that provide Critical National Infrastructure means that attacks will occur and some of those are likely to be successful.



However by sharing Cyber Threat Information across the ecosystem we can help provide effective cyber security which requires cooperation and collaboration among all the entities involved.

Increasing the information available for analysis allows better prediction, prevention and mitigation of cyber-attacks.



**Figure 4 – UK Energy CNI Vertical with C3ISP Threat sharing across the ecosystem**

We model the cyber eco-system of each of our targeted CNI and explore the potential benefits of exploiting C3ISP in the context of a dedicated MSS tailored to support that specific CNI. For example threat intelligence life cycle services covering SCADA / OT scenarios. In the UK CERT i.e. the NCSC provides a level of threat intelligence sharing through services such as CISP. In the United States the Electricity Information Sharing and Analysis Center (E-ISAC) gathers and analyzes security data, shares appropriate data with stakeholders, coordinates incident management, and communicates mitigation strategies with stakeholders using CRISP.

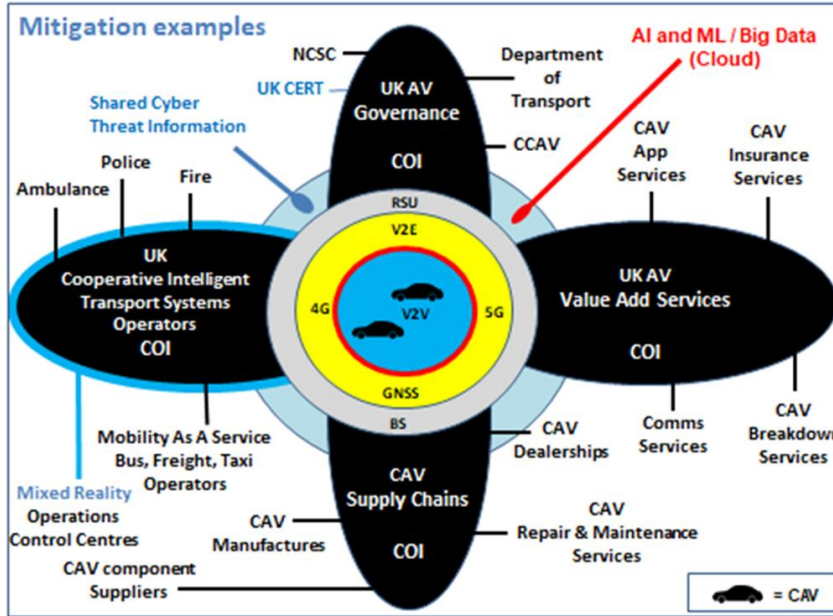
### 1.2.2. Focus on Connected Autonomous Vehicle Transport CNI

The evolution of the UK transport Infrastructure is illustrated below in Figure 2.4 by a simple high level architecture model focused on the Operational CAVs in the context of the UK Intelligent Road Infrastructure.

The CAV population in this simple model is a hybrid-mix of different Autonomy Levels (0, to 5, where 0 is a fully manual system and 5 fully autonomous) the percentage of each CAV Level being a function of time with the higher level autonomy population increasing. The CAV population will very likely consist of a mixture of ground, air and sea transportation systems interconnected to provide crucial links in supply chains and customer journeys.

## The UK CAV Eco-System – Mitigation through sharing CTI

In our complex VL4 systems of systems the scale and dynamic nature of the threat landscape coupled with the motivation of Threat Actors to focus on Cyber Eco-Systems that provide Critical National Infrastructure means that attacks will occur and some of those are likely to be successful.



However by sharing Cyber Threat Information across the Eco-system we can help provide effective cyber security which requires cooperation and collaboration among all the entities involved.

Increasing the information available for analysis allows better prediction, prevention and mitigation of cyber-attacks.



**Figure 5 - UK CAV Transport CNI Vertical with C3ISP Threat sharing pan-ecosystem**

Each CAV at level 1 and above will feature varying degrees of Vehicle to Vehicle (V2V) and more generally Vehicle to Everything (V2X) modes of communication. V2V will either use Dedicated Short Range Communication (DSRC) or C-V2X depending on which of these two competing and incompatible protocols is selected. In our paper we assume the adoption of 5G C-V2X for the UK CAV Eco-System, with the first significant 5G networks predicted to start going live in the UK by 2020.

We model the cyber eco-system of each of our targeted CNI and explore the potential benefits of exploiting C3ISP in the context of a dedicated MSS tailored to support that specific CNI. For example threat intelligence life cycle services covering CAV AI and 5G attack scenarios.

### 1.2.3. Focus on the Telecommunications CNI

We focus here on the ‘interdependence’ between the Electricity CNI and the Telecommunications CNI to explore the potential for federated cross CNI threat sharing.

Electricity is the most critical dependency of the Telecommunication cyber ecosystem. However not only is the telecoms industry itself wholly dependent on electrical power, the electrical power industry also depends on telecoms to manage their extensive network of generators and grid distribution.

The 5G Evolution of the Telecommunications sector will result in more devices, which increases power demand, which increases the need for more of the spectrum among energy utilities.

We include in the Telecommunications core ecosystem ISP providers and operational services as well as core optical fibre networks.

#### **1.2.4. C3ISP Common Theme for CNI Verticals**

The C3ISP platform provides the ability to put in place a powerful and customized Trust model between the many and diverse stakeholders that comprise a CNI vertical ecosystem. This covers the SMEs, the Enterprises, the governance bodies and the CERT (NCSC in the UK case).

It also can be extended to provide a federated Trust model for the sharing and dissemination of CTI across multiple interdependent CNI verticals. In the EU the threats to CNI verticals do not recognise national boundaries, hence the need for collaborative threat intelligence sharing across the EU in sectors such as Energy.

This C3ISP trust model and associated services could be configured to optimize and augment collaboration with extant CTI / MSS services in each CNI vertical. For example CISP operated by the NCSC in the UK and pan EU ISACAs such as the European Energy – Information Sharing & Analysis Centre (EE-ISAC).

In the processing and exploitation stage and the analysis and production stage of the intelligence life cycle the existing and extensible suite of C3ISP capabilities provide the potential for further growing our competitive differentiation. This is important for CNI which invariably have to deal with advanced threats.

#### **1.2.5. C3ISP Route to Market**

As detailed in the 3rd workshop report we see a key play-off between the need for widespread adoption (likely stimulated through free-to-access and open source) and the need to generate revenues to sustain the platform (likely via proprietary and commercial services). The key enablers for adoption are the CERTs, while the key drivers of commercial revenues will be the end-customers who see the largest value in exchanging threat information. However in order to reach these critical end customers we will work via direct and indirect routes, including resellers and market places.

Indirect routes such as resellers and ISPs are the key to gain adoption by end-customers as they have large existing client basis and trusted brands. On-boarding a few of these resellers and ISPs has the potential to put C3ISP into the hands of many. Typical resellers will include data-centre managers, IT infrastructure companies and IT business support organisations, there is also an increasing segment of specialist cyber security providers. The other indirect route is via marketplaces which unlike resellers are passive websites which offer advice on the right solutions to solve a given problem, an example of a growing specialist cyber site is <https://www.protectbox.com/>.

Less formal activities with regard to market engagement and raising the profile of the platform to further encourage adoption is via direct conversations with cybersecurity and developer communities. Via physical meet-ups and online forums such as LinkedIn we are



promoting and demonstrating the capability of C3ISP and this aims to increase word-of-mouth recommendations and increase uptake of the free-to-use aspects of the platform by curious developers and cyber-security experts. These bottom up activities are seen predominantly as awareness raising and community building and seek to build credibility in the community less-so with the aim of securing paying customers. These activities are covered in more detail in the dissemination report.

Below we detail brief strategies with regard to each key segment, in Annex 14 you will find a list of companies we are actively pursuing in each of these categories, some of these organisations are also within the consortium.

With regards to the steps taken to showcase the capability of C3ISP to our target consumers or resellers we will do the following:

1. **Engage:** Establish first contact with an interested partner
2. **Qualify:** Have initial sales call to establish interests and align expectations of the capability of C3ISP, confirm followup with appropriate stakeholders interest in the application of C3ISP
3. **Demonstrate & POC evaluations:** Demonstration, either F2F or via webinar/conference call. Provide access to cloud based showcase capability. Provide access to PoC free-to-access aspects of C3ISP including optional support from technical partner to advise on best practice.
4. **On-board:** Make available an open source C3ISP core platform as described in our business model in section 1.6.1 to encourage the adoption of C3ISP capabilities.
5. **Scale-up:** Individual partners may decide in future to follow-up to engage in paid for modules which may include on-going support as well as technical services

## CERTs

As CERTs underpin national cyber threat sharing initiatives, endorsements from CERTs will be key to the widespread adoption of C3ISP, and collaboration with CERTs will provide the credibility and network required. Justification could be made in countries who currently centre threat sharing around CERTs to provide C3ISP for free in return for endorsement or use-case based promotional activities. As C3ISP only offers true value once widely adopted it is essential in early stages of development to onboard any key network enablers to endorse the system for wider communities, and this approach would drive early use-cases of C3ISP. Furthermore, as national CERTs provide a single point of international coordination, endorsement from a national CERT will enable us to reach out to other national CERTs.

A direct route to collaboration with CERTs would be to arrange key stakeholder meetings through our partners network and demonstrations to highlight the key capabilities of C3ISP. As CERTs also support critical national infrastructure organisations the initial market focus for C3ISP would also align with this objective.

## **Direct to End Customers**

As described above we will work via both direct and indirect routes to reach the end users of C3ISP, this will include both large enterprises and SMEs. To drive commercial interest and generate revenue for the platform, a key mechanism will be through the open C3ISP cloud platform. In 2017 a report published by ENISA encourages organisations to invest time on Proof of Concepts (PoC) with an open source TIPs prior to making any significant investment. This allows the users to better understand the benefits of the system and help develop a business case internally for making further investments. This recommendation forms an important component of our route to market strategy for end user, as the C3ISP platform will be made available as a cloud hosted free-to-access, testing, and development platform with access to limited functionality. The free to access service is their to onboard users quickly, to quickly demonstrate value and to reach the underlying ambition of increasing the adoption of cyber threat sharing to increase industrial resilience to cyber attacks. This means end users in our target markets will be able to use this as a PoC when required to better understand the benefits of the platform and how its use can be scaled across the organisation.

We will also seek opportunities to demonstrate the commercial value of C3ISP along supply chains in our target markets. By engaging with large infrastructure organisations, enterprises and tier 1 suppliers, we can highlight the benefits of C3ISP to the associated supply chains, improving the resilience of both the large enterprises and their suppliers. We will also reach end users through interaction and collaboration with sector-specific Information Sharing and Analysis Centers (ISACs). These centers comprise of a broad range of industry stakeholders and provide a central resource for gathering information on cyber threats and allow two-way sharing of information between the private and the public sectors. For example, EE-ISAC is an European ISAC created in 2015 that serves the energy sector. It is composed of 22 members (different organisations including utilities, vendors, academia and other stakeholders active in the energy sector). As EE-ISAC member organisations are already sharing information such as real-time security data, reports on security incidents and cyber breaches, exploring ways to enhance their current threat intelligence arrangements could be effective in increasing the profile and adoption of C3ISP.

## **Indirect routes to market**

### **ISPs**

Internet Service Providers are increasing under pressure to start sharing information about malicious softwares and websites on a larger scale. C3ISP consortium partner BT is the first telecommunications provider in the world to do so. The commercial incentive for ISPs for adopting the C3ISP platform is to ensure their customers are well protected. Part of the value we bring to ISP's is that C3ISP sharing of threat intelligence can mitigate several possible kinds of attacks as DDoS and cyber-squatting. Partnerships with ISPs are therefore important to both wider adoption of the C3ISP platform and as a commercial revenue stream for value-add modules and managed services.

## **Re-sellers (including members from our partners' ecosystem)**

As mentioned other than the direct routes to market the C3ISP exploitation strategy also includes indirect routes to market. Partnering with technology re-sellers is an effective way to expand the user base for C3ISP, as these re-sellers will have large existing client bases that can be tapped into. There is a growing number specialist cyber security providers that look to embed innovative products and services into an integrated cyber offering, and we can position C3ISP as a key feature of their service offerings that drives added value. Through the consortium's existing engagements with the ecosystem, we will reach out directly to companies we know who are actively seeking new partnership opportunities, for us to better understand how C3IPS can fit into their existing offerings, the size of their client base, and the sectors they are focusing in.

## **Marketplaces**

On the other side re-sellers there are passive websites and marketplaces which seeks to offer advice on different cyber security solutions and act as a central repository of available solutions and capabilities in the market. There is potential for the C3ISP platform to be presented on these marketplaces in two ways. The first is as a productised offering, focused on the value-add proprietary modules as the main product, with the open source platform bolted on as part of that product offering. This flexible model allows for different partners to demonstrate their capabilities through utilising C3ISP, while at the same time increasing the adoption of the C3ISP open source platform. The second way is to put managed services for the C3ISP as the key offering on the marketplace, allowing existing users/customers to access further support.

### ***1.3. Innovation Workshops***

The programme is structured as follows:

- 1) **Workshop #1 (UNDERSTAND):** Light-touch exploration of the market gap, understanding value, barriers for adoption and potential business models.
- 2) **Workshop #2 (VALIDATE):** Test assumptions with a view to refine the value proposition.
- 3) **Workshop #3 (VALIDATE):** Test assumptions with a view to refine business model and the commercial opportunity.
- 4) **Engagement Activities:** Engage with potential end users and demonstrate C3ISP at CyberTech in Rome in September 2019 to promote adoption of the C3ISP framework.

### 1.3.1. Workshop #1 – London March 2018

This section reports on the first innovation workshop titled “*Building a route to market for new cyber security technologies*” held at Digital Catapult Centre on 14 March 2018.

This was the first of a programme of three workshops and one engagement event. The Cyber 101 programme aims to investigate where the commercial opportunities of the C3ISP technology lie, define potential value propositions and business models and promote the adoption of the new cyber security technology. It also looks to bring together consortium partners and external organisations to discuss and understand market needs and discover ways to commercially exploit this R&D project.

This section is organised as follows. Section 1.3.1.1 describes some workshop preparation and planning information. Section 1.3.1.2 presents a description of the stakeholder engagement process while Section 1.3.1.3 presents the objectives, format and content of the workshop. Summing up, Section 1.3.1.4 and Section 1.3.1.5 discuss about outcomes and next steps, respectively.

#### 1.3.1.1. Preparation and planning for workshop #1

The C3ISP Innovation Workshop was designed and structured by Digital Catapult. The preparation lasted over 2 months and included collaboration across the Programme Delivery, Marketing and Communication and Technology departments.

The first part of this report summarises how the workshop was prepared and planned, indicating the various steps that allowed it to happen.

The preparation and planning included:

- Consultations with consortium partners to agree the day to run the workshop at Digital Catapult Centre, London.
- Consultations with consortium partners and Digital Catapult cyber security technologists to determine which potential external leads and companies to approach.
- Creation of a workshop outline with objectives and benefits of taking part. This went live on Digital Catapult’s Website and featured a responsive design that assured access and navigation on multiple devices (see Annex 2).
- Promotion of the workshop’s objectives, expected outcomes and the realisation thereof on social media channels like Twitter and LinkedIn, enhanced by involving the wider Digital Catapult network.
- Reaching out by email and phone to interested parties explaining C3ISP and the objectives of the workshop (see Annex 3 for list of approached companies).
- Shortlisting of external participants based on interests and alignment with C3ISP (see Annex 4 for list of delegates).
- Selection of the C3ISP consortium speakers.
- Consultation with consortium partners and Digital Catapult cyber security technologists to effectively design three group activities covering ‘**Identifying Market Needs and Value Propositions**’, ‘**Addressing Barriers**’ and ‘**Business Models**’.
- Creation of several documents used to conduct and evaluate the workshop.
- Hiring an illustrator and a videographer for the workshop.

Several documents were developed to conduct and evaluate the workshop. These documents include:

- Workshop Agenda (Annex 5).
- Table Plan (Annex 6).
- Worksheets Handouts (Annex 7).
- Rules of the road (Annex 8).

#### *1.3.1.2. Stakeholder engagement*

As part of the scouting process, Digital Catapult reached out to a number of stakeholders that could potentially become suppliers, buyers or key partners for the commercialisation of the technology. It also reached out to organisations that have a vested interest in Cyber Security either because they want to protect their assets, infrastructure or data, that already provide cyber security services, or that act on behalf of government (i.e., CERT or National Cyber Security Agency).

Selected organisations were shortlisted according to the following criteria:

- Ownership of sensitive data.
- Ownership of network infrastructure (Internet Service Provider).
- Ownership of sensitive assets.
- Understanding of the Cyber Security market in UK and Europe.
- Possession of a significant Cyber Security Budget or a provider of cyber security services.

See Annex 3 for list of approached stakeholders.

#### *1.3.1.3. Objectives, Format and Content*

##### Overall objective

The objective of the Innovation Workshop was to understand where the commercial opportunities of the C3ISP technology lie. The C3ISP Innovation Workshop successfully engaged with the consortium partners as well as external companies including big enterprises and small & medium-sized Enterprises (SMEs) to express opinion and stimulate the discussion around C3ISP commercial potential, opportunities and business models.

##### Particular objectives

- Understand market needs and value propositions for the sharing of threat intelligence.
- Identify barriers of adoption and ways to overcome them.
- Discuss possibilities for future business models.

##### Format

The workshop was held at Digital Catapult Centre, London. It was held under the Chatham House Rules to facilitate open and productive discussion (see Annex 8), with delegates spread across various tables in order to stimulate collaboration and engagement during the group activities.

##### Content and delivery

To tailor the workshop to the C3ISP needs and expected outcomes as well as ascertain the current state of the technology, the market competitiveness and the maturity of the project, Digital Catapult brainstormed and designed every activity with the support of the innovation services team, technologists and project managers involved in the project to. This phase has been additionally supported and further adjustments have been done thanks to the interviews run during the external delegates selections where the interviewed industry experts have effectively indicated key points to be covered and raised important aspects such as unique selling points or competitive advantage of the technology when measured against current commercial and privately-owned options.

Digital Catapult undertook an analysis of all the different contributions to the workshop design and came up with the following structure which included three presentations and three open-discussion-type activities as follows:

- *Presentation #1*: Introduction to Digital Catapult
- *Presentation #2*: Welcome note from British Telecom
- *Presentation #3*: Introduction to C3ISP
- *Open discussion #1*: Identifying Market Needs and Value Propositions
- *Open discussion #2*: Addressing Barriers
- *Open discussion #3*: Business Models

#### 1.3.1.4. *Outcomes*

The workshop has stimulated the discussion to better understand market needs, investigate possible ways to address barriers for adoption of the technology, as well as identifying possible business models and topics that need further research.

In particular, the discussion revealed the following:

#### Identifying Market Needs and Value Propositions

Through the first open discussion Digital Catapult wanted to understand how businesses share threat intelligence today. For that, we asked the following questions:

##### A. *What do they share (internally and externally)?*

- Shared log files, customer information, threat indicators, protocol details, geopolitical information, net flow data, malware information and disk images. This information is normally not shared externally in order to avoid reputation damages.
- Success and impact stories regarding, for example, identifying threats for selling products and services.
- Strategic elements regarding industry and platforms (technical aspects are not shared).
- Low level IOC (indicator of compromise), very high-level info.

##### B. *How is this intelligence shared?*

- The intelligence is shared through industry reports, platforms, services and community sharing (ISAC), industry bodies, government, one-to-one communications based on trusted relationships.
- Using STIX, MISP and IODEF.
- Intelligence shared through BT Zeon, using Honeypots to gather information.

##### C. *What are the available market solutions for sharing?*

- Available market solutions for sharing include BT Zeon, Virus Total, Threat Connect, NC4, VERIS, enhanced data analytics, blogs and platforms.
- BT and BAE use enhanced data analytics systems to improve the analysts' experience; e.g. Digital Shadow.
- Threat intelligence feeds (e.g., CISCO).

*D. What are the main opportunities of C3ISP to improve threat intelligence in your business?*

- There are different opportunities for C3ISP to improve threat intelligence depending on different sectors as well as different types of organisations. There is potential to interconnect and partner with existing solutions also from a technical perspective in order to understand how to facilitate and allow the analysis of the data in an effective and as automatic as possible way.
- Opportunity to interact with standardisation bodies.
- Inter-operate with existing standards or quasi-standards such as STIX and MISP.
- Opportunities include being aware of attacks the first day they occur, harden systems, better protect organisations within a supply chain, identify if a company is a potential target, share threat intelligence in a secure and controlled manner, reassurance that a company's data will not be used in an undesirable way through DSA.
- Understanding the impact and usefulness of sharing threat intelligence.
- Possibility to increase interoperability between existing solutions.
- Remove barriers for reporting breaches.
- Sharing information timely.
- Understand what companies are willing to share, and what not.
- Sector view (finance), mitigate risk to the sector.

Addressing Barriers

With the second open discussion Digital Catapult wanted to understand the main barriers that are obstructing the adoption of new cyber security technologies. For that, we asked the following questions:

*A. What are the main barriers that would prevent this technology from becoming more widely used?*

- Main data barriers include scalability, usability, data utility against data obfuscation, trust between parties, trust in the platform, legal compliance/barriers, willingness and fairness of data sharing, reputational damage and consequences.
- Other barriers include investment in other platforms, complexity in deployment, legislation and GDPR, maintenance cost or complexity, being overshadowed by competitors huge marketing budgets.

*B. In which ways could we overcome some of these barriers?*

- DSA scalability (big data processing, conflict resolution, storage, analytics) can be overcome by:
  - Horizontally scaling cloud architecture.
  - Policy harmonisation tool for conflict resolution.
  - Reconciliation strategy.

- DSA usability can be overcome by:
  - Subset of natural language used by domain experts.
  - Building domain specific language.
  - Integration of partners networks.
- Data utility against data obfuscation can be overcome by:
  - Fostering interaction between decision makers and data consumers to find the right balance or trade-offs.
  - Incentivisation to share clearer data (rating or reputation system).
  - Building trust in techniques, platforms, networks.
- Trust between parties can be overcome by:
  - Reciprocity.
  - Reputation scoring.
  - Federation, trust communities (external).
  - Governance/arbitration.
- Trust in the platform can be overcome by:
  - Privacy preserving techniques.
  - Security of platform.
  - Trust in operator/developer of platform.
  - Failover to an alternative system (if trust is lost).
- Legal compliance/barriers can be overcome by:
  - Guidance/capability.
  - Mapping of local privacy laws etc.
- Willingness and fairness of data sharing can be overcome by:
  - Creating value and making it higher than the cost of not participating, for example by making it a requirement to participate to public contracts.
- Reputational damage and consequences can be overcome by:
  - Engagement of big players as early adopters.
- Investment in competitors' platforms can be overcome by
  - Making it free or low cost with training and material.
  - Easy integration with other platforms and or data.
- Legislation and GDPR can be overcome by:
  - The platform being compliant with GDPR and similar legislations. It should also fulfil further GDPR requirements and NIS directive.
- Cost can be overcome by:
  - Open data support community.
  - Government contribution and central funding.

*C. Does enforcement of sanitisation measures like anonymisation and encryption give sufficient assurance to share threat intelligence?*

- Not yet, but the following could support the cause:
  - Building trust and adding features incrementally.
  - Use of best practices (e.g. anonymisation and differential privacy) would help quantifying risk.



- Certification by an external body.
- External verification of parts of the framework.
- Usage control to prevent data being accessed.
- Anonymisation and analytics don't go together.

### Business Models

With the third open discussion Digital Catapult wanted to understand what the main considerations are when thinking of potential business models to commercialise C3ISP. For that, we asked the following questions:

#### *A. How would customers procure a solution like C3ISP?*

- As a technical partner, licensing model (purchase for implementation, support, integration).
- Depends on what is being procured (buying CTI).
- Could be on an as-a-service offering.
- Free software/platform but with paid support (Red Hat).
- Could buy a subset of capabilities as needed by my organisation.
- SaaS, depends what the service can offer.
- Insurance package, subscription model.

#### *B. Could this be sold better as a stand-alone offer or as an add-on to existing products or services?*

- Auxiliary service.
- Both are possible.
- Could be packaged with SIEM offerings, sold to SOC.
- Would want to use C3ISP alongside existing products, needs to interface to these.
- Could give platform for free, the value is in the network, make C3ISP the key way to reach everybody.
- Pay to join and pay for contributions.
- Cyber-Insurance package.

#### *C. Who would be the key influencers in purchasing decisions?*

- Head of cyber defence, CISO, Chief Digital Officer, SOC, CERTs, customer of customer.
- The SOC owner.
- Government, might mandate sharing.
- End-user analysts.

#### *D. What incentives could be used to increase chance of purchase?*

- Early players adoption.
- Freemium model, reduce initial economical barriers and increase sign up process efficiency.
- Endorsement or adoption of market operation (standards, easy integration).

- Free demo, data sharing in huge end with branches in different jurisdictions (DSAs).
- Freemium open source route.
- Could be a “requirement” to bid for EU government contract.
- Exclusive access to content.
- Value added through automation of threat intelligence input, and the curation of this threat intelligence.
- Consortium model might reduce competitors concerns, may be supported by ISACs.
- Additional content as part of a platform.

Some of the discussions revealed that there is a need to better understand the 'product strategy' before taking decisions on business models. Also, for the consortium to better understand product strategy, there is the need to have further insight into the results of the pilot projects.

Also, during the workshop, attendees completed a short feedback form regarding their experience (<https://www.tfaforms.com/4664994>).

Results from this feedback form are shown in Annex 12 and the workshop illustration is in Annex 9.

#### *1.3.1.5. Next steps*

##### Pilot projects

- Implementation and testing phase 1 completed October 2018. Showcase of pilots in Brussels.
- Implementation and testing phase 2 complete by October 2019.

##### Workshops

- Workshop #2 - Aligned with end phase 1 (Oct 2018).
- Workshop #3 - Summer 2019.
- Engagement Event - Aligned with end phase 2 (Oct 2019).

#### **1.3.2. Workshop #2 – Pisa October 2018**

The second Innovation workshop was held in Pisa in October 2018. It has stimulated a successful internal discussion around market needs and early adopters of the technology from the different pilots' perspectives, as well as defining a common value proposition. In particular, through the first open discussion, the C3ISP consortium focused on understanding the main differences between potential clients in the early market and the mainstream market, their needs and the way the project can address them. On the second part of the workshop, the focus moved on understanding and defining the value proposition for C3ISP, the promise of value to be delivered.

##### *1.3.2.1. 1. Preparation and planning for workshop #2*

The C3ISP Innovation Workshop #2 was designed and structured by Digital Catapult. The preparation lasted over 2 months and included investigation with external stakeholders on commercial potential of C3ISP at Cybertech Europe 2018 in Rome as well as collaboration with consortium partners and different areas across Digital Catapult including Programme Delivery, Marketing and Communication and Technology.

The first part of this report summarises how the workshop was prepared and planned, indicating the various steps that allowed it to happen.

The preparation and planning included:

- Consultations with consortium partners to agree the day to run the workshop at the National Research Council, Pisa (Italy).
- Creation of a workshop outline with objectives and benefits. Investigation with external stakeholders on the commercial potential of C3ISP at the Cybertech Europe 2018 conference in Rome.
- Consultation with consortium partners and Digital Catapult cyber security technologists to effectively design two group activities covering ‘Early Adopter Identification’ and ‘Value Proposition’.
- Creation of several documents used to conduct and evaluate the workshop.

Several documents were developed to conduct and evaluate the workshop. These documents include:

- Workshop Agenda
- Table Plan
- Worksheets Hand outs

#### *1.3.2.2. 2. Commercial Investigation Process*

As part of the investigation process, Digital Catapult interviewed a number of stakeholders that could potentially become suppliers, buyers or key partners for the commercialisation of the technology. The investigation process has taken place in Rome at the Cybertech Europe 2018 where Digital Catapult shared a stand with other two Horizon 2020 projects: Shield and Protective. The participation of C3ISP at Cybertech Europe 2018 has permitted to showcase the four pilot projects and get feedback from a variety of industry and research representatives that demonstrated a vested interest in Cyber Security either because they want to protect their assets, infrastructure or data, already providing cyber security services, or act on behalf of government (i.e. CERT or National Cyber Security Agency).

The results of the questionnaires have been relevant and helpful for the Workshop #2 design and preparation. See Annex 15 for the report on the interviews.

The interviewees represented a variety of bodies and organisations in the cybertech industry, with expertise in the following areas:

- Ownership of sensitive data.
- Ownership of network infrastructure (Internet Service Provider).
- Ownership of sensitive assets.
- Understanding of the Cyber Security market in UK and Europe.
- Possession of a significant Cyber Security Budget or a provider of cyber security services.

Further investigation has taken place at the Internet Festival 2018 in Pisa on October 12<sup>th</sup>. See Annex 15 for interview report details.

### *1.3.2.3. 3. Objectives, Format and Content*

#### Overall objective

The overall objective of the Innovation Workshop #2 was to understand where the commercial opportunities of the C3ISP technology lie.

The C3ISP Innovation Workshop #2, designed after the commercial investigation run at Cybertech Europe 2018, successfully engaged with the consortium partners to express opinion and stimulate the discussion around C3ISP commercial potential, opportunities and value propositions.

#### Particular objectives

1. Understand and identify early adopters of C3ISP with a perspective from each pilot.
2. Identify customers' pains and gains.
3. Identify products and services that can satisfy customer needs.

#### Format

The workshop was held at the National Research Council, Pisa. It was delivered as part of a wider C3ISP project consortium meeting, concomitantly with the Internet Festival 2018. The delegates were spread across various tables in order to stimulate collaboration and engagement during the group activities.

## Content and delivery

To tailor the workshop to the C3ISP needs and expected outcomes as well as ascertain the current state of the technology, the market competitiveness and the maturity of the project, Digital Catapult brainstormed and designed every activity with the support of the innovation services team, technologists and project managers involved in the project. This phase has been additionally supported and further adjustments have been made thanks to the interviews run at Cybertech Europe 2018 where the interviewees from industry and research bodies have effectively indicated key points that were addressed. See Annex for the report on the interviews.

Digital Catapult undertook an analysis of all the different contributions to the workshop design and came up with the following structure which included three presentations and two open-discussions as follows:

- Presentation #1: Refresher from the previous workshop
- Presentation #2: Introduction to C3ISP from HPE
- Presentation #3: Crossing the Chasm - Customer Characterisation from Digital Catapult
- Open discussion #1: Customer Characterisation
- Open discussion #2: Value Proposition

### *1.3.2.4. 4. Outcomes*

The workshop has stimulated the discussion to better understand market needs, identify early adopters of the technology with the different pilot project perspectives, as well as define a potential value propositions.

In particular, the discussion revealed the following:

#### Customer Characterisation

Through the first open discussion Digital Catapult wanted to understand the main differences between potential clients in the early market and the mainstream market, their needs and the way we can address them. Every pilot group has defined early market and mainstream market characteristics.

##### *A. Enterprise*

- *Early Adopter Mindset:*  
Companies working in military, law enforcement, smart cities and utilities sectors

because they are technology leaders in their industries, they have budget allocated for innovative solutions and they tend to be employed in public services.

- *Mainstream Adopter Mindset:*

Companies in the banking, healthcare, shipping and transportation sectors that apply traditional business models and use legacy technology in their core business so they are more business oriented.

## B. SME

- *Early Adopter Mindset:*

Early adopters need to gain more customers before taking advantage of C3ISP potential. Early adopters can encounter problems and don't necessarily have ready solutions to apply. Early adopters can pay on the usage to limit the use of resources.

- *Mainstream Adopter Mindset:*

Mainstream adopters rely on their markets and have guarantees in terms of customers. Mainstream adopters address problems with more experience but can also afford to use more resources.

## C. CERT

- *Early Adopter Mindset:*

Companies like the Italian telecommunication since we already have 3 of them in the pilot and probably are going to be the first users of C3ISP. Also, CERT in Italy is a public organisation, part of economic development ministry which means easy reach to bank industry. Insurance companies could be early adopters as well.

- *Mainstream Adopter Mindset:*

The use of C3ISP will probably need to be forced for entities like public administrations, considering that they will need to be forced also to use specific security standards. Large manufacturing companies may become natural adopters in the future.

## D. ISP

- *Early Adopter Mindset:*

Italian service providers and small companies without great security systems. ISPs companies that do security but not enough, ISPs that outsource all or part of security protections, ISPs that want to increase security for their partners and ISPs that want to protect confidentiality data, in compliance with GDPR..

- *Mainstream Adopter Mindset:*

Large ISPs as they already do similar things internally and they tend not to integrate anything to their internal systems.

## Value Proposition

With the second open discussion Digital Catapult wanted to understand and define the value proposition for C3ISP, the promise of value to be delivered. Every pilot group have first identified an early adopter, its pains and gains and finally defined products and services that can satisfy customer needs. The aspects analysed were:

- Customer Jobs: a description of what the targeted customers are trying to do including tasks they are trying to perform and complete, problems they are trying to solve or needs they are trying to satisfy.
- Customer Pains: a description of negative emotions, undesired costs and situations and risks that the targeted customers experience or could experience, before, during and after getting the job done.
- Customer Gains: a description of the benefits the targeted customers expect, desire or would be surprised by, including functional utility, social gains, positive emotions and cost savings.
- Product & Services: a list of all the features, products and services the value proposition is built around.
- Pain Relievers: an outline of how the products and services create value, how they alleviate customer pains, how they eliminate or reduce negative emotions, undesired costs and situations and risks the customer could experience before, during and after getting the job done.
- Gain Creators: a description of how the products and services described create customer gains including benefits the customer expects, desires or would be surprised by such as functional utility, social gains, positive emotions and cost savings.

### *A. Enterprise*

Customer: Company working in the military industry

- Customer Jobs:
  - National security
  - Social power and status
  - National interests to protect
  - Social assurance
  - Safety awareness.
- Customer Pains:
  - Cyber warfare awareness
  - Intel cathering live analysis
  - Damage recovery
  - Reputation losses.
- Customer Gains:
  - Efficiency and effectiveness in situational awareness for cyber defense
  - Improved information analysis and efficiency
  - Be one step ahead to discover ongoing attacks

- Demonstrate measurable and tangible improvement in situation awareness.
- Product and services:
  - Monitor and analysis of virtual assets
  - Solution to aggregate CTI of different origins with different disclosure profiles and analyse them effectively
- Pain relievers
  - Focused investigations on incidents involving assets
  - Focus on critical threats for critical assets (prioritisation)
  - Awareness of ongoing attacks
- Gain creators
  - Early detection may lead to a deterrent effect
  - Reputation gain to improved efficiency
  - Money and effort gain from better reactions to attacks

## *B. CERT*

Customer: Not specified (Italian telecommunication)

- Customer Jobs:
  - Keeping service availability
  - Protecting data privacy of employees
  - Gaining competitive advantage
  - Selling their reliability
- Customer Pains:
  - Having a dedicated SOC
  - Authorising and security best practices
  - Hiring dedicated people
  - Lack of authorised CTI analysis
  - Software and hardware update/upgrade
- Customer Gains:
  - Saving recovery costs
  - Actually being moved by a relevant cyber-attack
  - Increasing members of active controlling
  - Further threat recognition
  - Increasing privacy and accuracy
- Product and services:
  - Cloud infrastructure
- Pain relievers:
  - Prevent reputation loss
  - Prevent customer migration to competitors
  - Reducing insurance costs
- Gain creators:
  - Future update of best practices and procedures for defending against specific cyber-attack



### C. SME

Customer: GPS Case

- Customer Jobs:
  - Software as a service monitoring utility energy consumption
  - Maintain power/uptime of utility
  - Make customers have more confidence towards provider
  - Show customers more secure equipment/system
- Customer Pains:
  - Too costly to develop secure software in-house
  - Trade-off between technical presentation and user friendliness of utility data
  - Lose market occupation
- Customer Gains:
  - Avoid churn, avoid existing end-users leaving for other providers
  - User friendly
  - Secure personal data
  - Regulation compliance
  - Less investment and lower risk
  - Demonstrate social responsibility to public
- Product and services:
  - Display utilities data eg. smart meters in a secure way via C3ISP
  - Digital service (saas)
- Pain relievers
  - Save time for customers to implement security solution by buying complete software package. Also save costs.
  - C3ISP analysis results help mitigate risks by more proactively handling threat information
- Gain creators
  - Statistics on data to help customers produce marketing plan, based on C3ISP project in order to anonymise private user data
  - Secure cyber-physical utility infrastructure

### D. Internet Service Provider (ISP)

Customer: Not specified

- Customer Jobs:
  - Vulnerability assessment
  - Data confidentiality
  - Discover new security issues, attacks
  - Looking at its customers
  - Providing security guarantees
  - Stable and robust systems against attacks
- Customer Pains:

- Not quick enough
- Loss of face and reputation
- Malfunctioning
- Financial
- Difficulties in increasing user awareness
- Customer Gains:
  - Save effort
  - Save money and time
  - Increase of users
  - Being more robust against attacks
  - Increase reputation and credibility
  - Being more reactive when vulnerabilities are found
  - Better service provided
- Product and services:
  - Robust solutions
  - Adaptive solutions
  - Update regularly
  - Assurance of confidentiality and privacy preventions
  - Cutting edge innovation and solution
- Pain relievers
  - Providing more security, confidentiality and privacy in the treatment of customers' data
  - Provide securing solutions to customers in a unique and integrated way
  - Open source solutions
- Gain creators
  - Improve customers' reputation
  - Improve customers' compliance with respect to law
  - Save customers' money
  - Fully adaptive and integrated solution
  - Save money and time

Some of the discussions revealed that there is a need to better understand the 'product strategy' before taking decisions on business models. Also, for the consortium to better understand product strategy, there is the need to have further insight into the results of the pilot projects. These topics will be explored in the upcoming consortium activities.

### **1.3.3. Workshop #3 – Pisa April 2019**

The third Innovation workshop was held in Pisa in 2019. The third workshop for the C3ISP programme for exploitation focused on two areas:

- Proprietary vs open source exploitation opportunities

- Individual organisational alignment with a given exploitation strategy

These two areas were identified as key concerns for discussion as a result of the review of the initial exploitation plans proposed by consortium members and as a result of the previous two workshops. Initial exploitation plans highlight the differing needs of the research focused organisations and the commercially focused organisations, predominantly to do with open source vs proprietary concerns.

The workshop sought to identify key areas of focus for the go-to-market strategy and help us shape the business model for the platform and associated components of C3ISP.

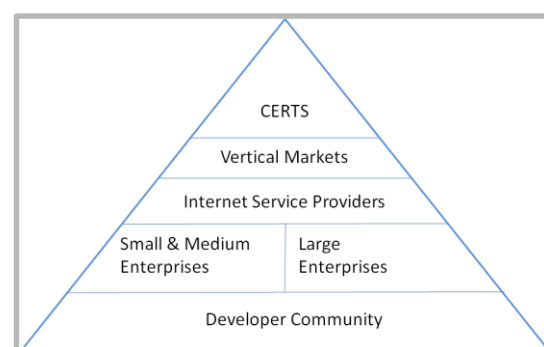
Digital Catapult conducted a two part workshop to first draw out the positive and negative impacts of various proprietary and open source approaches. Considering both extreme cases (totally open source, totally proprietary) and stepped approaches, with some elements proprietary and others open source.

The second part of the workshop based on a Harvard Business School article about 3M's approach to innovation (catalogued by *George Day*, December 2007 Issue) drew out the individual talents of the organisations and their alignment with the technology and the markets we are looking to apply the technology.

#### 1.3.3.1. Workshop #3 Conclusions

Through this workshop we have been able to gather a variety of results and an evidence base, which once reviewed has given us insights into the core ambitions of consortium members. We have also drawn on the experience of the members in both commercial environments and developer led environments as well as research environments. Key conclusion points:

- Although it is likely to increase complexity, in order to conform with the desires of the consortium and to reach the initial broad audience required to encourage adoption, a combined open source and proprietary approach will be the key focus
- Industry vertical focus will take president over the productised approach to ensure we produce solutions with specific customers in mind
- The larger commercially led organisations will be supported to build internal business cases for their own commercial teams to allow us to understand the ambition of these organisations to invest further in C3ISP
- Consideration will be given to the priority of the potential customers to enable wide scale adoption, who do we target early on and who is most able to influence the wider ecosystem, an initial hypothesis is illustrated here, the pyramid represents those with the most ecosystem influence over those with the least and this will be explored further through desk research
- Messaging going forward should be targeted to the markets which we are going to prioritise. The key concerns of the consortium are likely reflected in the market and the key words identified will be used within the messaging to different communities



Details of workshop 3 are provided in Annex 16

#### **1.3.4. Promotional activities**

Digital Catapult has promoted and disseminated the Workshop “*Building a route to market for new cyber security technologies*” through different communication channels:

- A promotional open call registration page for the event has been created on Digital Catapult website (see Annex 2).
- Promoted on social media channels and shared with approached stakeholders (see Annex 3).
- An informative C3ISP brochure has been created to better brief and inform external stakeholders (see Annex 10).
- During the workshop, Digital Catapult has retweeted C3ISP tweets from C3ISP official Twitter page (see Annex 11) to disseminate and communicate the event within the Digital Catapult ecosystem. The tweet reached various industries including data security, European institutions, media and research, technology blog and advertising, information technology.

