D9.3

Second exploitation and dissemination plan

WP9 – Exploitation, Dissemination, Communication and Standardization

C3ISP
Collaborative and Confidential Information Sharing and Analysis for Cyber Protection

Due date of deliverable: <30/09/2018>
Actual submission date: <30/09/2018>

28/09/2018

Version 1.3

Responsible partner: CNR
Editor: I.Matteucci
E-mail address: ilaria.matteucci@iir.cnr.it

Project co-funded by the European Commission within the Horizon 2020 Framework Programme		
	Dissemination Level	
PU	Public	✓
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	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: I. Matteucci (CNR), Paul Galwas (DIGICAT), Maria Prokopi (DIGICAT), Than Hai Nguyen (CEA), David Chadwick (UNIKENT), Jovan Stevovic (CHINO), Ian Herwono (BT), Selina Wang (BT), Patrizia Ciampoli (HPE), Charence Wong (3DRepo).

Approved by: List of reviewers: Than Hai Nguyen (CEA), Jovan Stevovic (CHINO)

Revision History

Version	Date	Name	Partner	Sections Affected / Comments
0.1	2018.03.13	Ilaria Matteucci	CNR	Initial draft of ToC
0.2	2018.06.08	P.A. Galwas	DIGICAT	Initial draft of plan for partner input and review
0.4	2018.07.30	Than Hai Nguyen	CEA	Contribution about standardization
0.5	2018.09.03	Ilaria Matteucci	CNR	Merge different contributions
0.6	2018.09.06	Ilaria Matteucci	CNR	Section about Dissemination and Communication and CNR individual exploitation plan
0.7	2018.09.10	Charles Fox	DIGICAT	DIGICAT Individual exploitation plan
0.8	2018.09.11	David Chadwick	UNIKENT	UNIKENT individual exploitation plan
0.9	2018.09.11	Jovan Stevovic	CHINO	CHINO individual exploitation plan and dissemination activities.
1.0	2018.09.13	Ian Herwono	BT	BT individual exploitation plan
1.1	2018.09.17	Patrizia Ciampoli	HPE	HPE individual exploitation plan
1.2	2018.09.18	Charence Wong	3DRepo	3DRepo individual exploitation plan
1.3	2018.09.20	Ilaria Matteucci	CNR	Final release for internal review
1.4	2018.09.26	Ilaria Matteucci	CNR	Final release after internal review

Executive Summary

This is the third document related to exploitation and dissemination activities of the C3ISP project. The first document, D9.1, reports about the exploitation and dissemination plan of the project, while D9.2 and D9.3 are report about the activities actually made and also some hints about the future especially related to the exploitation activities.

In particular, this document is the second report about the exploitation and dissemination activities that have been carried on within the second year of the C3ISP project. Indeed, this document extends and updates deliverables D9.2, which reported on the exploitation and dissemination at the end of month 12. 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.
- 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 for some C3ISP results.

Table of contents

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 **Errore. L'origine riferimento non è stata trovata.**, 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.

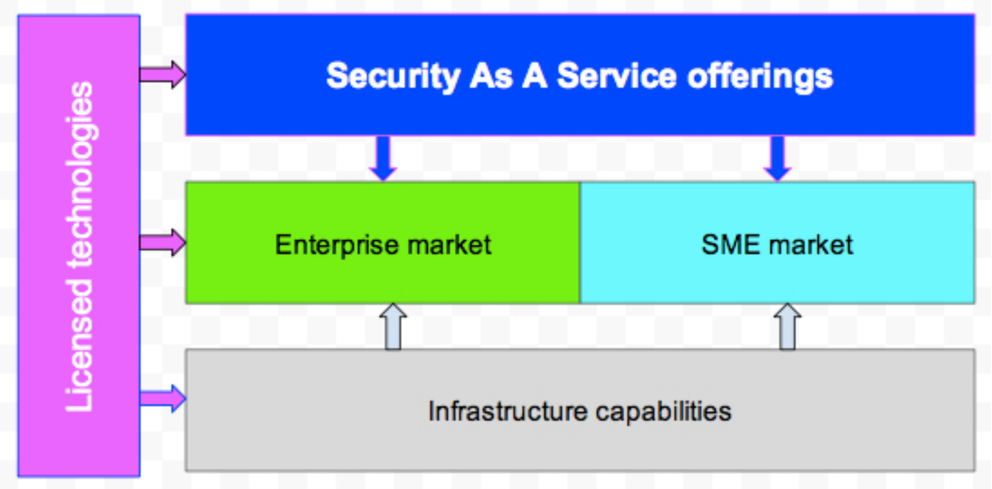


Figure 1. Schematic of C3ISP market context.

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. Innovation Workshop

1.2.1. Exploitation Innovation

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.

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 EVENT**: Engage with the European cyber security ecosystems to promote adoption of the C3ISP framework.

This section is organised as follows. Section 1.2.1.1 describes some workshop preparation and planning information. Section 1.2.1.2 presents a description of the stakeholder engagement process while Section 1.2.1.3 presents the objectives, format and content of the workshop. Summing up, Section 1.2.1.4 and Section 1.2.1.5 discuss about outcomes and next steps, respectively.

1.2.1.1. 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 Appendix 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 Appendix 3 for list of approached companies).
- Shortlisting of external participants based on interests and alignment with C3ISP (see Appendix 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 (Appendix 5).
- Table Plan (Appendix 6).
- Worksheets Handouts (Appendix 7).
- Rules of the road (Appendix 8).

1.2.1.2. 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 Appendix 3 for list of approached stakeholders.

1.2.1.3. 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 appendix 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

1.2.1.4. 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 Appendix 12 and the workshop illustration is in Appendix 9.

1.2.1.5. Next steps

Pilot projects

- Implementation and testing phase 1 complete by 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).

1.2.2. 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 Appendix 2).
- Promoted on social media channels and shared with approached stakeholders (see Appendix 3).
- An informative C3ISP brochure has been created to better brief and inform external stakeholders (see Appendix 10).
- During the workshop, Digital Catapult has retweeted C3ISP tweets from C3ISP official Twitter page (see Appendix 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.

1.3. 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.

We expect the approach will be carried forward and further developed in the Final Exploitation and Dissemination Reports (D9.4).

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.

1.3.1. 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 2 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.

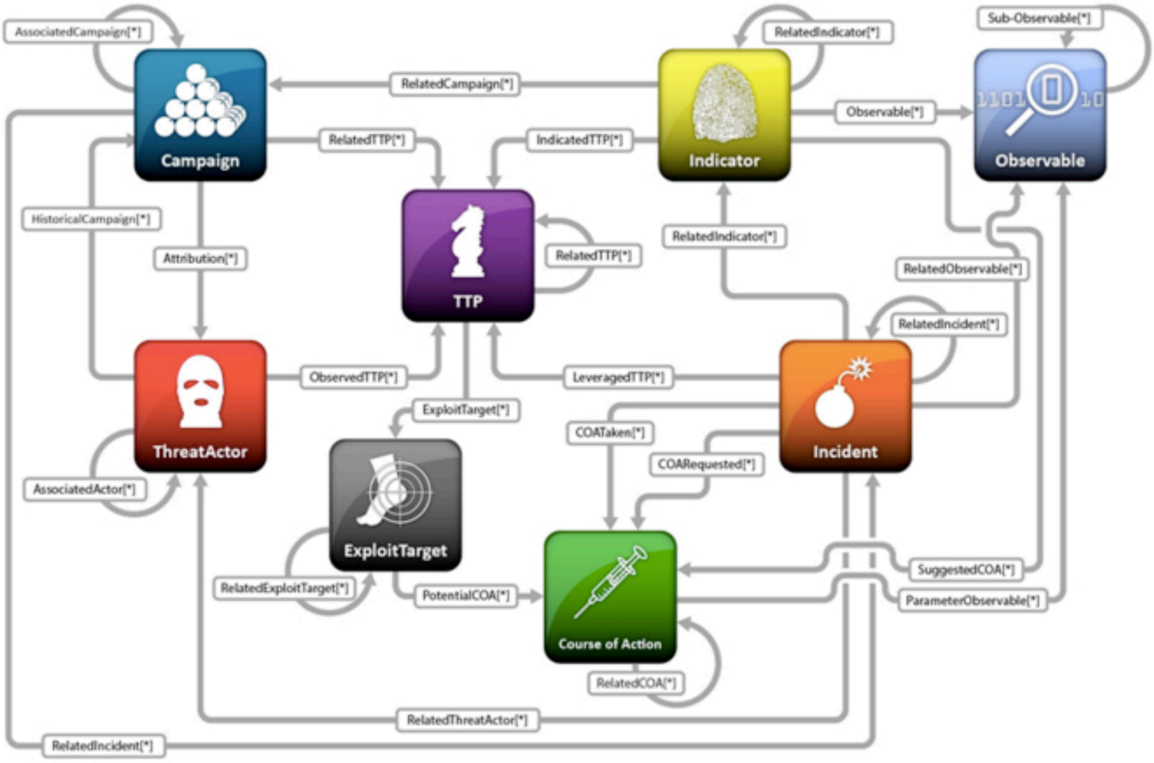


Figure 2: STIX language architecture ([2]).

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.

1.3.2. Threat intelligence providers

It is appropriate to consider the industrial threat intelligence provider market in terms of three main classes. Figure 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.