A professional video maker has recorded shots of the workshops and performed interviews to participants and partners for promotional matters. The video is available on the C3ISP web page.

#### **1.4. Industry state of the art**

This section provides a summary and analysis of the state of the art of the industrial markets related to the C3ISP project.

It seeks to partition the industrial markets that are relevant to C3ISP exploitation to classify potential market sectors and stakeholders who could benefit commercially from the outcomes of C3ISP.

In the following sections, we consider two market areas:

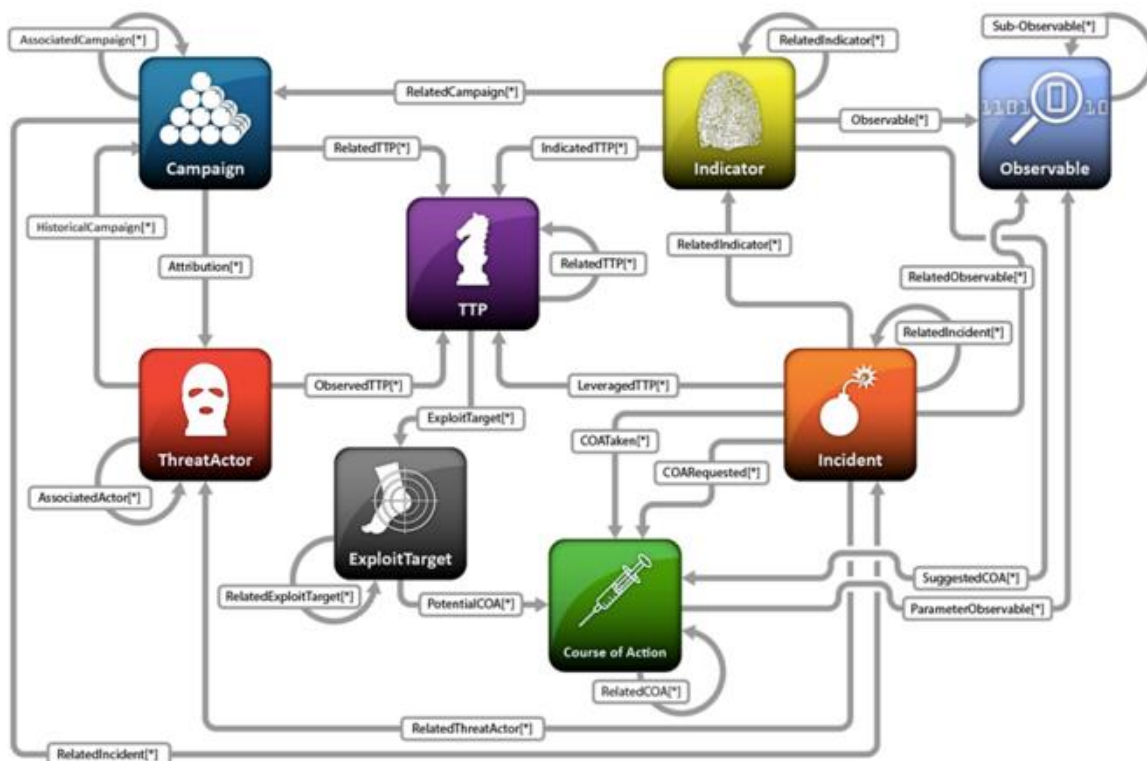
- Threat intelligence providers who would principally leverage (and interface with) propositions based on C3ISP outcomes
- Those reacting to threat intelligence – and in particular dealing with incidents – where C3ISP outcomes are expected to be especially valuable, and more deeply embedded in their operations.

Also in this section we include a summary of the C3ISP competitive landscape of Threat Intelligence Sharing Platforms as it stands today in 2019.

##### **1.4.1. Threat intelligence market context**

Interfacing with the threat intelligence market is key to achieving customer value. Therefore, we base the analysis on Structured Threat Information Expression (STIX™) [1], which is a language and serialization format that enables organizations to share cyber threat intelligence (CTI) with one another in a consistent and machine-readable manner. Figure 6 shows the architecture of the STIX language as a graph. It identifies the principal types of data object,

which are shown in the rectangular nodes, and the types of activity, which are denoted by the directed edges.



**Figure 6: STIX language architecture ([2]).**

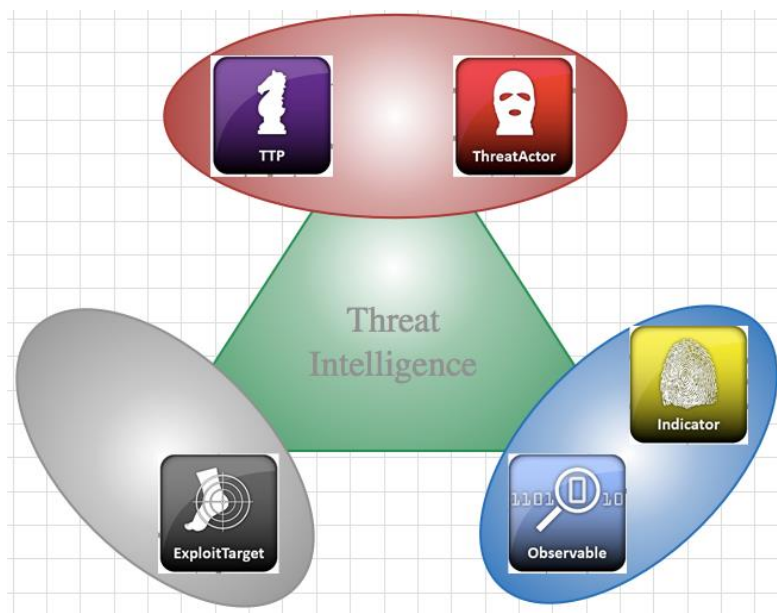
The threat intelligence market has three primary segments: *threat intelligence providers*, the modern *defences that consume threat intelligence* to identify and block targeted attacks, and *threat intelligence platforms (TIP)* which aggregate and collate threat intelligence.

The C3ISP project is primarily positioned as a contributing to the TIP market: its offerings must exist appropriately in the context of both threat intelligence providers and security products that consume threat intelligence.

### 1.4.2. Threat intelligence providers

It is appropriate to consider the industrial threat intelligence provider market in terms of three main classes. Figure 7 shows a partitioning in terms of the STIX data objects.

Each ellipse shows a type of intelligence that helps deal with an incident: *adversary intelligence*, and *vulnerability intelligence*, which together help assess risks; and *evidence* associated with a specific exploit. The central triangle shows the activities associated with responding to an exploit. We consider the market for each separately.



**Figure 7: Partitioning of the threat intelligence market by STIX objects.**

#### 1.4.2.1. Adversary intelligence

The red ellipse denotes the dangers posed a *Threat Actor* (TA) and the adversary’s *Tactics, Techniques and Procedures* (TTP).

Threat Actor research firms, such as Intel 471, FlashPoint Security, Cyveillance and iSIGHT Partners (acquired by FireEye), deploy expert analysts to track particular cyber criminals, hacktivist groups, or teams associated with nation state cyber espionage. They generate primarily research reports that contain detailed descriptions of the threat actors, including their TTP.

Several vendors sell subscriptions to reports that outline TTPs or publish intelligence of the TTP on the DarkWeb. This is particularly important, especially for TAs that are motivated by financial gain and are part of a ‘dark’ ecosystem that distributes and scales distinct aspects of their illegal activities.

#### 1.4.2.2. Vulnerability intelligence

The grey ellipse in Figure denotes the *ExploitTarget* (ET) – vulnerability intelligence, which a TA could use to compromise a system. An *ExploitTarget* is a vulnerability or weakness in software, systems, networks or configurations that is targeted for exploitation by the TTP of a *ThreatActor* [3].

A vulnerability database is a platform aimed at collecting, maintaining, and disseminating information about discovered vulnerabilities. As well as identifying and characterizing a vulnerability, the database will typically contain analysis of the vulnerability and information about how to desist an attacker.

Major vulnerability databases such as the Open Source Vulnerability Database (OSVDB) and National Vulnerability Database U.S (NVD) publish Common Vulnerabilities and Exposures (CVEs), which provide unique identification names, numbers and intelligence on specific *ExploitTargets*, primarily to facilitate sharing of critical patches and debugging information.

Vulnerability databases add to the CVE intelligence as the investigation of a vulnerability unfolds, and provide vulnerability scores, impact ratings and the requisite workaround. CVE

is paramount for linking vulnerability databases so critical patches and debugs can be shared to inhibit hackers from accessing sensitive information on private systems [4].

The OSVDB was founded in August 2002 and was launched in March 2004. It catalogues over 121,000 vulnerabilities spanning a 113-year period [5].

The National Vulnerability Database [6], formed in 2005, is a primary cyber security referral tool for individuals and industries alike providing informative resources on current vulnerabilities, and holds in excess of 50,000 records and publishes 13 new entries daily on average

#### 1.4.2.3. *Indicators and Observables*

The blue ellipse in Figure denotes the discrete *Observables* (Obs) that are manifested during an exploit, and associated *Indicators* (Inds), which are patterns of such Observables. Examples include of Indicators of Compromise (IoC), reputation of IP addresses and domain names, file finger prints, for example that help identify components of malware.

Internet Service Providers (ISPs) have differentiated themselves by offering reputation services for IP addresses and Internet domains, and Cisco, Tipping Point (HP), Corero, and McAfee (Intel) have incorporated IP reputation into their products, for example to enable blocking. Stand-alone IP reputation services also offer raw feeds of IP addresses scored on a risk scale.

Managed Security Service Providers (MSSPs) such as AT&T Network Security, BT, Dell SecureWorks, IBM Corp, Symantec, NTT Solutionary, and TrustWave, collect security event information (Observables) from their customers, so they are able to correlate and scrub that data, and often provide those feeds to customers.

Providers like ThreatGrid (acquired by Cisco) and LastLine spin up thousands of virtual machines—sandboxes and instrument them to extract IoC for malware which can include: source IP address, Command and Control (C&C) IP addresses (e.g. of Botnets), MD5 hashes of malware payload and its constituent parts.

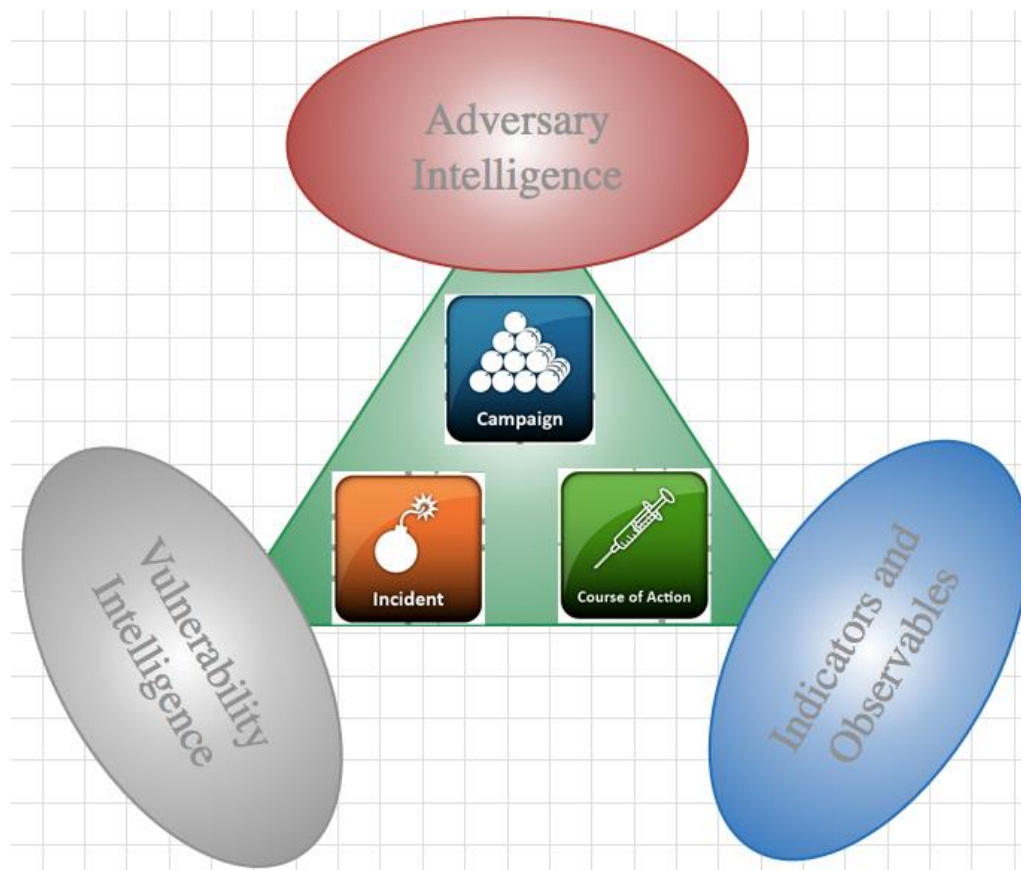
Vendors such as BrandProtect, Digital Shadows, and Recorded Future offer brand protection services that attempt to identify when a customer is being targeted or potentially the early planning stages of an attack.

#### 1.4.2.4. *Market development*

There has been significant disruption in the space of late. For examples FireEye acquired iSIGHT, IID sold to InfoBlox, LookingGlass acquired Cyveillance. And there have been new startups, including ACID Technologies, Comilion, Cyberint, Cyfort Security, Intsights, Sixgill, and Vigilance Networks [7]. This is representative of an early market that is still refining its capabilities and how they are bundled. There is also evidence of new technologies, products and services being acquired by mature market players as the market need becomes established and those new capabilities prove themselves.

### 1.4.3. **Reacting to threat intelligence**

Reacting to threat intelligence – especially in the context of dealing with a specific incident, is where C3ISP outcomes are expected to offer greatest customer value. Figure 8 shows the STIX entities that are associated with reacting to the various classes of threat intelligence that are considered above.



**Figure 8: Reacting to threat intelligence.**

The green triangle in Figure 8 denotes reaction to an incident, which comprises recognising an *Incident* (Inc) that describes an adversary’s actions, responding with a *Course of Action* (CoA) to an attack or taking preventative measures. The response may be conducted in the context of a *Campaign* (Cam), which describes a set of incidents and/or TTPs with a shared intent.

A CoA may also result from the process of risk management, which takes information from one or more threat intelligence capabilities, and applies them to the specific environment and operational requirements.

#### 1.4.3.1. Manual reaction

Traditionally, reacting has been a predominantly manual process, but increasingly the process has become automated.

For example, LookingGlass sends customized threat-related email alerts, and provides custom threat intelligence services and reports for executive security and brand security, as well as analyst support [8].

#### 1.4.3.2. Direct integration

Various products offer integration of threat intelligence feeds with security controls, but currently these are predominantly proprietary, and typically accept only a single type of intelligence feed.

For example, rather than requiring customers to download and handle data feeds, McAfee integrates reputation information from its cloud-based McAfee Global Threat Intelligence for files, web, web categorization, messages, network connections and certificates. These



reputation services are enabled by default in many Intel Security products, including McAfee Threat Intelligence Exchange [8].

Feeds from Infoblox may be used with the Infoblox DNS Firewall or a customer's security equipment; RSA and Verisign may be used only with a proprietary or limited number of third-party security systems [8].

Some regard RSA Live data as a key differentiator in the industry [8]. RSA Live data is converted into clickable metadata, enabling open source and other intelligence to be merged with a customer's data, making it more valuable. However, because RSA Live is integrated with the RSA NetWitness Suite, customers must have NetWitness Suite to access RSA Live data feeds [8].

#### *1.4.3.3. Threat intelligence platforms*

Threat Intelligence Platforms (TIPs) aggregate and analyse multiple threat intelligence feeds and may also make their results available directly to security enforcement tools.

The software and services coming from emerging players such as ThreatConnect, ThreatQuotient, and ThreatStream seek to aggregate and correlate threat data. They also offer a single portal for analyzing data not only from commercial providers, but from open-source threat data providers such as US-CERT [9]. This helps enterprises speed the process of digging out the relevant indicators of compromise [9].

#### *1.4.3.4. Open Source intelligence integration and sharing*

A number of Open Source Intelligence Libraries have begun to gain popularity offering the promise of more organized storage of the observables and an improved context around alerts [10]. Typically, they allow input in various formats, and their outputs can facilitate sharing and integration with downstream security capabilities.

The Collective Intelligence Framework (CIF) [11] helps ingesting IP addresses and domain names, with some support for hashes (for example of software components), and can output this information into multiple formats and integrate with various tools including Snort, Bro, Bind, TippingPoint, and Elsa.

Developed by REN-ISAC [12] (the Research Educational Networking Information Sharing and Analysis Center) the CIF platform is written in Perl, stores the observables in PostgreSQL, and provides web API as well as Chrome and Firefox extensions.

In 2013, MITRE Corporation offered its Collaborative Research into Threats (CRITs) threat intelligence library free of charge, with some legal restrictions [13]. CRITs integrates with TAXII servers to facilitate sharing intelligence, and allows manual input of STIX files, as well as domains, IPs, samples, emails, and other indicators, and will allow to output CSV, STIX, and JSON. One can adjust the confidence and impact of the indicators through the extensive REST API, so defenders can create multiple dynamic lists to update downstream specific systems.

Siemens open-sourced Mantis in 2013 [14]. It can import and process most of the current high language formats (IODEF, openIOC, STIX).

NATO's Malware Information Sharing Platform (MISP) was developed to help track and analyze rare malware [15][16]. It integrates with ArcSight, IDS (Snort), various sources (importing and exporting openIOC), GFI Sandbox, as well as XML, CSV, and a RESTful API. MISP federation allows for sharing.

#### 1.4.3.5. *Sharing intelligence*

With the increased availability of aggregating and analysing capabilities, together with some standardisation of data formats, intelligence sharing has been growing.

Open Source Collective Intelligence Framework provides a Federation Service that allows sharing among different CIF instances.

Startup TruStar promises to advance the security information sharing process by providing the means to anonymously report and share threat and breach data across enterprises, and potentially entire industries[17].

#### 1.4.3.6. *Shared incident response*

A Computer Security Incident Response Team (CSIRT) provides capabilities to consolidate management of *Incidents*, including recommending Course of Action. A CSIRT are also know as Computer Emergence Response Team (CERT), or a Computer Emergency Readiness Team.

The CERT division of the Software Engineering Institute (SEI) at Carnegie Mellon University has the mission to help organizations and national CSIRTs develop, operate, and improve their incident management capabilities, supporting the development of an international response team community by helping organizations develop, operate, and improve incident management capabilities. It has been instrumental in building a network of more than 50 national CSIRTs [18], and it maintains a list of list more than a hundred CSIRTs that have responsibility for an economy or a country [19].

For example, the Italian CERT, which is located at the Italian Ministry of Economic Development, is contributing to one of the C3ISP project pilots. They are the main reference point at the national level for the prevention and countermeasures against cybersecurity attacks. The Italian CERT currently exchanges information concerning incidents and threats with the major Internet Service Providers (ISPs) operating at national level.

For example, the UK national computer emergency response team, CERT-UK was announced in the 2012 report [20] on the 2011 HMG Cyber Security Strategy, publicly launched on 31 March 2014 [21] and closed in October 2016, when its functions were transferred to the National Cyber Security Centre (NCSC) which opened in October 2016 and is part of GCHQ [22].

There are instances of sharing across industry sectors too. For example, Avalanche emerged from the Financial Services Information Sharing and Analysis Center (FS-ISAC), which created a common platform to share. It was originally designed to facilitate sharing of indicators of compromise between the member organizations, but has been making inroads in other information sharing groups [22]. Starting as a free model, it now a quasi-commercial product supported by Soltra [24].

The Janet CSIRT supports UK universities in \*.ac.uk domain [25], and the CareCERT seeks to protect health and social care systems associated with the UK National Health Service (NHS) [26].

#### 1.4.3.7. *Sharing wider information*

Due to a widespread skill shortage in cyber security, a number of bodies have emerged to share more general security information than CERTS.

For example, started in October 2012 as a European project by 17 organisations from industry and research, the aim of the European CyberSpace Protection Alliance

Alliance (CYSPA) is to increase the capacity of industry to protect itself from cyber disruptions [27]. The strategy brought together EU stakeholders working together to articulate, embody and deliver the concrete actions needed to reduce cyber disruption.

CyberConnector is the online space open to private organisations, public administrations, Computer Emergency Response Teams (CERTs), law-enforcement agencies (LEAs) and individuals to create and enhance collective knowledge to improve cyber-security [28]. Hosting different communities focusing on the fight against botnets, cyber-risks assessment, social vulnerability assessments and more, CyberConnector hosts communities focusing on detecting and mitigating botnets, assessing cyber-risks, identifying needs in fighting cyber-terrorism and on-going collaborative European projects.

More specifically, the European Advanced Cyber Defence Centre (ACDA) [29] is a Horizon 2020 collaborative project building on an EU wide sharing of data consolidated in a clearing house, ACDC delivers solutions and creates a pool of knowledge to help organisations across Europe fight botnets.

Dogana is an advanced social engineering and vulnerability assessment framework – social-driven vulnerability assessment (SDVA) framework.

At a state level, the National Cyber Security Centre (NCSC) [30] is the UK's authority on cyber security, and also brings together and replaces CESG (the information security arm of GCHQ), the Centre for Cyber Assessment (CCA), and the cyber-related responsibilities of the Centre for the Protection of National Infrastructure (CPNI) [31].

ISPs also provide a key role in responding to incidents. For example, Registro.it is the Italian registration authority for Internet, handling registration requests and maintenance for each domain with .it extension. Being a registration authority, Registro.it receives registration requests and information from all the Italian Registrars (1400, most of them also act as Internet Service Providers – ISPs), which directly interact with the domain users (Registrants), offering also hosting services.

Registrars keeps important information about the Registrants and the domains, including connection and access logs. Registrars share this information directly with Registro.it when requested. Such an access is generally triggered by request from law enforcement authorities or external domain name authorities such as ICANN. Registrar-owned information are vital in detecting cybercrimes such as Domain Hijacking (i.e. impersonation of a domain owner with the aim of stealing a domain name and related services) or Cybersquatting (i.e. illegal appropriation of an unassigned or recently expired domain name with the aim of illegal exploitation). Moreover, access logs to specific domain names, may be useful in identifying Distributed Denial of Service (DDoS) attacks. Registrars are bound by regulations to preserve the privacy of stored data, thus, unless the disclosure is not required by law enforcement authorities the analysis of data performed by a third party is generally not viable.

#### *1.4.3.8. Market challenges*

Independent security researchers Ponemon reported in July 2016 on the benefits of threat intelligence and the challenges companies face when integrating threat intelligence with existing security platforms and technologies [32].

---

<sup>1</sup> <https://cyberconnector.eu/>

The findings are from 1072 survey responses from a high-quality network of industry stakeholders, across a wide range of market sectors: financial services (17 percent of respondents), public sector (11 percent of respondents), and health and pharmaceutical (10 percent of respondents).

60 percent of the respondents' organizations are located in North America, and 27 percent are in Europe. 69 percent of the respondents are from organizations with a global headcount of more than 1,000 employees. 12 percent operate in only one country.

Fifty-seven percent of respondents say threat intelligence drives decision-making within their organizations' security operations center (SOC). The primary users of threat intelligence are security leaders (81 percent of respondents), incident response teams (79 percent of respondents), IT leaders (59 percent of respondents) and IT operations (57 percent of respondents).

An average of almost 10 threat intelligence feeds are used in the organizations represented in this study. Companies are mostly using paid threat intelligence feeds (39 percent of respondents), open source (free) (28 percent of respondents) or a combination of feeds (33 percent of respondents). Forty-six percent of respondents believe paid feeds provide more actionable intelligence than free sources of threat data.

However, only 27 percent of respondents believe their organizations are very effective in utilizing threat data to pinpoint cyber threats. Reasons for ineffectiveness are: lack of staff expertise (69 percent of respondents), lack of ownership (58 percent of respondents) and lack of suitable technologies (52 percent of respondents).

Seventy percent of respondents say threat intelligence is often too voluminous and/or complex to provide actionable intelligence. As a consequence, 52 percent of respondents believe their companies need a qualified threat analyst to maximize the value of threat intelligence and such complexity may be preventing the use of threat data, since less than half (46 percent) of respondents say incident responders use threat data when deciding how to respond to threats.

Sixty-four percent of respondents believe the integration of a threat intelligence platform with other security technologies or tools is a difficult and time-consuming task. A similar percentage (62 percent of respondents) says SIEM integration is necessary to maximize the value of threat intelligence data.

Organizations mostly integrate threat intelligence into are Security Information and Event Management (SIEM) (52 percent of respondents), Intrusion Detection/Prevention Systems (IDS/IPSs) (49 percent of respondents), and firewalls (46 percent of respondents). Fifty-nine percent say such integration was very difficult (27 percent of respondents) or difficult (32 percent of respondents).

Fifty-six percent of respondents say their companies do not use standardized communication protocols. If they do, it is most likely unstructured PDFs or CSVs (59 percent of respondents) or TAXII/STIX/CyBox (48 percent of respondents).

#### *1.4.3.9. Managed Security Service Providers*

Managed Security Service Providers (MSSPs) can help their enterprise and SME customers by addressing barriers such as lack of staff expertise and lack of suitable technologies.

For example, BT offers its customers a Managed Security Service (MSS) in form of the BT Intelligent Protection Service (IPS) [33], a security solution that offers a holistic improvement to the way security policies for core security components like firewalls,

intrusion detection / prevention systems, malware scanning and integrity monitoring are provisioned and managed. IPS simplifies the way security policies are managed through a single, multi-tenant management portal that can be used by the customers to operate and monitor security services that are deployed on their VMs hosted in multiple cloud environments.

Using a MSS that is coupled with cloud hosting can ease data integration challenges, and partially delegate the integration of a threat intelligence platform with other security technologies or, at least in those deployments in the cloud.

However, the main limitation of the current BT MSS system is that the customers have to monitor any security notifications, alerts or events (CTI) being generated themselves, and that they are also responsible for the analysis of these security events and the undertaking of actions required to mitigate or eliminate them.

Also storage and analysis of data belonging to different customers is strictly segregated as it contains sensitive information; the customer trusts the MSS provider (MSSP), but not other customers, who may, for example be competitors. This strict segregation means that valuable additional intelligence that could be derived from analyzing pooled information across multiple customers is not currently available.

We have seen this reflected in the survey findings, where there appears to be a desire to increase the effectiveness of CTI, in particular making it less voluminous and complex, so that it is easier to action.

#### **1.4.4. C3ISP Competitive Landscape - Threat Intelligence Sharing platforms**

The “intelligence” provided by the majority of threat intelligence sharing platforms does not constitute “intelligence” in the traditional sense. In the context of information security “intelligence” is the product of the intelligence lifecycle model, which includes several activities like planning, data collection, analysis and, dissemination.

About three years ago, the majority of tools primarily focused on data collection and more or less neglected the other activities of the intelligence lifecycle. Therefore, those earlier threat intelligence platforms resemble data warehouses more than “real” intelligence sharing platforms.

Moreover, they provided limited analysis and visualization capabilities and lagged behind comparable knowledge sharing platforms and data mining solutions from other domains.

Today many Threat Intelligence Sharing platforms continue to only provide basic analysis capabilities, such as browsing, attribute based filtering and searching of information.

Additionally, only a small fraction of platforms implement pivot functionalities which enable the visualization of relationships between the threat intelligence constructs.

Today there are also many strong threat sharing platforms on the market that compete with C3ISP.

Some platforms, like IBM’s X-Force Exchange; the Malware Information Sharing Project (MISP) and Facebook’s ThreatExchange have evolved from architectures more akin to social networks. (Pricing of IBM X-Force Exchange <https://www.ibm.com/uk-en/marketplace/threat-intelligence-api/purchase#product-header-top>)

We need to focus on those competitors to C3ISP that cover the full four stages of the Threat Intelligence Life cycle. There are many for example that are strong on data collection but not much else.

In researching the competitive landscape for the exploitation of the C3ISP platform we have exploited some recent work in Australia. The results show a strong competitive landscape!

April 2019 - The Australian Cyber Security Centre (ACSC) has provisionally shortlisted half a dozen potential platforms that could make it easier to exchange threat intelligence with its partners. *Note: ACSC is the Australian equivalent of our UK NCSC*

<https://www.itnews.com.au/news/acsc-to-replace-cyber-threat-sharing-platform-518653>

The ACSC in early 2019 contacted six vendors that provide cyber threat intelligence platforms, inviting them to participate in a formal request for information process. Those vendors were identified after a market scan, but the centre has indicated it is open to rolling out other solutions — although its preference, documents released by the ACSC state, is for a commercial off-the-shelf (COTS) product.

The centre said it plans to invest in a platform that allows it to monitor threat intelligence from local and global sources, including CERTs.

“The solution will enable ACSC Partners to automatically receive threat intelligence, consisting of context-rich, actionable and timely information in a variety of formats, including advisories and automated indicator sharing,” a document issued by the ACSC states.

During the process, the centre assessed 10 platforms. The ACSC has provisionally assessed Anomali’s Threat Stream, Eclectic IQ, ThreatConnect’s TC Complete, NC4’s Soltra Edge, ThreatQuotient’s ThreatQ and TruSTAR’s Threat Intelligence as likely to meet its needs. The other platforms considered were IBM’s Qradar, FireEye, New Context, and ScoutPrime from Looking Glass.

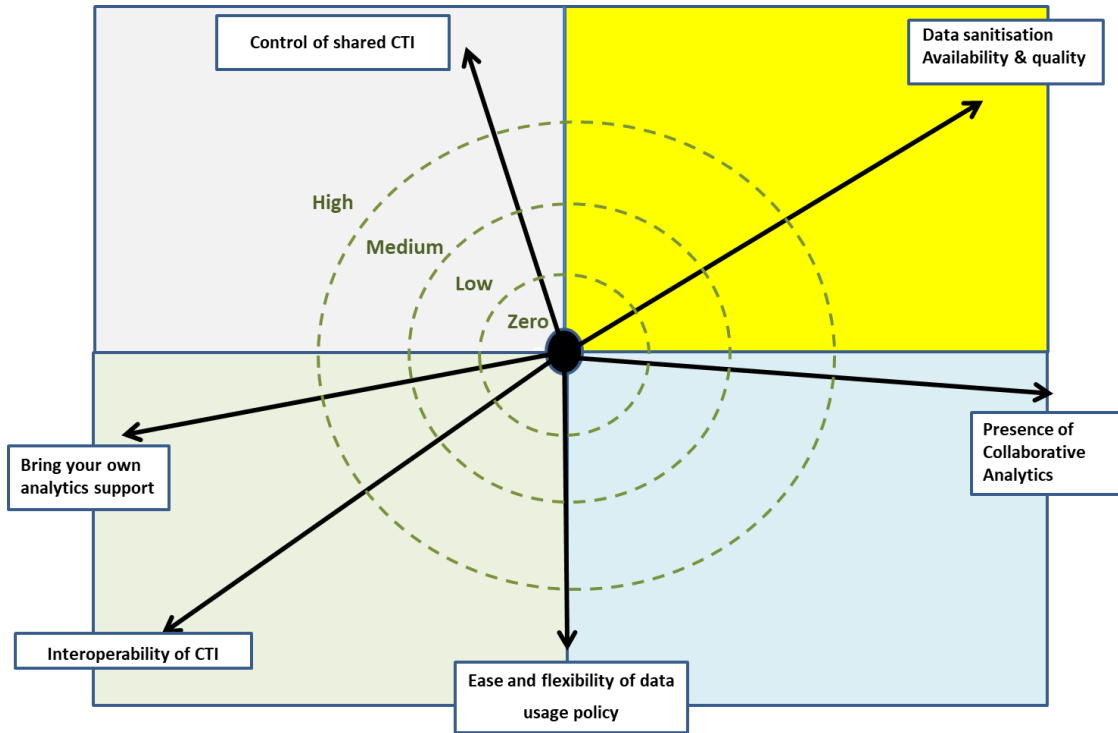
Many of these like EclecticIQ, ThreatConnect are strong competitors for C3ISP. To differentiate we need to ensure we have an open extensible platform and a strong eco-system of collaborative partners and credible early adopter proof points.

This is a useful and timely piece of market research into the state of the art competitive landscape for CTI sharing platforms and should help us position the C3ISP platform in that context.

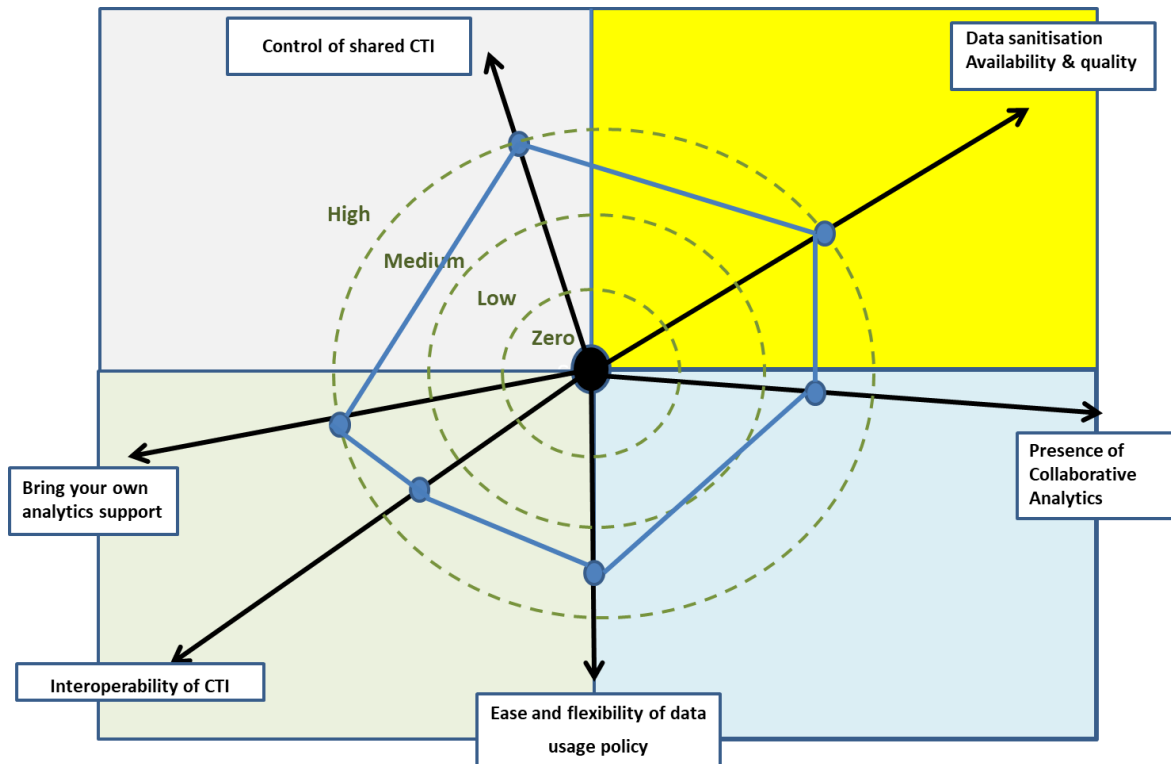
Annex 13: contains our initial research into the platforms short listed by ACSC. It shows that there are some significant well established Cyber Threat Information sharing platforms out there with capabilities that compete directly with the C3ISP platform services.

These are typically COTS platforms with flexible deployment options. An interesting paper from one of them ‘ThreatConnect’ provides some useful detailed insight into how these (COTS providers position themselves against Open Source platforms. Link to the paper provide here <https://threatconnect.com/resource/threat-intelligence-platforms-open-source-vs-commercial/>

We use spider diagrams to illustrate the competitive differentiation between C3ISP capabilities and those of the competing platforms. A generic example of the vectors used in the spider diagram is shown below.



The following spider diagram provides an example that summarises our C3ISP capabilities in this context.



As shown in Annex 13 existing commercial products such as ThreatConnect and EclecticIQ and Anomali’s Threat Stream match or exceed the C3ISP capabilities shown in the spider diagram. There are other competing platforms such as MISP where we do better in some areas such as our DSA control capabilities however the key point to make here is that there are well established strong commercial offerings in the market which reinforces our open source platform approach.

Pricing information on these competitor platforms is not widely published however we have determined some pricing information as shown below:

Threat Platform Supplier	Pricing Information
ThreatConnect TC Complete	As low as \$100,000 depending upon deployment and configuration options: <a href="https://www.scmagazine.com/review/threatconnect-tc-complete/">https://www.scmagazine.com/review/threatconnect-tc-complete/</a>
NC4 Soltra Edge Standard	starts at \$15,000/year: <a href="https://www.nc4.com/soltra-edge">https://www.nc4.com/soltra-edge</a>
Anomali	Starts at \$5,000: <a href="https://www.scmagazine.com/review/anomali-threatstream/">https://www.scmagazine.com/review/anomali-threatstream/</a>
VIII. IBM X-Force Exchange	Commercial API Threat intelligence feed for security investigations. Free Trials plus: Starting at £1,599.00 per 10,000 items per month

## 1.5. Intellectual Property

### 1.5.1. Approach

D9.1 [34]describes the approach to identifying, prioritizing and protecting Intellectual Property (IP) associated with the project.

This first step is IP identification. We begin in Section (1.5.2) by enumerating the components in the project design and system itself, then we [will] define the putative list of IP Items.

At this stage of the project, we perform a preliminary assessment of the potential value of IP associated with each component. Later this valuation will be performed for each IP Item to allow prioritisation of detailed consideration of IP protection measures.

### 1.5.2. Components

Table 1 lists *Components* that are directly associated with the project that could be associated with Intellectual Property.



Table 1 – Components potentially associated with IP

Subsystem	Component	Module	Owner	IPR		
				Current Open Source Availability	Goal after project end	
ISI	DSA Adapter	<a href="#">Continuous Auth Engine</a>	CNR	Yes	Yes	
		<a href="#">Obligation Engine</a>	SAP	No	Yes	
		<a href="#">DMO Engine</a>	SAP	No	No	
		<a href="#">Anonymisation Toolbox</a>	SAP	No	No	
		<a href="#">FPE toolset</a>	HPE	No	No	
		<a href="#">Pseudoanonymization toolbox</a>	UNIKENT	Yes	Yes	
		<a href="#">Event Handler</a>	CNR/SAP	No	Yes	
		<a href="#">DSA Adapter Front End</a>	CNR/SAP	No	Yes	
		<a href="#">Bundle Manager</a>	CEA	Yes		
	<a href="#">Format Adapter</a>		GPS	Yes	Yes	
	DPOS	<a href="#">DPOS (Hadoop)</a>	UNIKENT	Yes	Yes	
		<a href="#">Bundle Manager::DPOS API</a>	UNIKENT	Yes	Yes	
	ISI API	<a href="#">ISI API</a>	SAP/CNR	No	Yes	
<a href="#">Buffer Manager</a>		CHINO	Yes	Yes		
IAI	C3ISP Analytics Engine	<a href="#">C3ISP Analytics Engine</a>	CNR	Yes	Yes	
		<a href="#">FHE Analytics</a>	CEA	Yes	Yes	
		<a href="#">Interactive 3D Visualisation</a>	3DRepo	No	No	
	<a href="#">Service Usage Control Adapter</a>		CNR	Yes	Yes	
	<a href="#">Legacy Analytics Service</a>		BT	No	No	
	<a href="#">Virtual Data Lake</a>		BT	Yes	Yes	
DSA Manager	IAI API		CNR	Yes	yes	
		<a href="#">DSA Editor</a>		HPE	Yes	yes
		<a href="#">DSA Mapper</a>		CNR	Yes	yes
		<a href="#">DSA Store</a>		HPE	Yes	yes
CSS	Key & Encryption Manager	<a href="#">DSA Store API</a>	UNIKENT	Yes	yes	
		<a href="#">Identity Manager</a>		CNR	Yes	yes
		<a href="#">K&amp;E Core</a>			Yes	yes
		<a href="#">Key Management</a>			Yes	yes
	<a href="#">DPO - K&amp;E Mng</a>		CEA	Yes	yes	
	<a href="#">FHE - K&amp;E Mng</a>			Yes	yes	
	<a href="#">Secure Audit Manager</a>		HPE	Yes	yes	

Each component has an *ID* and short *Name*, and a *Type*.