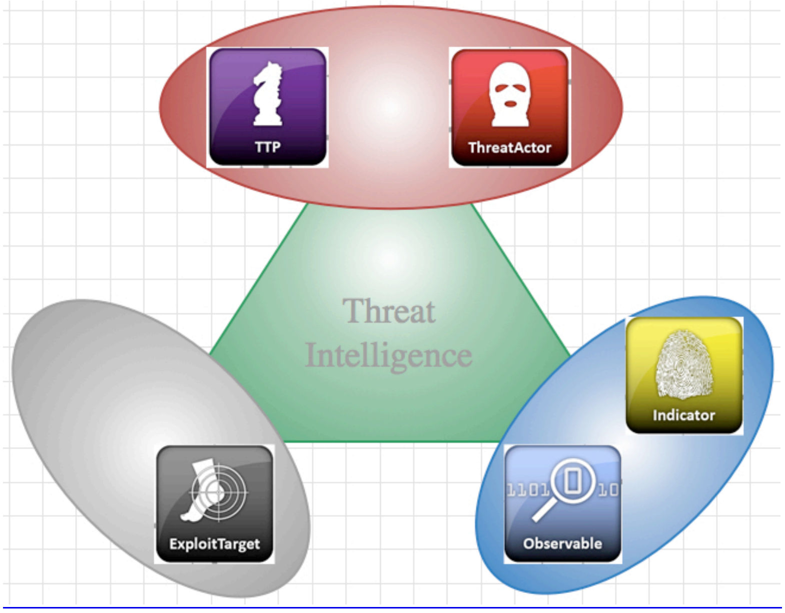


Figure 3: Partitioning of the threat intelligence market by STIX objects.

1.3.2.1. 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.

1.3.2.2. 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

1.3.2.3. 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.

1.3.2.4. 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.

1.3.3. 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 shows the STIX entities that are associated with reacting to the various classes of threat intelligence that are considered above.

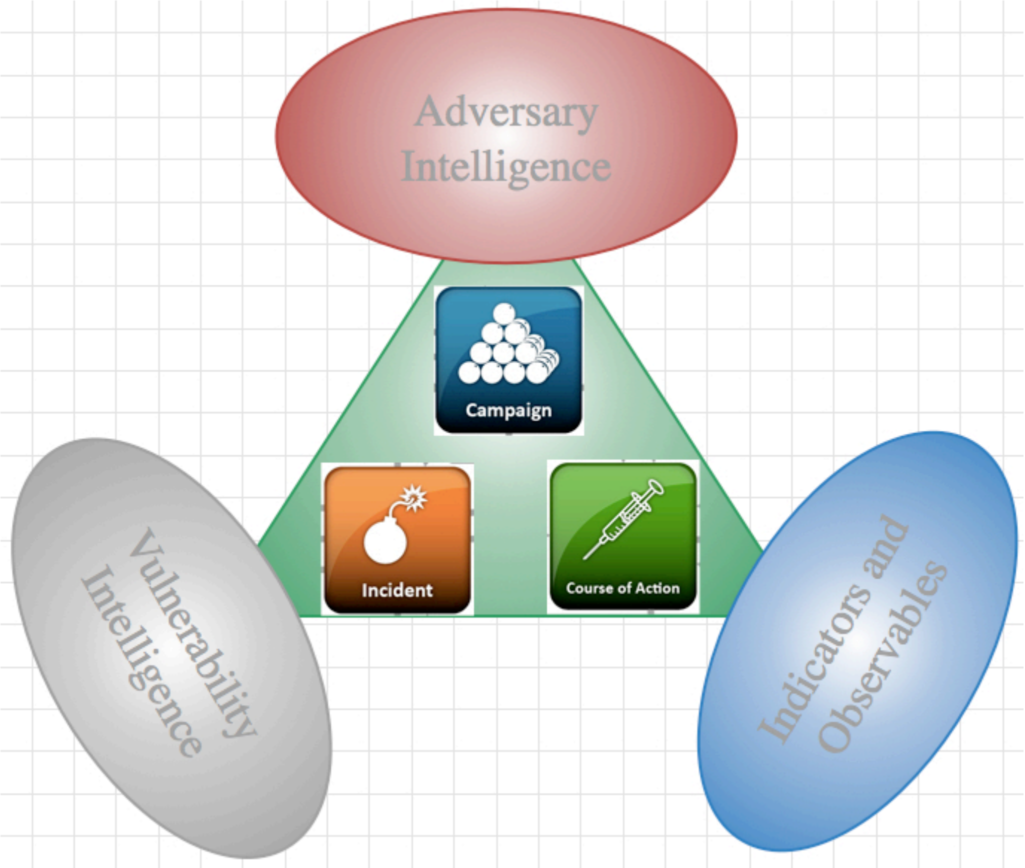


Figure 4: Reacting to threat intelligence.

The green triangle in Figure 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.

1.3.3.1. 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].

1.3.3.2. 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].

1.3.3.3. 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].

1.3.3.4. 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.

1.3.3.5. 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].

1.3.3.6. 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].

1.3.3.7. 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.

1.3.3.8. 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].

[1] 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).

1.3.3.9. 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. Intellectual Property

1.4.1. 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 (1.4.2) by enumerating the components in the project design and system itself, then we [will] define the putative list of IP Items.

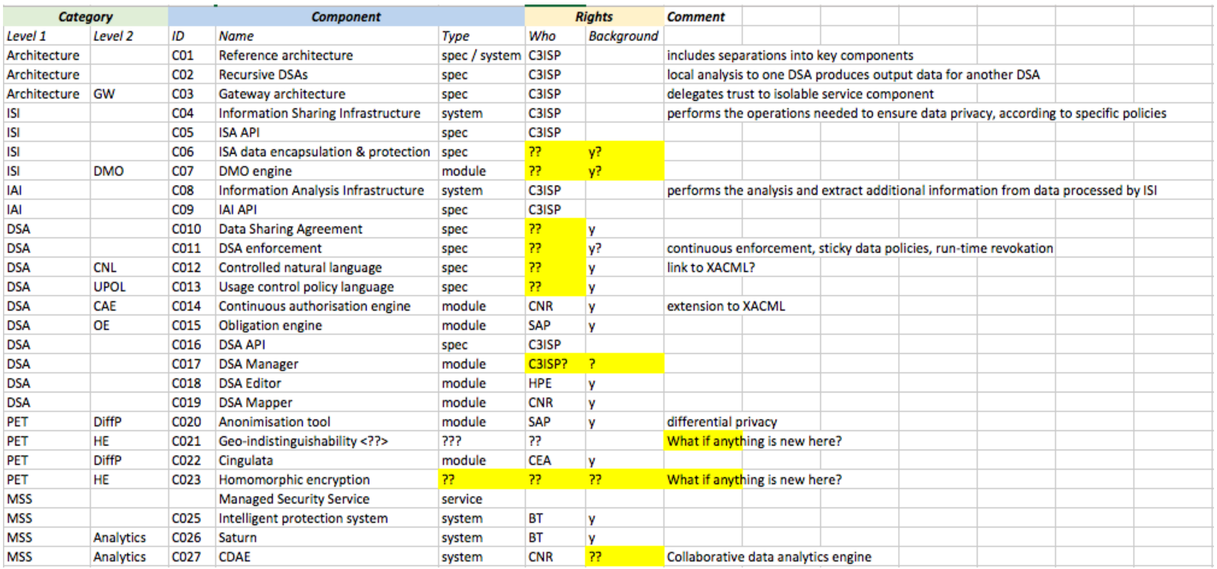
At this stage of the project, we perform a preliminary assessment of the potential value of IP associated with each component in Section (**Errore. L'origine riferimento non è stata trovata.**). Later this valuation will be performed for each IP Item to allow prioritisation of detailed consideration of IP protection measures.

1.4.2. Components

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

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

Table 1 – Components potentially associated with IP



Category		Component			Rights		Comment
Level 1	*Level 2*	*ID*	*Name*	*Type*	*Who*	*Background*	
Architecture		C01	Reference architecture	spec / system	C3ISP		includes separations into key components
Architecture		C02	Recursive DSAs	spec	C3ISP		local analysis to one DSA produces output data for another DSA
Architecture	GW	C03	Gateway architecture	spec	C3ISP		delegates trust to isolable service component
ISI		C04	Information Sharing Infrastructure	system	C3ISP		performs the operations needed to ensure data privacy, according to specific policies
ISI		C05	ISA API	spec	C3ISP		
ISI		C06	ISA data encapsulation & protection	spec	??	y?	
ISI	DMO	C07	DMO engine	module	??	y?	
IAI		C08	Information Analysis Infrastructure	system	C3ISP		performs the analysis and extract additional information from data processed by ISI
IAI		C09	IAI API	spec	C3ISP		
DSA		C010	Data Sharing Agreement	spec	??	y	
DSA		C011	DSA enforcement	spec	??	y?	continuous enforcement, sticky data policies, run-time revokation
DSA	CNL	C012	Controlled natural language	spec	??	y	link to XACML?
DSA	UPOL	C013	Usage control policy language	spec	??	y	
DSA	CAE	C014	Continuous authorisation engine	module	CNR	y	extension to XACML
DSA	OE	C015	Obligation engine	module	SAP	y	
DSA		C016	DSA API	spec	C3ISP		
DSA		C017	DSA Manager	module	C3ISP?	?	
DSA		C018	DSA Editor	module	HPE	y	
DSA		C019	DSA Mapper	module	CNR	y	
PET	DiffP	C020	Anonimisation tool	module	SAP	y	differential privacy
PET	HE	C021	Geo-indistinguishability <??>	???	??		What if anything is new here?
PET	DiffP	C022	Cingulata	module	CEA	y	
PET	HE	C023	Homomorphic encryption	??	??	??	What if anything is new here?
MSS			Managed Security Service	service			
MSS		C025	Intelligent protection system	system	BT	y	
MSS	Analytics	C026	Saturn	system	BT	y	
MSS	Analytics	C027	CDAE	system	CNR	??	Collaborative data analytics engine

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 *Rights* column 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.

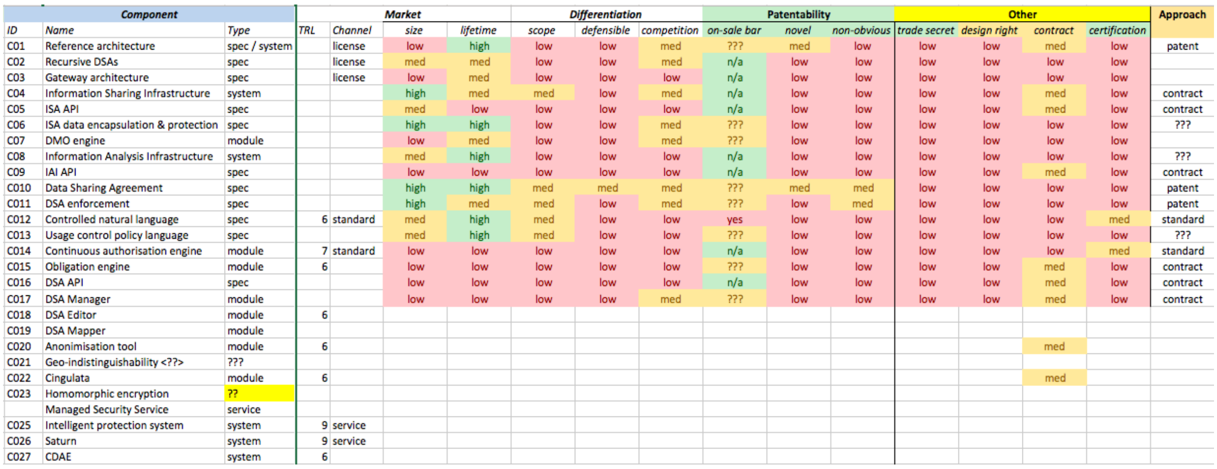
1.4.3. IP value assessment

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



Component			Market				Differentiation			Patentability			Other				Approach
ID	*Name*	*Type*	*TRL*	*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	
C03	Gateway architecture	spec		license	low	med	low	low	low	n/a	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	med	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			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	CDAE	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[2]
  - 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
  - *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 3rd party

[2] 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.

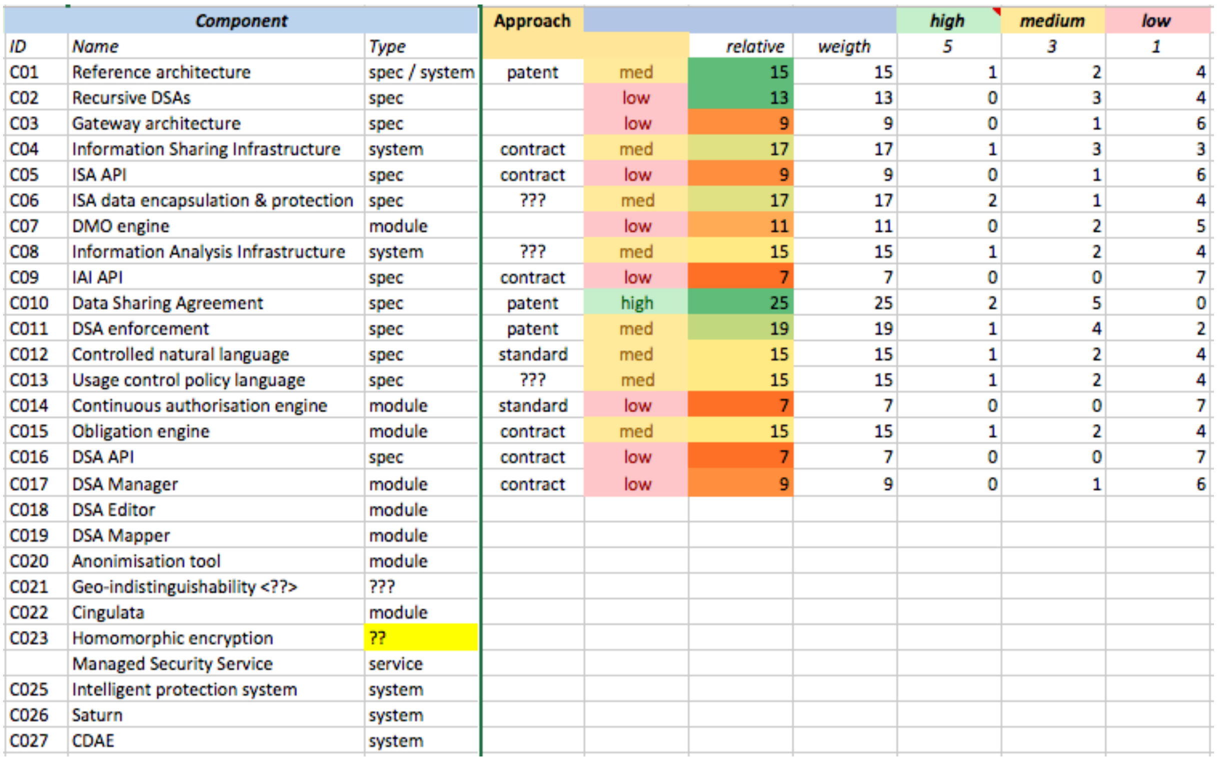
- *Certification*, where compliance and/or standards are used to enforce certain aspects of use of an IP Item
- *Approach*, is the suggested primary means of protection to be used for priority IP Items.

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

1.4.4. 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				high	medium	low
ID	Name	Type			relative	weigth	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.

1.5. Individual Exploitation Activities and Plan

1.5.1. 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 maturated 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.

1.5.2. 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.

1.5.3. 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.

1.5.4. BT

BT C3ISP researchers continued to share their knowledge and progress on C3ISP with other BT teams in security research, development and operational departments. As an outcome BT has started preparative works for deploying the C3ISP Framework and Pilot-specific software into a secure testbed environment that will have access to real data sources. Docker (https://www.docker.com) has been identified as the preferred technology for deploying the various C3ISP software packages. The testbed will be used to evaluate and validate C3ISP solutions and use cases such as collaborative analytics services, or policy-controlled data anonymization/sanitization. Furthermore, BT is also exploring ways on how C3ISP could interwork with the MISP platform [15]; this activity is initiated after the recent launch of BT online platform to allow sharing of data on the latest cyber threats with other ISPs in the UK [35].

1.5.5. SAP

SAP exploitation strategy relies on the valorisation of the C3ISP experiences for fulfilling internal needs. During the last year, also due to the enforcement of GDPR in May 2018, high interest was raised by anonymization tools and techniques therefore the internal dissemination and exploitation activities about C3ISP contributions benefitted from such attention.

Following up the contacts the SAP cyber-security team, a dedicated prototype has been developed for classification and anonymization of cybersecurity information. The prototype reuses concepts developed in C3ISP for specific use cases. The prototype is currently in evaluation.

A similar activity was also established with the SAP IT department, again on anonymization. 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 is released and currently under evaluation.

The exploitation plan for the third year relies on strengthening and reinforcing the collaboration with the entities involved with the prototype releases, in order to gather a critical mass of internal customers that could motivate stronger commitment on anonymization tools. Another element of interest is represented by enhancing the C3ISP support for MISP**Errore. L'origine riferimento non è stata trovata.** for its comprehensive tagging and more in general knowledge organisation, to trigger further activities with the SAP cyber-security team.

1.5.6. CEA

CEA researchers are actively involved in the development of C3ISP and continue to share their knowledges to build a secure analysis platform for C3ISP, especially an integration with Fully Homomorphic Encryption (FHE) technology. Within the second year, the C3ISP experiences and results allow to CEA security teams improving the performance and security parameters of Cingulata – a toolchain dedicated to FHE technology. Recently, thanks to C3ISP project, we have a first release Cingulata 1.0 in open-source version, this compilation toolchain is now available at https://github.com/CEA-LIST/Cingulata. The fact of integrating Cingulata in C3ISP project and deploying a version of Cingulata in open-source project offer to end users a flexibility to develop and deploy his own algorithm working with FHE. Our exploitation plan via C3ISP project is

- firstly, to initiate end users able to work with FHE
- secondly, to provide our expertise on performance and optimization to offer a robust solution for them.

1.5.7. DIGICAT

Digital catapult confirms that the methodology for exploitation innovation has been agreed (as detailed in D9.1, 1.6.2 Exploitation innovation). The 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.

A further two Innovation workshops are planned will follow at appropriate points within the life of the project. The second workshop will focus on validation of the value propositions. The third workshop will focus on the Completed Business Model Canvas – & Exploitation opportunity.

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.

1.5.8. 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.

1.5.9. 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.

1.5.10. 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.

1.5.11. 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.

1.6. 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 appears online immediately after the summer time.