Components are clustered by *Category* at two levels. The categories are mostly determined by the high-level, project-specific architecture into Information Sharing Architecture (ISA), Data Sharing Agreement (DSA); and also includes general categories: Architecture, Managed Security Services (MSS), and Privacy Enhancing Technologies (PETs).

The IPR - *Rights* columns summarises:

- *Who* – the organization – company or consortium - that has an owning interest in the component.
- Whether they declared *Background IP* associated with it.

Note that some components have background IP associated with earlier projects and their consortia. This includes BT.

The C3ISP architecture and API specifications are owned in terms of IPR by C3ISP.

### 1.5.3. IP value assessment

Table 2 a preliminary assessment of the potential value of IP associated with each component in Table 1 above.

The value is assessed by considering for each IP Item:

- The potential market that could be accessible or influenced by the IP.
- The extent to which the IP is different from current and potential future competition.

- The ease with which a patent is likely to be viable.
- The effective means of IP protection, including patents.

Table 2 – Intellectual Property prioritisation

ID	Component		TRL	Market			Differentiation			Patentability		Other				Approach	
	Name	Type		Channel	size	lifetime	scope	defensible	competition	on-sale bar	novel	non-obvious	trade secret	design right	contract		certification
C01	Reference architecture	spec / system		license	low	high	low	low	med	???	med	low	low	low	med	low	patent
C02	Recursive DSAs	spec		license	med	med	low	low	med	n/a	low	low	low	low	low	low	low
C03	Gateway architecture	spec		license	low	med	low	low	low	n/a	low	low	low	low	low	low	low
C04	Information Sharing Infrastructure	system			high	med	med	low	med	n/a	low	low	low	low	med	low	contract
C05	ISA API	spec			med	low	low	low	low	n/a	low	low	low	low	med	low	contract
C06	ISA data encapsulation & protection	spec			high	high	low	low	med	???	low	low	low	low	low	low	???
C07	DMO engine	module			low	med	low	low	med	???	low	low	low	low	low	low	???
C08	Information Analysis Infrastructure	system			med	high	low	low	low	n/a	low	low	low	low	low	low	???
C09	IAI API	spec			low	low	low	low	low	n/a	low	low	low	low	med	low	contract
C010	Data Sharing Agreement	spec			high	high	med	med	med	???	med	med	low	low	low	low	patent
C011	DSA enforcement	spec			high	med	med	low	med	???	low	med	low	low	low	low	patent
C012	Controlled natural language	spec		6 standard	med	high	med	low	low	yes	low	low	low	low	low	low	standard
C013	Usage control policy language	spec			med	high	med	low	low	???	low	low	low	low	low	low	???
C014	Continuous authorisation engine	module		7 standard	low	low	low	low	low	n/a	low	low	low	low	low	med	standard
C015	Obligation engine	module		6	low	low	low	low	low	???	low	low	low	low	med	low	contract
C016	DSA API	spec		6	low	low	low	low	low	n/a	low	low	low	low	med	low	contract
C017	DSA Manager	module			low	low	low	low	med	???	low	low	low	low	med	low	contract
C018	DSA Editor	module		6													
C019	DSA Mapper	module															
C020	Anonimisation tool	module		6											med		
C021	Geo-indistinguishability <??>	???															
C022	Cingulata	module		6											med		
C023	Homomorphic encryption																
	Managed Security Service	service															
C025	Intelligent protection system	system		9 service													
C026	Saturn	system		9 service													
C027	COAE	system		6													

The columns in Table 3 are:-

- Potential *market* opportunity that could be unlocked by the IP, and its readiness:
  - Ultimate available market *size* and *lifetime*
  - Expected Technology Readiness Level (*TRL*) of the associated component(s) at the completion of the project
  - Likely *Channel* to market, e.g. technology licensing, product sale, or service provision
- Degree of *Differentiation* that the IP Item, in these aspects:
  - *Scope* of the IP Item relative to value and adoption in currently unforeseen markets
  - *Defensibility* of the IP Item relative to future IP that seeks to displace or circumvent it
  - Degree of *Competition* in the IP domain and market for similar IPs.
- Ease *Patentability* of the IP Item, characterized by:
  - Whether the *On-sale bar* has been breached<sup>2</sup>
  - Sufficiency of *Novelty* and *Non-obviousness* of the potential claims associated with the IP Item, which are fundamental pre-requisites for a successful patent.
- Identify effective means of IPR protection, including using:
  - *Trade secret*, which requires that key information about the IP Item are kept confidential

<sup>2</sup> In the US, the on-sale bar invalidates a US Patent application if (speaking loosely) key claims have been offered to the market more than 12 months before the patent is filed.

- *Design Rights*, which can apply in the EU for designs and/or contents of databases
- *Contract*, where a legal agreement is used to protect an IP Item, and specifically specifies rights and obligations in its use (etc) by a 3<sup>rd</sup> party
- *Certification*, where compliance and/or standards are used to enforce certain aspects of use of an IP Item
- *Approach*, is the suggested primary means of protection to be used for priority IP Items.

Each cell in the table is rated as *high*, *medium* or *low*, where high denotes a relatively positive opportunity or advantage.

### 1.5.4. IP Item prioritization

Table 4 shows some example estimates for the [provisional] relative priority of protecting the IP associated with each Component.

Table 4 – Prioritisation for component IP protection

Component			Approach		relative	weigh	high	medium	low
ID	Name	Type					5	3	1
C01	Reference architecture	spec / system	patent	med	15	15	1	2	4
C02	Recursive DSAs	spec		low	13	13	0	3	4
C03	Gateway architecture	spec		low	9	9	0	1	6
C04	Information Sharing Infrastructure	system	contract	med	17	17	1	3	3
C05	ISA API	spec	contract	low	9	9	0	1	6
C06	ISA data encapsulation & protection	spec	???	med	17	17	2	1	4
C07	DMO engine	module		low	11	11	0	2	5
C08	Information Analysis Infrastructure	system	???	med	15	15	1	2	4
C09	IAI API	spec	contract	low	7	7	0	0	7
C010	Data Sharing Agreement	spec	patent	high	25	25	2	5	0
C011	DSA enforcement	spec	patent	med	19	19	1	4	2
C012	Controlled natural language	spec	standard	med	15	15	1	2	4
C013	Usage control policy language	spec	???	med	15	15	1	2	4
C014	Continuous authorisation engine	module	standard	low	7	7	0	0	7
C015	Obligation engine	module	contract	med	15	15	1	2	4
C016	DSA API	spec	contract	low	7	7	0	0	7
C017	DSA Manager	module	contract	low	9	9	0	1	6
C018	DSA Editor	module							
C019	DSA Mapper	module							
C020	Anonimisation tool	module							
C021	Geo-indistinguishability <??>	???							
C022	Cingulata	module							
C023	Homomorphic encryption								
	Managed Security Service	service							
C025	Intelligent protection system	system							
C026	Saturn	system							
C027	CDAE	system							

The priority is a normalised, weighted average of the number of high, medium and low cells in the columns: market, differentiation and patentability (excluding the on-sales bar). The weighting is high 5, medium 3, low 1.

## ***1.6. The C3ISP Platform Exploitation Plan***

The C3ISP platform exploitation plan builds on the provision of an open source core platform upon which an extensible set of proprietary and open source Cyber Threat Intelligence (CTI) application modules can be built. Examples of such proprietary application modules include the various SME, Enterprise, CERT and ISP Pilot functionalities that have already been developed by the C3ISP consortium members.

The showcasing of these capabilities using a hosted demonstration instance of the C3ISP core platform together with its existing application modules will be available to help engage potential customers and partners to take part in collaborative Proof of Concept (PoC) demonstrations.

The C3ISP consortium members can individually exploit these showcases and PoC exercises to help sell their proprietary modules to partners wishing to integrate C3ISP capabilities into their own platforms, or to sell fully operational instances of C3ISP directly to customers.

The C3ISP platform exploitation plan is supported by a light weight informal governance structure being put to support both the C3ISP live demonstration, for use in expo/conferences and early sales conversations, and the on-going test and development instance of the C3ISP platform.

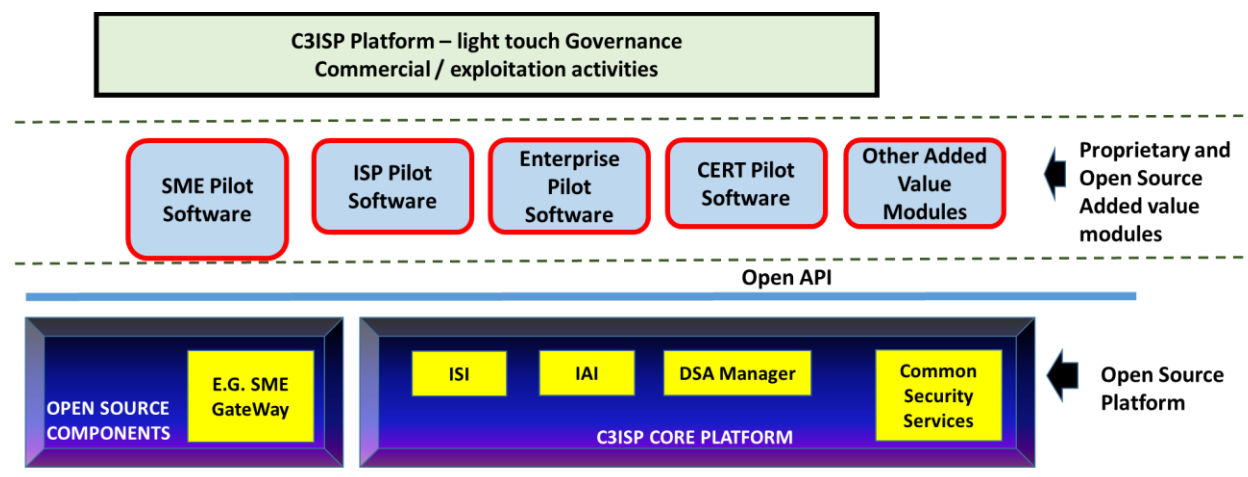
The C3ISP partners have the option to periodically review the potential for setting up a separate C3ISP legal entity (company) in the event that the operation of live C3ISP platform services by a single operating company becomes a commercially attractive option to the consortiums stakeholders.

### **1.6.1. C3ISP Our Business Model**

Our business model is designed to exploit the C3ISP platform in a way that both maximises the socio-economic benefits of the C3ISP services to the EU and that maximises the adoption of the platform. Our approach is also designed to complement the individual exploitation plans of our consortium members.

Figure 9 provides a schematic view of the C3ISP domain from our business model perspective. It highlights the fact that the C3ISP core platform will be provided as Open-source and that the extensible suite of value added modules that use this core platform can be either proprietary or open source.

It is expected that the Pilot modules for example will be proprietary in line with the individual exploitation plans of associated members although some (such as the SME Pilot example shown below) may feature Open source components.



**Figure 9 – The C3ISP Open Source Platform / Added value Modules canvas**

As well as being made available on GitHub the C3ISP platform will be made available as a hosted show case and on-going test and development platform of C3ISP services.

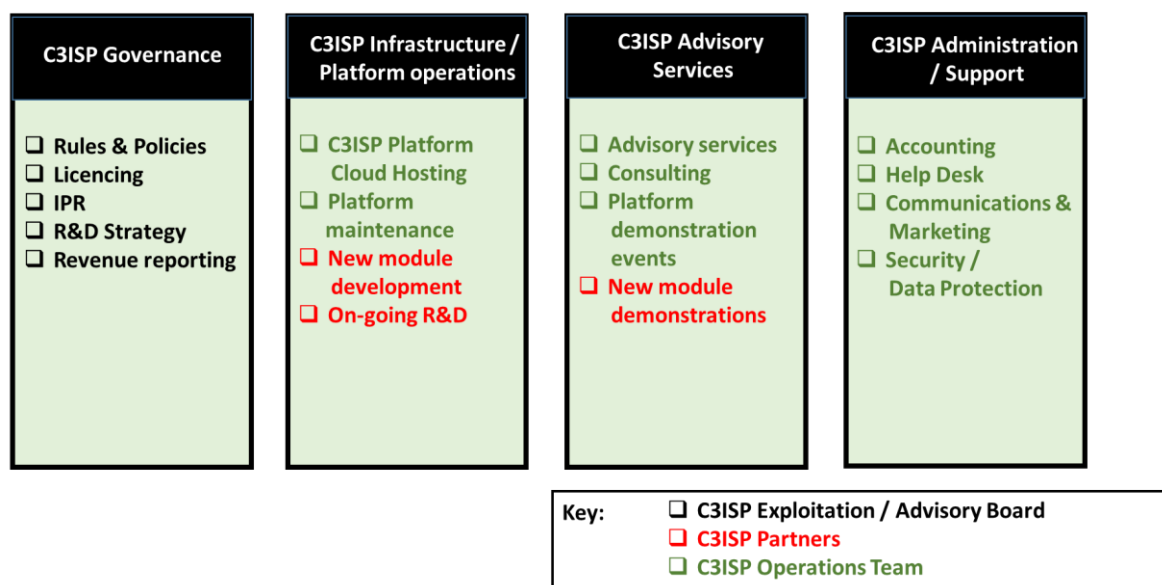
In this mode the C3ISP hosted demonstration platform will serve as a Proof of Concept (POC) demonstrator to our target market sector customers. As described earlier in this paper this POC approach is an integral part of potential future routes to market strategy.

As also shown in figure 9 there is a light weight informal governance structure that will be put in place to manage the exploitation of the C3ISP platform.

Our exploitation plan for the platform aims to use this POC approach to support C3ISP consortium members and our wider partnership community in selling C3ISP products and services into our target market sectors.

If at some future point the C3ISP partners decided that there was a compelling business case to create revenue generating commercial C3ISP platform service offerings then a more formal governance structure would be adopted and could for example be a simple Governance value chain as illustrated in Figure 10

## C3ISP Governance Value Chain



**Figure 10 C3ISP Governance Value Chain – potential future option**

As shown in Figure 10 the four components of such a value chain provide a range of services from the overall governance of policy and strategy through to the cloud based hosting and operation of the show case and on to the provision of advisory services and customer tailored POC demonstrations as well as marketing and administrative support services. These diverse services could be provided by the three key entities highlighted in Figure 10 i.e.:

- The C3ISP Exploitation / Advisory Board
- The C3ISP Operations Team
- The C3ISP Partners

**The C3ISP Exploitation and Advisory Boards** would be responsible for the overall governance of the rules and policy, revenue / cost balance and of course for meeting the overall exploitation objectives. The Board is comprised of senior representatives of the consortium and partner organisations.

**The C3ISP Operations team** would in such a scenario be in charge of hosting (using a Cloud provider) and maintaining and providing POC show cases of the platform (including any Added value modules).

**The C3ISP Partner Community** will include a range of types of organisation from Universities and industry bodies through to commercial companies.

Some could engage with us with on-going Research & Development including the development of POCs of new added value modules especially those tailored for specific market verticals such as CNI Energy sector and CNI Autonomous Vehicle CAV sector.

Also for adding on-going innovative capabilities to customer segments such as SME's, Enterprise, ISP's and CERTS. Our partner community will also be a key part of our targeted customer engagement strategy and may in some cases also be providers of managed security services platforms which C3ISP can augment.

The Business model below addresses the costs associated with operating the Governance Value chain in the event that it was decided to adopt this commercial model at some future point, with the following approach to revenue generation.

#### *1.6.1.1. C3ISP Revenue Streams*

The C3ISP Operations Team would be in charge of hosting (using a Cloud provider) and maintaining the platform as well as running POC demonstrations as part of our Customer engagement strategy.

The operation and maintenance of the show-case platform is in one respect part of pre-sales costs. Members of the consortium and our partner community will be using it to engage with customers with the objective of selling:

- Value added modules to third parties operating our open source C3ISP platform as a service to their own customers.
- Live operational instances of the C3ISP platform as a service, to their customers.

This would provide a revenue opportunity for the C3ISP operations team through the provision of Advisory, Consulting and support services to those members and Partners both during pre-sales and post sales periods.

In order to be able to cover such C3ISP governance value chain costs some revenue would need to be generated. As a possibility to sustain the show case platform operations and wider governance team we consider the following potential options:

- Membership fees.
- Revenues from platform users.
- Commission on consulting requests delivered by the C3ISP community.

The value of the membership fees would be tailored to the size of the member / partner organisation with different membership categories for Universities, SME's and Large Enterprises.

Revenues from platform services where offered would likely to be based on licence models that provide a similar degree of flexibility e.g. to encourage the participation of SME's.

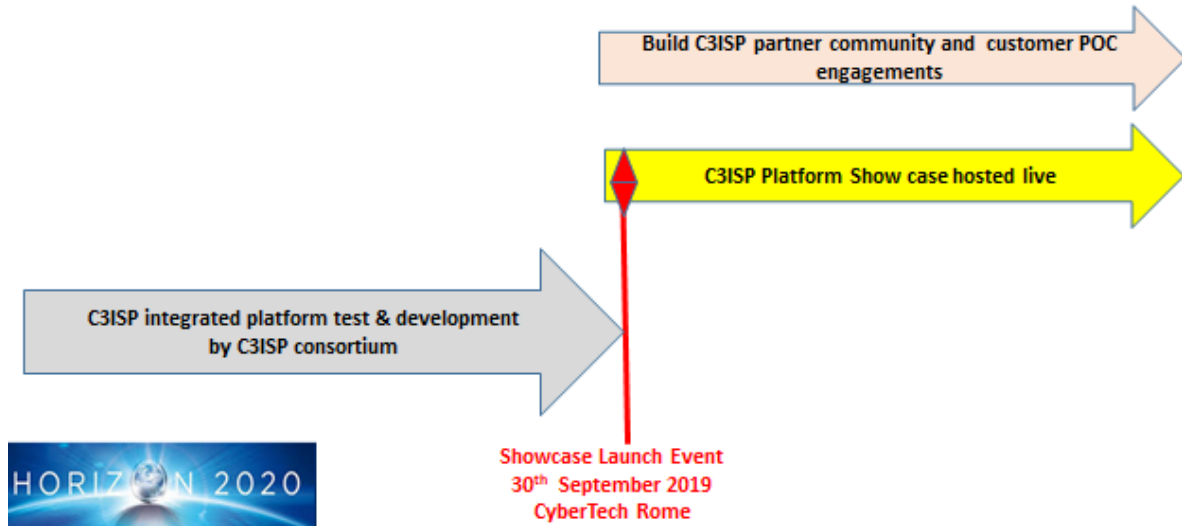
Similarly once we have established relationships with the reseller market we would expect to gain revenues from licensing to approved resellers. These revenues would be commission based and will be less lucrative than direct sales opportunities for C3ISP however will be essential in gaining widespread adoption.

Just to be clear the current model is a light weight informal governance structure and not the formal governance value chain.

#### **1.6.2. C3ISP Platform Exploitation Plan on a page**

The showcasing of the C3ISP platform capabilities using a hosted demonstration instance of the C3ISP core platform together with its existing application modules is available to be used to help engage potential customers and partners to take part in collaborative Proof of Concept demonstrations. As shown in Figure 11 the launch show event will be held in September 2019 in Cyber Tech Rome.

### C3ISP Platform Development and sustain plan on a page



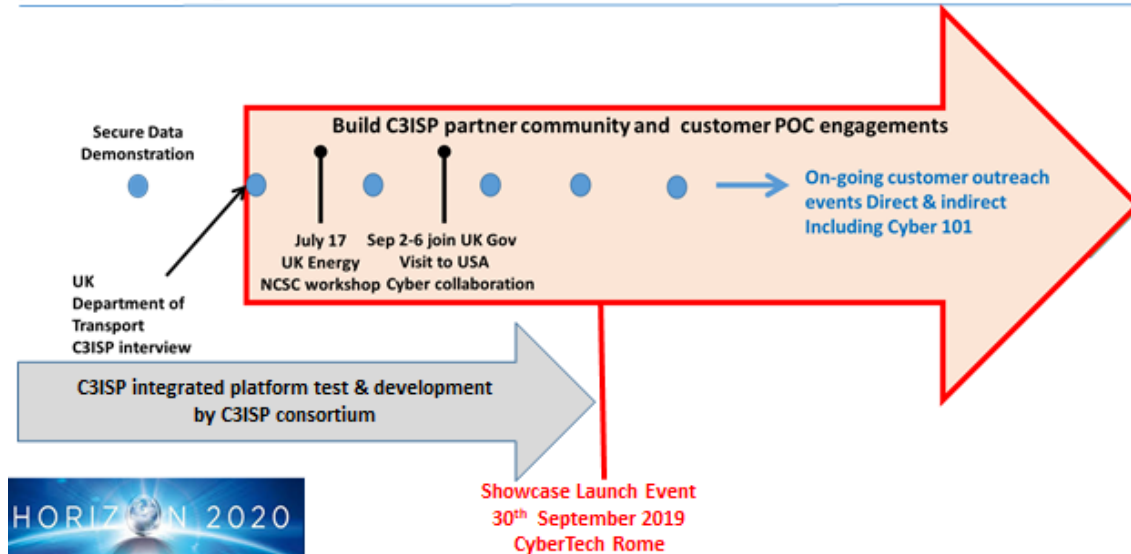
**Figure 11 – C3ISP Platform Exploitation plan on a page.**

The C3ISP consortium members can individually exploit these showcases and POC exercises to help sell their proprietary modules to partners wishing to integrate C3ISP capabilities into their own platforms, or to sell live operational instances of C3ISP directly to customers.

The C3ISP platform exploitation plan features a light weight informal governance structure to support this C3ISP showcase and on-going test and development instance of the C3ISP platform.

Figure 12 below provides a more focused view on the Customer and partner engagement work stream and the associated activities.

### C3ISP Platform Development and sustain plan on a page



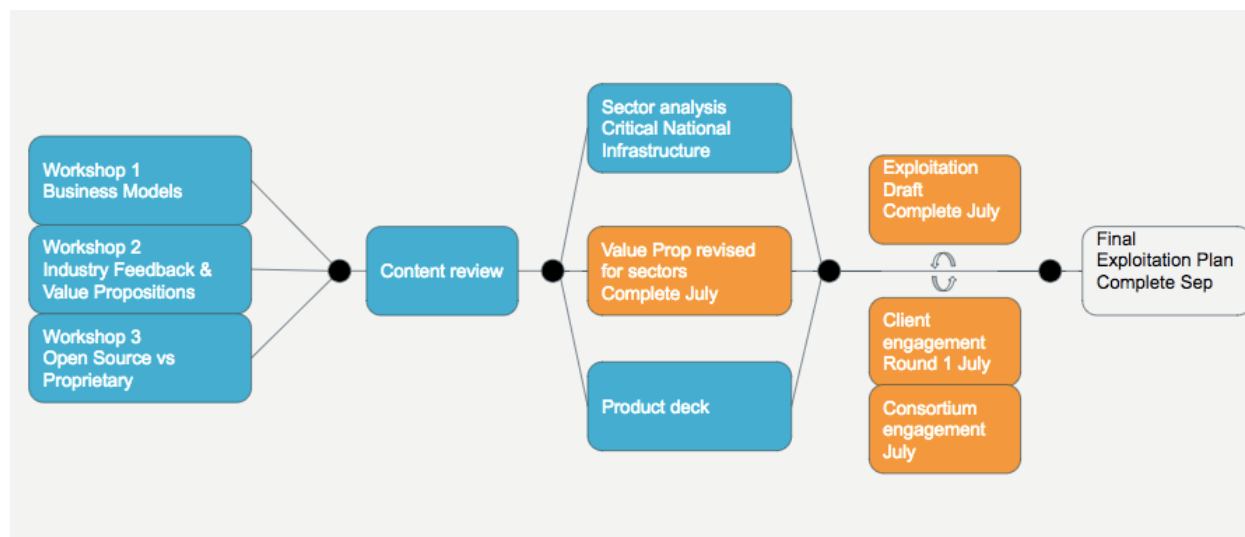
**Figure 12 – C3ISP Platform Exploitation plan - focus on customer & partner engagements**



### 1.6.3. Report of C3ISP Platform Exploitation Activities

The C3ISP exploitation activities to date i.e. as at 30<sup>th</sup> September 2019 are summarised here:

#### C3ISP Exploitation Activities to date



**Figure 13 – C3ISP Exploitation activities to-date.**

Following the three workshops we delivered to discuss business models and C3ISP value proposition, we then focused on engagement with the potential clients and partners for C3ISP to validate our exploitation strategy and business model.

As mentioned earlier in this document we will begin our exploitation plan with Critical National Infrastructure sectors, and are actively engaging with key stakeholders in these three sectors.

#### Some of the activities completed are:

- C3ISP hosted UK National Cyber Security Centre and UK BEIS Energy Sector workshop (July 2019) – Completed see summary in Annex 17.
- Secure Data Demonstration (June)
- Sales calls and client engagement (e.g. with Department of Transport) (June-July)
- Calls with potential partners and re-sellers of C3ISP (e.g. cyber security service providers through Digital Catapult’s Cyber 101 programme)
- Participation (via Digital Catapult) in the UK governments USA East Coast Cyber Security Expert Mission exploring international collaboration opportunities. (Pending)
- Engagement with and demonstration to industry at CyberTech Europe in Rome September 2019.

**Sector and organisation target customers engagement and contacted:**

<b>Energy:</b>	BP, EDF, DANFOSS, Costain
<b>Transport:</b>	Thales, BAE Systems, Transport for London, Virgin Trains, Association of British Ports
<b>Telecoms:</b>	Siemens, Ericsson, Semtech, (BT), Vodaphone
<b>Cyber:</b>	Elemendar, BreachAware, Clym, Panaseer, RedSift, ProtectBox
<b>CERTS:</b>	NCSC, (Cert Italia)

The above exploitation activities helped the consortium refine and validate our business model and value proposition.

**Other activities in the final months of the project included:**

- Scheduled 1 2 1 with consortium members for updates on individual exploitation plans
- Final exploitation showcase/demonstration(s) (Sept)
  - o Industry engagement and demo via Cyber Tech Rome conference Rome (24th/25th Sep);
  - o Industry Engagement and Demonstrations

**Customer Interviews/On-boarding**

DigiCat led the process of identifying client leads. Through consultation with the business development function at Digital Catapult and the Cyber security expertise the target sectors were narrowed down from Critical National Infrastructure to the Energy, Transport, Telecommunications and Government Sector. Further more the reseller market was identified as an opportunity especially for the SME products in development. A shortlist of companies was compiled which included:

- BP
- EDF
- Alstom
- Thales
- Seimens
- BT
- Vodafone
- Micro Focus
- SSE
- BAE System
- **Elemendar**
- BreachAware
- Clym
- Panaseer
- **Redsift**
- **Protectbox**
- Virgin Trains
- ABP

- UK Water
- **Department for Transport**
- BT
- **HS2**
- Telefonica
- Transport for London
- Vodafone Group
- BEIS
- NCSC

Those in bold have been successfully converted from email communications to a telephone qualification call and have been primed for a demonstration of the full C3ISP product. Furthermore additional customers have been engaged via the BEIS and NCSC workshop, as well as the Cyber 101 Deep Dive activity. Interview reports are provided in Annex 21.

In total Digital Catapult expect to have converted circa 30 potential customers to circa 10 engaged customers via these activities. These successful conversions demonstrate a high level of success (1 in 3) as we targeted those with who Digital Catapult already held strong relationships. The C3ISP organisation going forward will seek to further leverage the strong internal connections of key partners such as BT and SAP who have extensive potential client bases.

You can find the product deck which has been used to qualify potential customers in annex 18 of this document.

## 1.7. Individual Exploitation Activities and Plan

### 1.7.1. CNR

CNR mainly exploits the C3ISP results in the development of the Pilot. CNR is actively involved in the ISP Pilot and in the CERT one. In fact, being the Registro.it, one of the main actors in the ISP Pilot, part of CNR, the expertise and results matured within the second year of the project has been put in place to further extend and enhance functionalities of providers in such a way that the adoption of the C3ISP solutions to discover and mitigate security attack is straightforward.

#### T9.1 Exploitation and Innovation Activity.



#### CNR

- CNR being a RTO exploited the current results in several directions, mainly **new research and innovation projects** for:
  - Cyber Threat Information -> New H2020 projects Cyber SANE & SPARTA Pilot network
  - Set up of the CNR Cyber Security Observatory and
  - Definition of the Tuscan Cyber Security Observatory
  - Data Usage control -> EIT Digital Project for 2019 (also with BT)
  - New in-kind services for Italian ISPs



### **1.7.2. ISCOM-MISE**

ISCOM-MISE is a Pilot provider so it exploits the C3ISP results in the deployment and refinement of the CERT Pilot with the aim of make the service more secure and private.

### **1.7.3. HPE**

HPE delivers its consulting activities under the brand “HPE Pointnext”. Inside HPE Pointnext six different Competence Centers of Excellence (COE) exist, with a worldwide scope, to bring specific competences and innovations to customers. Among them, Security, Data Analytics, Hybrid IT, Data Center Facilities COEs, deal with topics related to the C3ISP project.

As Data Sharing is a growing Security theme, anticipated by the project, the object of the HPE team working in C3ISP is to make those COEs aware of the existence of the C3ISP Framework and to include it into their offering portfolio. In particular, this also brings consulting services opportunities in the area of policy and compliance management, in addition to the system integration activities. Our objective is to leverage on these groups for enabling them to face specific needs raised by customers with the problem of sharing (confidential) CTI information and address their privacy and compliance concerns.

HPE will add the C3ISP demo to the HPE Technology Showroom at HPE Italian headquarter.

A submission describing the C3ISP solution to HPE WW “Tech Con 2020” conference in US has been accomplished September 2019. Selection process results to be announced November 2019.

HPE has presented the solution to the HPE WW IT Security CEO (Centre of Excellence), to include the solution in their offering toward customers presales activities.

HPE C3ISP team had a word with the Cloud28plus ([www.cloud28plus.com](http://www.cloud28plus.com)) initiative to adopt the solution inside the ecosystem. Execution time has been suggested to be delayed to the end of the project as the whole solution will be more mature.

HPE participated to the Cybersecurity Day, 16th November 2017 (Pisa, Italy) where Claudio Caimi had a talk about C3ISP, and HPE approaches several prospects/partners.

### **1.7.4. BT**

BT C3ISP researchers continued to share their knowledge and progress on C3ISP with other BT teams in security research, development and operational departments. A stable version of the C3ISP Framework and ENTERPRISE and SME Pilots’ software has been deployed in a secure test-bed environment on BT premises, for the purposes of external/third-party evaluation and demonstrations to potential customers..

This test-bed will be continually updated and improved to provide a basis for showcasing C3ISP to internal and external customers, even after the project ends. Furthermore, BT agreed to release the final version of C3ISP Gateway, a software component developed in the SME Pilot to make it easy for SMEs to interact with C3ISP Framework’s components and services, under an open source license (Apache License, Version 2.0).

BT has also collaborated with HPE to enable the deployment of C3ISP software using container technology (i.e. Docker). This collaboration is still ongoing and will smoothen the

path towards exploiting C3ISP technologies within and with-out BT, particularly to allow for policy-controlled data sanitization, data anonymisation and data sharing among different communities (e.g. dev/ops, researchers, analysts, etc.). BT is exploring further collaboration opportunities with SAP and HPE to achieve that objective.

BT C3ISP researchers have also engaged with the BT team which is in charge of BT-hosted MISP platform [15] [35], in order to discuss potential use cases for C3ISP and MISP integration. BT has been collaborating with CNR to tackle the associated technical challenges, e.g., importing C3ISP analytics result into MISP platform and vice versa.

BT researchers have also started discussions with BT's internal innovation consultants to look into further exploitation channels within BT and through BT's customers. BT is actively exploring C3ISP exploitation opportunities with BT Ireland's Advanced Analytics Team, under the BT Ireland Innovation Centre (BTIIC) project, which has also been given partial funding by Invest Northern Ireland (Invest NI).

In this respect, the trial of the C3ISP anonymisation and pseudo-anonymisation components' integration with BT's analytics software should begin in Q4 of the current financial year (January 2020) and if successful, BT will be able to showcase the commercial results in the next financial year.

#### **1.7.5. SAP**

SAP exploitation strategy relied on the valorisation of the C3ISP experiences for fulfilling internal needs. However, we are able to report that the exploitation activities over-fulfilled the initial expectations, in that concrete follow-up exploitation activities with project partners have been identified.

The already reported market interest for anonymisation solutions, also as aid towards GDPR compliance, permitted to establish an internal transfer in an SAP product (SAP Data Custodian) together with a number of other PoCs and internal collaborations; even more importantly, though, this led to the identification of concrete steps to materialize a collaboration with BT on an anonymisation solution. Such opportunity results particularly interesting also in the light of the SAP.io start-up program as explained below.

Internal exploitation activities are reported in the following of this section.

SAP Data Custodian is a multi-cloud SaaS application, deployed on cloud providers like Google Cloud Platform (GCP), Amazon Web Services (AWS), and Microsoft Azure. It addresses global data protection regulations, and offers enterprise customers with comprehensive data control and monitoring across cloud environments. In such scenario, an add-on was released in September, allowing customers to use our approaches to detect personal information in processed data.

Another important exploitation opportunity is represented by the participation to the SAP.io program, an internal intrapreneurship project that aims at launching start-ups for SAP employees. Our proposal reached a significant consensus, ranking between the 9<sup>th</sup> and the 13<sup>th</sup> place over 250+ proposals. At the time of submission, the process is still ongoing, if successful, this would allow to launch a new company, fully supported by SAP but with its own budget to enter the market with the ideas and contributions developed in C3ISP by the SAP team.

A PoC was released for the SAP cyber-security team, focussing on classification and anonymization of cybersecurity information. The prototype reuses concepts developed in C3ISP for specific use cases. The prototype was positively evaluated however a change in the

technical infrastructure prevented our PoC to enter production. Follow-up actions are triggered to continue our collaboration after the termination of the project.

A similar activity was also established with the SAP IT department, again on anonymisation. In particular, the objective here is to anonymize information and logs coming from devices of the SAP workforce when investigations and incident analysis need to take place. The prototype was positively assessed and was used for several months in production for sanitizing data for forensic investigations.

### 1.7.6. CEA

CEA researchers are actively involved in the development of C3ISP and continue to share their knowledge to build a secure analysis platform for C3ISP, especially an integration with Fully Homomorphic Encryption (FHE) technology.

Within the second and third year, the C3ISP experiences and results allowed the CEA security teams to improve the performance and security parameters of Cingulata – a toolchain dedicated to FHE technology. Recently, thanks to C3ISP project, we have a second release Cingulata 2.0 in open-source version, this compilation toolchain is now available at <https://github.com/CEA-LIST/Cingulata> . It also benefits of CinguParam, our tool for automatic parameter generation tool available at <https://github.com/CEA-LIST/CinguParam>.

The fact of integrating Cingulata in C3ISP project and deploying a version of Cingulata in open-source offer to operation users a flexibility to develop and deploy his own algorithm working with FHE. Our exploitation plan is

- To initiate end users able to work with FHE without deep knowledge in cryptography
- To provide our expertise on performance and optimization to offer a robust solution for them.
- During the last year of project, the CEA direction accepted an excellent strategy to build a dedicated FHE platform based on C3ISP framework and Cingulata open-source library. This FHE platform will be deployed in public cloud, which allows the users to freely test and deploy their FHE algorithms. It will be a strategic step towards the adoption of this technology for industry partners.

### 1.7.7. DIGICAT

Digital catapult confirms that the methodology for exploitation innovation has been agreed (as detailed in D9.1, 1.6.2 Exploitation innovation). The innovation workshops were described earlier in section 1.3 of this report. Digital Catapult’s individual contribution in setting these up is summarised below.

The first Innovation workshop (titled: “Building a route to market for new cyber security technologies”) was held at Digital Catapult Centre in London on 14 March 2018. The workshop focused on ‘Identifying Technology Applications and Target Markets’.

This first workshop was designed and structured by Digital Catapult. The preparation lasted over 2 months and included collaborative work with the Programme Delivery, Marketing and Communication and Technology departments.

The outcomes of this workshop include a better understanding of market needs, possible ways to address barriers for adoption of the technology as well as identifying possible business models and topics that need further research.

During the workshop, Digital Catapult retweeted C3ISP tweets from the C3ISP official Twitter page to disseminate and communicate the event within the Digital Catapult ecosystem. The tweet reached various industries including data security, European institutions, media and research, technology blog and advertising, information technology.

The second innovation workshop was designed and structured by Digital Catapult. The preparation lasted over 2 months and included investigation with external stakeholders on commercial potential of C3ISP at Cybertech Europe 2018 in Rome as well as collaboration with consortium partners and different areas across Digital Catapult including Programme Delivery, Marketing and Communication and Technology.

The third workshop held in Pisa in April 2019 was also designed and structured by Digital Catapult. We conducted a two part workshop to first draw out the positive and negative impacts of various proprietary and open source approaches. Considering both extreme cases (totally open source, totally proprietary) and stepped approaches, with some elements proprietary and others open source

In addition, Digital Catapult established processes and plans to perform regular assessment of the added value of C3ISP results against the industry and research state-of-the-art, as detailed in D9.1; established the Exploitation Board, including representation from each research and industrial user partner; established the processes and shared technical capabilities to protect and manage knowledge and intellectual property associated with C3ISP.

DigiCat also performed an initial business state-of-the-art analysis on threat intelligence and defined approach to Open Innovation workshops to define and validate business scenarios and models.

DigiCat participated in the TRUESSEC final symposium was held on December 12<sup>th</sup>, 2018 at the University De Lille and was hosted by the TRUESSEC partners and included its Advisory Board and a number of EU sister projects including the C3ISP project.



Truessec is a Horizon 2020 Project that is focused on certification and labeling of trustworthiness properties from a multidisciplinary perspective and with emphasis on human rights.

The project has been exploring the current situation, the barriers, and the benefits of security and privacy labels; engaging stakeholders in the discussions, and issuing recommendations that may foster the adoption and acceptance of labels.

Digital Catapult represented the C3ISP project and along with five other EU sister projects gave a presentation on our project and took part in group discussion on exploitation. The sister projects that participated were the EU-SEC Project, the VESSEDIA Project, the SAFERtec Project 6, the ANASTACIA Project and the CANVAS Project.

The C3ISP presentation provided an overview of the C3ISP project and its partners including our vision and approach to collaborative and confidential information sharing and analysis for Cyber Protection.

In discussion we highlighted the importance of trust in the C3ISP context in particular as it applies to the trustworthy definition, analysis, management, enforcement and dissolution of data sharing rules encoded in the C3ISP Data Sharing Agreements (DSAs).

Discussion sessions/ working group during the day also discussed the exploitation strategies for Truessec and some of the challenges around creating or facilitating Trust labels of the multidisciplinary scope covered by Truessec.

The sister projects at the session included:

- **EU-SEC** **Project**
  - The project “European Security Certification Framework” (EU-SEC) aims to create a European framework for certification schemes and evaluation concepts to secure cloud infrastructures
- **VESSEDIA** **Project**
  - The project aims at enhancing safety and security of information and communication technology (ICT) and especially the Internet of Things (IoT).
- **ANASTACIA** **Project**
  - The ‘Advanced Networked Agents for Security and Trust Assessment in CPS / IOT Architectures’ Project exploring a holistic solution enabling trust and security by-design for Cyber Physical Systems (CPS) based on IoT and Cloud architecture.
- **CANVAS** **Project**
  - Aims to unify technology developers with legal and ethical scholar and social scientists to approach the challenge how cybersecurity can be aligned with European values and fundamental rights.
- **SAFERtec** **Project**
  - The SAFERtec project seeks to in-depth explore the involved vulnerabilities of connected vehicles, apply innovative techniques for attack modeling, experimentally validate the quantification of security assurance levels and also contribute to relevant standards.



DigiCat also participated in a workshop run by Hermeneut which is another sister Horizon 2020 project in London in January 2019. This workshop was focused on the cyber resilience of the UK's road transport eco-system as it evolves towards one dominated by Connected Autonomous Vehicles (CAVs).

DigiCat presented C3ISP's potential to enhance the cyber resilience of this CAV eco-system. Participants included representatives from the UK governments department for Transport.

Following the workshop success, C3ISP and Hermeneut published a white paper on a new perspective on Cyber Risk (Ref 36).

The white paper looks into applying the benefit harm index as a new approach to modelling risk assessment of cyber ecosystems and their socio-economic impacts to the UK's evolving connected and autonomous vehicle ecosystem. It includes a section on mitigations through the use of C3ISP based sharing of cyber threat intelligence.