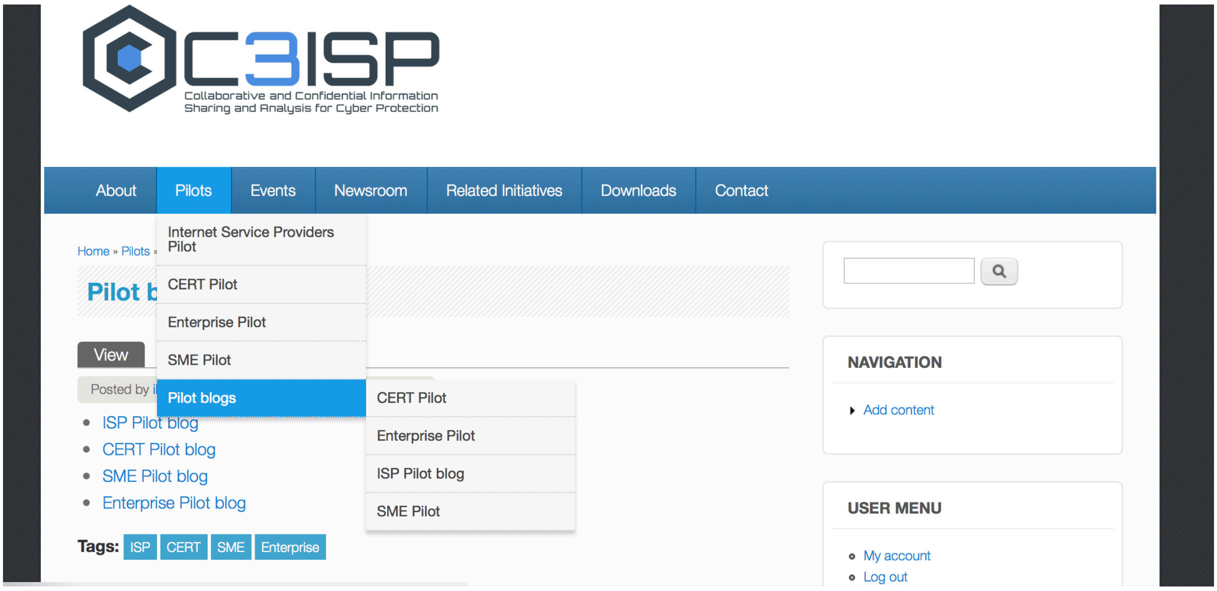


Figure 2. Pilot blogs section in C3ISP webpage.

1.6.1. 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[3] 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?*"[4] 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

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

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

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

1.6.2. 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.

1.6.3. 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

1.6.4. 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 has been carried on within the second 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
Event Participation	3D Repo	Digital Construction Week 2017	18/10/2017 – 19/10/2017	London, UK	Digital construction, engineering, design, manufacturing, and operation experts
Event Organisation	Uni-Kent	Meeting with Secure Data (https://www.secdata.com/aboutus/) to discuss the gathering and use of CTI	18 September 2018	Univ of Kent	Senior staff from Secure Data and researchers from Kent
Event Organisation	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
Event Participation	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.
Event Organisation	CNR	Cyber Security day	17/11/2017	Pisa, Italy	C3ISP was promoted at winter school
Event Organisation	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
Event Participation	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

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

					for SAPs most relevant internal stakeholders
Event Organisation	DigiCat	Innovation Workshop	14/3/2018	London, UK	Overall objective: Understand where the commercial opportunities of the C3ISP technology are
Event Participation	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.
Event Organisation	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.
Event Participation	Uni-Kent	Academic Centres of Excellence in Cyber Security Research Conference	27-28/06/2018	Stratfort upon Avon, UK	academic conference

Event Participation	BT	IEEE CNS 2018 and 4th IEEE Workshop on Security and Privacy in the Cloud	30 May - 1 June 2018	Beijing, China	2018 IEEE Conference on Communications and Network Security, 4th IEEE Workshop on Security and Privacy in the Cloud
Event Participation	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
Event Participation	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
Event Participation	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
Event Participation	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
Event Participation	GridPocket Systems (GPS)	Industry 4.0 conference	20/05/18	Technical University Koszalin	presentation of the project C3ISP during the discussuon - audience of about 70 people
Event Participation	GridPocket Systems (GPS)	Środkowopomorskie Targi	22/03/18	Koszalin Expo-Hall	participate in the Fair, presentation at the conference, audience of about 100 people
Event Participation	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

Event Organization	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.
Event Organization	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.
Event Participation	CNR	The 7th 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.
Event Participation (Booth)	CNR & DC	Italy cybertech conference	27-28 September 2018	Rome, Italy	CNR and DC presents the C3ISP project at the CyberTech Conference.
Event Participation	CNR	ESORICS 2018 conference	3-7 September 2018	Barcelona, Spain	CNR partecipates and organize a workshop to ESORICS conference
Event Participation	GPS	Reliability and Cybersecurity	18-19/09/2018	Kazimierz Dolny, Poland	GPS participates to the event presenting C3ISP results.

2.2. Planned Dissemination Activities

Some dissemination activities for the next year of the project are already planned (see next table).

Category	Lead Partner	Title	Date	Location/Source
Event Organisation	DigiCat	Innovation Workshop	ott-18	TBC

Event Organisation	DigiCat	Innovation Workshop	Summer 2019	TBC
Event Organisation	DigiCat	Expolitation Workshop	Aligned with end phase 2 (September 2019)	TBC
Press Release	HPE	TBC	Pending	Italy
Event Participation	CNR	Cyber Security Day at Internet festival	12 Octobre 2018	Pisa, Italy
Event Participation	3D Repo	Digital Construction Week trade show	17-18 October 2018	London, UK
Event Organisation	3D Repo	British Information Modelling	15-ott-18	London, UK
Press Release	GPS	pending	February 2019	Poland
Event Participation	GPS	Cybersecurity, IoT, SmartGrid	2019 H1	Poland
Event Participation	GridPocket SAS	Cybersecurity, IoT, SmartGrid	2019 H1	France, Holand, Germany
Press Release	3DRepo	British Information Modelling	October 2018	London, UK
Press Release	3DRepo	Cyber Security Day at Internet festival	October 2018	Pisa, Italy
Press Release	CNR	Cyber Security Day at Internet festival	October 2018	Pisa, Italy
Event Participation	CHINO	Pioneers Health	October 2018	Wien, Austria
Event Participation	CHINO	Medica	November 2018	Dusseldorf, Germany
Event Participation	CHINO	Frontiers Health	November 2018	Berlin Germany

2.3. Publications

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

Conference/Workshop

- 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.
- Fabio Martinelli, Francesco Mercaldo, Christina Michailidou, Andrea Saracino: Phylogenetic Analysis for Ransomware Detection and Classification into Families, in proceedings of International Conference on Security and Cryptography (SECRYPT), 2018, ICETE (2) 2018: 732-737.
- Giampaolo Bella, Francesco Marino, Gianpiero Costantino, Fabio Martinelli: Getmewhere: A Location-Based Privacy-Preserving Information Service. PDP 2018: 529-532
- 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. SMARTCOMP 2018: 315-320
- Fabio Martinelli, Christina Michailidou, Paolo Mori, Andrea Saracino: Too Long, did not Enforce: A Qualitative Hierarchical Risk-Aware Data Usage Control Model for Complex Policies in Distributed Environments. CPSS@AsiaCCS 2018: 27-37
- Fabio Martinelli, Francesco Mercaldo, Andrea Saracino: POSTER: A Framework for Phylogenetic Analysis in Mobile Environment. AsiaCCS 2018: 825-827
- Andrea Saracino, Francesco Restuccia, Fabio Martinelli: Practical Location Validation in Participatory Sensing Through Mobile WiFi Hotspots. TrustCom/BigDataSE 2018: 596-607
- Malika Izabachène, Ilaria Chillotti, Nicolas Gama, Mariya Georgieva "Faster Packed Homomorphic Operations and Efficient Circuit Bootstrapping for TFHE" in Asiacrypt 2017.
- Francesco Di Cerbo, Fabio Martinelli, Ilaria Matteucci, Paolo Mori. Towards A Declarative Approach to Stateful and Stateless Usage Control for Data Protection. WEBIST 2018, Seville.
- Francesco Di Cerbo, Marco Rosa. Bringing Access Control Tree to Big Data. 1st International Workshop on Emerging Technologies for Authorization and Authentication ETAA 2018.
- Francesco Di Cerbo and Slim Trabelsi. Towards Personal Data Identification and Anonymization Using Machine Learning Techniques. In European Conference on Advances in Databases and Information Systems 2018 Sep 2 (pp. 118-126). Springer, Cham.

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 Distante, 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.

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.

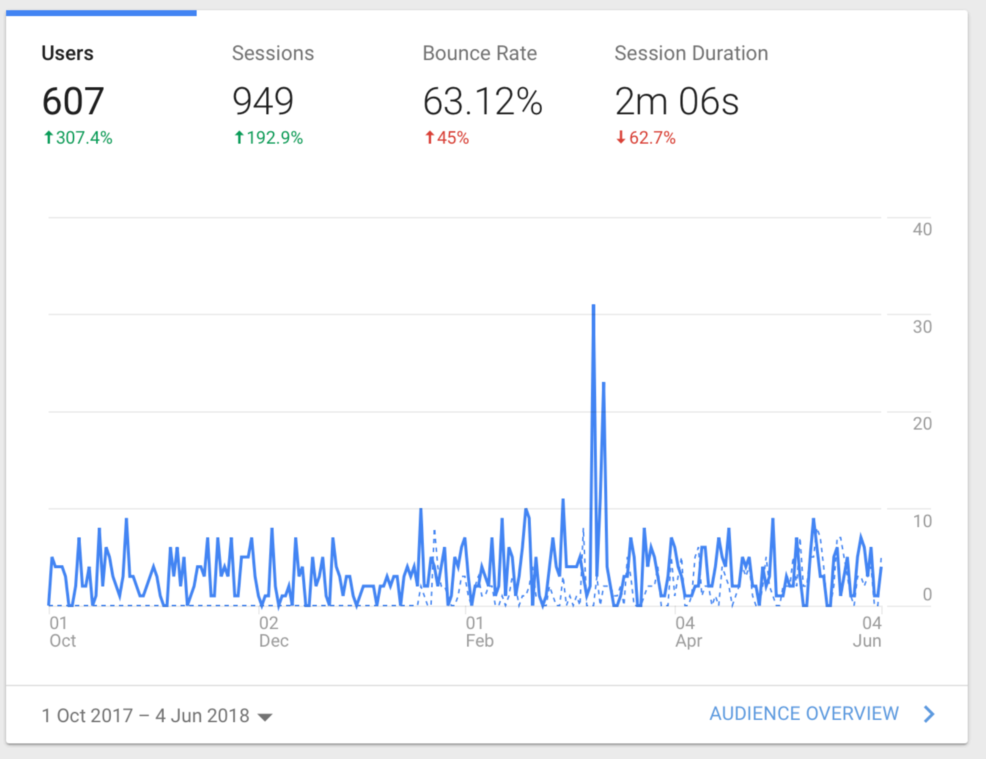


Figure 3. Distribution of visitors within the second year of the project.

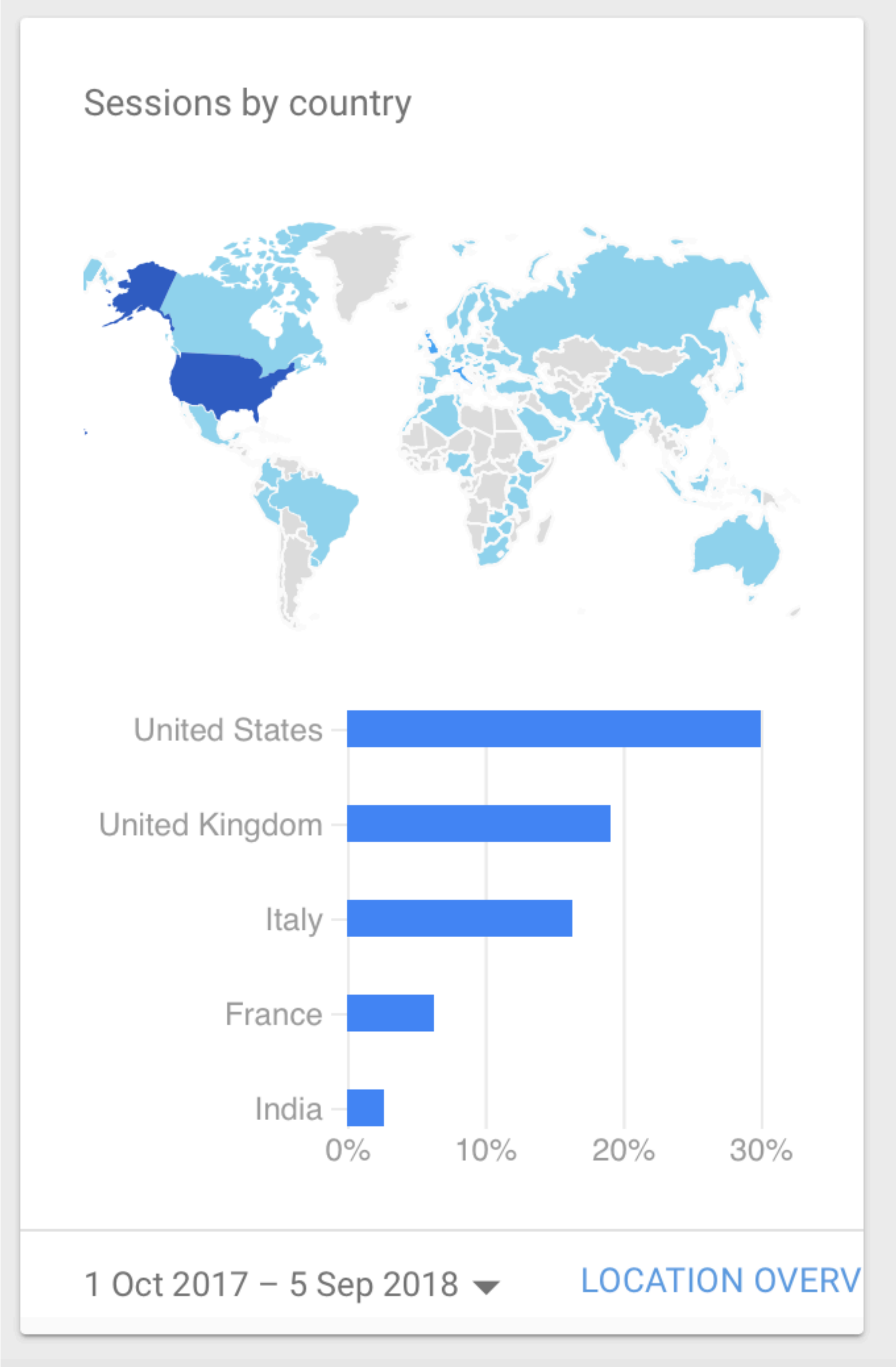


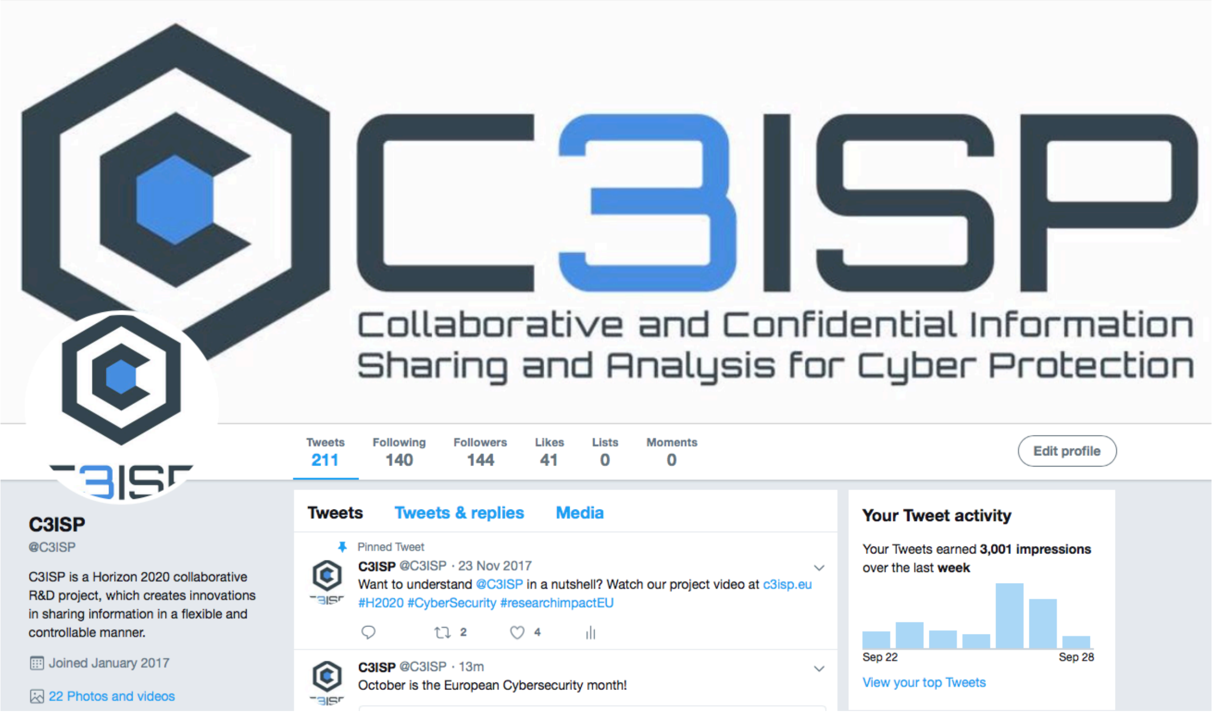
Figure 4. Distribution of sessions per country.

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	https://www.facebook.com/GridPocketSystems/

Social Media	GridPocket SAS	Facebook GridPocket (France)	18 posts regarding the project C3ISP - 28 followers	https://www.facebook.com/gridpocket/
Social Media	GridPocket Systems (GPS)	LinkedIn GPS SA	11 posts regarding the project C3ISP - 44 folowers	https://www.linkedin.com/company/gridpocket-systems-s-a-/
Social Media	GridPocket SAS	LinkedIn Gridpocket, Sophia-Antipolis, France	11 posts regarding the project C3ISP - 211 folowers	https://www.linkedin.com/company/gridpocket-sophia-antipolis-france/
Social Media	GridPocket SAS	GridPocket (R&D)	extensive discussion regarding the project C3ISP - tab R&D	http://gridpocket.com/en/

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



C3ISP
@C3ISP

C3ISP is a Horizon 2020 collaborative R&D project, which creates innovations in sharing information in a flexible and controllable manner.