DigiCat also set up and held a workshop with the UK government's department for Business, Energy and Industrial Strategy (BEIS) and the UK National Cyber Security Centre (NCSC) in London on July 2019. This workshop was focused on the cyber resilience of the evolving Energy Sector component of the UK's Critical National Infrastructure (CNI). DigiCat presented both a new perspective on cyber risk from the Hermeneut Horizon 2020 project and the potential for capabilities based on the C3ISP platform to enhance the cyber resilience of the UK's Energy CNI. Further details on this workshop are provided in Annex 17.

DigiCat took part in a UK government mission in September 2019: i.e. the US East Coast Cyber Security Global Expert Mission and explored and discussed with US organisations opportunities for UK business in the US market including cyber security domains such as CTI sharing.

DigiCat set up the C3ISP demonstration / stand at CyberTech Rome in September 2019 which was attended by a number of C3ISP partners including BT, SA, CNR and HPE. See Annex 22 for our report on this event.

### **1.7.8. UKENT**

The University of Kent is working closely with the SME Pilot to help SMEs to easily configure and use the C3ISP infrastructure. In particular, Kent is instrumental in building the C3ISP Gateway, a software component designed to make it easy for SMEs to interact with the C3ISP infrastructure. The intention is to make this software open source and free to use when the project completes, thereby maximizing its value to the European community and SMEs worldwide.

Preliminary negotiations have taken place with SecureData for sharing customer data, and discussing C3ISP principles for future potential exploitation.

### **1.7.9. GPS**

Utilities hold a lot of private information from their customers. As part of its collaboration with these utilities, GridPocket can represent an access point to this data. Ensuring a high level of security in its IT infrastructure is mandatory for GridPocket. The C3ISP project,

therefore, demonstrates that GridPocket is really committed to achieving this goal of securing all its environment.

In addition, GridPocket is responsible of the Format Adapter's technical implementation. This Format Adapter helps to translate CTI data to STIX standard format. GridPocket intends to make this component open source as it is also promoting the usage of STIX standard format when sharing information over its business partners.

GridPocket is launching a commercial exploitation of C3ISP as part of its PowerVAS platform.

Target market : utility companies (electric, gas, water) in Europe. Presentations, demos and talks has been organised at major European energy trade shows and conferences (Essen, Vienna, Paris, London) as well as on private meetings (Poland, France, Monaco, Belgium, Spain)

Product integration : part of the Advanced Security Shield feature offered additionally to the three layers (frontend, processing, storage) cloud PowerVAS Platform

Business model : evaluating possibility of subscription based model

Participated in C3ISP exploitation and innovation workshops, which were held in London at the Digital Catapult Centre on 14th March 2018 and at the National Research Council of Italy in Pisa on 11th October 2018.

### 1.7.10. CHINO

CHINO is mainly exploiting C3ISP for internal platform improvements and marketing activities its customers and partners. For CHINO security is a fundamental aspect, and C3ISP project is being used everywhere possible to demonstrate CHINO commitment to state-of-the-art processes and quality standards. This means that CHINO uses C3ISP logos and material in all service presentations, demos, and talks where its company and work is described.

Chino are providing a solution for storing health data in compliance with the EU regulations. We are exploiting our participation in the c3isp project for marketing purposes. We show our customer how security and privacy are important for us and for their data and how C3ISP could be leveraged in the future to have a more secure and safe environment for us within our offer.



### 1.7.11. 3DRepo

As a SME pilot project partner of C3ISP, 3D Repo has already benefited from the project in multiple ways. 3D Repo is a cloud-based collaboration platform for building information modelling with clients in the public and private sector in Europe and North America.

Cyber security is important to 3D Repo and its clients, especially since a number of high-profile public infrastructure projects, such as EDF’s Hinkley Point C nuclear power station, and large-scale private developments are hosted on the platform.

Exposure to the latest research from academic institutions and commercial products from the C3ISP project has been beneficial to 3D Repo’s efforts to improve its platform and an opportunity to influence the development of cyber security technologies.

Third parties, such as Highways England, have already expressed interest in the automated generation of 3D visualisations demonstrated on the platform for C3ISP.

3D Repo will be hosting/participating in the following events:

1. British Information Modelling – 8<sup>th</sup> October 2019
2. Digital Construction Week – 16<sup>th</sup> – 17<sup>th</sup> October 2019

### 1.8. Pilot Blogs

Aiming at providing an always up-to-date proof of how C3ISP results are exploited, in particular, in the scenario depicted by the four pilots of the project, each pilot has its own blog on the C3ISP web page.

The blogs have been created within the second year of the project and appeared online during the second year and have continued online since then.

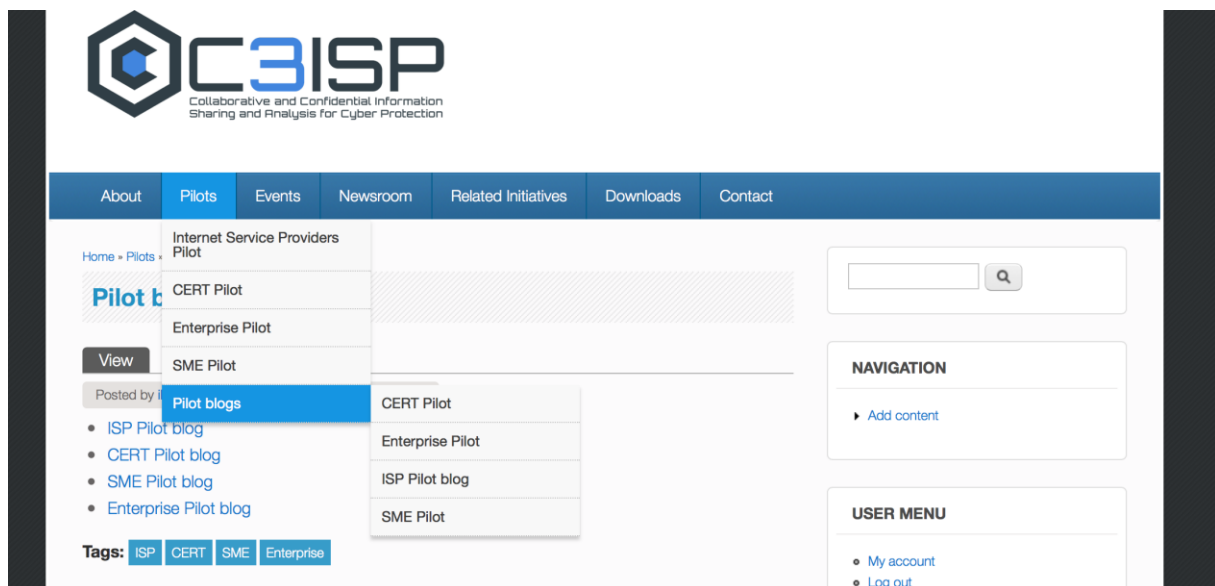


Figure14. Pilot blogs section in C3ISP webpage.

### 1.8.1. ISP Pilot Blog

This pilot aims at performing collaborative analysis of data coming from a federation of Internet Service Providers (ISPs) to detect cyber-crimes attempts in time and to quickly identify cyber-security attacks. ISPs provide to single subjects or companies access to the Internet and additional related to services like DNS, mail, news, FTP, and so on.

Since cyber-security has become a relevant topic in the ISP world, there is an open debate<sup>3</sup> trying to clarify whether ISPs should provide strong security solutions to protect themselves and their customers. In particular, should ISPs proactively protect their resources and customers with security controls and filters or are customers responsible for their own security? On one side, the CIO magazine with the article, “*Seeing No Evil: Is It Time To Regulate the ISP Industry?*”<sup>4</sup> claims that ISPs should provide security solutions. Instead, from the ISP point of view, security solutions cannot be supported only by ISPs since customers are responsible for keeping their own systems secure.

In any case, since ISPs have an advantageous position in the network, they can have a much wider impact on the overall state of security. In fact, a lack of security management at the ISP layer can generate security issues that may impact the ISP itself and its customers. As an example, Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks are aimed at disabling access to various Internet services for legitimate users, or Domain Name System (DNS) information may be exploited to redirect Internet traffic with malicious intent.

This pilot focuses on providing security analytics to ISPs that can benefit from a federation that securely and privately exchanges Cyber Threat Information (CTI). In addition, ISPs will benefit from data-manipulation operations, e.g., data-anonymisation and Data Sharing Agreements (DSAs) to protect, regulate and guarantee an expected privacy level of the data with the C3ISP Framework. In addition, part of the ISP pilot is Registro.it, which is the Italian registration authority for Internet domains and manages registration requests and information from about 1400 Italian Registrars (most of them act as Internet Service Providers – ISPs). In particular, within the ISP Pilot, Registro.it aims at expanding its business by offering security services to ISPs to protect their servers and services.

The most important services offered to ISPs, which benefit from the collaboration sharing of CTI within C3ISP, are:

- **Monitoring of connections to malicious hosts.** This refers to the analysis of network logs, e.g., NetFlow, using the homomorphic encryption to discover malicious traffic and connections in a privacy-preserving way.
- **Monitoring of Domain Generation Algorithm DNS-request.** This aims at detecting DNS requests that malwares may generate using time-based algorithms, e.g., [www.fgd2iwya7vinfutj5wq5we.com](http://www.fgd2iwya7vinfutj5wq5we.com).
- **Detection of brute force and DDoS attacks on services.** This aims at detecting brute-force and DDoS attacks by executing security analytics on log of services.
- **Malware spreading analysis.** Malware commonly spreads as email attachments. Relying on e-mails analysis, the C3ISP security analytics creates profiles of the malicious emails (e.g., sender, email body) and their attachments (e.g., document

---

<sup>3</sup> <https://www.techrepublic.com/article/should-isps-be-accountable-for-overall-internet-security/> . Last Update: January 2018

<sup>4</sup> <https://www.cio.com/article/2448243/it-strategy/seeing-no-evil--is-it-time-to-regulate-the-isp-industry-.html>

name) to support mail servers for blocking malicious emails and preventing further spreading.

### **1.8.2. CERT Pilot Blog**

The High Institute of Information and Communication Technologies (ISCOM), which is a Directorate of the Italian Ministry of Economic Development (MISE), hosts the Italian CERT, which is the main public organization in Italy informing private users and companies of novel cybersecurity threats, and fosters the adoption of good practices for system security. The CERT provides services of custom notification about cybersecurity information, to both large and small companies in Italy, by pairing news about threats and vulnerabilities, with those companies whose have an actual interest in specific subtopics.

The process of information and news collection, and subsequent delivery to the correct interested party(es) has been done up to now by a human operator in a semi-automated way. This is a limitation to the amount of information that can be processed and introduces the possibility of mistakes. Furthermore, the privacy of exchanged information is at risk, exposing the CERT at legal risks such as those specified in GDPR.

The introduction of C3ISP in the CERT operations, aims at tackling all these issues by providing a platform able to handle data in a completely privacy aware manner, which gives to data providers tools to define their own security and privacy policies, which will be enforced in a way, which is totally transparent to the CERT.

Furthermore, C3ISP empowers the CERT operative workflow by adding a large set of new operations that can be performed on data, providing cutting-edge, research-based technologies for the analysis of spam emails and traffic, and malware detection. Through C3ISP the CERT becomes able to process automatically larger set of information, delivering new and more accurate information to the interested recipient, with limited to no active user interaction. This also improves the timeliness in which information is extracted and delivered, in an environment where being faster than the attacker might imply the difference between receiving or not damages, whose recovery and consequences might cost even millions of Euro.

For this reason, several major companies have already shown their interest in the C3ISP technologies and in the new services offered by the CERT.

The main new services offered by the CERT through C3ISP are in a nutshell:

- Spam email filtering: Automatic analysis of large email sets, which separates good emails (ham) from unsolicited ones (spam).
- Spam email classification and campaign clustering: Currently spam emails are used to damage recipients in several ways, from distributing malicious software, to steal user credentials by performing phishing attacks. C3ISP is able to classify spam email files according to their type, so as to make the user(s) aware of the actual risks contained in received emails.
- Malware classification: Binary analysis for malware detection, exploiting features which make the system able to identify also new and unknown threat (Zero-day attacks).

The C3ISP framework is able to operate also on anonymized pieces of information, hence it is possible to use the functionalities offered by the CERT as-a-service, without having to disclose the actual information content to the CERT itself. This would improve the user acceptance of the CERT offered services.

### **1.8.3. SME Pilot Blog**

Focusing on the business case for SMEs and relevance of C3ISP:

The aim of the C3ISP SME Pilot is to enable SMEs to collect and share their Cyber Threat Information (CTI) data with the C3ISP platform in such a manner that each SME remains in full control of what is shared and how it is shared, preserving the confidentiality of their sensitive data. Vendors or service providers of Managed Security Service (MSS) solutions (such as the BT Intelligent Projection Service) can enhance their offerings with the C3ISP-enabled CTI sharing capability. This allows for constant feedback from SMEs about threats detected by their MSS agents deployed on their infrastructure. This threat intelligence can be rapidly promulgated to the other C3ISP partners and thus enhance the product/service capability and the SMEs experience and level of protection.

Where SMEs wish to outsource the security management aspect of their infrastructure by using MSS solutions, Managed Security Service Providers (MSSP), who typically only offer services to large enterprises, could consider extending their market to include SMEs. Usually the complexity and ROI to deal with many SMEs would be prohibitive, but the integrating capability of C3ISP should enable sufficient automation and scale to allow a group of SMEs to be effectively treated as a single enterprise, in order to derive a cost-effective solution tailored to SMEs needs.

The business value of joining the C3ISP platform for an SME derives from the effective scale that the sharing of CTI brings, which means that an SME gains access to what is effectively an enterprise-scale threat intelligence and response capability that it would otherwise not have access to. The scale derives from the sharing community of SMEs which together should see a range of CTI analogous to that seen across a larger enterprise. The quantity and quality of this capability can be further augmented by C3ISP's ability to share CTI with other organizations including ISPs and CERTs etc. The sharing of CTI data on C3ISP helps provide earlier detection of cyber threats and attacks on the SME participants with the potential to significantly reduce and or avoid business impacts

### **1.8.4. Enterprise Pilot Blog**

If you are providing security services for your customers, you are surely interested in protecting them better, more efficiently and more effectively. The Enterprise Pilot of C3ISP focusses on this challenge, tackling a concrete problem: i.e. how to improve early detection of threats and your analytical tools by using customer's data.

Normally your customers are pretty conservative about what you can and can't do with their data. However, would your customers be more assured about sharing their threat intelligence data if you offered them capabilities such as:

- Advanced sanitization measures, including differential privacy techniques.
- Sophisticated information sharing mechanisms, allowing the definition of fine-grained control policies (in natural language!) for data processing.
- Specially crafted analytics, fully compliant with data policies previously defined, adopting AI or Full Homomorphic Processing for maximum confidentiality.
- An effective sharing model, able to give back credit and advantages to the customers willing to share their data for additional purposes.

We are working to deliver all these capabilities, as part of our engagements in the C3ISP project. We are targeting enterprise use cases coming from Managed Security Service (MSS)

providers. We defined models where malware spreading is studied considering data coming from multiple customers, using differential privacy techniques (especially geo-indistinguishability) to blur identifiable attributes (e.g. identities, locations) of infected systems at the same time, preserving the utility of the remaining data. These capabilities provide to MSS customers, analysts and third parties like CERTs, with the business benefits that come from early Threat detection and Malware spreading forecasts.

We also aim to optimize the business case for using these services, by understanding the appreciation of our proposal by customers and thus by studying how it can be best introduced in today's market. So, if you are interested, if you want to know more or even share your thoughts on these ideas, feel free to get in contact through our social media.

## 2. Dissemination and Communication

Dissemination and Communications activities have been carried on within the second and third year of the project through:

- participation and organization of events.
- scientific publications.
- improvement of the web page and related activities on it.
- communication activities.

### 2.1. Participation and organization of events

Category	Lead Partner	Title	Date	Location	Audience
<b>Event Participation</b>	3D Repo	Digital Construction Week 2017	18/10/2017 – 19/10/2017	London, UK	Digital construction, engineering, design, manufacturing, and operation experts
<b>Event Organisation</b>	Uni-Kent	Meeting with Secure Data ( <a href="https://www.secdata.com/aboutus/">https://www.secdata.com/aboutus/</a> ) to discuss the gathering and use of CTI	18 September 2018	Univ of Kent	Senior staff from Secure Data and researchers from Kent
<b>Event Organisation</b>	CNR/ISCOM-MISE	CSM - European Cyber - Security Month	19/10/2017	Pisa, Italy	General public, acting as 'EU digital citizens' and specific groups focused on Member States stakeholders from public and private organisations e.g. IT experts, NIS authorities, Education
<b>Event Participation</b>	HPE	CTI – EU   Bonding EU Cyber Threat Intelligence	30/10/2017 – 31/10/2017	Rome, Italy	Those interested in CTI, Information sharing, Active defence, Automation of CTI, etc.
<b>Event Organisation</b>	CNR	Cyber Security day	17/11/2017	Pisa, Italy	C3ISP was promoted at winter school
<b>Event Organisation</b>	CNR	NeCS cyber security PhD Winter School	12/02/2018 - 16/02/2018	Trento, Italy	C3ISP and its partners support the the NeCS cyber security PhD Winter School
<b>Event Participation</b>	SAP	SAP Security Expert Summit	13/02/2018 – 14/02/2018	St Leon/Rot, Germany	Promotion of C3ISP at a reference event for the security community, but also



					for SAPs most relevant internal stakeholders
<b>Event Organisation</b>	DigiCat	Innovation Workshop	14/3/2018	London, UK	Overall objective: Understand where the commercial opportunities of the C3ISP technology are
<b>Event Participation</b>	Uni-Kent	Meeting	feb-18	Munich	Huawei has had a previous project with some similarities to C3ISP, and so they are very interested in our results. They would be willing to test our pilot software, and perhaps even provide a case study.
<b>Event Organisation</b>	3DRepo	British Information Modelling industrial event	27/6/2018	London, UK	from organisations such as BuroHappold, the Transport Research Lab (TRL) and Atkins, delegates at the evening seminar and networking event will also be able to get hands-on with some of the newest Building Information Modelling (BIM) technology including patent-pending clash and change detection solutions from 3D Repo. The British Information Modelling event is free to attend although pre-registration is required.
<b>Event Participation</b>	Uni-Kent	Academic Centres of Excellence in Cyber Security Research Conference	27-28/06/2018	Stratford upon Avon, UK	academic conference
<b>Event</b>	BT	IEEE CNS 2018 and 4th	30 May - 1	Beijing,	2018 IEEE

<b>Participation</b>		IEEE Workshop on Security and Privacy in the Cloud	June 2018	China	Conference on Communications and Network Security, 4th IEEE Workshop on Security and Privacy in the Cloud
<b>Event Participation</b>	SAP	SAP Security Expert Summit	18/03/2019 – 19/03/2019	St Leon/Rot, Germany	Promotion of C3ISP at a reference event for the security community, but also for SAPs most relevant internal stakeholders
<b>Event Participation</b>	DigiCat	Cloud and Cyber Security Expo	13th March, 2019	London	Hosted panel on Innovation in the age of GDPR at the expo. Broad audience of cyber security and cloud infrastructure providers seeking new solutions. Audience of 50 – 60 in public area
<b>Event Participation</b>	DigiCat	Cyber UK	22 April 2019	Glasgow	Hosted a panel on Near Future Impacts of AI and discussed the role of threat sharing in protecting against the impact of more advanced cyber attacks powered by AI. The audience was predominantly cyber security experts from across industry room of 60 - 70
<b>Event Organisation</b>	SAP	SAP C3ISP exploitation workshop	3/06/2019	Paris, France	Definition of value proposition for C3ISP assets with SAP's internal stakeholders
<b>Event Organisation</b>	DigiCat	Innovation Workshop 2: Commercial Opportunity Workshop	11 Oct, 2018	Pisa	Workshop to explore the commercial opportunities of C3ISP with the consortium
<b>Event Organisation</b>	DigiCat	Innovation Workshop 3: Open vs Proprietary Workshop	02, April, 2019	Pisa	Workshop at the consortium meeting in PISA to identify the potential

					business model with regards to the creation of open source and proprietary functionality
<b>Event Organisation</b>	DigiCat, SAP, BT	Cyber 101 Deep Dive	22 Aug, 2019	London	A Deep Dive with 3 threat sharing SMEs who are possible re-users or re-sellers of C3ISP with SAP
<b>Event Organisation</b>	DigiCat	BEIS/NCSC Workshop	17 July 2019	London	UK government department for Business, Energy and Industrial Strategy and representatives from the NCSC.
<b>Event Participation</b>	DigiCat plus CNR, BT, SAP, HPE	C3ISP exhibition / engagement stand at Cyber Tech Rome	24, 25 September 2019	Rome	Engagement with potential customers at the premier European Cyber Security Conference / Exhibition. See Annex 22
<b>Event Participation</b>	CNR, BT	ICISSP 2018, 4th International Conference on Information Systems Security and Privacy	22/01/2018 – 24/01/2018	Funchal, Portugal	Researchers and practitioners that address security and privacy challenges that concern information systems
<b>Event Participation</b>	GridPocket SAS	E-World Essen Expo & Summit	06/02/18	Essen, Germany	participate in the Fair, presentation at the conference, audience of about 100 people
<b>Event Participation</b>	GridPocket SAS	Workshop DigiCat	14/03/18	London, UK	Overall objective: Understand where the commercial opportunities of the C3ISP technology are Particular objectives: 1. Understand market needs and value propositions for sharing of threat
<b>Event Participation</b>	GridPocket Systems (GPS)	Spotkanie informacyjne GPS i Politechnika	16/03/18	Technical University Koszalin	presentation of the project C3ISP during the discussion - audience of about 40 people

<b>Event Participation</b>	GridPocket Systems (GPS)	Industry 4.0 conference	20/05/18	Technical University Koszalin	presentation of the project C3ISP during the discussion - audience of about 70 people
<b>Event Participation</b>	GridPocket Systems (GPS)	Środkowopomorskie Targi	22/03/18	Koszalin Expo-Hall	participate in the Fair, presentation at the conference, audience of about 100 people
<b>Event Participation</b>	GridPocket SAS	Smart Energies Expo&Summit 2018	05-06/06/2018	Paris, France	participate in the Fair, presentation at the conference, audience of about 250 people
<b>Event Organization</b>	CNR	1st International Workshop on Behavioral Analysis for System Security (BASS 2018)	26-28/07/2018	Porto, Portugal	CNR has organized in Porto, a workshop co-located with the conference SECRYPT 2018, named 1st International Workshop on Behavioral Analysis for System Security (BASS 2018). The workshop has acknowledged the C3ISP workshop.
<b>Event Organization</b>	CEA	Cingulata workshop	03/07/2018	Palaiseau, France	CEA has organized a tutorial workshop to present Cingulata compiler toolchain and the CRTE to the members of FUI project ANBLIC. The workshop has acknowledged the C3ISP project.
<b>Event Participation</b>	CNR	The 7 <sup>th</sup> International Workshop on Security, Privacy and Performance in Cloud Computing (SPCLOUD 2018)	July 16 – 20, 2018	Orléans, France	CNR is involved in the organization of the events. CNR also presents there results of the C3ISP project.
<b>Event Participation (Booth)</b>	CNR & DC	Italy cybertech conference	27-28 September 2018	Rome, Italy	CNR and DC presents the C3ISP project at the CyberTech Conference.
<b>Event Participation</b>	CNR	ESORICS 2018 conference	3-7 September 2018	Barcelona, Spain	CNR participates and organize a workshop to

<b>Event Participation</b>	GPS	Reliability and Cybersecurity	18-19/09/2018	Kazimierz Dolny, Poland	ESORICS conference
<b>Event Participation</b>	CHINO	Pioneers Health	October 2018	Wien, Austria	GPS participates to the event presenting C3ISP results.
<b>Event Participation</b>	CHINO	Medica	November 2018	Dusseldorf, Germany	
<b>Event Participation</b>	CHINO	Frontiers Health	November 2018	Berlin Germany	
<b>Event Participation</b>	CNR	Cyber Security Day at Internet festival	12 Octobre 2018	Pisa, Italy	
<b>Event Participation</b>	GPS	Cybersecurity, IoT, SmartGrid	2019 H1	Poland	Participate at the fair, presentation at the conference.
<b>Event Participation</b>	GridPocket SAS	Cybersecurity, IoT, SmartGrid	2019 H1	France, Holand, Germany	Participate at the fair, presentation at the conference.
<b>Event Participation</b>	3D Repo	Digital Construction week trade show.	17-18 October 2018	London	
<b>Event Organisation</b>	DigiCat	Exploitation Workshop	Aligned with end phase 2 (September 2019)	Cyber Tech Rome plus external stakeholder evaluation in London	Exhibit / demonstrate C3ISP at Cyber Tech.
<b>Event Organisation and Participation</b>	Uni-Kent	Kent Cyber Security Forum	5 September 2019	University of Kent, UK	Approx 100 people from industry, the public sector and Academia (staff and students)
<b>Event Organisation and Participation</b>	CNR, SAP	ESORICS 2019 conference	23-27 September 2019	Luxembourg	CNR participates and organize a workshop to ESORICS conference, SAP participates to both for dissemination activities.

## 2.2. Press Releases

- 3D Repo Cyber security project aimed at protecting construction industry assets wins funding 3/3/2017 <http://www.pbctoday.co.uk/news/bim-news/cyber-security-project-aimed-protecting-construction-industry-assets-wins-funding/31372>  
IT and construction
- CNR Cyber security project aimed at protecting construction industry assets wins funding 12/10/2018 [https://www.ilsole24ore.com/art/tecnologie/2018-10-11/aziende-e-pa-lezione-cybersecurity-arriva-portale-cnr-113410.shtml?uud=AE865JLG&refresh\\_ce=1](https://www.ilsole24ore.com/art/tecnologie/2018-10-11/aziende-e-pa-lezione-cybersecurity-arriva-portale-cnr-113410.shtml?uud=AE865JLG&refresh_ce=1) Digital industry

- 3D Repo British Information Modelling 28/6/2018  
<http://3drepo.org/bim-event-speakers-make-plea-for-digital-transformation-in-construction/> IT and construction
- 3DRepo British Information Modelling 22/10/2018  
<http://3drepo.org/bim-event-marks-start-of-successful-digital-construction-week-for-3d-repo/> IT and construction
- DC Consortium assembles to deliver C3ISP project dedicated to help the fight against cyber crime 3/8/2017 <https://www.digicatapult.org.uk/projects/c3isp/> Digital industry
- GridPocket Konsorcjum realizuje projekt c3isp "collaborative and confidential information sharing and analysis for cyber protection 24/4/2017  
"https://www.gridpocket.com/pl/badania.html
- <https://ru-ru.facebook.com/pg/GridPocketSystems/notes/> " Digital industry
- C3ISP CERT Pilot Press release 8/4/2019  
<https://www.c3isp.eu/content/cert-pilot-press-release> Digital industry
- C3ISP SME Pilot Press release 8/4/2019  
<https://www.c3isp.eu/content/sme-pilot-press-release> Digital industry
- C3ISP Enterprise Pilot Press release 8/4/2019  
<https://www.c3isp.eu/content/enterprise-press-release> Digital industry
- C3ISP ISP Pilot Press release 8/4/2019 <https://www.c3isp.eu/content/isp-pilot-press-release> Digital industry

### 2.3. Publications

Within the second and third year of the project, the following publication related to the C3ISP topics and results have been produced:

#### *Conference/Workshop*

- Fabio Martinelli, Francesco Mercaldo, Andrea Saracino BRIDEMAID: An Hybrid Tool for Accurate Detection of Android Malware ACM Asia Conference on Computer and Communications Security (ASIACCS)
- Fabio Martinelli, Iliaria Matteucci, Paolo Mori, Andrea Saracino Concurrent History-based Usage Control Policies MODELSWARD 2017
- Gianpiero Costantino, Fabio Martinelli, Iliaria Matteucci, Marinella Petrocchi Analysis of Data Sharing Agreements International Conference on Information Systems Security and Privacy (ICISSP 2017)

- Mario Luca Bernardi, Marta Cimitile, Fabio Martinelli, Francesco Mercaldo A Fuzzy-based Process Mining Approach for Dynamic Malware Detection IEEE International Conference on Fuzzy Systems
- Mario Luca Bernardi, Marta Cimitile, Fabio Martinelli, Francesco Mercaldo A Time Series Classification Approach to Game Bot Detection 7th ACM International Conference on Web Intelligence, Mining and Semantics (WIMS)
- Mario Luca Bernardi, Marta Cimitile, Fabio Martinelli, Francesco Mercaldo Game Bot Detection in Online Role Player Game through Behavioural Features 12th International Conference on Software Technologies (ICSOFT)
- Fabio Martinelli, Francesco Mercaldo, Vittoria Nardone, Antonella Santone How Discover a Malware using Model Checking ACM Asia Conference on Computer and Communications Security (ASIACCS)
- Mina Sheikhalishahi, Fabio Martinelli Privacy Preserving Clustering over Horizontal and Vertical Partitioned Data The 22nd IEEE Symposium on Computers and Communications
- Mina Sheikhalishahi, Fabio Martinelli Privacy-Utility Feature Selection as a Privacy Mechanism in Collaborative Data Classification The 26th IEEE International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE 2017)
  
- Mina Sheikhalishahi, Fabio Martinelli Privacy-Utility Feature Selection as a tool in Private Data Classification 14th International Conference on Distributed Computing and Artificial Intelligence (DCAI 2017)
- Antonio La Marra, Fabio Martinelli, Paolo Mori, Andrea Saracino. Implementing Usage Control in Internet of Things: A Smart Home Use Case, , IEEE Trustcom 2017
- Ian Herwono and Fadi Ali El-Moussa. Collaborative Tool for Modelling Multi-Stage Attacks. 3rd International Conference on Information Systems Security and Privacy - ICISSP 2017”, 19-21 February 2017, Porto, Portugal.
- Malika Izabachène, Iliaria Chillotti, Nicolas Gama, Mariya Georgieva. Faster Packed Homomorphic Operations and Efficient Circuit Bootstrapping for TFHE" in Asiacrypt 2017.
- Sergiu Carpov, Donald Nokam Kuate, Sebastien Canard, Renaud Sirdey. Running compression algorithms in the encrypted domain: a case-study on the homomorphic execution of RLE, proceedings of the Privacy, Security and Trust 2017
- Kalpana Singh, Renaud Sirdey, François Artiguenave, David Cohen and Sergiu Carpov. Towards confidentiality-strengthened personalized genomic medicine embedding homomorphic cryptography, proceedings of the 3rd International Conference on Information Systems 2017 Security and Privacy
- Giubilo, Fabio; Sajjad, Ali; Shackleton, Mark; Chadwick, David W.; Fan, Wenjun; de Lemos, Rogério. “An Architecture for Privacy-preserving Sharing of CTI with 3rd

- party Analysis Services”. In: 12th International Conference for Internet Technology and Secured Transactions (ICITST), 11-14 December 2017, Cambridge, UK.
- Jozef Dobos, Carmen Fan, Pavol Knapo and Charence Wong; "Applications of Web3D Technology in Architecture, Engineering and Construction" in the 23rd International ACM Conference on 3D Web Technology
  - Xiao-Si Wang, Ian Herwono, Francesco Di Cerbo, Paul Kearney, Mark Shackleton. "Enabling Cyber Security Data Sharing for Large-scale Enterprises Using Managed Security Services". Proceedings of 2018 IEEE Conference on Communications and Network Security (CNS), 30 May - 1 June 2018, Beijing China.
  - Ian Herwono and Fadi Ali El-Moussa. Automated Detection of the Early Stages of Cyber Kill Chain. 4th International Conference on Information Systems Security and Privacy - ICISSP 2018, 22-24 January 2018, Funchal, Portugal.
  - Andrea Saracino, Francesco Restuccia, Fabio Martinelli. Practical Location Validation in Participatory Sensing Through Mobile WiFi Hotspots, TrustCom/BigDataSE
  - Fabio Martinelli, Francesco Mercaldo, Andrea Saracino. POSTER: A Framework for Phylogenetic Analysis in Mobile Environment, AsiaCCS 2018
  - Ian Herwono , Fadi Ali El-Moussa. A System for Detecting Targeted Cyber-Attacks Using Attack Patterns, Information Systems Security and Privacy. ICISSP 2017
  - Gianpiero Costantino, Antonio La Marra, Fabio Martinelli, Paolo Mori, Andrea Saracino. Privacy Preserving Distributed Computation of Private Attributes for Collaborative Privacy Aware Usage Control Systems, SMARTCOMP2018
  - Giampaolo Bella, Francesco Marino, Gianpiero Costantino, Fabio Martinelli. Getmewhere: A Location-Based Privacy-Preserving Information Service, PDP 2018
  - Fabio Martinelli, Francesco Mercaldo, Christina Michailidou, Andrea Saracino. Phylogenetic Analysis for Ransomware Detection and Classification into Families, International Conference on Security and Cryptography (SECRYPT), 2018
  - Alberto Ferrante,, Miroslaw Malek, Fabio Martinelli, Francesco Mercaldo, Jelena Milosevic. Extinguishing Ransomware - A Hybrid Approach to Android Ransomware Detection, International Symposium on Foundations & Practice of Security (FPS), 2017
  - Davide Maiorca, Francesco Mercaldo, Giorgio Giacinto, Corrado Aaron Visaggio, Fabio Martinelli. R-PackDroid: API package-based characterization and detection of mobile ransomware, In proceedings of Symposium On Applied Computing (SAC), 2017
  - Gerardo Canfora, Giovanni Cappabianca, Pasquale Carangelo, Fabio Martinelli, Francesco Mercaldo, Ernesto Rosario Russo, Corrado Aaron Visaggio. Mobile Silent and Continuous Authentication using Apps Sequence, 14th International Conference on Security and Cryptography (SECRYPT)
  - Aniello Cimitile, Fabio Martinelli, Francesco Mercaldo. Machine Learning meets iOS Malware: Identifying Malicious Applications on Apple Environment, 3rd International Conference on Information Systems Security and Privacy (ICISSP 2017)



- Aniello Cimitile, Fabio Martinelli, Francesco Mercaldo, Vittoria Nardone, Antonella Santone. Formal Methods Meet Mobile Code Obfuscation Identification of Code Reordering Technique, The 26th IEEE International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE-2017)
- Fabio Martinelli, Francesco Mercaldo, Vittoria Nardone, Antonella Santone. Car Hacking Identification through Fuzzy Logic Algorithms, IEEE International Conference on Fuzzy Systems

### *Journal*

- Francesco Mercaldo, Andrea Di Sorbo, Corrado Aaron Visaggio, Aniello Cimitile, Fabio Martinelli: "An Exploratory Study on the Evolution of Android Malware Quality", Journal of Software: Evolution and Process, 2018
- Maria Francesca Carfora, Fabio Martinelli, Francesco Mercaldo, Vittoria Nardone, Albina Orlando, Antonella Santone, Gigliola Vaglini: A "Pay How You Drive" Car Insurance Approach through Cluster Analysis, Soft Computing, 2018
- Mario Luca Bernardi, Marta Cimitile, Fabio Martinelli, Francesco Mercaldo: Driver and Path Detection through Time-Series Classification, Journal of Advanced Transportation, 2018
- Mario Luca Bernardi, Marta Cimitile, Damiano Distanti, Fabio Martinelli, Francesco Mercaldo: Dynamic Malware Detection and Phylogeny Analysis using Process Mining, International Journal of Information Security, 2018
- Gerardo Canfora, Fabio Martinelli, Francesco Mercaldo, Vittoria Nardone, Antonella Santone, Corrado Aaron Visaggio: LEILA: formal tool for identifying mobile malicious behaviour, IEEE Transactions on Software Engineering, 2018
- Ian Herwono and Fadi Ali El-Moussa. A System for Detecting Targeted Cyber-Attacks Using Attack Patterns. In: P. Mori, S. Furnell, O. Camps (eds) Information Systems Security and Privacy. ICISSP 2017. Communications in Computer and Information Science, vol 867. Springer, Cham. June 2018.

### *White paper*

- Charles Fox and Brian MacAulay - A New Perspective on Cyber Risk (Applied to the evolving UK Energy Grid Eco-System), @ <https://www.c3isp.eu/download/publications-list/new-perspective-cyber-risk-applied-evolving-uk-energy-grid-ecosystem>
- Charles Fox and Brian MacAulay - Applying the benefit harm index, a new approach to modelling risk assessment of cyber ecosystems and their socio-economic impacts

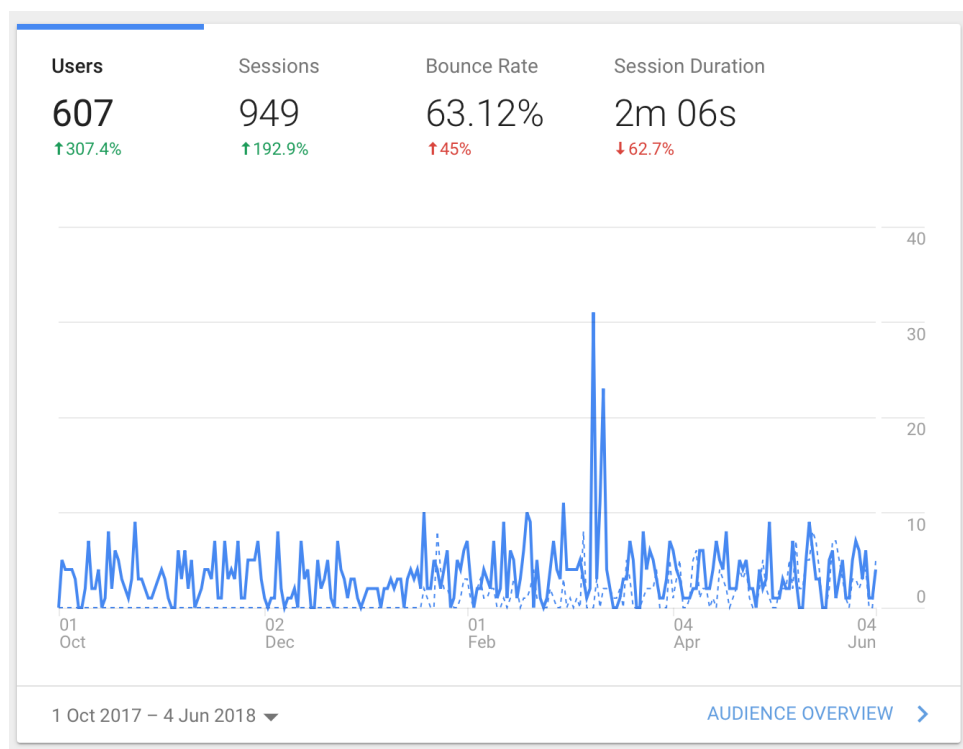
to the UK’s evolving connected and autonomous vehicle ecosystem, @ <https://www.digicatapult.org.uk/news-and-views/publication/a-new-perspective-on-cyber-risk/>

- David W Chadwick, Wenjun Fan, Gianpiero Constantino, Rogerio De Lemos, Francesco Di Cerbo, Ian Herwono, Paolo Mori, Ali Sajjad, Xiao-Si Wang, Mirko Manea. “A cloud-edge based data security architecture for sharing and analyzing cyber threat information”. Future Generation Computer Systems, Online Aug 2019 at <https://doi.org/10.1016/j.future.2019.06.026>

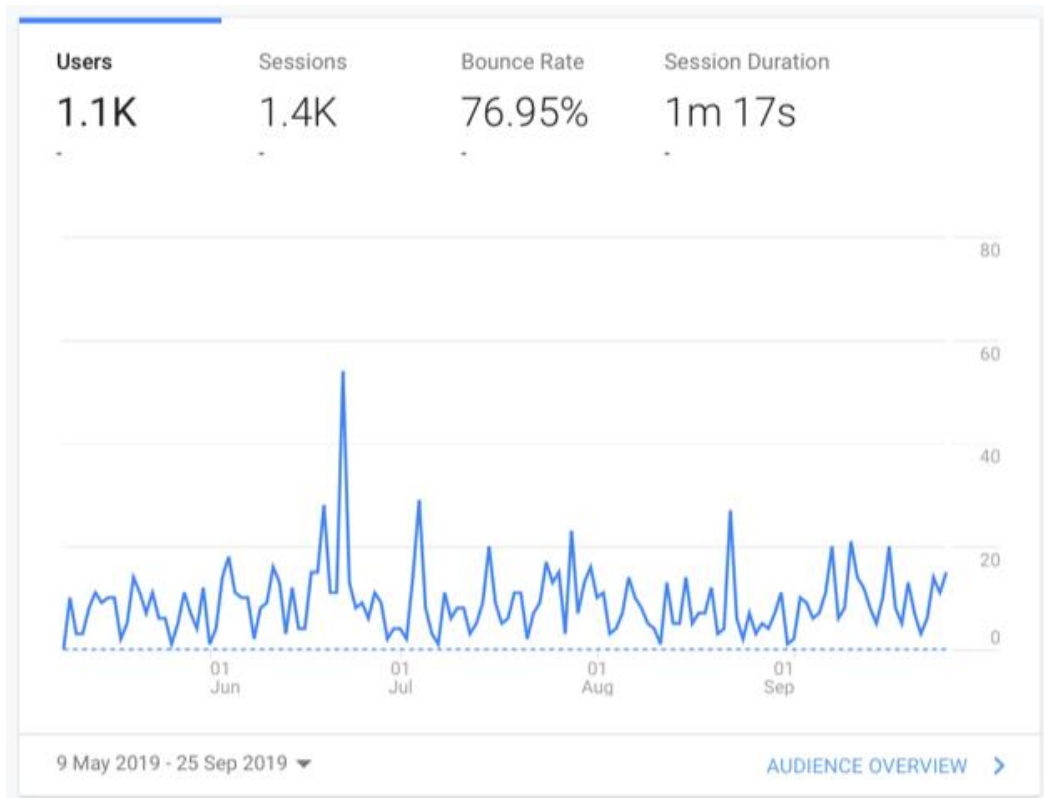
## 2.4. Communication activities

### 2.4.1. C3ISP WebPage

The C3ISP Web Page reports on the activities of the project. It is the main dissemination and communication mean and it is quite visited from users of different countries all over the world.