Joined January 2017

22 Photos and videos

C3ISP @C3ISP · 23 Nov 2017
Want to understand @C3ISP in a nutshell? Watch our project video at c3isp.eu #H2020 #CyberSecurity #researchimpactEU
2 4

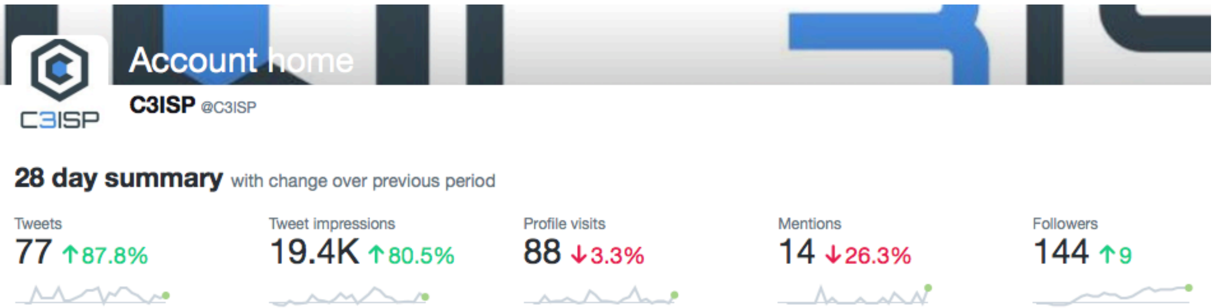
C3ISP @C3ISP · 13m
October is the European Cybersecurity month!

Your Tweet activity

Your Tweets earned **3,001 impressions** over the last **week**

Figure 5. C3ISP Twitter account.

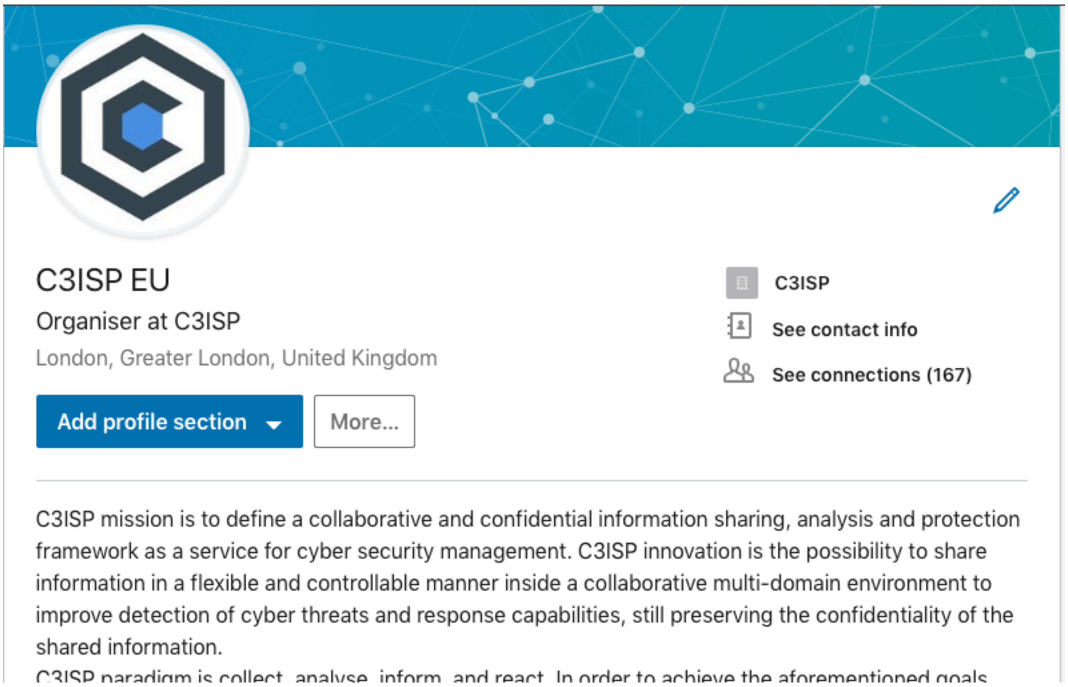
Just for have an idea, in the last months the analytics related to the Twitter C3ISP account are in the following figure.



28 day summary with change over previous period

Tweets	Tweet impressions	Profile visits	Mentions	Followers
77 ↑87.8%	19.4K ↑80.5%	88 ↓3.3%	14 ↓26.3%	144 ↑9

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


C3ISP EU

Organiser at C3ISP

London, Greater London, United Kingdom

C3ISP mission is to define a collaborative and confidential information sharing, analysis and protection framework as a service for 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.

C3ISP paradigm is collect, analyse, inform, and react. In order to achieve the aforementioned goals

Figure 6. C3ISP LinkedIn Account.

2.4.3. Other Communication activities

2.4.4.

Category	Lead Partner	Title	Date	Source	Audience
Blog	3D Repo	BIM Event Speakers Make Plea for Digital Transformation in Construction	29/6/2018	http://3drepo.org/category/press-releases/	All partner stakeholders
Flyer v2	DigiCat	Updated project Brochure/Flyer	1/7/2018	https://c3isp.eu/download/others-list	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, 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 maturated.

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 will propose and validate with the consortium members a simple Framework for mapping the C3ISP capabilities and architectural sub systems to the corresponding standards. We will use this framework to collaborative and holistically identify gaps in the standards and to thus identify opportunities to fill those gaps where appropriate.

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". *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/

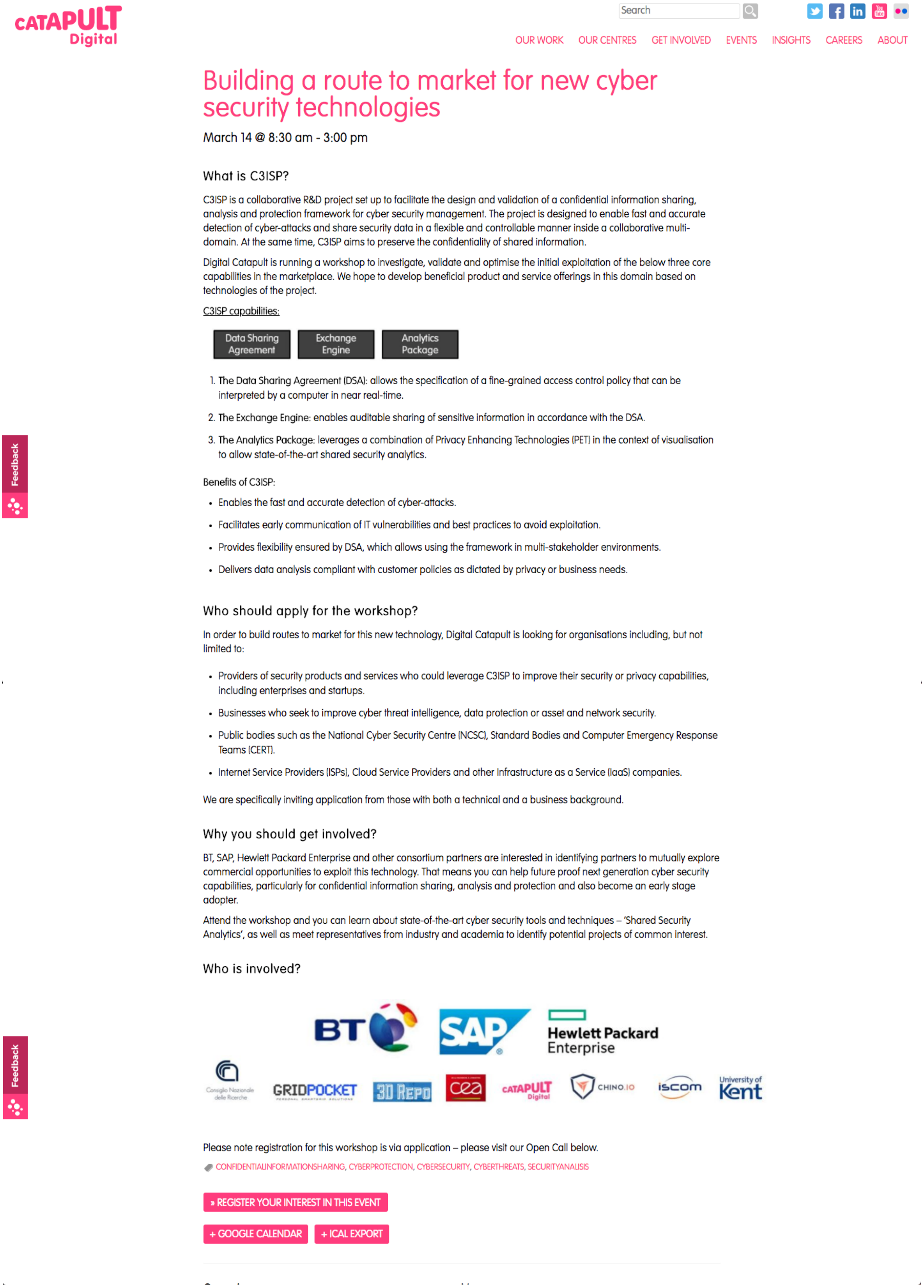
Appendix 1. Glossary

Table 5 - Glossary

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

Appendix 2

C3ISP "Building a route to market for new cyber security technologies" Open Call



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:

Data Sharing Agreement | Exchange Engine | Analytics Package

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, SECURITYANALISIS

» REGISTER YOUR INTEREST IN THIS EVENT

+ GOOGLE CALENDAR + ICAL EXPORT

Appendix 3

List of Approached Companies

Citicus

Acuity Risk Management

Assuria

SentryBay

Cybsafe

CyberLytic

Silicon:Safe

SaltDNA

Autocrypt Solutions

Uleska Limited

ProtectBox

Ansec AI

Titan IC

Aramar

Panaseer

Meterian

SocialOptic

Circadian

PixelPin

Themis Consulting

Xenadata

RazorSecure

Elliptic

Verizon

Swivel Secure

Lujam Internet Security

Intruder

Becrypt

Clearswift

ZoneFox

Privitar

Cyberlytic

Perception Cyber Security

Cyber Sparta

Verasseti

Cynation

Modux

Surevine

Cybershield Group

Digital Shadows

Riskaware

Corvid

RazorSecure

Elliptic

Prosyn Ltd

Protectimus

BAE Systems

Thales

Appendix 4

List of Attending Companies

List of Attendees

BT

HPE

SAP

Digital Catapult

National Research Council

3d Repo

GridPocket

CEA

University of Kent

BAE Systems

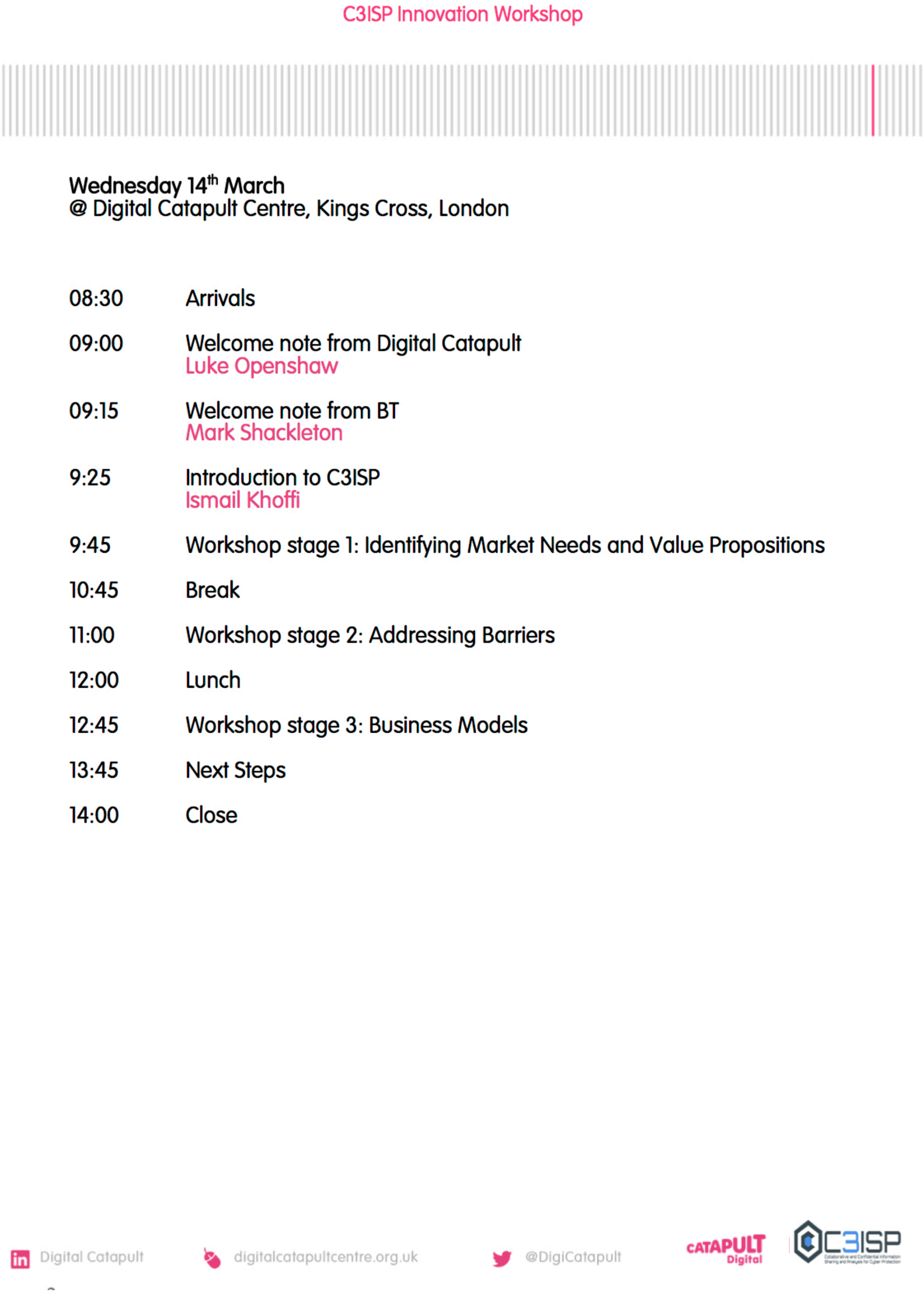
Clearswift
Surevine

Verizon

Thales

Appendix 5

Workshop 1 Agenda



C3ISP Innovation Workshop

Wednesday 14th March
@ Digital Catapult Centre, Kings Cross, London

08:30	Arrivals
09:00	Welcome note from Digital Catapult Luke Openshaw
09:15	Welcome note from BT Mark Shackleton
9:25	Introduction to C3ISP Ismail Khoffi
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