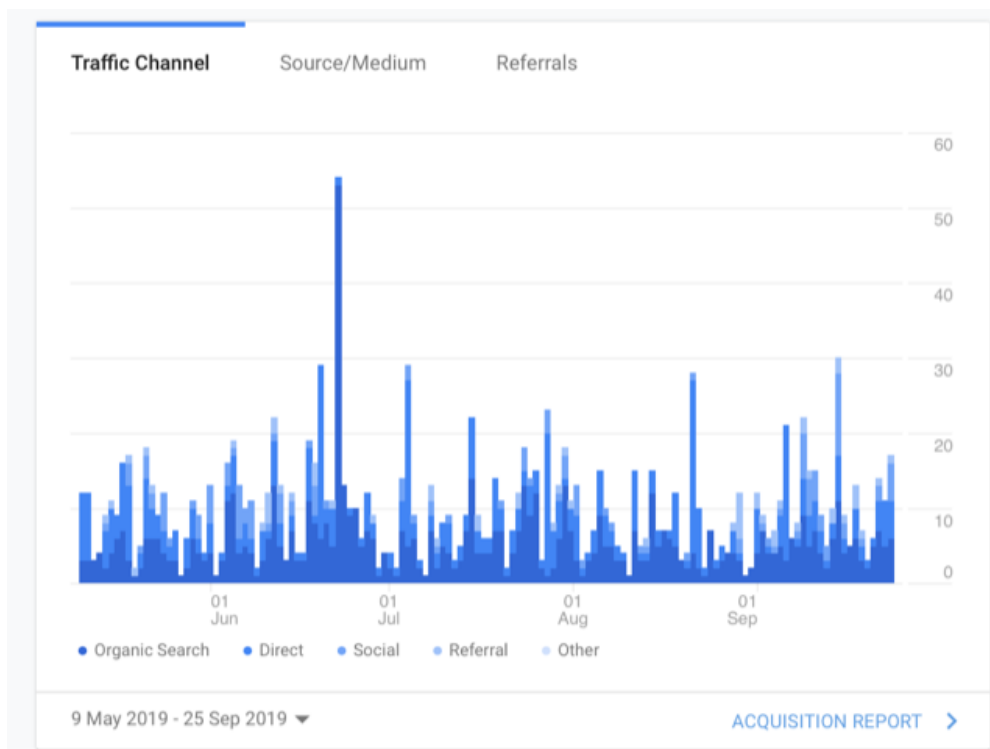


**Figure 15. Distribution of visitors within the second year of the project.**



**Figure 15a – Distribution of visitors during third year - May to September 2019**

Note: Google Analytics crashed in May resulting in loss of statistics to web sites including C3ISP.eu.



**Figure 15b – C3ISP site acquisition report**

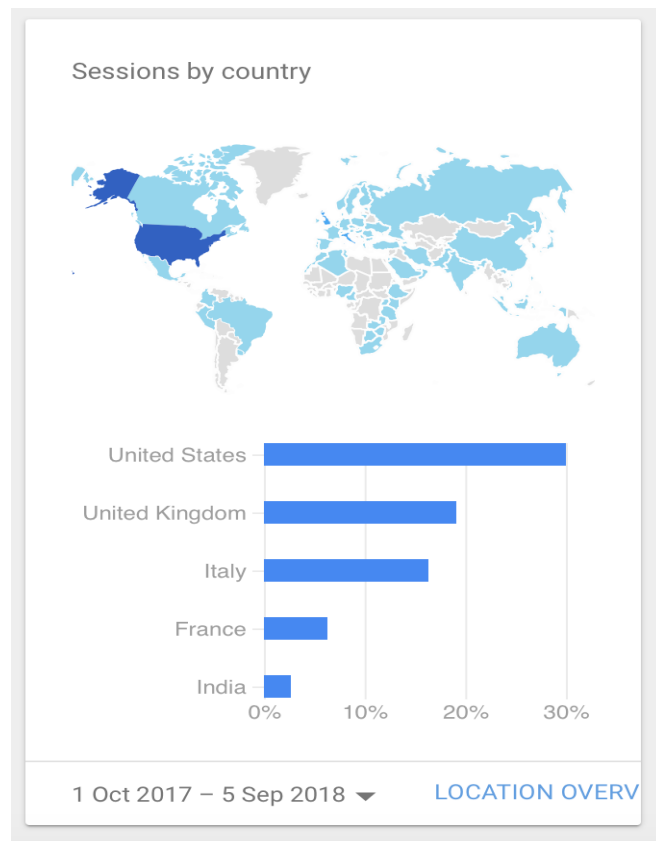


Figure 16. Distribution of sessions per country.

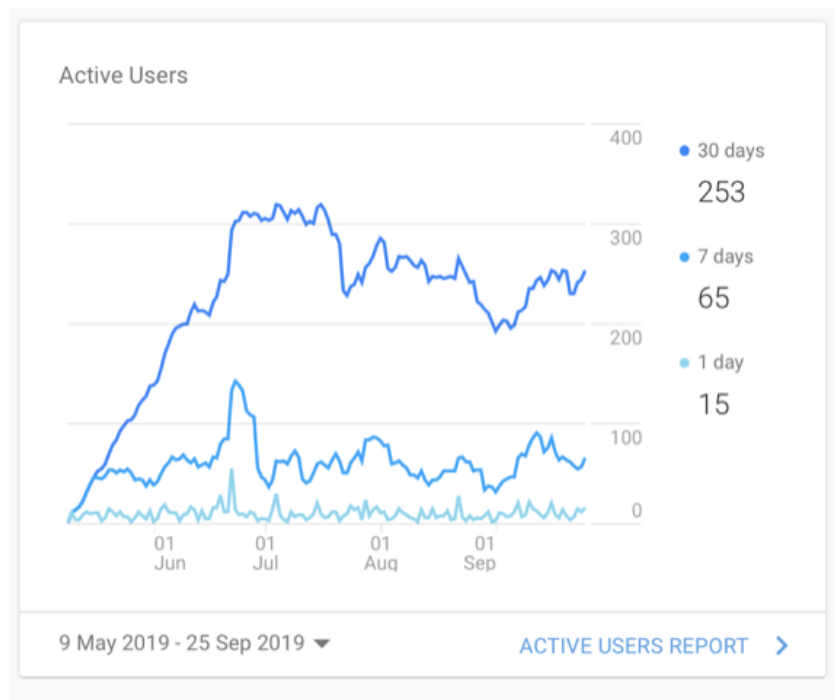


Figure 16a – Active Users

### 2.4.2. Social Media

Category	Lead Partner	Title	Date	Location/Source
Social Media	GridPocket Systems (GPS)	Facebook GridPocket Systems (Poland)	18 posts regarding the project C3ISP - 21 followers	<a href="https://www.facebook.com/GridPocketSystems/">https://www.facebook.com/GridPocketSystems/</a>
Social Media	GridPocket SAS	Facebook GridPocket (France)	18 posts regarding the project C3ISP - 28 followers	<a href="https://www.facebook.com/gridpocket/">https://www.facebook.com/gridpocket/</a>
Social Media	GridPocket Systems (GPS)	LinkedIn GPS SA	11 posts regarding the project C3ISP - 44 followers	<a href="https://www.linkedin.com/company/gridpocket-systems-s-a-/">https://www.linkedin.com/company/gridpocket-systems-s-a-/</a>
Social Media	GridPocket SAS	LinkedIn Gridpocket, Sophia-Antipolis, France	11 posts regarding the project C3ISP - 211 followers	<a href="https://www.linkedin.com/company/gridpocket-sophia-antipolis-france/">https://www.linkedin.com/company/gridpocket-sophia-antipolis-france/</a>
Social Media	GridPocket SAS	GridPocket (R&D)	extensive discussion regarding the project C3ISP - tab R&D	<a href="http://gridpocket.com/en/">http://gridpocket.com/en/</a>

Both C3ISP Twitter and LinkedIn accounts are very active and received attention by more than one hundred of followers or connections.

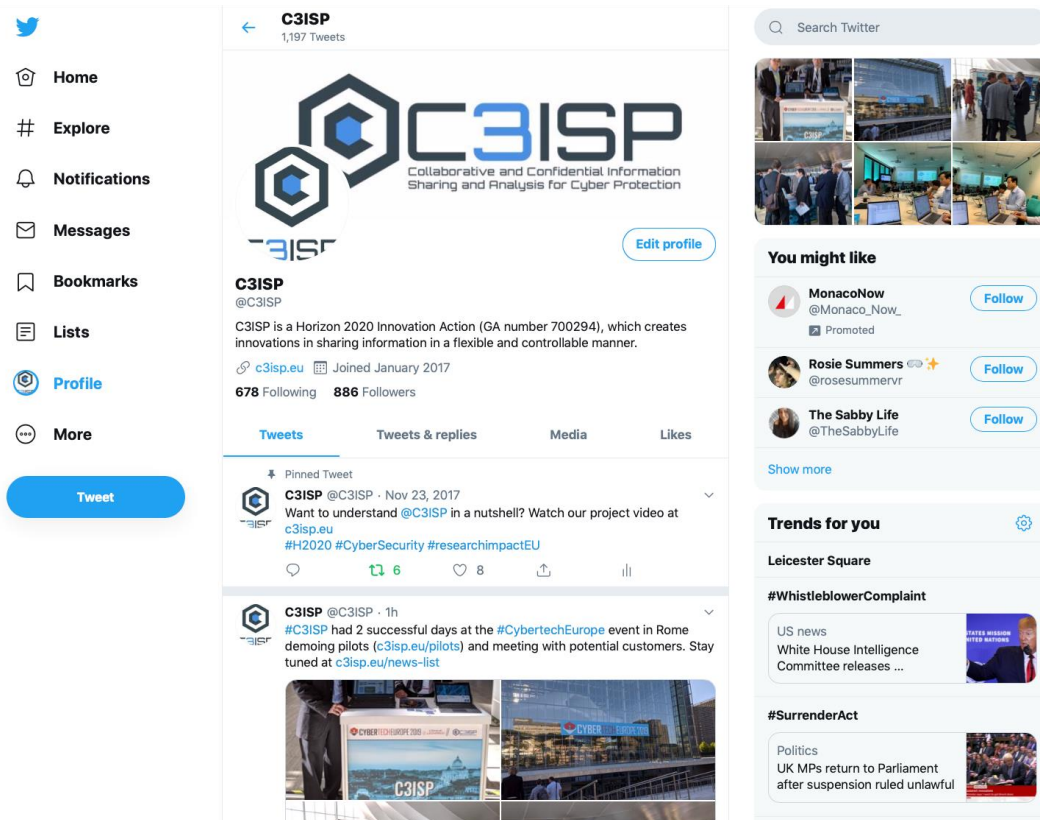


Figure 17. C3ISP Twitter account.

Highlight here is 868 followers as at September 2019 and 1,197 tweets.

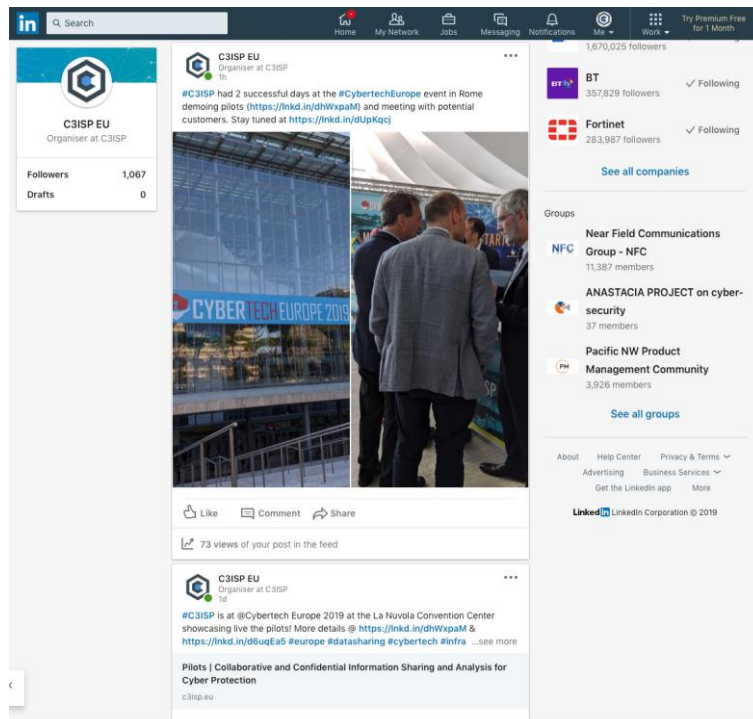
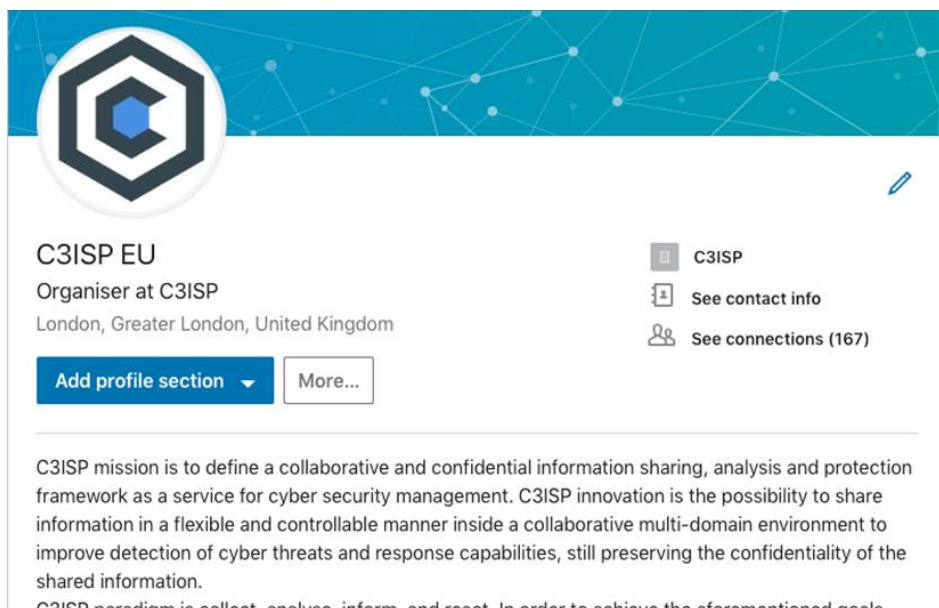


Figure 18. C3ISP reaches over 1000 followers after CyberTech Rome 2019

The other social media account of the project is the one DigitCatapult made on LinkedIn.



Our C3ISP LinkedIn account has over 500 connections.

### 2.4.3. Other Communication activities

Category	Lead Partner	Title	Date	Source	Audience
<b>Blog</b>	3D Repo	BIM Event Speakers Make Plea for Digital Transformation in Construction	29/6/2018	<a href="http://3drepo.org/category/pres-s-releases/">http://3drepo.org/category/pres-s-releases/</a>	All partner stakeholders
<b>Flyer v2</b>	DigiCat	Updated project Brochure/Flyer	1/7/2018	<a href="https://c3isp.eu/download/others-list">https://c3isp.eu/download/others-list</a>	C3ISP brochure is updated with the latest information on the project to support all partners in the promotion of the project
<b>Flyer v3</b>	DigiCat	Updated project Brochure/Flyer	20/8/2019	<a href="https://c3isp.eu/download/others-list">https://c3isp.eu/download/others-list</a>	C3ISP brochure is updated with the latest information on the project to support all partners in the promotion of the project

### **3. Standardization**

In line with what it has been described in D9.2 and 9.3, some investigations have been carried on performing an of the standardisation state-of-the-art by exploiting direct active link with standard and initiative, such as OASIS XACML, BSI and TRUESSEC.eu.

Within the second year of the project, the idea of trying to propose some project solution as possible standards has been matured.

#### **3.1. *CEA Contribution to Standardization***

In order for Homomorphic Encryption (HE) to be adopted in medical, health, and financial sectors to protect data and patient and consumer privacy, the question is how to make standardized this technology, most likely by multiple standardization bodies, government agencies and especially an important part of standardization is broad agreement on security levels for varying parameter sets. Some kind of discussions was addressed during the HE standardization workshop over March 15-16 2018 on MIT Stata Center, hosted at Microsoft Research in Redmond, Cambridge, USA. CEA team and other research groups around the world who have made libraries for general-purpose homomorphic encryption available.

#### **3.2. *DigiCat contribution to Standard***

Going forward DigiCat will lead the co-ordination of a clear strategy and methodological approach for orchestrating C3ISP's contributions to influence standards/technical recommendations bodies:

1. Gap analysis of standard status and requirements - Throughout the project, consortium members will regularly monitor evolutions and gaps in the relevant standardisation landscape, e.g. to identify new/incubation standardisation initiatives relevant to C3ISP.
2. Prioritised engagement on specific standards with the associated standard body. This will include building on the work with OASIS.
3. Liaison with the standard body to recommend development of new standards or to support specific evolution of existing ones.

We have proposed and validated with the consortium members a simple Framework as shown below for mapping the C3ISP capabilities and architectural sub systems to the corresponding standards.



C3ISP Sub Systems & Environmental domains	Functions	Standards / Body	Generic / C3ISP created/ driven	Questions / Suggestions
ISI	Provides API for managing data protected objects (DPOs) i.e. CTI with Data Sharing Agreement (DSA)	STIX (Structured Threat Information Expression), TAXII (Trusted Automated Exchange of Indicator Information) – originally created by Stix project, now maintained by <a href="#">OASIS CTI TC</a>	Generic	<i>Have members been active in developing STIX 2.1? If so we should highlight.</i>
IAI	e.g. provides API to access Information Analytics Infrastructure	No known standards body – Standards gap identified	Potential to be C3ISP driven	
DSA Manager	Provides tools for creating DSAs, which comprise data sharing policies and usage control policies	DSAs are based on the <a href="#">OASIS XACML Standard</a> with extensions originally created by the <a href="#">EC COCO cloud project</a> .	C3ISP created	<i>Should we add Web Ontology Language (OWL)?</i>
CSS	Identity Management	Currently using <a href="#">JETF LDAP</a> but are migrating to <a href="#">OpenID Connect</a> from the OpenID Foundation	Generic	....
	Homomorphic Encryption	Homomorphic Encryption based on <a href="#">Cingulata Toolchain</a> created by CEA team. Standardized work for this tool is in process with respect to requirements from <a href="#">Homomorphic Encryption Security Standard</a>	Generic	<i>What is current state of our FHE performance?</i>
External Analytics Tools	e.g. Immersive Visualiation	Gap?		
Others		Does the C3ISP TIP intend to inject Threat data in formats other than STIX 2, e.g. STIX 1, email, REST API ?		

Table 1 – Mapping standards to the C3ISP Sub system framework

We have used this framework to collaborative and holistically identify gaps in the standards and to thus identify opportunities to fill those gaps where appropriate.

### 3.3. Individual Consortium members contribution to Standard Activities

The individual contribution to standards by C3ISP consortium members is show in the next table.

Consortium Member	
BT	o Provided insights into relevant standards that BT is using in its existing background technology.
3D REPO	o 3D Repo has held numerous meetings with various representatives of building SMART UK and US in order to push the standardisation of the cybersecurity initiatives within our specific industry o 3D Repo has also contributed to the National Infrastructure report in the UK to push the C3ISP cybersecurity agenda.
CNR	o In the first year of the project CNR started to investigate standard processing to support activity in this task.
HPE	o HPE jointly work with UNIKENT to assess the standardization bodies that could be exploited for C3ISP standardization effort. In particular OASIS group was selected as the most appropriate venue to possibly evaluate standardization of key C3ISP Framework artifacts, like the XACML extensions for the DSA policy enforcement language.
UNIKENT	o The University of Kent joined OASIS on behalf of the consortium, so that input from consortium members can be fed into the relevant OASIS standards and standards meetings. CNR has identified potential input to the XACML group concerning enhancements it has made for usage control. The University of Kent is a member of BSI and gets access to ISO standards. We notified the consortium that a new standard on Data Sharing Agreements is being proposed, but due to ISO copyright rules, we could not make the contents available to other consortium members <b>Standards Activities / Contributions</b> as none of them were members of their National Bodies.
CEA	<ul style="list-style-type: none"> <li>o Provided a first release Cingulata 1.0 in open-source version in Feb. 2018, this compilation toolchain is now available at <a href="https://github.com/CEA-LIST/Cingulata">https://github.com/CEA-LIST/Cingulata</a>. The fact of integrating Cingulata in C3ISP project and deploying a version of Cingulata in open-source offer to operation users a flexibility to develop and deploy his own algorithm working with FHE. Our exploitation plan is             <ul style="list-style-type: none"> <li>o To initiate end users able to work with FHE</li> <li>o To provide our expertise on performance and optimization to offer a robust solution for them.</li> <li>o Pro – active in standardisation consortium for FHE technology, the last workshop was held at MIT, Cambridge MA, USA, March 15th – 16th 2018. Via this workshop, CEA’s team actively keep update and looking for recommendations to make Cingulata more easy to use.</li> </ul> </li> <li>o Organized a tutorial workshop to present Cingulata compiler toolchain, the CRTE (runtime environment) and the</li> <li>o C3ISP works to the members of FUI project ANBLIC.</li> </ul>

Consortium Member	Standards Activities / Contributions
CEA - Continued	<p><b>API standardization activities :</b></p> <p>CEA team was invited in writing 3 white papers for API standardization corresponding to 3 cryptographic scheme : BFV/BGV, TFHE and CKKS. White paper consists of defining API in high-level concept and focus on presenting</p> <ul style="list-style-type: none"> <li>- what an application developer needs to know, to understand</li> <li>- how to use the scheme,</li> <li>- what the core terminology is about, and to link its security to what is presented in the security standard.</li> </ul> <p><b>Workshop activities:</b></p> <ul style="list-style-type: none"> <li>- CEA team has attended the Third Homomorphic Encryption Standardization Workshop, in Toronto, Canada on October 20, 2018</li> </ul> <p><b>Opensource activities:</b></p> <ul style="list-style-type: none"> <li>- A release version for Cingulata is officially available since 12th June in GitHub : <a href="https://github.com/CEA-LIST/Cingulata">https://github.com/CEA-LIST/Cingulata</a></li> </ul> <p>This version allows Cingulata Framework supporting TFHE library, the performance of algorithm based on TFHE is clearly improved in comparison to the one using BFV/BGV library.</p> <p>In terms of storage, the size of data encrypted with TFHE is always in constant size, not depended to algorithm but the security parameter, whereas the size of data generated from BFV/BGV scheme is depended on multiplicative depth of algorithm.</p>

**Table 3.2 – Individual contribution to standards activities by C3ISP consortium members**

Consortium Member	Standards Activities / Contributions
CHINO	o Participated to the discussions among partners regarding the standardization objectives of the project.
GRIDPOCKET	o Provided insights into relevant standards that GPS is using in its existing background technology. For example c3ISP Format Adaptor helps to translate CTI data to STIX
SAP	o Provided insights into relevant standards that SAP is using in its existing background technology.
DIGICAT	o Performed an initial search of review materials of state-of-the-art analysis on threat intelligence standards. o Explored possible links with TRUESSEC.eu. o Initiated project relationship with BSI.
ISCOM-MISE	?

**Table 3.2 – Individual contribution to standards activities by C3ISP consortium members - *continued***

## 4. References

- [1] OASIS Open. (2017). Sharing threat intelligence just got a lot easier. Retrieved 25 October 2017, from <https://oasis-open.github.io/cti-documentation/>
- [2] MITRE. (2017). About STIX. Retrieved 25 October 2017, from <https://stixproject.github.io/about/>
- [3] OASIS Open. (2017). STIX Objects. Retrieved 25 October 2017, from <https://oasis-open.github.io/cti-documentation/stix/intro>
- [4] Yun-Hua, G; Pei, L (2010). "Design & Research on Vulnerability Databases": 209–212.
- [5] Karlsson, M (2012). "The Edit History of the National Vulnerability Database and similar Vulnerability Databases".
- [6] NIST. "[NVD Primary Resources](https://nvd.nist.gov/)". *National Vulnerability Database*. Retrieved 25 October 2017, from <https://nvd.nist.gov/>
- [7] Stiennon, R. (2016). Researching the threat intelligence space. CSO. Retrieved 25 October 2017, from <http://www.csoonline.com/article/3047197/techology-business/researching-the-threat-intelligence-space.html>
- [8] Tittel, E. (2017). Comparing the top threat intelligence services. April 2017. TechTarget. Retrieved 25 October 2017, from <http://searchsecurity.techtarget.com/feature/Comparing-the-top-threat-intelligence-services>
- [9] Wilson, T. (2015). Threat intelligence Platforms: The Next ‘Must-Have’ For Harried Security Operations Teams. Dark Reading. Retrieved 25 October 2017, from <http://www.darkreading.com/threat-intelligence-platforms-the-next-must-have-for-harried-security-operations-teams/d/d-id/1320671>
- [10] Poputa-Clean, P. (2015). Automated Defense Using Threat Intelligence to Augment Security, Mark Stingley Accepted: January 2015
- [11] CSIRTGadgets. Collective Intelligence Framework. Retrieved 25 October 2017, from <http://csirtgadgets.org/collective-intelligence-framework/>
- [12] REN-ISAC. (2017). Research & Education Networking Information Sharing & Analysis Centre. Retrieved 25 October 2017, from <https://www.ren-isac.net/>
- [13] CRIT. (2015). Wiki Home page. Retrieved 25 October 2017, from <https://github.com/crits/crits/wiki>
- [14] Siemens. (2013). The MANTIS Cyber-Intelligence Management Framework. Retrieved 25 October 2017, from <http://django-mantis.readthedocs.org/en/latest/>
- [15] MISP. MISP - Open Source Threat Intelligence Platform & Open Standards for Threat Information Sharing. Retrieved 25 October 2017, from <http://www.misp-project.org/>

- [16] CIRCL. Malware Information Sharing Platform MISP – A Threat Sharing Platform. Retrieved 25 October 2017, from <http://www.circl.lu/services/misp-malware-information-sharing-platform>
- [17] Wilson, T. (2015) Threat Intelligence Platforms: The Next ‘Must-Have’ For Harried Security Operations Teams. DARKReading. February 2015. Retrieved 25 October 2017, from <http://www.darkreading.com/threat-intelligence-platforms-the-next-must-have-for-harried-security-operations-teams/d/d-id/1320671>
- [18] SEIa. (2017). Incident Management. Software Engineering Institute, Carnegie Mellon University. Retrieved 30 October 2017, from <http://www.cert.org/incident-management/>
- [19] SEIb. (2017). List of Nation CSIRTs. Carnegie Mellon University. Retrieved 30 October 2017, from <http://www.cert.org/incident-management/national-csirts/national-csirts.cfm?>
- [20] ORG. (2017). CERT-UK. Open Rights Group Wiki. Retrieved 30 October 2017, from <https://wiki.openrightsgroup.org/wiki/CERT-UK>
- [21] HMG. (2014). UK Launches first national CERT. Cabinet Office. 31 March 2014. Retrieved 25 October 2017, from <https://www.gov.uk/government/news/uk-launches-first-national-cert>
- [22] Hansard. (2016). Intention to transfer CERT-UK to the new National Cyber Security Centre: Written statement – HCWS653. Hansard. 24 March 2016. Retrieved 30 October 2017, from <http://www.parliament.uk/business/publications/written-questions-answers-statements/written-statement/Commons/2016-03-24/HCWS653/>
- [23] SANS. (2016). From the Trenches: SANS 2016 Survey on Security and Risk in the Financial Sector. October 2016. Retrieved 8 November 2017, from <https://www.sans.org/reading-room/whitepapers/analyst/trenches-2016-survey-security-risk-financial-sector-37337>
- [24] NC4. (2017). SOLTRA EDGE. Retrieved 30 October 2017, from <http://www.soltra.com/>
- [25] Jisc. (2017). Janet Network CSIRT. Retrieved 30 October 2017, from <https://www.jisc.ac.uk/csirt>
- [26] NHS. (2017) Data and cyber security: protecting information and data in health and case. NHS Digital. Retrieved 30 October 2017, from <https://digital.nhs.uk/cyber-security>
- [27] CORTE. (2012). CYSPA. Retrieved 30 October 2017, from <http://www.corte.be/activities/road-security/corte-activities/eu-funded-projects/cyspa>
- [28] CyberConnector. (2017). CyberConnector – Collective Knowledge Base to Improve Cyber-security. Engineering. Retrieved 30 October 2017, from <https://cyberconnector.eu/>
- [29] ACDC. (2017). Advanced Cyber Defence Centre. Retrieved 30 October 2017, from <https://www.acdc-project.eu/>
- [30] NCSCa. (2017). The National Cyber Security Centre. Crown copyright. Retrieved 30 October 2017, from <https://www.ncsc.gov.uk/>

- [31] NCSCb. (2017). About us. NCSC. Retrieved 30 October 2017, from <https://www.ncsc.gov.uk/about-us>
- [32] Ponemon. (2016). *The Value of Threat Intelligence: A Study of North American and United Kingdom Companies*, Ponemon Institute, July 2016
- [33] Source: Requirements for the SME Pilot, D5.1
- [34] D9.1 – First exploitation and Dissemination plan.
- [35] BT takes on global cybersecurity threats. ITProPortal. Retrieved 12 September 2018, from <https://itproportal.com/news/bt-takes-on-global-cybersecurity-threats/>
- [36] Digital Catapult white paper - A new perspective on Cyber Risk [https://assets.ctfassets.net/nubxhjiwc091/SKgHfURDIDYiAqNd0kV4Y/b9335a1e706a7f0f5be3809877d0888a/Final - A New Perspective on Cyber Risk.pdf](https://assets.ctfassets.net/nubxhjiwc091/SKgHfURDIDYiAqNd0kV4Y/b9335a1e706a7f0f5be3809877d0888a/Final_-_A_New_Perspective_on_Cyber_Risk.pdf)

## ANNEX 1 : Glossary

Table 5 - Glossary

<b>Acronym</b>	<b>Definition</b>
<i>AaaS</i>	Application as a Service
<i>BIM</i>	Building Information Management
<i>CERT</i>	Community Emergency Response Team
<i>CSP</i>	Cloud Service Provider
<i>CSSA</i>	Cyber Security Sharing and Analytics
<i>DDoS</i>	Distributed Denial of Service
<i>DSA</i>	Data Sharing Agreement
<i>ETD</i>	Enterprise Threat Detection
<i>GIS</i>	Geographic Information System
<i>IaaS</i>	Infrastructure as a Service
<i>IP</i>	Intellectual Property
<i>ISP</i>	Internet Service Provider
<i>MSS</i>	Managed Security Service
<i>OEM</i>	Other Equipment Manufacturer
<i>PTC</i>	Patent Cooperation Treaty
<i>SME</i>	Small and Medium Enterprise
<i>SVN</i>	Apache Subversion
<i>TI</i>	Threat Intelligence, also Cyber Threat Intelligence (CTI)

# ANNEX 2 - C3ISP “Building a route to market for new cybersecurity technologies”

## C3ISP “Building a route to market for new cyber security technologies” Open Call





[OUR WORK](#) [OUR CENTRES](#) [GET INVOLVED](#) [EVENTS](#) [INSIGHTS](#) [CAREERS](#) [ABOUT](#)

### Building a route to market for new cyber security technologies

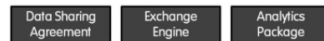
March 14 @ 8:30 am - 3:00 pm

#### What is C3ISP?

C3ISP is a collaborative R&D project set up to facilitate the design and validation of a confidential information sharing, analysis and protection framework for cyber security management. The project is designed to enable fast and accurate detection of cyber-attacks and share security data in a flexible and controllable manner inside a collaborative multi-domain. At the same time, C3ISP aims to preserve the confidentiality of shared information.

Digital Catapult is running a workshop to investigate, validate and optimise the initial exploitation of the below three core capabilities in the marketplace. We hope to develop beneficial product and service offerings in this domain based on technologies of the project.

#### C3ISP capabilities:



1. The Data Sharing Agreement (DSA): allows the specification of a fine-grained access control policy that can be interpreted by a computer in near real-time.
2. The Exchange Engine: enables auditable sharing of sensitive information in accordance with the DSA.
3. The Analytics Package: leverages a combination of Privacy Enhancing Technologies (PET) in the context of visualisation to allow state-of-the-art shared security analytics.

#### Benefits of C3ISP:

- Enables the fast and accurate detection of cyber-attacks.
- Facilitates early communication of IT vulnerabilities and best practices to avoid exploitation.
- Provides flexibility ensured by DSA, which allows using the framework in multi-stakeholder environments.
- Delivers data analysis compliant with customer policies as dictated by privacy or business needs.

#### Who should apply for the workshop?

In order to build routes to market for this new technology, Digital Catapult is looking for organisations including, but not limited to:

- Providers of security products and services who could leverage C3ISP to improve their security or privacy capabilities, including enterprises and startups.
- Businesses who seek to improve cyber threat intelligence, data protection or asset and network security.
- Public bodies such as the National Cyber Security Centre (NCSC), Standard Bodies and Computer Emergency Response Teams (CERT).
- Internet Service Providers (ISPs), Cloud Service Providers and other Infrastructure as a Service (IaaS) companies.

We are specifically inviting application from those with both a technical and a business background.

#### Why you should get involved?

BT, SAP, Hewlett Packard Enterprise and other consortium partners are interested in identifying partners to mutually explore commercial opportunities to exploit this technology. That means you can help future proof next generation cyber security capabilities, particularly for confidential information sharing, analysis and protection and also become an early stage adopter.

Attend the workshop and you can learn about state-of-the-art cyber security tools and techniques – ‘Shared Security Analytics’, as well as meet representatives from industry and academia to identify potential projects of common interest.

#### Who is involved?



Please note registration for this workshop is via application – please visit our Open Call below.

CONFIDENTIALINFORMATIONSHARING, CYBERPROTECTION, CYBERSECURITY, CYBERTHREATS, SECURITYANALYSIS

[» REGISTER YOUR INTEREST IN THIS EVENT](#)

[+ GOOGLE CALENDAR](#) [+ ICALEXPORT](#)

Feedback

Feedback



## ANNEX 3 - List of Approached Companies

### List of Approached Companies

Citicus	Swivel
Acuity Risk Management	Secure Lujam
Assuria	Internet Security
SentryBay	Intruder
Cybersafe	Becrypt
CyberLytic	Clearswift
Silicon:Safe	ZoneFox
SaltDNA	Privitar
Autocrypt Solutions	Cyberlytic
Uleska Limited	Perception Cyber Security
ProtectBox	Cyber Sparta
Ansec AI	Verasseti
Titan IC	Cynation
Aramar	Modux
Panaseer	Surevine
Meterian	Cybershield Group
SocialOptic	Digital Shadows
Circadian	Riskaware
PixelPin	Corvid
Themis Consulting	RazorSecure
Xenadata	Elliptic
RazorSecure	Prosyn Ltd
Elliptic	Protectimus
Verizon	BAE Systems
	Thales

## **ANNEX 4 - List of Attending Companies**

### List of Attending Companies

#### List of Attendees

BT

HPE

SAP

Digital Catapult

National Research Council

3d Repo

GridPocket

CEA

University of Kent

BAE Systems

Clearswift

Surevine

Verizon

Thales

## ANNEX 5 - Workshop 1 Agenda

### Workshop 1 Agenda

#### C3ISP Innovation Workshop



Wednesday 14<sup>th</sup> March  
@ Digital Catapult Centre, Kings Cross, London

08:30	Arrivals
09:00	Welcome note from Digital Catapult <i>Luke Openshaw</i>
09:15	Welcome note from BT <i>Mark Shackleton</i>
9:25	Introduction to C3ISP <i>Ismail Khoffi</i>
9:45	Workshop stage 1: Identifying Market Needs and Value Propositions
10:45	Break
11:00	Workshop stage 2: Addressing Barriers
12:00	Lunch
12:45	Workshop stage 3: Business Models
13:45	Next Steps
14:00	Close

# ANNEX 6 - Workshop 1 Table Plan

## Workshop 1 Table Plan

### Table Plan

#### Table 1

Selina - BT  
Mirko - HPE  
Cherlaine - DC (Facilitator)  
Thanh – CEA  
Glen – Huawei  
Shadi – Cynation

#### Table 3

Mark - BT  
Maria P- DC (Facilitator)  
Alex – Thales  
Marko – Grid Pocket  
Alyn - Clearswift

#### Table 2

Joshua - BT  
Wayne - DC (Facilitator)  
John - Surevine  
Kieron – 3D Repo  
Andrew – BAE Systems  
Jean - SAP

#### Table 4

Claudio - HPE  
Francesco – SAP  
Ismail - DC (Facilitator)  
Theo – UniKent  
Opeoluwa – Verizon  
Gianpiero - BT



# ANNEX 7 – Workshop 1 – worksheets

## 7.1. Worksheet 1: Identifying Market Needs and Value Propositions



### 1. Identifying Market Needs and Value Propositions

How businesses currently share threat intelligence?	Main opportunities of C3ISP to improve threat intelligence
<ul style="list-style-type: none"><li>• What do they share (internally and externally)?</li><li>• How is the intelligence shared?</li><li>• What are the available market solutions for sharing?</li></ul>	

## 7.2 Worksheet 2: Addressing Barriers



### 2. Addressing Barriers

Data Sharing Barriers	Other Barriers
Barrier 1: _____ Overcome by...	Barrier 1: _____ Overcome by...
Barrier 2: _____ Overcome by...	Barrier 2: _____ Overcome by...
Barrier 3: _____ Overcome by...	Barrier 3: _____ Overcome by...
Is enforcement of sanitization measures sufficient to share threat intelligence?	

### 7.3. Worksheet 3: Business Models



## 3. Business Models

QUESTION:	ANSWER:
How would customers buy or procure a solution like C3ISP?	
Could this be sold better as a standalone offer or as an add-on to existing products or services?	
Who would be the key influencer in purchasing decisions?	
What incentives could be used to increase chance of purchase? (e.g. free trial)	

## ANNEX 8 - Workshop 1 - rules of the road

### Workshop 1 - rules of the road



## Rules of the Road

### Non-confidentiality and IP notice



With regards to the C3ISP Innovation Workshop on the 14<sup>th</sup> of March 2018 all attendees agree to the following:



1 All information that you share at the workshop shall be considered **non-confidential** (i.e. “in the open”), so you choose what you disclose to others. If you do share information then be aware that you are sharing it openly and participants are free to talk to others about their experiences.



2 If there comes a point in the activity when you feel that it is more appropriate for a conversation to move to a “closed” mode (i.e. to be confidential), then let us know and your Catapult lead will make appropriate arrangements.



3 The workshop is an environment where new ideas are generated, and sharing is encouraged. You agree to be respectful of others' thoughts and ideas.



4 You acknowledge that other attendees may use, share and publish any new ideas generated by you at the workshop, with attribution where appropriate. This includes sharing ideas with third parties not present at the workshop who may take action and independently use the new ideas.



5 If you use an idea generated by someone else at the workshop, you do so at your own risk and agree not to claim or register that idea as your own.



6 Attendees at the workshop that choose to present or discuss any pre-existing material that is protected by intellectual property rights (IPR) – such as software code – are deemed to be the owner (or licensee) of such IPR and so have the right to present or discuss it at the workshop.



7 If you do present or discuss any of your pre-existing intellectual property (IPR) during the workshop, you must clearly advise others that it is your IPR, and other participants agree not to use it, unless they obtain the right to do so from you outside of the workshop.

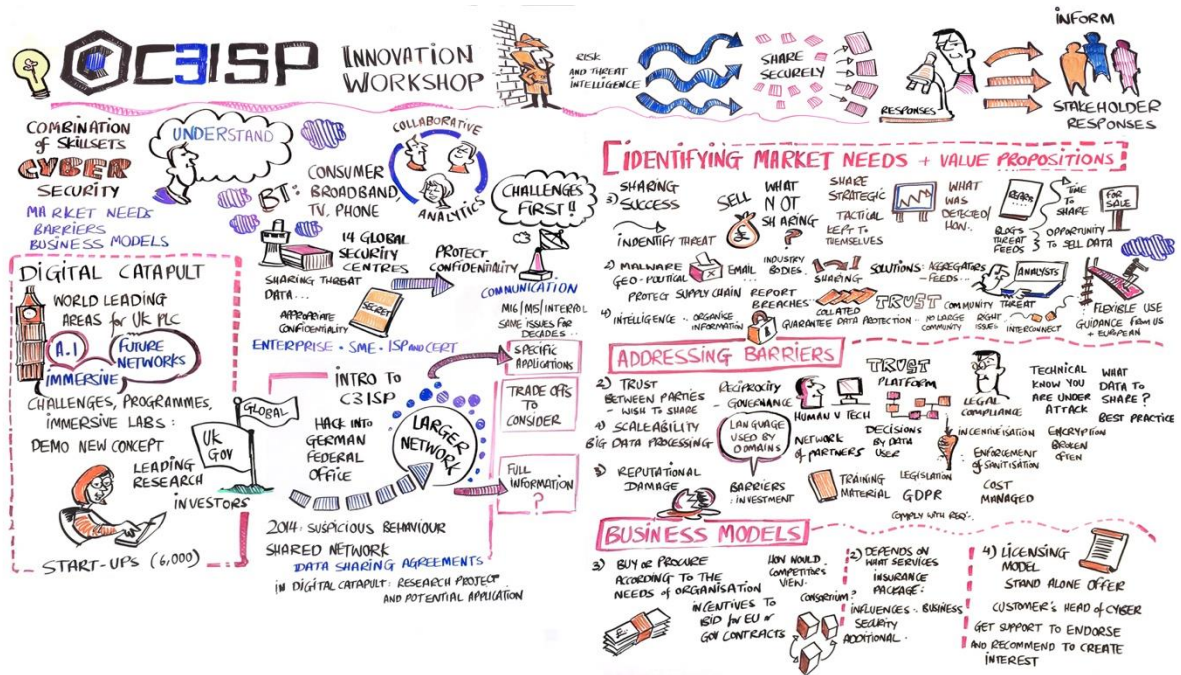
“Intellectual property” includes proprietary know-how, copyrighted material, inventions, patent rights, and any other type of intellectual property whether registered or unregistered

**If you have any questions regarding the Rules of the Road please speak to a member of the facilitation team.**



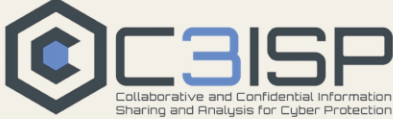
# ANNEX 9 - Workshop 1 - Illustration

## Workshop 1 - Illustration



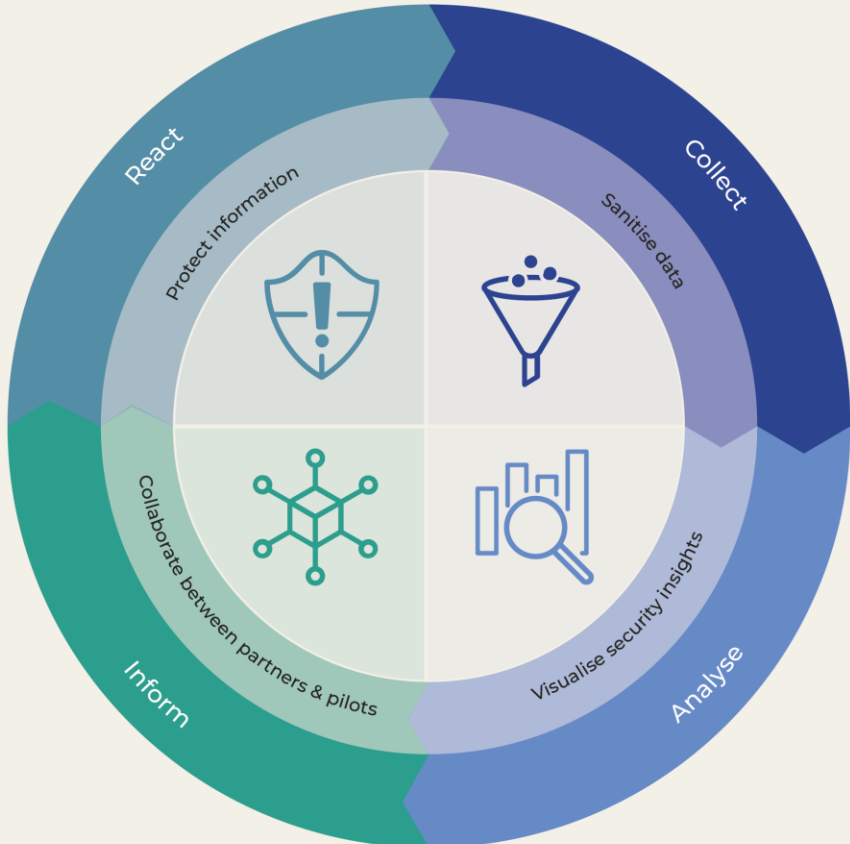
# ANNEX 10 - C3ISP Brochure

## C3ISP Brochure



Find out more  
[www.c3isp.eu](http://www.c3isp.eu)


### Cyber-Security Framework



C3ISP provides a flexible framework allowing automated, fast, and collaborative cyber threat information (CTI) sharing and analysis to allow a more complete understanding and faster mitigation of cyber risks.

ref: NIST800-150

#### Design process for the pilots





Icon design by  
Gulfarm Services  
Nespa Project



The C3ISP Project is supported by funding under the Horizon2020 Framework Program of the European Commission DS 2015F1, GA 700294

# ANNEX 11 - Workshop Tweets

## Workshop Tweets

This screenshot shows the Twitter profile of Digital Catapult (@DigiCatapult). The profile header includes the name, handle, and statistics: 24.5K tweets, 7,366 following, 26K followers, 13K likes, and 34 lists. A 'Follow' button is visible. The main content area displays three tweets:

- A tweet from Digital Catapult: "Investment Forum Meeting. The forum will be an opportunity to identify ... digitalcatapultcentre.org.uk" with 1 retweet and 1 like.
- A retweeted tweet from Digital Catapult: "C3ISP @C3ISP · Mar 14 We are running our #C3ISP #cybersecurity Innovation Workshop at @DigiCatapult. Working collaboratively to identify market needs and value propositions. Among our attendees were @bt\_uk @HPE @SAP @StampaCnr" with 5 retweets and 9 likes. It includes a photograph of a workshop session.
- A retweeted tweet from Digital Catapult: "UK Business Angels @UKBAngels · Mar 13 Guest speaker @JeremyS1 CEO of @DigiCatapult talking on the future & massive uptake of #AR #VR in broad industry applications in training & education #IMOLTechInvest" with 4 retweets and 7 likes.

At the bottom of the visible tweets, there is a tweet from Digital Catapult dated Mar 13: "#immersedinNI got off to a great start yesterday at #sxsw. We discussed".

This screenshot shows the Twitter profile of Digital Catapult (@DigiCatapult) with updated statistics: 24.7K tweets, 7,362 following, 26.6K followers, 13K likes, and 34 lists. A 'Follow' button is visible. The main content area displays three tweets:

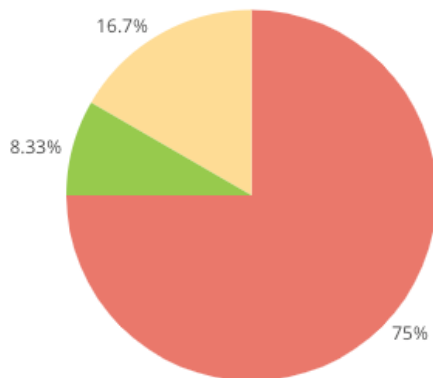
- A tweet from Digital Catapult dated Jun 1: "We've been working collaboratively to identify market needs and value propositions in the first #c3isp #cybersecurity Innovation Workshop with our partners @bt\_uk @HPE @SAP @StampaCnr. Listen to what participants are saying about the workshop here: [c3isp.eu/news-list](https://c3isp.eu/news-list)" with 2 retweets and 2 likes. This tweet is highlighted with a red border and includes a link to a video.
- A tweet from Digital Catapult dated May 31: "Have you signed up to our newsletter? Keep up to date with open calls, meetups and events by registering your details at the bottom of our homepage: [ow.ly/cJBs30kgNmF](https://ow.ly/cJBs30kgNmF)" with a 'Don't miss out' graphic below it.

## ANNEX 12 – Workshop 1 - Feedback Form Results

### Feedback Form Results

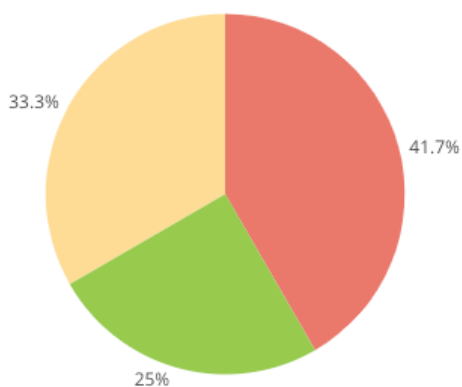
1. Overall, how would you rate your experience at the C3ISP Workshop?

2.



CHOICE	RESPONSES	PERCENTAGE
Very Satisfied	9	75%
Satisfied	2	16.7%
Unsatisfied	1	8.33%
Neutral	0	0%
Very Unsatisfied	0	0%

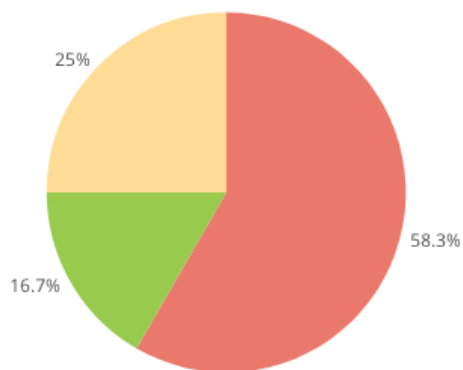
2. I attended...&nbsp;



CHOICE	RESPONSES	PERCENTAGE
on behalf of a large organis...	5	41.7%
on behalf of C3ISP Consortium	4	33.3%
on behalf of a small or med...	3	25%
as an academic	0	0%
on behalf of Digital Catapult	0	0%

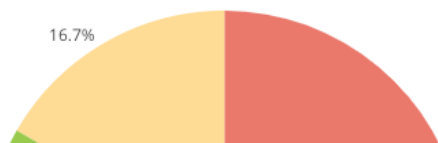
3. Which of the following statements do you agree with?&nbsp;





**4. Which aspect of the Workshop is of most value for you overall?**



CHOICE	RESPONSES	PERCENTAGE
Interacting with other parti...	7	58.3%
Workshops	3	25%
Talks	2	16.7%

**5. Please rate the value of the workshop?**



	CHOICE	RESPONSES	PERCENTAGE
	5 Very useful	8	66.7%
	3 Generally interesting	2	16.7%
	2 Some value	1	8.33%
	4 Quite useful	1	8.33%
	1 No interest	0	0%

## ANNEX 13 - C3ISP Competitor Details

### C3ISP Competitor Details

#### **EclecticIQ**

EclecticIQ Platform for Cyber Threat Intelligence <https://www.eclecticiq.com/platform>

EclecticIQ Platform is a Threat Intelligence Platform (TIP) that empowers threat analysts to perform faster, better, and deeper investigations while disseminating intelligence at machine-speed.

#### **EclecticIQ as C3ISP Competition – our view**

The EclecticIQ CTI platform looks like a strong competitor to C3ISP it enables CTI sharing with third parties allowing selective anonymisation and uses STIX and TAXII protocols for standard interoperability and taxonomies. It features strong graphical analytics tools and strong integration of IOC (Indicators of Compromise) and IOA (Indicators of Attack) into security controls. The following list of features is impressive:

#### **Features**

##### **Share intelligence with ISACs, ISAOs, interest groups and other sharing communities**

Exchange intelligence with ISACs, ISAOs, industry interest groups and other sharing communities through emerging industry standards STIX and TAXII, as well as community-specific protocols, anonymized where necessary.

##### **Maximize the value of information sharing with full support of STIX and TAXII standards**

EclecticIQ is an active participant in the development of STIX and TAXII, OASIS-backed standards for sharing cyber threat intelligence data across sharing communities. Through the use of these standards, organizations enable higher levels of automation in information-sharing, leading to a smarter shared response to cyber threats.

##### **Turn the diversity of threat data into actionable intelligence**

Integrate, normalize and consolidate sources of incoming cyber threat intelligence from multiple formats, both structured and unstructured, into a central intelligence repository.

Enrich incoming information using external databases or internal databases, based on powerful rule sets to improve context.

Supported data formats include open sources, communities and commercial intelligence suppliers, as well as emails, and other unstructured sources.

##### **Conducts triage and focus on the most important tasks**

Discover the most relevant intelligence from the central intelligence repository, allowing you to focus on the day's most pressing threats.

Set policy-based alerts based on advanced search logic and network graph correlation matrices.

Qualify threats based on proximity, confidence, threat level or other factors fully customizable to your own workflow and taxonomy

**Make sense of intelligence with powerful graphing capabilities and advanced search**

Powerful graphing capabilities help you make sense of incoming intelligence. See clear connections between entities based on their shared characteristics, helping you to place each piece of information into the right context.

Advanced search tools allow you to explore the full collection of intelligence in the repository.

Pivot easily to uncover hidden correlations across multiple large datasets.

**Create structured intelligence based on observable incidents, attack patterns and other data points.**

Manage structured intelligence concerning adversary tools and methods, threat actors, campaigns and courses of action; and unstructured, multi-paragraph intelligence reports.

Supported entities: Observables, Indicators, Actors, Malware, Vulnerabilities, Attack Patterns or other TTPs, Campaigns, Incidents, Courses of Action and Report.

**Integrate structured intelligence into existing security controls**

Improve the capabilities of enterprise detection, prevention and response systems by boosting the signal-to-noise ratio of relevant cyber threat intelligence.

Automatically deliver intelligence feeds, including Indicator of Compromise (IOC) and Indicator of Attack (IOA), into existing security controls:

- Security Information and Event Management (SIEM) from HPE ArcSight, IBM QRadar, Splunk and others
- Intrusion Detection
- End Point Protection and Monitoring
- Incident Workflow
- Native bidirectional integrations with SIEM software.

The extensive EclecticIQ Platform API enables unlimited inbound/outbound integration.



## Anomali's Threat Stream

Anomali's Threat Stream CTI platform <https://www.anomali.com/platform>

Deployment options include cloud, on premises and air gapped.

### **Anomali's Threat Stream as C3ISP Competition – our view**

The Anomali CTI platform looks like another competitor to C3ISP

#### **Features**

##### **Collaboration features include:**

Sharing intelligence amplifies more than just your own defenses - it protects the community at large. Anomali enables organizations to share intelligence and collaborate on investigations with internal teams and established partners.

- Instantaneous bi-directional sharing of intelligence
- Maintain full control of privacy levels and shared information
- Proactively respond to security events before they become breaking news
- Align yourself with industry peers through [Information Sharing and Analysis Centers \(ISACs\)](#)
- Benefit from security expertise, research, and recommended responses of other organizations

##### **Secure Platform for Trusted Collaboration**

Anomali provides a complete threat sharing platform, trusted by more ISACs and ISAOs to power secure collaboration. ISAC partner benefits include:

- Branded threat sharing community portal
- Dedicated Trusted Circle on the Anomali platform
- Admin access to vet and control membership
- STIX/TAXII server for programmatic access
- Anomali Analyst licenses for all community members
- Industry-specific research from Anomali Threat Analysis Center, <= Competes with our proposed C3ISP CNI focused approach!
- Community training, education and support

##### **Overview of features**

- Collect intelligence from premium feeds, OSINT, STIX/TAXII, ISACs
- Evaluate and purchase intelligence feeds via Anomali APP Store
- Apply machine learning optimized threat intelligence and reduce false positives
- Normalize disparate sources and enrich with additional threat context
- Give your analysts decision advantage and improve situational awareness

**An example ISAC that Anomali has partnered with (again relevant to C3ISP our C3ISP CNI focused approach):**

The Energy Sector Security Consortium, Inc. (EnergySec) is a United States 501(c)(3) non-profit corporation formed to support energy sector organizations with the security of their critical technology infrastructures. Through our membership program, we support collaborative initiatives and projects that help enhance the cybersecurity resiliency of these organizations. Today, our community includes more than 5000 individuals representing more than 500 organizations. The development of the EnergySec information sharing efforts and workforce development remain a key focus areas of EnergySec as it continues to develop programs and other efforts to meet the needs of the energy sector into the future.

## ThreatConnect's TC Complete

ThreatConnect® <https://threatconnect.com/solution/intelligence-sharing/>

This platform makes it easier to share information across organizations and industries. This in turn allows these groups to use threat intelligence for a more proactive defense.

### **Threat Connect's TC Complete as C3ISP Competition – our view**

This platform is a viable proven competitor. Playbooks provide a differentiator. However there is no mention of anonymisation in the context of their platforms sharing of threat information which would be a C3ISP differentiator.

### **Features**

#### **Threat Information Sharing**

ThreatConnect's powerful capabilities create a complete solution for all businesses and communities whether your organization is an information sharing analysis center (ISAC), a single enterprise sharing across departments, or in a private community with your partners.

#### **Collaboration with Industry Groups**

Our strategic partnerships and integration capabilities with respected organizations greatly simplify collaboration efforts. Whether it's using the ThreatConnect Platform to get all members working out of one solution, or ingesting ISAC provided data feeds, we let community members share their threat intelligence and their resources for an improvement in the protection of their assets. Using their TAXII server, all ThreatConnect customers can collect and send STIX formatted threat intelligence and connect compatible TAXII clients directly to indicator watch lists in ThreatConnect. Our TAXII server provisions unique ThreatConnect-exclusive metrics like observations, false positives, and Threat Assess scores.

#### **Analytics**

ThreatConnect's CAL™ (Collective Analytics Layer) provides anonymized, crowdsourced intel about your threats and indicators. It leverages the collective insight of the more than the thousands of analysts who use ThreatConnect around the globe to provide you with even more context regarding your indicators and threats. The more you know about a threat and the sooner you know it, the better equipped you are to fight it.

**Review by SC Labs magazine** – Their findings summarised below:

**Strengths:** Dashboards are easy to drill down into information; has a modern look and feel.

**Weakness:** Cost is a bit high; support options could be slightly more encompassing.

**Verdict:** Solid solution that has a lot to offer. Playbooks are a nice touch and really help this product stand out.

## NC4's Soltra Edge

NC4's Soltra Edge platform has a strong reputation as a TIP (Threat Information Platform)

### **NC4's Soltra Edge as C3ISP Competition – our view**

Another strong competitor, very strong on the standards such as STIX, TAXII etc. and it also features anonymisation and trust groups. Established reputation - most widely adopted cyber threat intelligence communication platform in the world.

The following features include marketing pitch but highlights what they see as their differentiators:

#### **Features**

Proven in research by the Johns Hopkins Applied Physics Laboratory, which used Soltra Edge for automated information sharing, to reduce threat-response time by 98 per cent to under a minute from awareness to decision, and under 30 seconds from decision to action

Founded by DTCC and FS-ISAC, our founding companies helped to drive the adoption and sharing of CTI to help protect the financial sector and to deploy that technology for the benefit of all other industries.

Acquired by NC4 in late 2016, we are more committed than ever to building cyber threat intelligence sharing capabilities for our members.

Relied on by over 2,800 domestic and foreign companies and governments, Soltra Edge is the most widely adopted cyber threat intelligence communication platform in the world.

We are experts who are heavily invested in driving and maintaining the MITRE & DHS created, and now Oasis managed, efforts of the Cyber Threat Intel Committee to improve the STIX & TAXII standards.

#### **Flexible**

Soltra Edge is open and flexible. It doesn't lock you in to a closed and limited platform.

#### **Standards Driven**

Other solutions only say they're STIX/TAXII compatible, but there are limitations under the hood. Soltra Edge is built on the STIX & TAXII standards and is built to integrate with non-standard sources

#### **Why Soltra Edge**

Using Soltra Edge as your central intelligence repository to filter and control the information that is sent to other applications and devices in your cybersecurity stack avoids unnecessary tasks and alerting, and allows your organization to apply lessons learned in the form of filters and controls.

Soltra Edge is a proven solution, having been tested and implemented in the financial services sector. NC4 Soltra hosts the FS-ISAC's Soltra Edge repository. As your CTI router, Soltra Edge makes adding additional routes easy.

#### **Additional benefits include:**

- Reduce manual labor required to collect, collate, process and disseminate intelligence data within environments resulting in significant cost savings
- Enable sharing communities and private trust groups <= **Competes with C3ISP**

- Support all eight STIX core constructs
- Manage CTI sharing with TLP markings and additional privacy and security controls
- Operate as both a server and a client
- Run on a virtual appliance or install on a physical server
- Run on-premise or in NC4's secure data center
- Connect users to open, non-proprietary, communities
- Enable two-factor authentication

## ThreatQuotient's ThreatQ

The ThreatQ platform <https://www.threatq.com/> has taken a threat-centric approach to security operations. This approach allows security teams to prioritize based on threat and risk, collaborate across teams, automate actions and workflows and integrate point products into a single security infrastructure.

Deployment options include cloud, on premises, virtual instance and dedicated appliance.

### The ThreatQ TIP as C3ISP Competition – our view

Another viable competitor The Threat library is a powerful feature. Support standard such as STIX and TAXII however no mention of anonymisation / control which is a C3ISP differentiator.

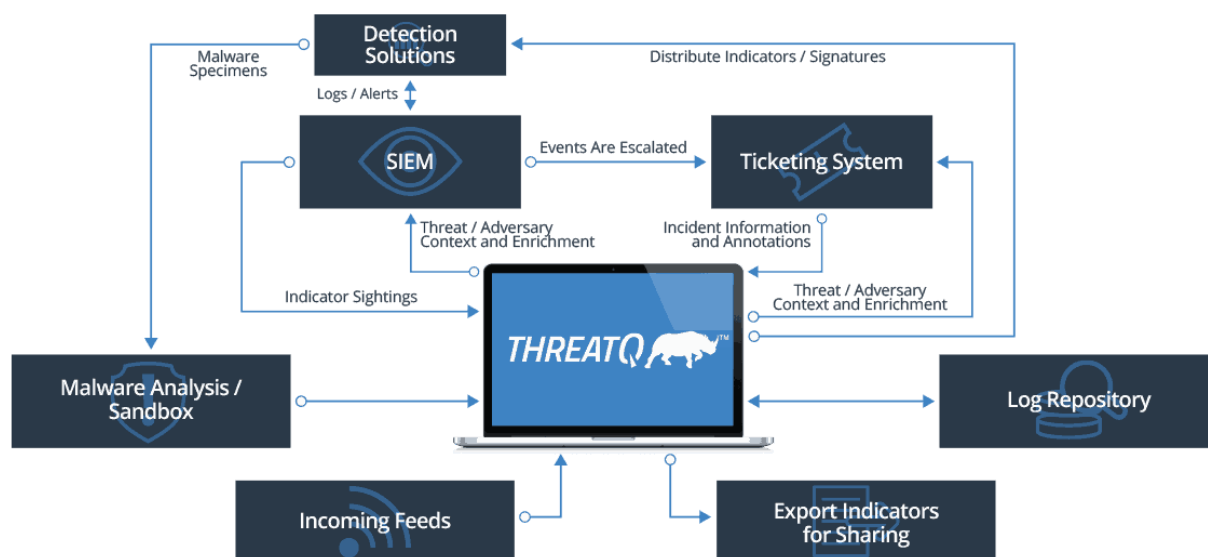
### Features

The most important part of your threat operations and management framework is the tool that brings it all together.

ThreatQ delivers the first open and extensible threat intelligence platform to provide defenders the context, customization and collaboration needed for increased security effectiveness and efficient threat operations and management.

### ThreatQ Architecture

ThreatQ is an open and extensible threat intelligence platform, supporting both standard and custom integrations with feeds and security systems. Through these integrations the platform automates the aggregation, operationalization and use of threat intelligence across the entire security infrastructure, supporting multiple use cases, increasing security effectiveness and accelerating security operations.



### The Threat Library

Central repository of relevant and contextual intelligence customized for your unique environment.

- Self-tuning
- Structured and unstructured data import
- Context from external + internal data
- Custom enrichment source for existing systems

## TruSTAR's Threat Intelligence

The TruSTAR TIP <https://www.trustar.co/product/threat-intelligence-platform>

### **The TruSTAR TIP as C3ISP Competition – our view**

Another viable competitor Strong on analytics and data sharing controls.

#### **Features**

Facilitates intelligence exchange and collaboration with peers, partners, ISACs/ISAOs, and supply chain partners all in one platform.

#### **Data sharing security controls**

Enclaves are secure data repositories used for storing, managing, and enriching sensitive events.

A TruSTAR Enclave allows users to analyze and enrich investigations with trusted, relevant intelligence sources, including information shared by your partners and peers, while allowing you to maintain protective access controls.

#### **Automated Redaction**

Sharing outside of your team or organization? Our redaction engine will keep your legal and compliance folks happy by allowing you to control visibility of all shared data. Easily scrub sensitive information from reports before releasing to your partners. Our natural language processing (NLP) engine instantly identifies potential PII terms to redact.

#### **Collaborate With the Right Access & Permissions**

By allowing you to granularly define user permissions for who can access and interact with what data, we ensure you can adhere to any compliance requirements. With in-app chat and ability to capture notes on investigations, your teams are empowered to collaborate with ease to add context to ongoing analyses and IOCs.

#### **Analysis Visualization**

We represent threat intelligence the way a human analyst actually looks at it. TruSTAR's link analysis visualizations give you the WHY and HOW of threat events by showing you how IOCs connect to threats inside and beyond your Enclave. Your analysts' time is extremely valuable – you'd better be sure you're providing them with a tool optimized for their needs and efficiency.

## MISP – Co Finance by the EU

MISP - Open Source Threat Intelligence Platform & Open Standards for Threat Information Sharing. <https://www.misp-project.org/>

More than 6000 organisations worldwide are using MISP.

CEF (Connecting Europe Facility) funding under CEF-TC-2016-3 - Cyber Security has been granted from 1st September 2017 until 31th August 2019 as *Improving MISP as building blocks for next-generation information sharing*.



**Co-financed by the European Union**

Connecting Europe Facility

### **The MISP Open source platform as C3ISP Competition – our view**

MISP is another competitor platform in many areas including ability for secure data sharing and use of STIX. Well defined Open Source governance model useful as a baseline perhaps for a C3ISP Open source governance model.

Initially built to support NATO Computer Incident Response Capability Technical Centre (NCIRC TC) missions, MISP allows sharing of technical characteristics of malware within a trusted community, without having to share information about the context of the incident.

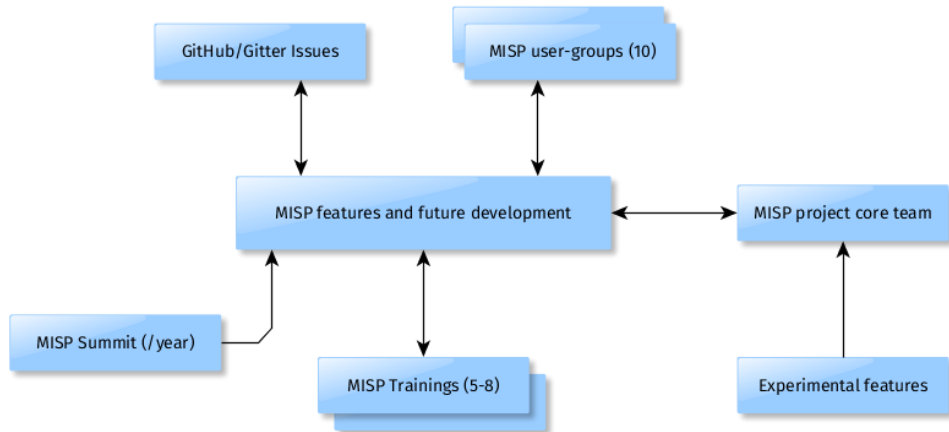
### **Features**

#### **MISP Model of Governance**

MISP project is a large open source project with the goal to make viable tools and format to improve information sharing at large. In order to achieve our goals, the MISP project gathers feature requests, feedback and bug reports from different sources.

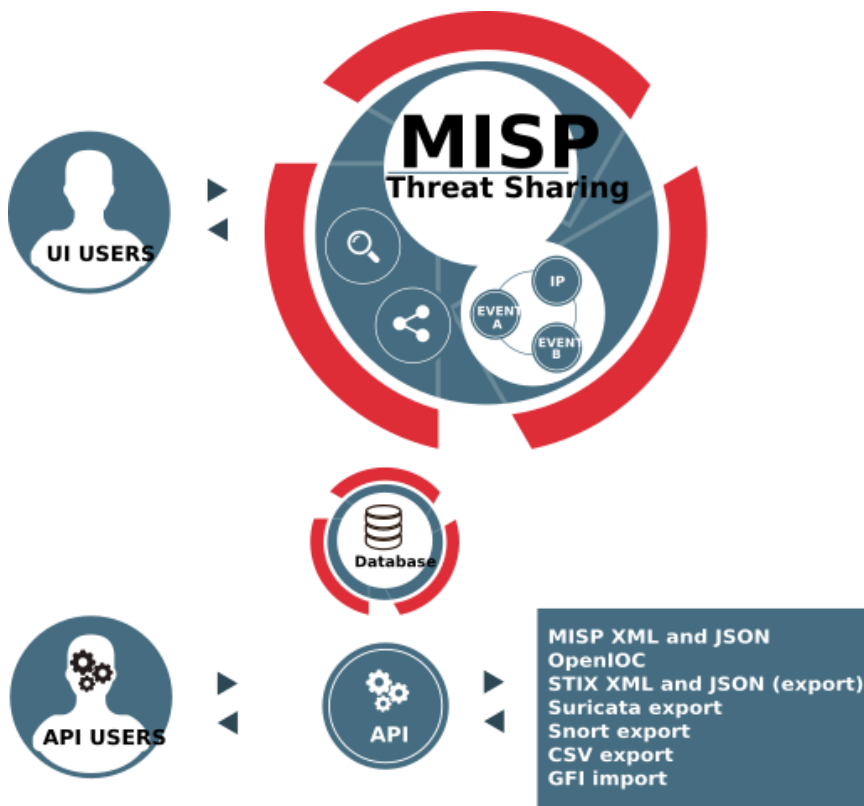


As described in the graph below, we have various sources that we use, including MISP user-groups, direct community feedback via GitHub, MISP trainings and the yearly MISP s



summits.

MISP is a threat intelligence platform for sharing, storing and correlating Indicators of Compromise of targeted attacks, threat intelligence, financial fraud information, vulnerability information or even counter-terrorism information



- An **efficient IoC and indicators** database allowing to store technical and non-technical information about malware samples, incidents, attackers and intelligence.
- Automatic **correlation** finding relationships between attributes and indicators from malware, attacks campaigns or analysis. Correlation engine includes correlation between attributes and more advanced correlations like Fuzzy hashing correlation (e.g. ssdeep) or CIDR block matching. Correlation can be also enabled or event disabled per attribute.
- A flexible data model where complex [objects](#) can be expressed and [linked together](#) to express threat intelligence, incidents or connected elements.
- Built-in **sharing functionality** to ease data sharing using different model of distributions. MISP can synchronize automatically events and attributes among different MISP. Advanced filtering functionalities can be used to meet each organization sharing policy including a **flexible sharing group** capacity and an attribute level distribution mechanisms.
- An **intuitive user-interface** for end-users to create, update and collaborate on events and attributes/indicators. A **graphical interface** to navigate seamlessly between events and their correlations. Advanced filtering functionalities and [warning list](#) to help the analysts to contribute events and attributes.
- **storing data** in a structured format (allowing automated use of the database for various purposes) with an extensive support of cyber security indicators along fraud indicators as in the financial sector.
- **export**: generating IDS (Suricata, Snort and Bro are supported by default), OpenIOC, plain text, CSV, MISP XML or JSON output to integrate with other systems (network IDS, host IDS, custom tools)
- **import**: bulk-import, batch-import, free-text import, import from OpenIOC, GFI sandbox, ThreatConnect CSV or MISP format.
- Flexible **free text import** tool to ease the integration of unstructured reports into MISP.
- A gentle system to **collaborate** on events and attributes allowing MISP users to propose changes or updates to attributes/indicators.
- **data-sharing**: automatically exchange and synchronization with other parties and trust-groups using MISP.
- **feed import**: flexible tool to import and integrate MISP [feed](#) and any threatintel or OSINT feed from third parties. Many [default feeds](#) are included in standard MISP installation.

- **delegating of sharing:** allows a simple pseudo-anonymous mechanism to delegate publication of event/indicators to another organization. <= **Competes with C3ISP differentiator**
- Flexible **API** to integrate MISP with your own solutions. MISP is bundled with [PyMISP](#) which is a flexible Python Library to fetch, add or update events attributes, handle malware samples or search for attributes.
- **adjustable taxonomy** to classify and tag events following your own classification schemes or [existing taxonomies](#). The taxonomy can be local to your MISP but also shareable among MISP instances. MISP comes with a default set of well-known [taxonomies and classification schemes](#) to support standard classification as used by ENISA, Europol, DHS, CSIRTs or many other organisations.
- **intelligence vocabularies** called MISP galaxy and bundled with existing [threat actors, malware, RAT, ransomware or MITRE ATT&CK](#) which can be easily linked with events in MISP.
- **expansion modules in Python** to expand MISP with your own services or activate already available [misp-modules](#).
- **sighting support** to get observations from organizations concerning shared indicators and attributes. Sighting [can be contributed](#) via MISP user-interface, API as MISP document or STIX sighting documents. Starting with MISP 2.4.66, [Sighting has been extended](#) to support false-negative sighting or expiration sighting.
- **STIX support:** export data in the STIX format (XML and JSON) including export/import in STIX 2.0 format.
- **integrated encryption and signing of the notifications** via PGP and/or S/MIME depending of the user preferences.

MISP (Open Source Threat Intelligence and Sharing Platform) software facilitates the exchange and sharing of threat intelligence, Indicators of Compromise (IOCs) about targeted malware and attacks, financial fraud or any intelligence within your community of trusted members.

MISP sharing is a distributed model containing technical and nontechnical information which can be shared within closed, semi-private or open communities. Exchanging such information should result in faster detection of targeted attacks and improve the detection ratio, whilst also reducing the number of false positives.

NATO documentation on original MISP platform

<https://www.ncia.nato.int/Documents/Agency%20publications/MISP%20leaflet.pdf>

Open source tools released under the GNU General Public License, including the Malware Information Sharing Platform (MISP), Collective Intelligence Framework (CIF), Collaborative Research Into Threats (CRITs) and MANTIS Cyber-Intelligence Management

Framework. The Open Threat Exchange (OTX) and Soltra Edge platform are free-to-use but were not released under an open source license.

## **IBM X-Force Exchange**

Provides a cloud-based threat intelligence sharing platform that enables users to research threats, collaborate with peers and take action

### **Features**

#### **Access to a wealth of threat intelligence data**

IBM X-Force Exchanges provides an open platform that adds context to indicators of compromise (IOC) with a mix of human-and machine-generated insights. It offers timely threat intelligence that is dynamically updated every minute. The software delivers web threat monitoring of over 25 billion web pages and is supported by a database of over 96,000 vulnerabilities. It offers deep intelligence on millions of spam and phishing attacks and monitors reputation data with malicious IP addresses.

#### **Collaborative platform for sharing threat intelligence**

You can connect with industry peers to validate findings, share a collection of IOC to aid in forensic investigations, or add context to threats through peer collaboration via private groups and shared collections.

#### **Integrated solution to help quickly stop threats**

The solution is designed for third-party integration with support for Structured Threat Information Expression (STIX) and Trusted Automated Exchange of Indicator Information (TAXII)—the established standards for automated threat intelligence sharing. It allows for integration between IBM Security products and X-Force Exchange-sourced actionable intelligence. Application programming interface (API) enables you to connect threat intelligence to security products.

#### **Easy-to-use interface for organizing and annotating findings**

Once a report is created, users can add comments to provide additional insight and context for other users or add the report to a Collection. Users can also provide feedback to the X-Force team to trigger an analysis of the specific report, which can lead to content updates. Setting custom notifications and watchlists enables users to receive relevant advisories on their areas of interest.

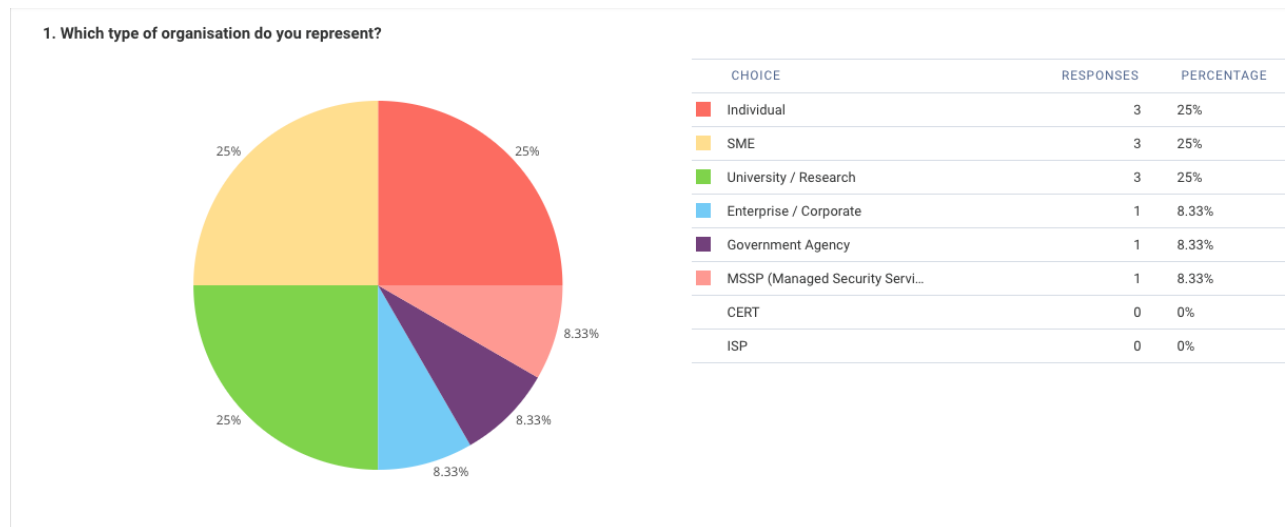
## ANNEX 14: C3ISP Route to Market - Customer Outreach

Industry	Company name
Energy	BP
Energy	EDF Energy
Transport	Alstom
Transport / Energy	Thales
Telecoms	Siemens
Cyber Security	Micro Focus
Energy	SSE
Transport	BAE Systems
Cyber Security	Elemendar
Cyber Security	BreachAware
Cyber Security	Clym
Cyber Security	Panaseer
Cyber Security	RedSift
Cyber Security	Protectbox
Transport	Virgin Trains
Transport	Associated British Ports
Energy	UK Water Ltd
Transport	Department for Transport
Telecoms	BT
Transport	HS2
Telecoms	Telefonica
Transport	TfL
Telecoms	Vodafone Group

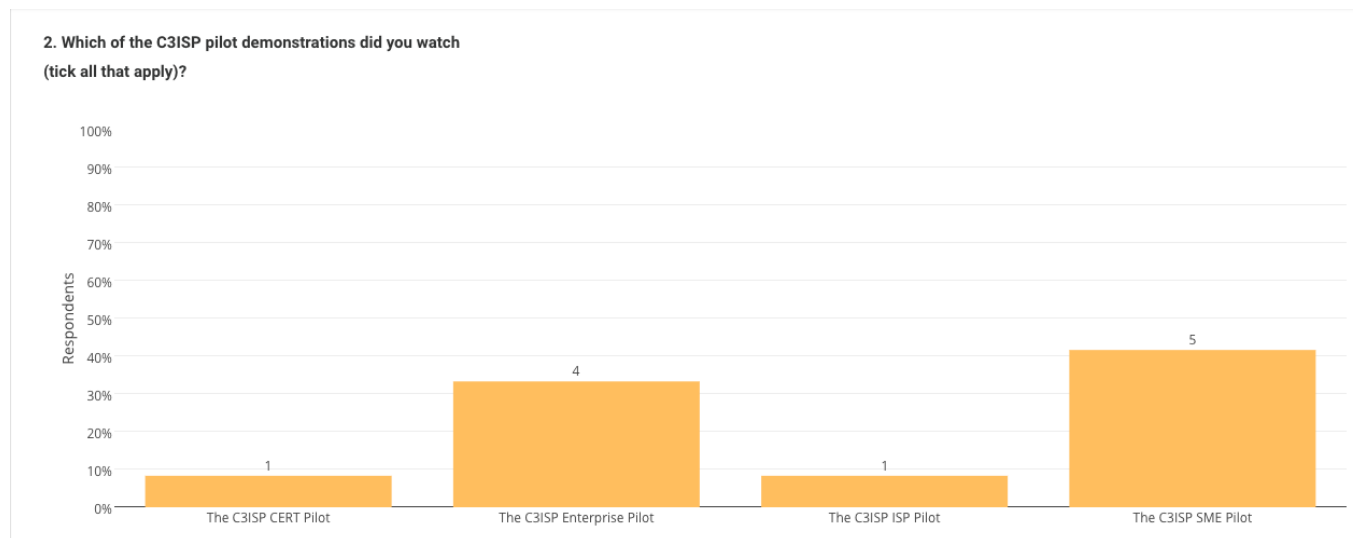
## ANNEX 15: C3ISP Workshop 2 – Interviews Report

### Investigation Report

#### 1. Which type of organisation do you represent?



#### 2. Which of the C3ISP pilot demonstrations did you watch (tick all that apply)?



#### 3. Does your organisation deal with sensitive information of any kind? What type of information?

- *Type: University/Research*  
Personal data, nominative data, sensitive personal identifying information (PII).
- *Type: Government Agency*  
NA
- *Type: SME*  
Mainly employees data.  
Customers data.
- *Type: Enterprise/Corporate*  
Yes.
- *Type: MSSP (Managed Security Services Provider)*  
Internal network information from customers. Customers' security incidents..

#### 4. Have you experienced any kind of cyber-attack? What type?

- *Type: Research/University*  
Yes, malware attacks, ddos attacks, phishing emails.
- *Type: Government Agency*  
NA
- *Type: SME*  
Malware attack on one node.
- *Type: Enterprise/Corporate*  
No.
- *Type: MSSP (Managed Security Services Provider)*  
NA.

#### 5. How did you react or would react in case of cyber-attack?

- *Type: Research/University*  
Outsourcing the solution to an internal expert or a public entity.  
It depends on the type of attack.  
Gamed the attacker.
- *Type: Government Agency*  
NA
- *Type: SME*  
Loss of continuity of its services (non vital for the business).  
We have a partner dealing with security and data protection.  
Panic, shut down, investigation, fix security hole and re-open.  
I would start the data and systems cleaning process with the support of competent entities or specialised tools.  
We have alerted the provider, we have isolated the website from which the threat came and we have done the DB fix.

- *Type: Enterprise/Corporate*  
NA.
- *Type: MSSP (Managed Security Services Provider)*  
NA.

**6. Do you currently share Cyber Threat Intelligence (CTI) data? If so, how do you currently share this data?**

- *Type: Research/University*  
No.
- *Type: Government Agency*  
NA
- *Type: SME*  
No.
- *Type: Enterprise/Corporate*  
Looking into this.
- *Type: MSSP (Managed Security Services Provider)*  
No.

**7. Do the C3ISP services give you the confidence to share your data? If not, what would you need to give you that confidence?**

- *Type: Research/University*  
Yes.
- *Type: Government Agency*  
We understand the importance of sharing threat intelligence and also the importance of using DSA to control what is shared/anonymised
- *Type: SME*  
Yes, compliance with GDPR and internal disclosure policies, it is fundamental. I still don't know C3ISP very well and I don't use its services.
- *Type: Enterprise/Corporate*  
NA.
- *Type: MSSP (Managed Security Services Provider)*  
We would like to see this technology being proven at operations for some years before we adopt it.

**8. What would be the most significant business benefits to your organisation through using C3ISP services?**



- *Type: Research/University*  
Knowing and predicting threat attacks in advance.  
A better security with also more possibilities in terms of system analytics.  
C3ISP and sharing in general is important in order to implement reactive mitigation measures.  
  
Open source for accelerators.  
You stay in business
- *Type: Government Agency*  
NA
- *Type: SME*  
Continuity, compliance with GDPR.  
Not many benefits for my organisation (we are still just a few and we don't manage sensible data), however this could be very useful for my clients.  
  
Probably the defense against cyber attacks on our DB.
- *Type: Enterprise/Corporate*  
Enhance our product/synergy.
- *Type: MSSP (Managed Security Services Provider)*  
Being able to jointly analyse and view information from multiple customers.

**9. What additional C3ISP services would you suggest that would bring business benefits to your organisation?**

- *Type: Research/University*  
NA  
The personalisation of the anonymisation level.  
IT security companies sharing CTI.
- *Type: Government Agency*  
C3ISP should look at analysing the competitive landscape of similar products.
- *Type: SME*  
Anonymised data samples for research.  
The anonymisation and then the analytic elaboration of data could be useful in the future.  
Firewalling, cloud, cryptography, data injection and test/verification.
- *Type: Enterprise/Corporate*  
NA.
- *Type: MSSP (Managed Security Services Provider)*  
NA.

**10. What do you see as the main barriers to your organisation adopting C3ISP services? How could we overcome these barriers?**

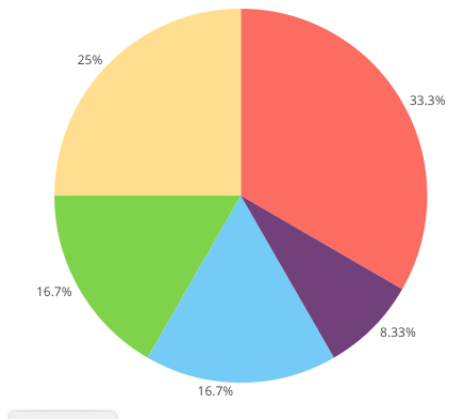
- *Type: Research/University*  
Learning and training for employees.  
Fundings, government infrastructure.
- *Type: Government Agency*  
NA
- *Type: SME*  
Additional workload for IT/Security people (severely understaffed). Give awareness of benefits to the management.  
There aren't particular barriers at the moment.  
The main barrier is our diffidence in using the cloud, we don't want to put our data on cloud. We could overcome this barrier only if C3ISP provides services and tools deployable on site, on our own server.
- *Type: Enterprise/Corporate*  
NA.
- *Type: MSSP (Managed Security Services Provider)*  
Reluctancy of customers to exchange CTI. This can be overcome slowly over time if C3ISP technology is proven in operations..

**11. What would be your preferred approach to integration of C3ISP with legacy systems? If your organisation offers security as a service, do you think C3ISP platform could integrate easily with your analytics tools?**

- *Sector: Research/University*  
Learning and training for employees.  
Attempting to revamp the current information systems and then try to merge them.  
Yes.  
SME to cloud based.
- *Sector: Government Agency*  
NA
- *Sector: SME*  
It is a problem that my company (DigItalynn) can help to solve.  
Our preferred approach would be that C3ISP provides firewall hardware to us.
- *Type: Enterprise/Corporate*  
NA.
- *Type: MSSP (Managed Security Services Provider)*  
Integrate C3ISP as an extra component in our SOC (Security operations centre), especially for visualisations.

**12. What form of C3ISP procurement model would your organisation find most attractive?**

12. What form of C3ISP procurement model would your organisation find most attractive?



CHOICE	RESPONSES	PERCENTAGE
Security as a service (Cloud...	4	33.3%
Other	3	25%
(no answer)	2	16.7%
One off (ready to use)	2	16.7%
Fixed monthly / Annual licen...	1	8.33%
Variable license cost depend...	0	0%
Variable license cost depend...	0	0%

## ANNEX 16: C3ISP Workshop 3 – Report



---

# C3ISP Exploitation Workshop 3

## Summary of results and impact on exploitation plan

---

Author: Jamie Harrison, Head of Innovation Programmes, Digital Catapult

Report Date: 17 April 2019

Activity: 02 April 2019 at CNR, Pisa



## Introduction

The third workshop for the C3ISP programme for exploitation focused on two areas:

- Proprietary vs open source exploitation opportunities
- Individual organisational alignment with a given exploitation strategy

These two areas were identified as key concerns for discussion as a result of the review of the initial exploitation plans proposed by consortium members and as a result of the previous two workshops. Initial exploitation plans highlight the differing needs of the research focused organisations and the commercially focused organisations, predominantly to do with open source vs proprietary concerns.

The workshop sought to identify key areas of focus for the go-to-market strategy and help us shape the business model for the platform and associated components of C3ISP.

## In summary

Digital Catapult conducted a two part workshop to first draw out the positive and negative impacts of various proprietary and open source approaches. Considering both extreme cases (totally open source, totally proprietary) and stepped approaches, with some elements proprietary and others open source.

The second part of the workshop based on a Harvard Business School article about 3M's approach to innovation (catalogued by *George Day*, December 2007 Issue) drew out the individual talents of the organisations and their alignment with the technology and the markets we are looking to apply the technology.

The conclusions of these workshops will be used as an evidence base to create an exploitation strategy for the consortium. The strategy will address how we can achieve long term value from the project.

## Part 1

Key outcomes from part one point toward a more open source over proprietary approach however the hybrid approach (which allowed for a baseline open source platform with proprietary services) also fared well in the assessment. The key concerns of the consortium, those scoring the top weighting of 5, are summarised by the terms below:

- Access to opportunity
- Adoption
- Trusted platform owner
- Exploitation opportunity
- Developer engagement
- Commercial opportunity
- Added value

- Maintenance
- Complexity
- Control
- Quality

<b>Fundamental</b> Adoption Quality Exploitation opportunity	<b>Commercial/Market</b> Access to opportunity Commercial opportunity Added value Trusted platform owner
<b>Platform development</b> Developer engagement	<b>Operational</b> Maintenance Control Complexity

A simple grouping allows us to see the concerns in four specific areas, some of these key points could be grouped under multiple headings (such as complexity, developer engagement or access to opportunity) however the alignment has been based on the extended comment which can be seen in the Annex.

Taking each of these headings in turn we can consider what impact this could have on a given business model and the broader exploitation plan.

### **Fundamental**

**Adoption:** Adoption was discussed as one of the most crucial areas for success, as to some extent the success of a threat sharing platform requires a reasonably large number of threats being collected from multiple sources. However the diversity of these sources is less of a concern. The consortium discussed both the need for broad adoption but suggested success could be found through industry specific focus. Pay-walls preventing widespread access was also highlighted as a key issue regarding proprietary approaches..

**Quality:** Most pressing in relation to the open source vs proprietary debate was the impact on quality and quality control. It was largely accepted that a fully open source platform would sacrifice quality compared to proprietary solutions. This point was challenged by influencing factors such as the benefits of transparency to an open source and trust-sensitive community where a fully open source solution feeds transparency.

**Exploitation Opportunity:** Incentives broadly were discussed however clear exploitation opportunities for contributing organisations, either internal or external to the consortium was seen as a fundamental need, as without a clear benefit to adoption of the platform the platform would struggle to gain attention. It was also highlighted as a concern around the

impact of organisational control and contributors would need to be confident that any controlling organisation would not make any changes that could adversely impact exploitation opportunities.

#### Impact of Fundamental section on exploitation plan

When considering these three fundamental concerns the conclusions to test would be:

- To find a solution which can provide an easily accessible and deployable solution for each of our target segments to encourage wide adoption
- To offer a high quality solution some control over the open source component is required
- When promoting the solution there should be clear value in investing either time to adopt the platform or in developing solutions on the platform which protect the interests of developing parties and commercial organisations alike

#### **Platform Development**

Developer engagement: Highlighted by the Open Source group, developer engagement was seen as a key driver behind the success of similar platforms in the Open Source community. If a platform is seen as too rigid and inflexible it may not find traction.

#### Impact of the Platform Development section on the exploitation plan

- The exploitation plan must ensure not to ‘lock out’ developers
- We must consider ‘bottom up’ routes to market by engaging developers in early exploitation to drive adoption within an organisation
- We should provide clear instructions to ensure developers can understand the parameters of working with C3ISP

#### **Commercial/Market**

Access to opportunity: This was seen as a key benefit of a combined approach where there is an obvious exploitation route that could be commercially protected and sold, when combined with some open source (easy access) components could help strike a balance between adoption and exploitation.

Commercial opportunity: Again highlighted as a core benefit of a combined approach as this will incentivise adoption by commercial entities which in turn add credibility to the platform. In other groups it was highlighted that the platform should not suffer for want of commercial gain, as it is not immediately obvious as to the size of the addressable market for the services as they stand.

**Added Value:** The fully commercial group suggested that greater added value can be gained through a packaged approach. Protecting the integrity of a platform allows it to be seen both as a standalone platform and a differentiator as added value to others. It also increases the opportunity to sell installation, integration and support as added services for a commercially focused organisation.

**Trusted Platform Owner:** Inherent to both the adoption of the platform and the willingness to invest in developing on the platform or deploying the platform, ensuring the market has full belief in the platform owner will be essential to success regardless of the open source vs proprietary nature. However should any of the platform be protected it will be the organisation controlling the protected element that would need to engender trust in their practices most.

**Impact of Commercial/Market on the exploitation plan:**

- It is clear that there is a commercial interest in the platform from the consortium members based on their market knowledge and we will need to test the ‘willingness to pay’ metric with those who maybe customers to ensure the level of potential return would be worth the effort to protect the work.
- The added value (as part of this discussion) could be packaged into a core value of the exploitation model if it is a Software as a Service approach. The exploitation plan should consider whether the overall approach is prohibitive or beneficial to those looking to sell added value services on top. Training modules and accessing benefits quickly are also big influencers in this area.
- Once the core commercial exploitation areas are established the merits of promoting under the banner of one organisation over another and the potential pros and cons of each should be tested. The ability to gain backing from an existing consortium partner however cannot be assumed and would need support to sell internally to consortium organisations own internal teams.

## **Operational**

**Maintenance:** The benefit of total open source is that it passes over responsibility to maintain the platform to others once ‘given’ to the community. However fundamental to the platform is the ability to maintain up to date and accurate threat intelligence and records. Total open source risks adaptation to the functionality which could in turn negatively impact the platforms ability to share effectively.

**Control:** Highlighted in the mixed groups there was a foreseen challenge in ensuring that any open components could not be modified to negatively impact the proprietary components. Control was an underlying theme as too much control was seen as a negative impact regarding commercial endeavours and lack of control was acknowledged as a fundamental result of open source applications.



**Complexity:** Complexity in contracts, organisational structures, formal agreements, partnerships, route to market and commercial plans each where highlighted as potential undoings in the combined approach. The more the proposed strategy leans toward open source or proprietary the less complex the solution was envisaged. Middle ground approaches lose out in this aspect.

Impact of Operational on the exploitation plan:

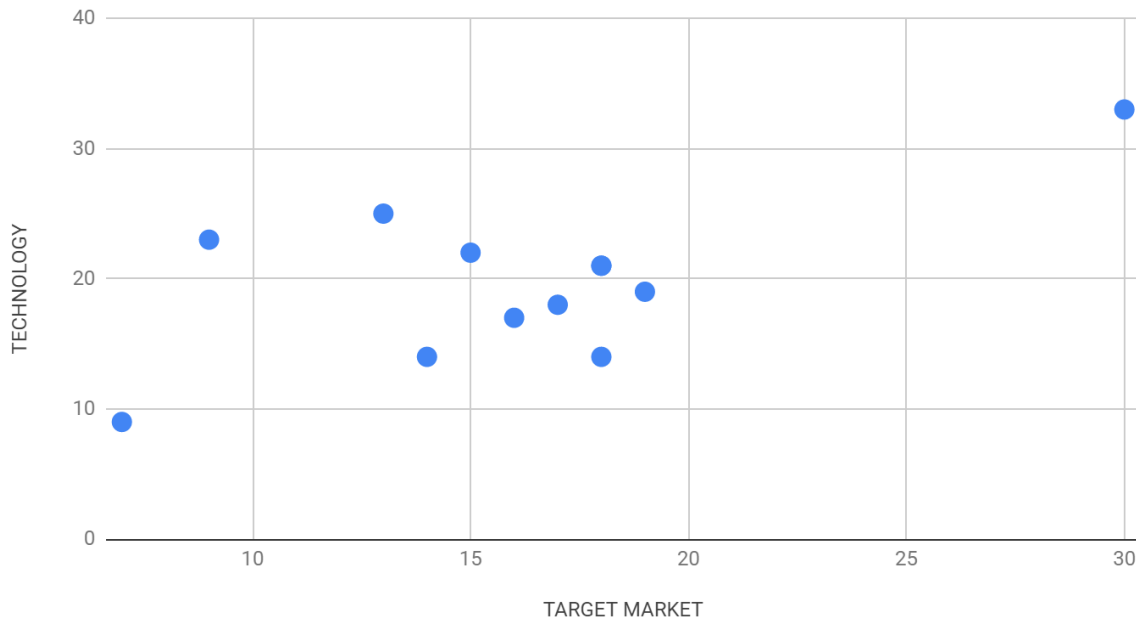
- Reducing complexity is essential, drawing clear lines between where open source functionality starts and stops will be difficult and should not increase frustrations with early deployments. One approach could be to allow early adopters to benefit from full functional deployments, on the premise that added value services could be sold on top. These early deployments could yield large benefits from user testing and similar outputs
- Adoption of the platform relies on clear structures to share threat intelligence, some protection should be in place to retain the integrity and to optimise the core functionality above all else. Therefore some management will need to govern this aspect which in turn requires funding to ensure the integrity of the governing organisation. Only in exceptional circumstances have projects maintained by an open source community yielded long term, well maintained core functionality.
- The long term engagement of consortium members and ownership of the platform should be simplified, ideally to one or two core organisations pioneering the exploitation of the platform in a commercial context where, if required, others could be background influencers with small stakes in the business and its outcomes.

## Part 2

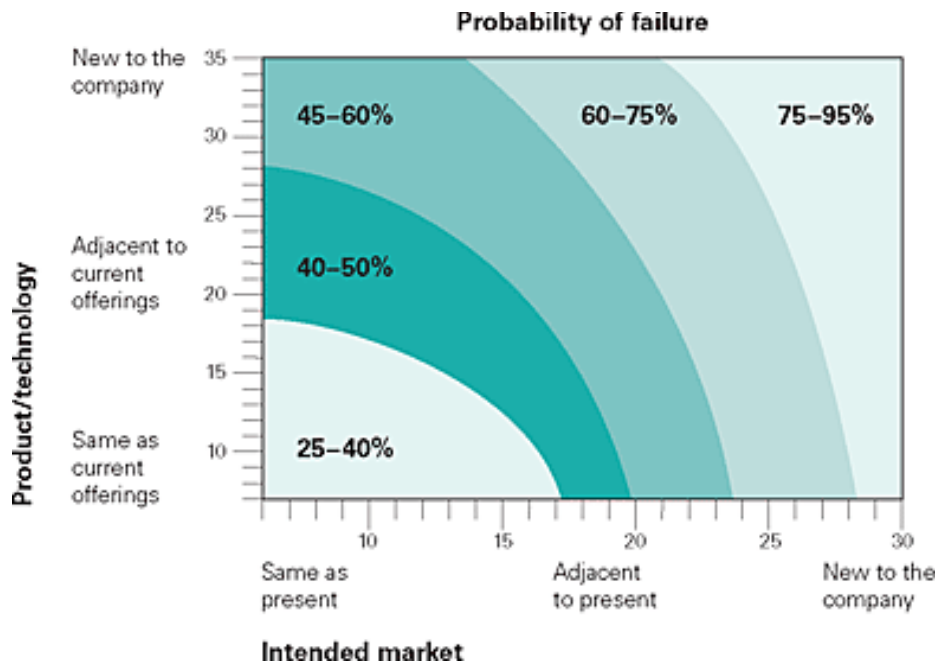
The second workshop sought to identify the strengths of each consortium organisation in the cyber security market and with regards to their technical strengths. This exercise is commonly used in large organisations to understand the pipeline of new products and services in development to ensure they are taking a balance of high risk and low risk projects forward. Here it has been adapted to highlight the key organisations required to engage in addressing the market and technologies and how we can best utilise existing relationships to reach into the appropriate developer communities and customer communities.

The outcome is summarised by this chart:

C3ISP Team Focus



Each blue circle represents an organisation in the consortium, the x-axis figures represent the maturity in the target market(s) and the y-axis represents the maturity in the technology(s). For the organisation in the bottom left of the graph this represents a low risk activity and research suggests a high chance of success with limited impact to organisational bottom line, conversely, those in the top right would seek to gain the most, however the chance of success is much lower. The graph below illustrates the common values associated with each layer, reproduced from the Harvard Business Review article *Is It Real? Can We Win? Is It Worth Doing?: Managing Risk and Reward in an Innovation Portfolio* (George Day, December 2007 Issue)



Consortium members requested, as this was a ‘gut feel’ review based on the individuals knowledge in the room, for us to keep the organisational names anonymous. What we can see from diving into the results is where the consortium strengths lie.

The areas where there is most consortium alignment with more than 7 responses with positive alignment (scoring 4 or 5 on a likert scale) are:

#### Technology:

- Current development capability (7 of 13)
- Technology competency (8 of 13)
- Expected quality standard (7 of 13)

#### Market:

- Brand promise (9 of 13)
- Current customer relationships (10 of 13)

When discussed briefly with the consortium the response correlated with the results of the previous session and positive alignment can be seen between the points regarding: quality as a focus; alignment with strong brands and building on existing relationships in the consortium.

#### Impact on the exploitation plan

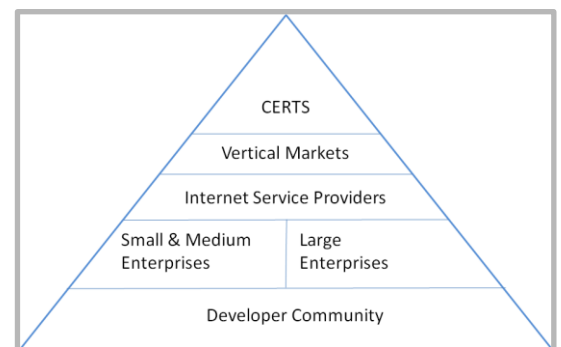
- We will first identify key target market verticals and then look to align with the companies in the consortium which have the most brand equity in that vertical to begin to make traction with a potential customer base

- We will focus in on consortium members with commercial exploitation ambitions to understand how the functionality employed within the solution can best be managed to enable us to reach the highest number of early adopters
- We will look to run activities which engage a customer and user base across all consortium members as this is a key strength across the organisations in response

### In conclusion

Through this workshop we have been able to gather a variety of results and an evidence base, which once reviewed has given us insights into the core ambitions of consortium members. We have also drawn on the experience of the members in both commercial environments and developer led environments as well as research environments. Key conclusion points:

- Although it is likely to increase complexity, in order to conform with the desires of the consortium and to reach the initial broad audience required to encourage adoption, a combined open source and proprietary approach will be the key focus
- Industry vertical focus will take president over the productised approach to ensure we produce solutions with specific customers in mind
- The larger commercially led organisations will be supported to build internal business cases for their own commercial teams to allow us to understand the ambition of these organisations to invest further in C3ISP
- Consideration will be given to the priority of the potential customers to enable wide scale adoption, who do we target early on and who is most able to influence the wider ecosystem, an initial hypothesis is illustrated here, the pyramid represents those with the most ecosystem influence over those with the least and this will be explored further through desk research
- Messaging going forward should be targeted to the markets which we are going to prioritise. The key concerns of the consortium are likely reflected in the market and the key words identified will be used within the messaging to different communities



## ANNEX 16.1

Full results from part 1 of this workshop

<b>Scenario A: Proprietary platform with free to access services</b>			
	Pros	Cons	
4	access to a quality community, fueled by collected money and smart incentives, better than MISP and other open source solutions TAG: COMMUNITY	why should one pay for C3ISP when they can get MISP for free TAG: COMPETITION	4
5	more focussed analytics, bigger added value than open source solutions TAG: ADDED VALUE	company running the business must invest in securing payment infrastructure and licensing TAG: OVERHEAD	3
4	pay for using cybersecurity as-a-service (support, integration) TAG: ADDED VALUE	paying may hurdle community growth and lead to lower adoption, for example by SMEs TAG: ADOPTION	5
5	up-to-date and accurate threat detection, continuously updated TAG: MAINTENANCE	what happens at service termination? how can I get control on this aspect TAG: DEPENDENCE	4
3	sharing with less trustworthy peers, but in a secure environment so that sensitive information misuse is impossible TAG: MONITORING	one needs to trust the entity running the service to adhere and implement securely the service and data owner's policies TAG: TRUST PLATFORM OWNER	5
21	TOTAL PROS	TOTAL CONS	21
Rationalised Score: 0*			

\*Facilitator notes on final score from team working on Scenario A

- the discussions focussed on trust and started from opposite assumptions: paying to be a means to fuel a community VS paying as hurdle to community growth, revenue stream beneficial to run services with added value VS trust in the way services are run

- choosing this option would address the main cons with a convincing approach, better would be to focus on delivering the pros in the way they are formulated. Addressing correctly the cons would automatically end up in fulfilling the pros, leading to a convincing offering.

<b>Scenario B: Open Core Platform with Proprietary Services</b>			
Scr	Pros	Cons	Scr
5	the possibility to gain money from a component will attract many sector vertical Private companies to add their module TAG: COMMERCIAL	it is heterogeneous and complex environment TAG: COMPLEXITY.1	5
5	gaining money from a component, allows many players to jump in as open source contributors TAG: ACCESS TO OPPORTUNITY	if someone modifies an open component we don't know the impact on the proprietary components TAG: CONTROL	5
3	the model is better compared to a full proprietary model, because the proprietary will remain the only owner not involving an ecosystem of contributors TAG: ENGAGEMENT	issues with commercial exploitation since limitations can be introduced by single decisions of the owners of the proprietary components TAG: EXPLOITATION	4
3	the model is better compared to a full open source model, because the proprietary is likely to attract less proprietary companies and thus reduce the number of contributors to the open source components TAG: ENGAGEMENT	unsure of the quality of contribution on the open source component TAG: O/S VALUE	1
4	the model is better compared to a full proprietary model, because in a sense it avoids lock-in TAG: AVOIDS LOCK-IN	complex licence management TAG: COMPLEXITY.2	3
20	TOTAL PROS	TOTAL CONS	18
Rationalised Score: +2			

<b>Scenario C: Total Proprietary System</b>			
Scr	Pros	Cons	Scr
5	Control of commercial exploitation  TAG: EXPLOITATION	Difficulty in securing first users as proprietary nature increases barriers to usage  TAG: BARRIER TO ENTRY	4
4	Control of functionality development, reduces the need for a complex board arrangement as is common on Open Source platforms  TAG: COMPLEXITY	Companies who could see the biggest benefit from functionality may not be able to afford access  TAG: FORESSEEN BENEFITS	3
3	Quality and therefore reputational control of the services and the additional functionality developed  TAG: QUALITY CONTROL	All development has to be completed by a central organisation which restricts the personalisation of the service  TAG: PACE OF DEVELOPMENT	3
3	Central organisation can better instruct users on how to best use functionality to get faster results and can centralise the learning  TAG: IMPLEMENTATION	The C3ISP platform requires a broad user base and restricting the potential reach through proprietary application could adversely impact the effectiveness of the platform  TAG: EFFECTIVENESS	4
1	Big revenues could be generated from fewer clients if the value exchange clear and not easily accessible elsewhere  TAG: REVENUE GENERATION	Increased marketing costs to reach markets that can pay for the service  TAG: COST OF MARKETING	2
16	TOTAL PROS	TOTAL CONS	16
RATIONALISED SCORE: 0			



<b>Scenario D: Total Open Source</b>			
Scr	Pros	Cons	Scr
4	<p>consortium consists of research organizations that promote open source to easily spread research activities</p> <p>TAG: CONSORTIUM SKILLS</p>	<p>It is difficult to make money for private companies</p> <p>TAG: RETURN ON INVESTMENT.1</p>	2
3	<p>easier for the others to adapt, adopt and rust the framework</p> <p>TAG: ADAPTION</p>	<p>You will not have highest quality components like if they were proprietary components</p> <p>TAG: QUALITY</p>	5
5	<p>easier to create an involved community [spot bugs, share ideas, develop plugins and so on]</p> <p>TAG: DEVELOPER ENGAGEMENT</p>	<p>Depending on the license commercial use might be restricted (e.g. GPL)</p> <p>TAG: LICENSE</p>	1
3	<p>because being closed source would create a false sense of security versus the transparency provided by open source</p> <p>TAG: TRANSPARENCY</p>	<p>Project might not attract developers because they cannot earn money from it</p> <p>TAG: RETURN ON INVESTMENT.2</p>	3
3	<p>big enterprises developer can help SMEs in developing secure software using open source</p> <p>TAG: COLLABORATION</p>	<p>It is easier to find vulnerabilities that are not patched quickly and so the platform risks to be vulnerable more than the closed source model</p> <p>TAG: VULNERABILITY</p>	4
18	TOTAL PROS	TOTAL CONS	15
RATIONALISED SCORE: +3			

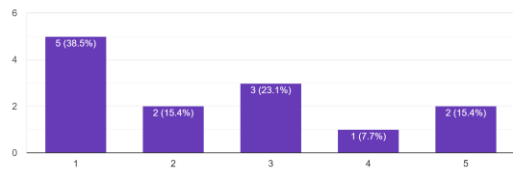
PROS	GROUP	SCORE	CONS	GROUP	SCORE
REVENUE GENERATION	C	1	QUALITY OF OPEN SOURCE	B	1
COLLABORATION	D	3	LICENSE	D	1
QUALITY CONTROL	C	3	COST OF MARKETING	C	2
ENGAGEMENT	B	3	RETURN ON INVESTMENT.1	D	2
TRANSPARENCY	D	3	MONITORING	A	3
OVERHEAD	A	3	COMPLEXITY.2	B	3
ENGAGEMENT	B	3	FORESSEEN BENEFITS	C	3
IMPLEMENTATION	C	3	PACE OF DEVELOPMENT	C	3
ADAPTION	D	3	RETURN ON INVESTMENT.2	D	3
COMPETITION	A	4	COMMUNITY	A	4
AVOIDS LOCK-IN	B	4	ADDED VALUE.2	A	4
COMPLEXITY	C	4	EXPLOITATION	B	4
DEPENDENCE	A	4	BARRIER TO ENTRY	C	4
CONSORTIUM SKILLS	D	4	EFFECTIVENESS	C	4
ACCESS TO OPPORTUNITY	B	5	VULNERABILITY	D	4
ADOPTION	A	5	ADDED VALUE.1	A	5
TRUST PLATFORM OWNER	A	5	MAINTENANCE	A	5
EXPLOITATION	C	5	COMPLEXITY.1	B	5
DEVELOPER ENGAGEMENT	D	5	CONTROL	B	5
COMMERCIAL	B	5	QUALITY	D	5

ANNEX 16.2

Aggregate results from part 2 of the workshop- Technology

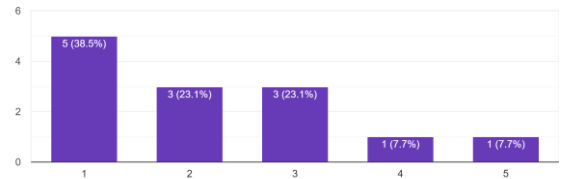
Our current development capability is...

13 responses



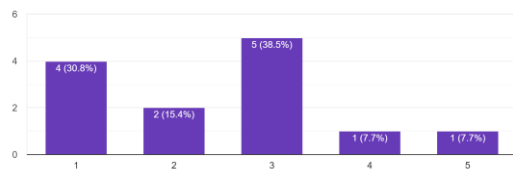
Our technology competency is...

13 responses



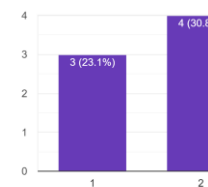
Our data management service is...

13 responses



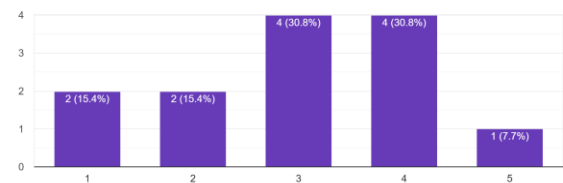
The expected quality standa

13 responses



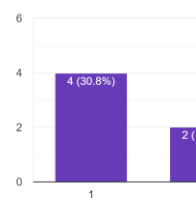
The required knowledge and science base are...

13 responses



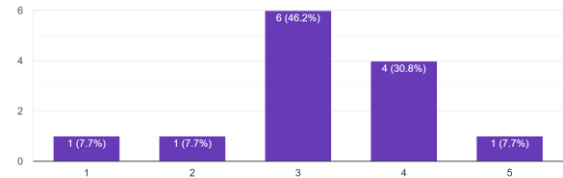
Our digital service delivery

13 responses



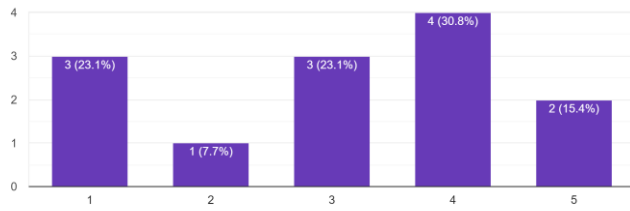
The necessary product and service functions are...

13 responses

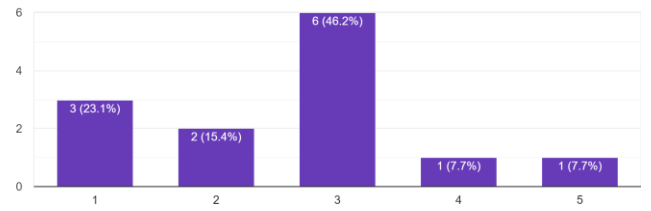


Annex 16.3 – part 2 of the workshop, aggregate results - Market

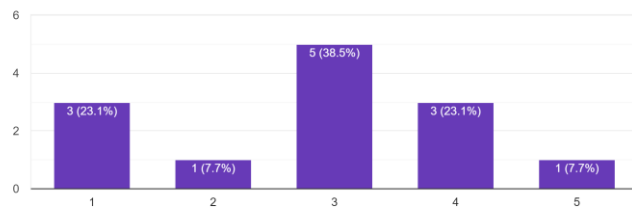
The competitive set (make up of existing or potential competitors) will...  
13 responses



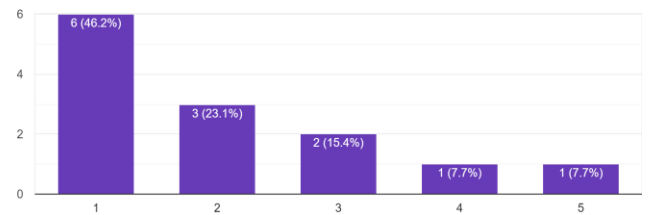
Customer behaviour and decision making processes will...  
13 responses



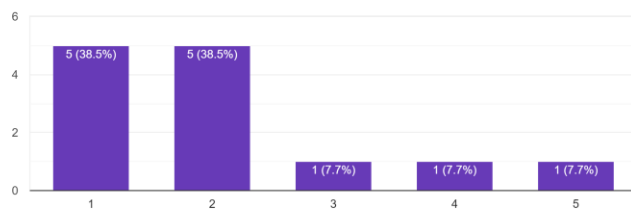
Our distribution and sales activities will...  
13 responses



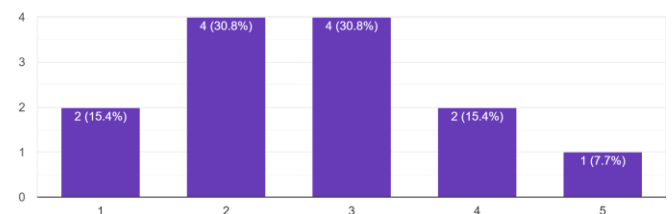
Our brand promise is...  
13 responses



Our current customer relationships are...  
13 responses



Our knowledge of competitors' behaviour and intentions is  
13 responses



### TECHNOLOGY AND SERVICE EXPERTISE

Please answer the following questions based on your understanding of your companies technical and service capabilities in the context of C3ISP for your chosen market segment

**3. Our current development capability is... \***

Mark only one oval.

	1	2	3	4	5	
fully applicable	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	not applicable

**4. Our technology competency is... \***

Mark only one oval.

	1	2	3	4	5	
fully applicable	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	not applicable

**5. Our data management service is... \***

Mark only one oval.

	1	2	3	4	5	
fully applicable	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	not applicable

**6. Our digital service delivery system is... \***

Mark only one oval.

	1	2	3	4	5	
fully applicable	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	not applicable

Organisation details...

**7. The required knowledge and science base are... \***

Mark only one oval.

	1	2	3	4	5	
identical to those of our current offerings	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	completely differ from those of our current offerings

**8. The necessary product and service functions are... \***

Mark only one oval.

	1	2	3	4	5	
identical to those of our current offerings	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	completely differ from those of our current offerings

**9. The expected quality standards in delivery are... \***

Mark only one oval.

	1	2	3	4	5	
identical to those of our current offerings	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	completely differ from those of our current offerings

## **ANNEX 17: C3ISP Hosted workshop for UK BEIS & NCSC**

C3ISP hosted a workshop in London for representatives from the Department for Business, Energy and Industrial Strategy – BEIS and the UK National Cyber Security Centre – NCSC. The workshop explored cyber risk assessments and the sharing of threat intelligence information across the UK's evolving Smart Energy Grid.

The workshop was held on July 17<sup>th</sup> 2019 at the Digital Catapult Centre in London and was hosted by C3ISP an EU Horizon 2020 project. The workshop participants explored together a number of specific cyber threat scenarios that could potentially create cyber chain reactions across the cyber eco-system associated with the UK smart grid at various stages of its digital transformation including future state scenarios.

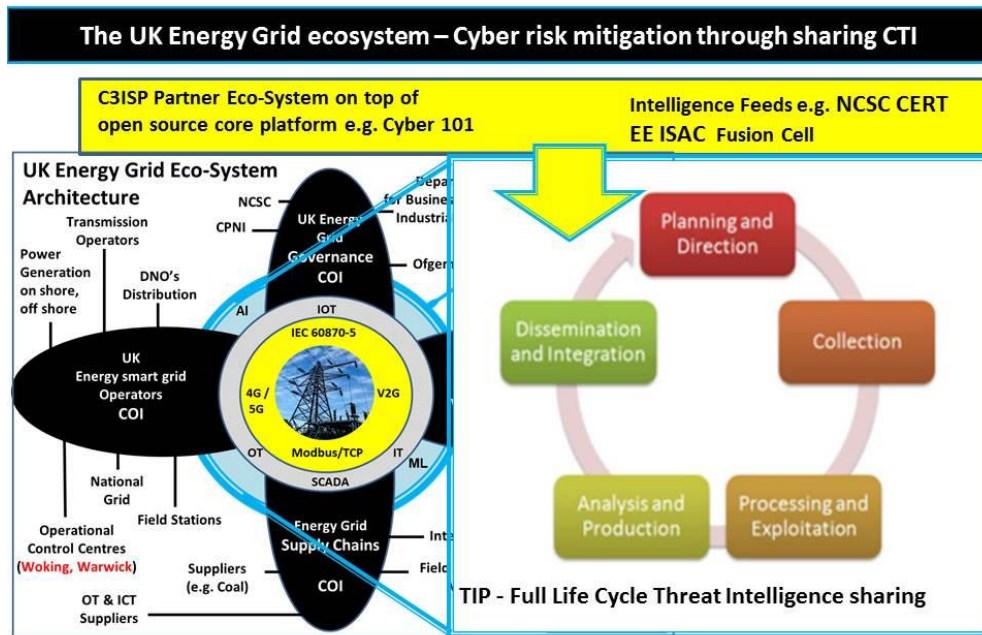
As well as assessing the potential systemic impacts associated with such cyber-attack scenarios the workshop consider the potential mitigation benefits of the sharing of threat intelligence across the public , private stakeholder community forming the UK smart energy grid.

Digital Catapult presented a new approach to Cyber risk in this context which integrates ideas from economics and complexity science into a new approach to understanding dynamic and emergent threats. We worked with and were joined in the workshop by representatives from the Energy Systems Catapult.

Digital Catapult also gave a presentation on the C3ISP project and the potential for exploiting C3ISP Cyber Threat Information sharing capabilities to help mitigate such emergent systemic risks to the Cyber ecosystems of the UK's Critical National Infrastructures.

We then focused in particular to show how C3ISP capabilities could be deployed in the context of the UK Energy Grid ecosystem and the ability for it to form part of a wider collaborative threat intelligence eco-system together with EE-ISAC and NCSC initiatives such as CISP.

An example slide from the workshop is next highlighting the potential deployment of the C3ISP platform to complement CTI capabilities in the context of the UK Energy grid CNI ecosystem.



The workshop attracted participants with a high level of expertise in the smart energy sector including experts in cyber security from NCSC.



## ANNEX 18 – C3ISP PRODUCT DECK



### Collaborative and Confidential Information Sharing and Analysis for Cyber Security



July 2019



The C3ISP method

- Collect
- Analyse
- Inform
- React

2 Collaborative and Confidential Information Sharing and Analysis for Cyber Security

## What is C3ISP?



C3ISP offers a collaborative and confidential information sharing, analysis and protection framework as a service for improved cyber security management.



C3ISP innovation is the possibility to share information in a flexible and controllable manner inside a collaborative multi-domain environment to improve detection of cyber threats and response capabilities, still preserving the confidentiality of the shared information. The C3ISP paradigm is collect, analyse, inform, and react.



C3ISP has been built through the collaboration of leading cyber security experts from across Europe whose input has been invaluable.

3 Collaborative and Confidential Information Sharing and Analysis for Cyber Security

## The C3ISP consortium



4 Collaborative and Confidential Information Sharing and Analysis for Cyber Security

## What problems are we addressing?



**Lack of trust  
in recipients**



**Legal and  
organisational  
barriers**



**Lack of control  
of shared data**



**Interoperability**

5 Collaborative and Confidential Information Sharing and Analysis for Cyber Security

## What is the current impact on the market of not using C3ISP?



**Closed threat  
sharing platforms**

Don't provide a full view  
Reliant on the reach of  
the vendor

**Vulnerable  
supply chains**

You are only as strong as  
your weakest supplier

**Risk of sharing  
sensitive  
information**

This can lead to a lack of  
cooperation and collaboration  
resulting in less effective cyber  
security

6 Collaborative and Confidential Information Sharing and Analysis for Cyber Security

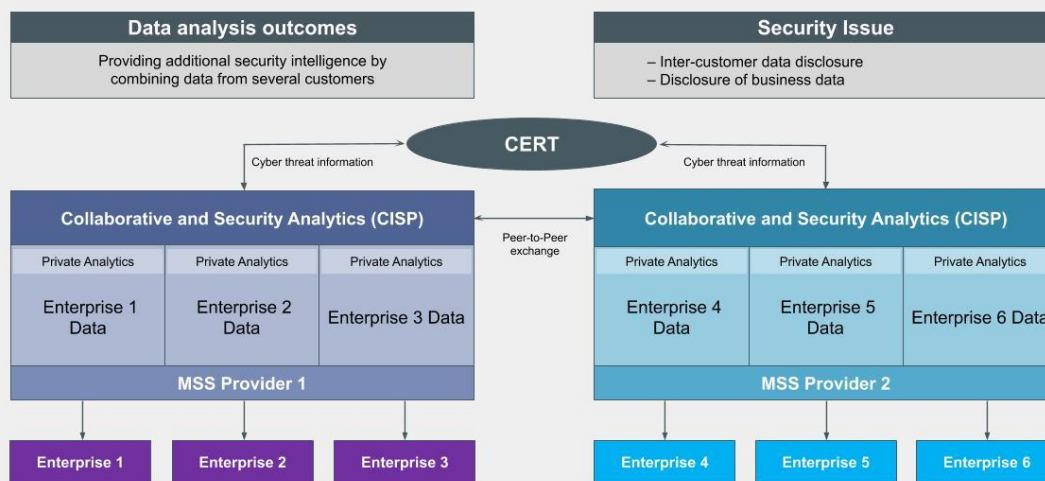
## How does C3ISP work?

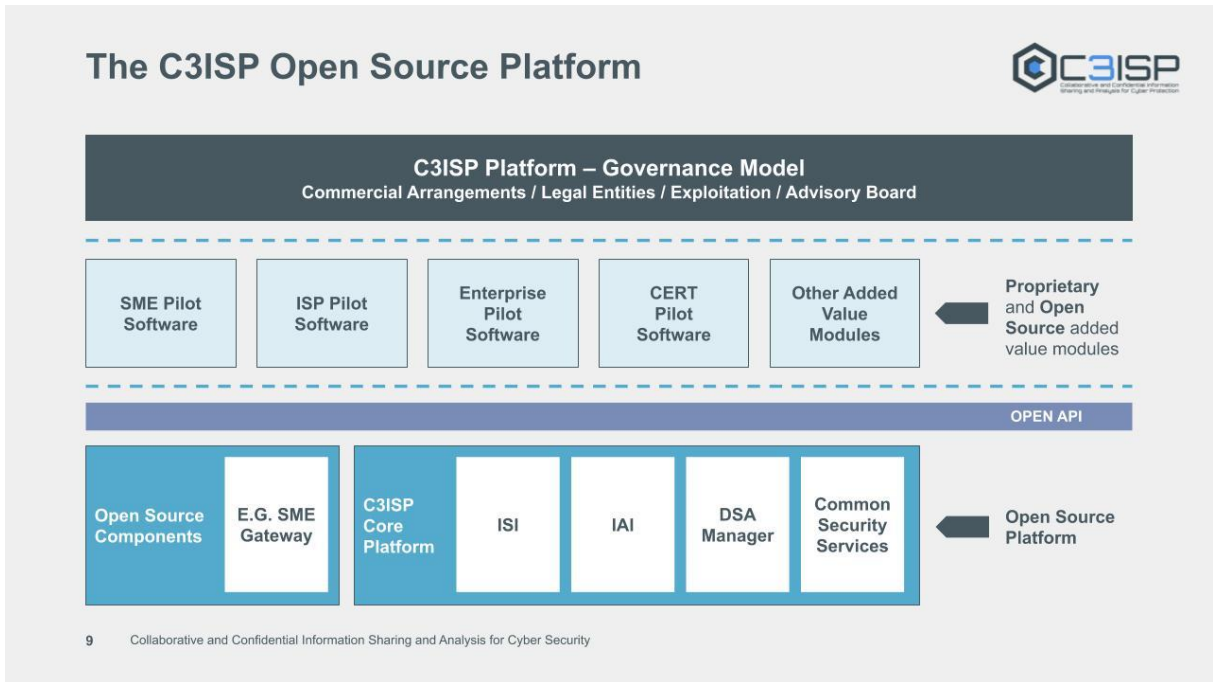


By balancing privacy, accuracy and performance across the threat intelligence sharing process:

- A company engaged with the C3ISP platform is subject to a cyber security attack.
- The cyber threat details and measures to combat the issue are shared on the platform.
- Other organisations engaged with the platform are notified of the threat, along with the details, and can now take appropriate actions to safeguard themselves from a similar cyber attack.
- This is done in a way where each stakeholder can control the confidentiality and anonymity of the data that they share.
- This allows for efficient and effective security measures to be taken by all parties on the platform.

## Prototype of Enterprise Platform





**Stay in touch**



**Jamie Harrison**  
Head of Innovation Practice  
jamie.harrison@digicatapult.org.uk

**Katy Ho**  
Senior Programme Lead  
katy.ho@digicatapult.org.uk

**Charles Fox**  
Security Lead  
charles.fox@digicatapult.org.uk

11 Collaborative and Confidential Information Sharing



**Thank you**



## ANNEX 19 - Letter of support Secure Data

Letter of support

### SECUREODATA

TRUSTED CYBERSECURITY EXPERTS

Prof David W Chadwick Cornwallis Building School of Computing University of Kent Canterbury CT2 ZNF

27th June 2019

#### C3ISP project

Dear David

Thank you very much for your time last week explaining your C3ISP project. From what I saw I think you are working on a very interesting concept of sharing data intelligence in a secure manner which looks exciting. As we discussed, Andrew and I are members of the Managed Security Forum (MSF) which is an organisation initiated by Sir Iain Lobban (Ex Director of GCHQ), Paul Stokes (CEO of Prevalent AI) and Andy France (Ex Deputy Director of GCHQ). The purpose of the MSF is for leading Cyber Security Businesses who have a security presence here in the UK to share knowledge and ideas to improve security for the good of all UK businesses. Members who attend this forum are "C" level/Senior managers within their organisations. Please see the list of organisations who attend below:

BAE Systems, CGI, Cognizant, Computacenter, Countercept, DXC Technologies, Fujitsu, ITC Secure, NCC Group, NCSC, NTT Security, Optiv, Reliance ACSN, SecureData, SecureWorks, Symantec, Telstra, Verizon, Atos, eSentire, Nettitude, Skout Secure Intelligence and Blue Voyant.

Some topics we have collaborated on to date are:

Created a shared guide to managed security Standardising security language in the security space.

Diversity in Security

- Supporting the students within the University Technical College's (UTC's)

Based on what I have seen I can visualise your concept project (providing it is true open source) working well with the MSF's concept vision of working together to improve the overall defence of businesses in the UK. Can I politely ask you to contact the consortium on my behalf to request that we share your project idea with the MSF forum when we next meet in September? If

enough members agree then we could explore how the MSF works together to advance the solution.

Can you please discuss with the consortium and let me know their thinking and if they are happy to proceed on this basis?

Kind regards

Kevin James Operations Director

[www.secddata.com](http://www.secddata.com)

**SecureData Head Office** Hermitage Court / Hermitage Lane Maidstone, Kent ME16 9NT

CYBER ESSENTIALS

**mu pci iso SE**

Company registration number 04365896 VAT nn GR683651313



## ANNEX 20 – Mutual Non-Disclosure Agreement

### Evaluation Agreement

between

**CNR**, PIAZZALE ALDO MORO 7, ROMA ITALY ("CNR")

**MINISTERO DELLO SVILUPPO ECONOMICO**, VIALE AMERICA 201, ROMA ITALY ("MISE")

**HEWLETT PACKARD ITALIANA SRL**, Via G Di Vittorio 9, Cernusco sul Naviglio, MI ITALY ("HPE")

**BRITISH TELECOMMUNICATIONS PUBLIC LIMITED COMPANY**, Newgate street 81, LONDON UK ("BT")

**SAP SE**, Dietmar-Hopp-Allee 16, 69190 Walldorf GERMANY („SAP“)

**COMMISSARIAT A L ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES**, RUE LEBLANC 25, PARIS FRANCE ("CEA")

**THE CONNECTED DIGITAL ECONOMY CATAPULT LIMITED**, LEVEL 9 101 EUSTON ROAD, LONDON UK ("DigiCat")

**UNIVERSITY OF KENT**, THE REGISTRY CANTERBURY, UK ("UniKent")

**GRIDPOCKET SYSTEMS SPOLKA AKCYJNA**, UL ABRAHAMA 1A GDANSK POLAND ("GridPocket")

**Chino Srls**, Via S. G. Bosco, Rovereto ITALY ("Chino")

**3D Repo Ltd**, c/o EIT Digital, Centre House Block C, 56 Wood, LONDON UK ("3DRepo")

(hereinafter „**Partner**“)

and

(hereinafter „**Evaluator**“ and collectively „**Party or Parties**“).

#### 1. Scope

The Partners have signed a consortium agreement laying down the terms and conditions for the execution of the EU funded Project entitled “**C3ISP**” hereinafter „**Project**“. The project aims at developing and evaluating novel cyber security approaches and technologies, especially focused on collaboration in data analysis. In connection with the Project the Partners and Evaluator may deliver to each other, upon the execution of this Agreement, Project Results of Partner and Confidential Information as defined below (the party disclosing such Confidential Information being the “**Disclosing Party**” and the party receiving such Confidential Information being the “**Receiving Party**”).

2. As used herein, “**Project Result**” shall mean \_software artefacts, in any form \_(binaries, virtual machine images etc). Further as used herein, “**Confidential Information**” shall mean all information which Disclosing Party protects against unrestricted disclosure to others, furnished by the Disclosing Party or its Representatives

(defined below) to the Receiving Party or its Representatives in connection with the Evaluation that (i) the Disclosing Party or its Representatives designates as confidential at the time of disclosure or (ii) should reasonably be understood to be confidential given the nature of the information and the circumstances surrounding its disclosure, including but not limited to, information that is related to: (a) the business plans or operations of the Disclosing Party; (b) the research and development or investigations of the Disclosing Party; (c) the business of any customer or partner of the Disclosing Party; (d) Disclosing Party's properties, employees, finances, operations; (e) any information about or concerning any third party (which information was provided to the Disclosing Party subject to an applicable confidentiality obligation to such third party); (f) software and related documentation ("**Disclosing Party's Software**") including the following information regarding Disclosing Party's Software: (i) computer software (object and source codes), programming techniques and programming concepts, methods of processing, system designs embodied in Disclosing Party's Software; and (ii) discoveries, inventions, concepts, designs, flow charts, documentation, product specifications, application program interface specifications, techniques and processes relating to Disclosing Party's Software; and (g) product offerings, content partners, product pricing, product availability, technical drawings, algorithms, processes, ideas, techniques, formulas, data, schematics, trade secrets, know-how, improvements, inventions (whether patentable or not), marketing plans, forecasts and strategies. The term Confidential Information always includes the term Project Results as regards the below sections.

3. Confidential Information shall not be reproduced in any form except as required to accomplish the intent of this Agreement. Any reproduction of any Confidential Information of a Disclosing Party shall remain the property of the Disclosing Party and shall contain any and all confidential or proprietary notices or legends which appear on the original. The Receiving Party: (a) shall take all reasonable steps (defined below) to keep all Confidential Information strictly confidential; (b) shall not disclose or reveal any Confidential Information to any person other than Representatives of either party who are actively and directly participating in the Evaluation or who otherwise need to know the Confidential Information for the purpose of the Evaluation; (c) shall not use Confidential Information for any purpose other than in connection with the Evaluation; and (d) shall not disclose to any person (other than Representatives of either party who are actively and directly participating in the Evaluation or who otherwise need to know for the purpose of the Evaluation) any information about the Evaluation, or the terms or conditions or any other facts relating thereto, including, without limitation, the fact that discussions are taking place with respect thereto or the status thereof, or the fact that Confidential Information has been made available to the Receiving Party or its Representatives without the prior written consent of the Disclosing Party or Parties. As used herein "**reasonable steps**" means those steps the Receiving Party takes to protect its own similar proprietary and confidential information, which shall not be less than a reasonable standard of care. As used herein, "**Representatives**" shall mean (i) employees, consultants and contractors of Receiving Party; and (ii) attorneys, accountants, or other professional business advisors of Receiving Party. The Receiving Party shall be responsible for any breach of the terms of this Agreement by it or its Representatives. Notwithstanding the foregoing the Partners are entitled to communicate and publish their project results according to the terms of the consortium agreement for the Project.

4. The above restrictions on the use or disclosure of the Confidential Information shall not apply to any Confidential Information that: (a) is independently developed by Receiving Party without reference to the Confidential Information, or is lawfully received free of restriction from a third party having the right to furnish such Confidential Information; (b) has become generally available to the public without breach of this Agreement by Receiving Party; (c) at the time of disclosure to Receiving Party was known to such party free of restriction; or (d) Disclosing Party agrees in writing is free of such restrictions.

5. Neither party is required to disclose any particular information to the other and any disclosure is entirely voluntary and is not intended to be construed as: (a) creating a commitment as to any product, including the development or functionality of any product; (b) soliciting any business or incurring any obligation not specified herein; or (c) prohibiting either party from associating themselves with competitors of the other party for purposes substantially similar to those involved herein.

6. During the course of this Agreement, Evaluator may provide input regarding Partners Project Results, without limitation, evaluation, comments or suggestions regarding the possible creation, modification, correction, improvement or enhancement of Partners Project Results (collectively "**Evaluation**"). Evaluator grants to Partner a non-exclusive, perpetual, irrevocable, worldwide, royalty-free license, with the right to sublicense to Partner's licensees and customers, under all relevant Evaluator intellectual property rights, to use, publish, and disclose such Evaluation and to display, perform, copy, make, have made, use, sell, and otherwise dispose of Partner's and its sublicensee's products or services embodying Evaluation in any manner and via any media Partner chooses, with or without reference to the Evaluator. Partner shall be entitled to use Evaluation for any purpose without restriction or remuneration of any kind with respect to Evaluator and/or its representatives.

•

Except for the license granted above to use Evaluation provided by Evaluator at its sole discretion, Partner acquires no title or interest in any pre-existing or independently developed data, information, or intellectual property of Evaluator under this Agreement. Evaluator acknowledges that the information related to Partner's Software, products, services, business or technology plans, disclosed to it under this Agreement, is only intended as possible strategies, developments, and functionalities of the Partner products or services and is not intended to be binding upon Partner to any particular course of business, product strategy, and/or development.

•

7. Nothing in this Agreement shall prohibit or restrict either party's right to develop, make, use, market, license or distribute products or services similar to or competitive with those of the other party disclosed in the Confidential Information as long as it shall not thereby breach this Agreement. Each party acknowledges that the other may already possess or have developed products or services similar to or competitive with those of the party disclosed in the Confidential Information. Further, a Receiving Party shall not be in violation of this Agreement due to the use of any Residuals (defined below) resulting from authorized access to or work with Confidential Information of the Disclosing Party. The term "**Residuals**" means information in non-tangible form which may be incidentally retained in the unaided memory of Representatives of the Receiving Party who have had access to the Confidential Information, so long as such persons have not studied the information for the purpose of replicating the same from memory; provided, however, that in no event shall Residuals include any information that such persons know or a reasonable person would know was Confidential Information of the Disclosing Party. Nothing in this Section shall be deemed to grant any right, title or interest in or to any patents or copyrights of the Disclosing Party. Neither party shall have any obligation to limit or restrict the assignment of such persons or to pay royalties for any work resulting from the use of Residuals.

8. In the event that the Receiving Party or any of its Representatives are requested pursuant to, or required by, applicable law or regulation or by legal process to disclose any Confidential Information or any other information concerning the Disclosing Party or the Evaluation, the Receiving Party shall provide the Disclosing Party with prompt notice of such request or requirement in order to enable the Disclosing Party (i) to seek an appropriate protective order or other remedy; (ii) to consult with the Receiving Party with respect to the Disclosing Party's taking steps to resist or narrow the scope of such request or legal process; or (iii) to waive compliance, in whole or in part, with the terms of this Agreement. In the event that such protective order or other remedy is not obtained in a timely manner, or the Disclosing Party waives compliance, in whole or in part, with the terms of this Agreement, the Receiving Party or its Representative shall use commercially reasonable efforts to disclose only that portion of the Confidential Information which is legally required to be disclosed and to require that all Confidential Information that is so disclosed will be accorded confidential treatment.

9. Upon the Disclosing Party's written request, the Receiving Party shall (at the Receiving Party's election) promptly return or destroy (provided that any such destruction shall be certified by a duly authorized Representative of the Receiving Party) all Confidential Information of the Disclosing Party and all copies, reproductions, summaries, or extracts thereof or based thereon (whether in hard-copy form or on intangible media, such as electronic mail or computer files) in the Receiving Party's possession or in the possession of any Representative of the Receiving Party; provided, however: (i) that if a legal proceeding has been instituted to seek disclosure of the Confidential Information, such material shall not be destroyed until the proceeding is settled or a final judgment with respect thereto has been rendered; and (ii) that the Receiving Party shall not, in connection with the foregoing obligations, be required to identify or delete Confidential Information held in archive or back-up systems in accordance with general systems archiving or backup policies.

10. Neither party shall be under any legal obligation or have any liability to the other party of any nature whatsoever with respect to any proposal, term sheet, letter of intent, or draft agreement relating to any potential relationship or transaction (other than with respect to the confidentiality and other matters set forth herein). Any business decision either party makes in anticipation of definitive agreements is at the sole risk of the party making the decision, even if the other party is aware of or has indicated approval of, such decision. Either party can end the discussions at any time, for any reason, and without liability to the other and each party shall bear its own costs resulting from the discussions.

11. Without prejudice to the rights and remedies otherwise available to either party hereto, each party hereto shall be entitled to seek equitable relief by way of injunction or otherwise if the other party or any of its Representatives breach or threaten to breach any of the provisions of this Agreement.

12. The Receiving Party acknowledges that neither the Disclosing Party nor its Representatives nor any of the officers, directors, employees, agents or controlling persons of such Representatives makes any express or implied representation or warranty regarding the Confidential Information, including, without limitation, any representation or warranty as to the completeness or accuracy of the Confidential Information.

13. This Agreement shall be governed by and construed in accordance with the laws of Germany, without giving effect to its principles or rules regarding conflicts of laws, other than such principles directing application of German law. The parties hereby submit to venue in, and jurisdiction of the courts located in Karlsruhe, Germany for purposes relating to this Agreement. In the event that any of the provisions of this Agreement shall be held by a court or other tribunal of competent jurisdiction to be unenforceable, the remaining portions hereof shall remain in full force and effect. The United Nations Convention on Contracts for the International Sale of Goods shall not apply to this Agreement.

•

14. This Agreement constitutes the entire understanding between the parties hereto as to Confidential Information disclosed hereunder and merges all prior discussions between them relating thereto. Notwithstanding the foregoing, in the event the parties have entered into, or enter into in the future, other agreements which contain terms concerning ownership or use of work product or software license provisions and rights, then this Agreement shall not supersede either party's rights and obligations as provided in such other agreements, unless such other agreement specifically provides otherwise. Neither party will assign or transfer any rights or obligations under this Agreement without the prior written consent of the other party. No amendment or modification of this Agreement shall be valid or binding on the parties unless made in writing and signed on behalf of each of the parties by their respective duly authorized officers or representatives. Any waiver of a provision of this Agreement shall not be deemed a subsequent waiver of the same or any other provision of this Agreement. It is further understood and agreed that no failure or delay by either party hereto in exercising any right, power or privilege hereunder shall operate as a waiver thereof, nor shall any single or partial exercise thereof preclude any other or further exercise thereof or the exercise of any right, power or privilege hereunder.

15. The term of this Agreement shall be for the duration of the Project. It enters into force upon signature by all Parties and ends, insofar all Parties agree unanimously in writing to terminate the cooperation, or if Evaluator accedes to the Project as official project partner by signing the cooperation agreement or latest at **20 September 2019**. In the case the Project is extended in the future, this agreement shall be extended accordingly. The provisions herein concerning the disclosure, protection and use of Confidential Information shall survive the termination or expiration of this Agreement.

This Agreement may be executed in counterparts or by facsimile, each of which shall be deemed an original, and all of which together shall constitute one and the same agreement.

Accepted and Agreed to by:

**MUTUAL NON-DISCLOSURE AGREEMENT**

**Evaluator**

**SAP SE**

---

By

---

Typed

---

Title

---

Date

---

By

---

Typed

---

Title

---

Date

---

By

---

Typed

---

Title

---

Date



*The C3ISP Project is supported by funding under the Horizon 2020 Framework Program of the European Commission DS 2015-1, GA #700294*

## ANNEX 21 – C3ISP Exploitation engagement interview reports

### Giorgos - Elemendar 25/06

Have they looked into the website / understand?

- CISP without the 3
- C3ISP has a bit of a broad scope
- “Platform to share information between people who trust each other?”

\*Charles gives real life example as to describe the platform, energy transport etc\*

- Tailored cloud platform for specific sectors

“I get it now.” - G

Elemendar intro

- Created off the back of a GCHQ accelerator
- 2 years old
- <https://www.elemendar.com/>
- Had government contracts
- Worked with an energy company also
- Lorka (?) programme based at olympic park

Potential synergy with C3ISP?

- Aim to provide PoC to target market sectors - C
- Prove we can work across threat intelligence life cycle stages - C
- Elemendar x C3ISP - C
- Speaks very much to our long term vision - G
- Not enough data to get a system trained up for us - G
- With larger install base, would look to make use of customer feedback - G
- Would hope to have larger quality open source data in future - G
- Supports that notion^ - G
- Share details of white paper with Catapult (can request)

Generic usage case

As a company, as an SME, what security systems do you currently use for yourself? How do you protect yourself?



*The C3ISP Project is supported by funding under the Horizon 2020 Framework Program of the European Commission DS 2015-1, GA #700294*



How are SMEs safeguarding themselves from cyber threats? Threat sharing?

- They are in CISP
- IASME GDPR certification
- Cybersmart - specialise in SME and supply chain security
  - Strong network
- Standard pre packaged solutions - G3,cloud platforms, cybersmart
- Product - automatic patching
- Automated security testbed, as application becomes more exposed

What in your view are the current gaps in the market? Opp for platform like C3ISP?

- Likes the different stages point
- No shortage on what you can do at collection stage
- Any expert can go in collection
- No shortage of sources
- Not going to talk about direction, cannot offer advice
- Processing is where we start to get some of those challenges
  - Operator tooling
  - A lot of low hanging fruit
  - Data quality
- The products that are out there, quality can vary a lot
  - Can sometimes be more work than others
  - A lot of inconsistency in quality
  - Not technical compliance but the utility of what you get
  - Things change quickly and you can't expect people to keep up with that
  - CABS Campaign Against Bad Stix
- Dissemination
  - Probably between people?
  - They don't really touch this
  - How to make it easier, more relevant
  - Industry focus models are definitely helping with that
  - Sometimes people can't afford to pay for the whole thing
  - Tough for small organisations to pay, lack of budget compared to bigger players
    - There is a business case for this point as the weakest players are a threat to the whole chain

Who are the key competitors / players?



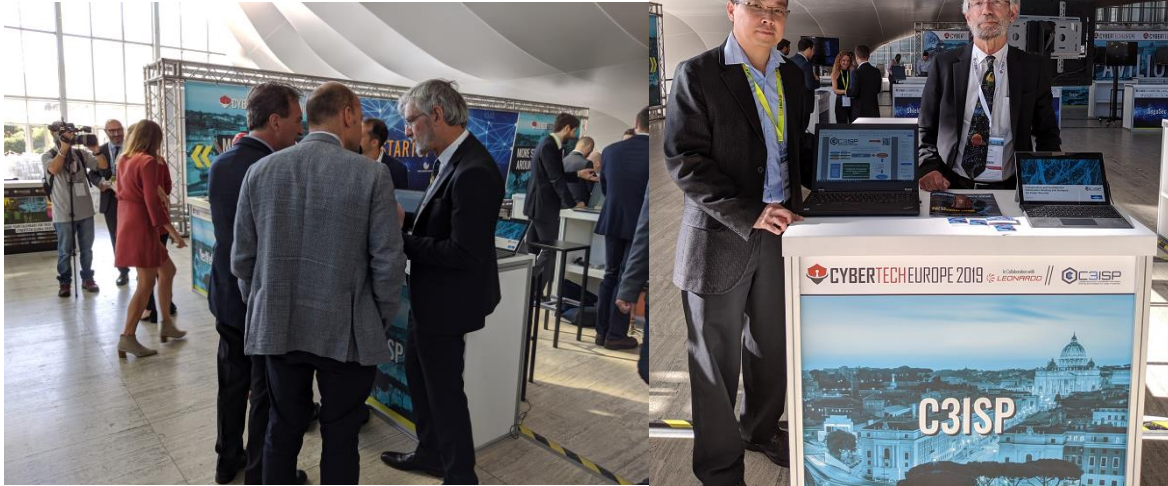
*The C3ISP Project is supported by funding under the Horizon 2020 Framework Program of the European Commission DS 2015-1, GA #700294*

- CISP
- The open threat sharing platform by neumatic?
- Open source tech
- Recorded future
- Threat connect
- A lot of sharing happens without people noticing
  - built into browsers and operating systems
- Individual researchers , independent researchers
- Hidden peer to peer networks



*The C3ISP Project is supported by funding under the Horizon 2020 Framework Program of the European Commission DS 2015-1, GA #700294*

## ANNEX 22 C3ISP Industry Engagement - CyberTech Rome 2019



C3ISP project returned to Rome to take part again in CyberTech Europe which was held in Rome this year on 26th and 27th of September 2019. CyberTech Europe is one of the world major Conference and exhibition events focusing on Cyber Technologies and Security and attracting thousands of attendees not just from Europe but internationally. This was a perfect venue for the C3ISP project to exhibit its capabilities and to demonstrate the C3ISP Pilots to a diverse audience that included Research institutions and Government Agencies, as well as private companies from different market sectors including Defence. The C3ISP Pilots were demonstrated live in the Exhibition hall.



We had interest from a number of organisations from across Europe and even one from Russia. An online survey / analysis of industry engagement was carried by the organisations we engaged with resulting in the following report.



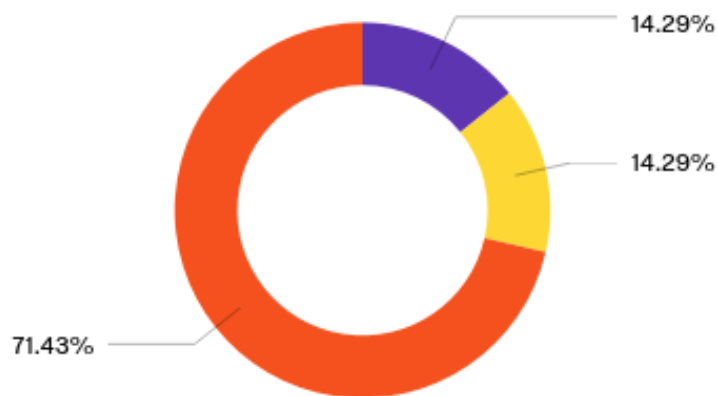
*The C3ISP Project is supported by funding under the Horizon 2020 Framework Program of the European Commission DS 2015-1, GA #700294*

# Default Report - C3ISP at CyberTech Rome

*C3ISP WP4 Evaluation Analyst*

September 26th 2019, 4:16 pm CEST

**17 - The demo showed that analysing the data that have been aggregated/merged from multiple companies gives better insights than only considering a single company dataset**



■ not applicable/not assesable   
 ■ 1- strongly disagree   
 ■ 2   
 ■ 3   
 ■ 4   
 ■ 5- strongly agree

#	Field	Minimum	Maximum	Mean	Std Deviation	Variance	Count
1	The demo showed that analysing the data that have been aggregated/merged from multiple companies gives better insights than only considering a single company dataset	2.00	6.00	5.29	1.39	1.92	7



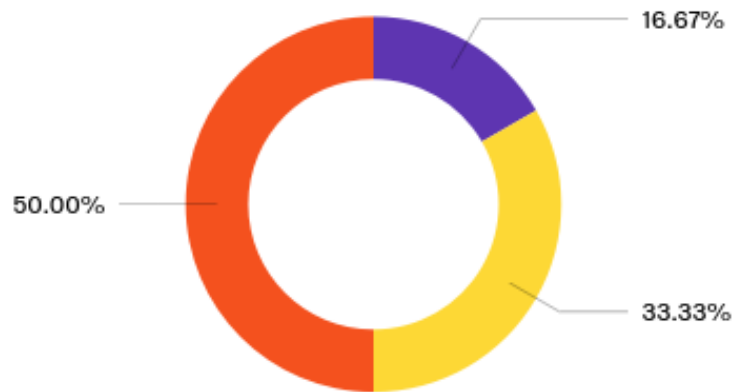
*The C3ISP Project is supported by funding under the Horizon 2020 Framework Program of the European Commission DS 2015-1, GA #700294*

#	Answer	%	Count
1	not applicable/not assesable	0.00%	0
2	1- strongly disagree	14.29%	1
3	2	0.00%	0
4	3	0.00%	0
5	4	14.29%	1
6	5- strongly agree	71.43%	5
	Total	100%	7



*The C3ISP Project is supported by funding under the Horizon 2020 Framework Program of the European Commission DS 2015-1, GA #700294*

**Q46 - The solution demonstrated a good trade-off between data privacy (i.e. anonymised IP address) and information utility (i.e. usefulness for analysis)**



■ not applicable/not assesable   
 ■ 1- strongly disagree   
 ■ 2   
 ■ 3   
 ■ 4   
 ■ 5- strongly agree

#	Field	Minimum	Maximum	Mean	Std Deviation	Variance	Count
1	The solution demonstrated a good trade-off between data privacy (i.e. anonymised IP address) and information utility (i.e. usefulness for analysis)	2.00	6.00	5.00	1.41	2.00	6

#	Answer	%	Count
1	not applicable/not assesable	0.00%	0
2	1- strongly disagree	16.67%	1
3	2	0.00%	0
4	3	0.00%	0
5	4	33.33%	2



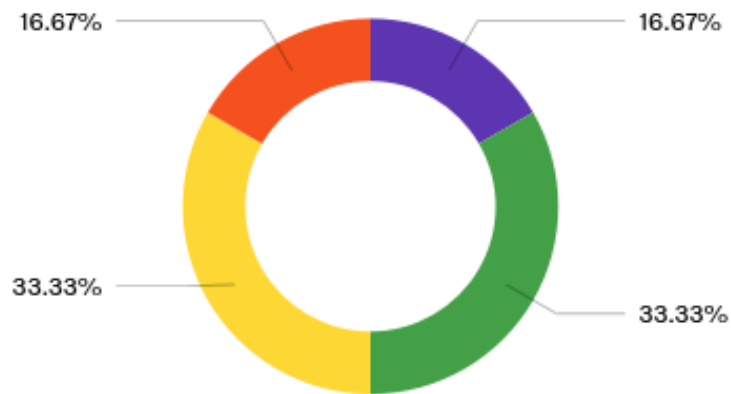
*The C3ISP Project is supported by funding under the Horizon 2020 Framework Program of the European Commission DS 2015-1, GA #700294*

6	5- strongly agree	50.00%	3
	Total	100%	6



*The C3ISP Project is supported by funding under the Horizon 2020 Framework Program of the European Commission DS 2015-1, GA #700294*

**Q47 - The sharing policy can enforce access control, anonymisation and encryption of sensitive data attributes prior to sharing it to a third party. I feel more comfortable to share my company's security data this way**



■ not applicable/not assesable 
 ■ 1- strongly disagree 
 ■ 2 
 ■ 3 
 ■ 4 
 ■ 5- strongly agree

#	Field	Minimum	Maximum	Mean	Std Deviation	Variance	Count
1	The sharing policy can enforce access control, anonymisation and encryption of sensitive data attributes prior to sharing it to a third party. I feel more comfortable to share my company's security data this way	2.00	6.00	4.33	1.25	1.56	6

#	Answer	%	Count
1	not applicable/not assesable	0.00%	0
2	1- strongly disagree	16.67%	1
3	2	0.00%	0



*The C3ISP Project is supported by funding under the Horizon 2020 Framework Program of the European Commission DS 2015-1, GA #700294*

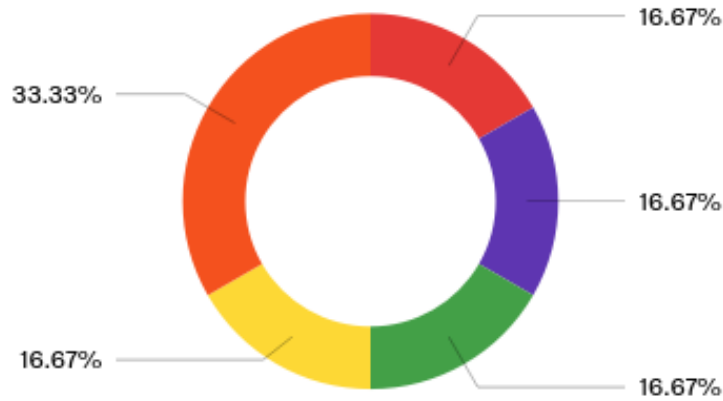


4		3	33.33%	2
5		4	33.33%	2
6		5- strongly agree	16.67%	1
		Total	100%	6



*The C3ISP Project is supported by funding under the Horizon 2020 Framework Program of the European Commission DS 2015-1, GA #700294*

**Q52 - The overall system performance is acceptable**



■ not applicable/not assesable   
 ■ 1- strongly disagree   
 ■ 2   
 ■ 3   
 ■ 4   
 ■ 5- strongly agree

#	Field	Minimum	Maximum	Mean	Std Deviation	Variance	Count
1	The overall system performance is acceptable	1.00	6.00	4.00	1.91	3.67	6

#	Answer	%	Count
1	not applicable/not assesable	16.67%	1
2	1- strongly disagree	16.67%	1
3	2	0.00%	0
4	3	16.67%	1
5	4	16.67%	1
6	5- strongly agree	33.33%	2
	Total	100%	6



*The C3ISP Project is supported by funding under the Horizon 2020 Framework Program of the European Commission DS 2015-1, GA #700294*

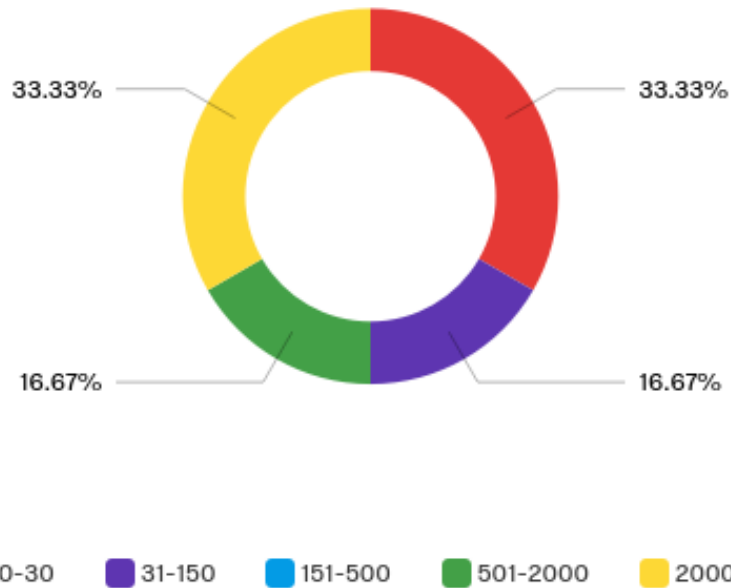
**Q43 - ENT-AT-30: Do you have any considerations you wish to share at this point ?**

benefit  
carry great  
project  
criteria test dataset  
predict case  
import  
analytic



*The C3ISP Project is supported by funding under the Horizon 2020 Framework Program of the European Commission DS 2015-1, GA #700294*

### Q50 - Company size



#	Field	Minimum	Maximum	Mean	Std Deviation	Variance	Count
1	Company size	1.00	5.00	3.17	1.67	2.81	6

#	Answer	%	Count
1	0-30	33.33%	2
4	31-150	16.67%	1
2	151-500	0.00%	0
3	501-2000	16.67%	1
5	2000+	33.33%	2
	Total	100%	6



*The C3ISP Project is supported by funding under the Horizon 2020 Framework Program of the European Commission DS 2015-1, GA #700294*

### Q51 - Company Business Sector



- Telecommunications   ■ Managed Security Service Provider   ■ Application Security
- Professional Services   ■ Travel & Transportation
- Engineering, Construction & Operation   ■ Media   ■ Sports & Entertainment
- Healthcare   ■ Public Sector   ■ Higher Education & Research   ■ Defense and Security
- Banking   ■ Insurance   ■ Retail   ■ Consumer Products   ■ Life Sciences
- Wholesale Distribution   ■ Utilities   ■ Mill Products   ■ Oil and Gas   ■ Chemicals
- Mining   ■ Automotive   ■ Industrial Machinery & Components
- Aerospace and Defense

#	Field	Minimum	Maximum	Mean	Std Deviation	Variance	Count
1	Company Business Sector	4.00	30.00	19.83	9.46	89.47	6

#	Answer	%	Count
1	Telecommunications	0.00%	0



The C3ISP Project is supported by funding under the Horizon 2020 Framework Program of the European Commission DS 2015-1, GA #700294

31	Managed Security Service Provider	0.00%	0
30	Application Security	33.33%	2
4	Professional Services	16.67%	1
5	Travel & Transportation	0.00%	0
6	Engineering, Construction & Operation	0.00%	0
7	Media	0.00%	0
8	Sports & Entertainment	0.00%	0
9	Healthcare	0.00%	0
10	Public Sector	0.00%	0
11	Higher Education & Research	0.00%	0
12	Defense and Security	16.67%	1
13	Banking	0.00%	0
14	Insurance	0.00%	0
15	Retail	0.00%	0
16	Consumer Products	0.00%	0
17	Life Sciences	0.00%	0
18	Wholesale Distribution	0.00%	0
19	Utilities	16.67%	1
20	Mill Products	0.00%	0
21	Oil and Gas	0.00%	0
22	Chemicals	0.00%	0
23	Mining	0.00%	0
24	Automotive	16.67%	1
26	Industrial Machinery & Components	0.00%	0
27	Aerospace and Defense	0.00%	0
	Total	100%	6



*The C3ISP Project is supported by funding under the Horizon 2020 Framework Program of the European Commission DS 2015-1, GA #700294*



*The C3ISP Project is supported by funding under the Horizon 2020 Framework Program of the European Commission DS 2015-1, GA #700294*