Digital Catapult digitalcatapultcentre.org.uk @DigiCatapult

Appendix 6

Workshop 1 Table Plan

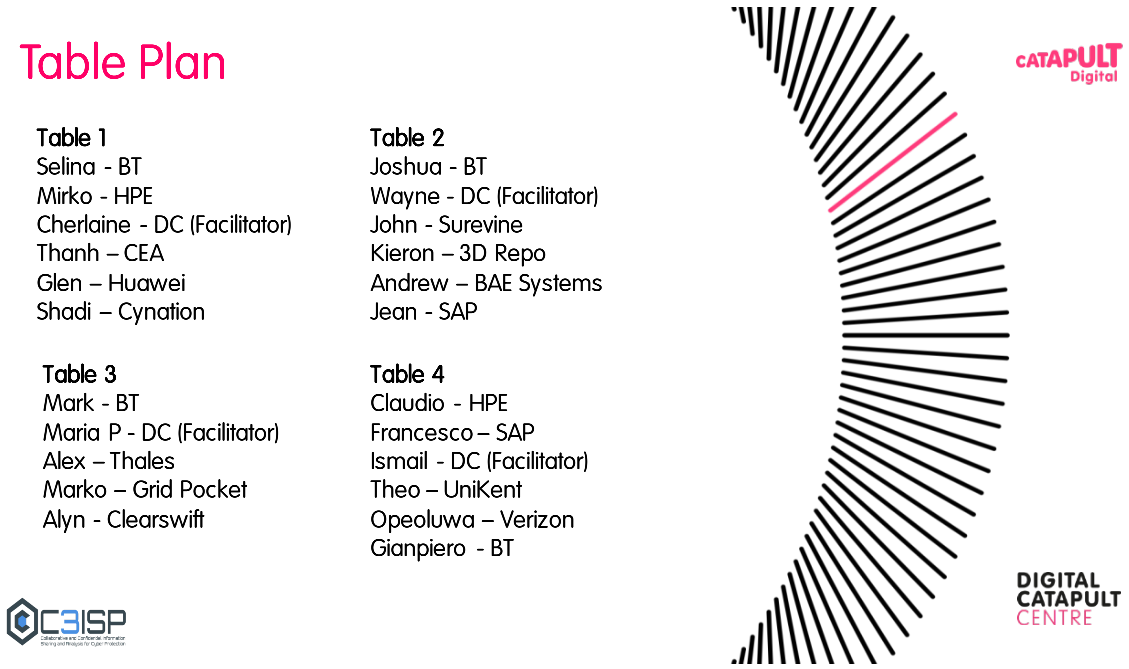


Table Plan

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

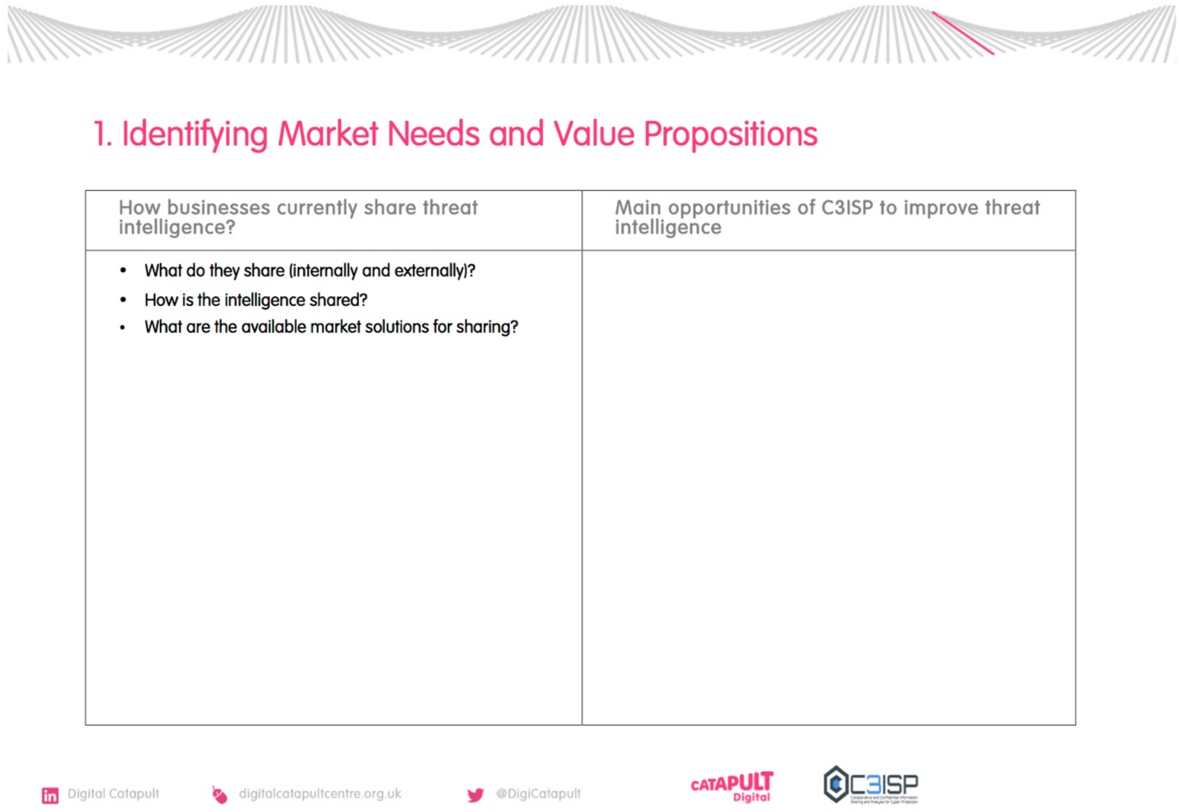
Table 2
Joshua - BT
Wayne - DC (Facilitator)
John - Surevine
Kieron – 3D Repo
Andrew – BAE Systems
Jean - SAP

Table 4
Claudio - HPE
Francesco – SAP
Ismail - DC (Facilitator)
Theo – UniKent
Opeoluwa – Verizon
Gianpiero - BT

C3ISP
Collaborative and Confidential Information Sharing and Analysis for Cyber Protection
CATAPULT Digital
DIGITAL CATAPULT CENTRE

Appendix 7

7.1. Worksheet 1: Identifying Market Needs and Value Propositions



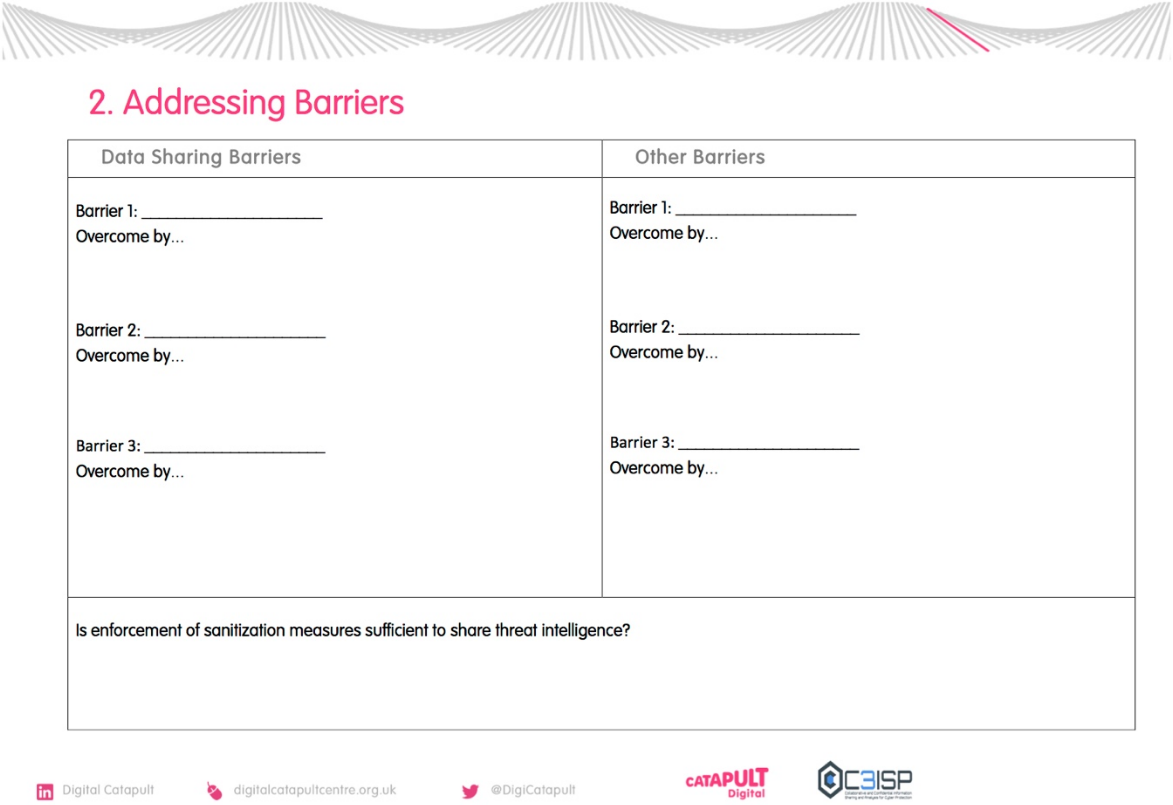
1. Identifying Market Needs and Value Propositions

How businesses currently share threat intelligence?	Main opportunities of C3ISP to improve threat intelligence
• What do they share (internally and externally)? • How is the intelligence shared? • What are the available market solutions for sharing?	

Digital Catapult digitalcatapultcentre.org.uk @DigiCatapult

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

7.2. Worksheet 2: Addressing Barriers



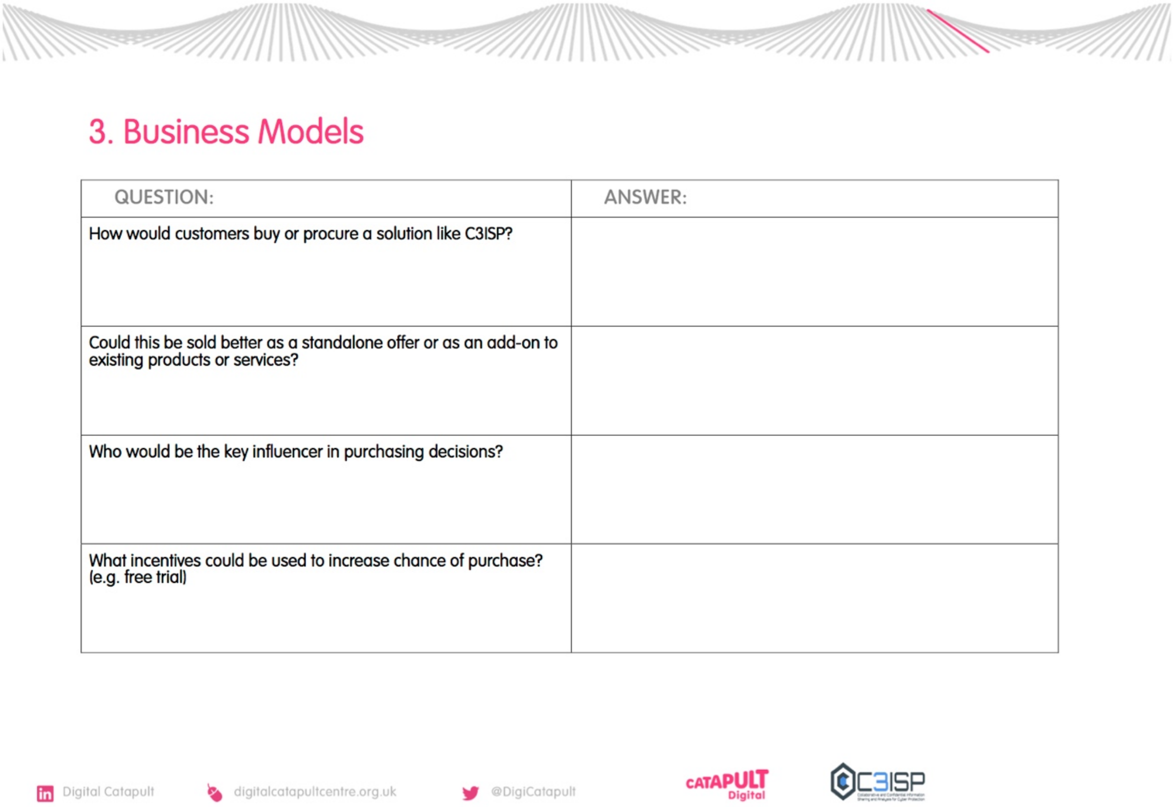
2. Addressing Barriers

Data Sharing Barriers	Other Barriers
Barrier 1: ____________________ Overcome by... Barrier 2: ____________________ Overcome by... Barrier 3: ____________________ Overcome by...	Barrier 1: ____________________ Overcome by... Barrier 2: ____________________ Overcome by... Barrier 3: ____________________ Overcome by...

Is enforcement of sanitization measures sufficient to share threat intelligence?

Digital Catapult digitalcatapultcentre.org.uk @DigiCatapult

7.3. Worksheet 3: Business Models



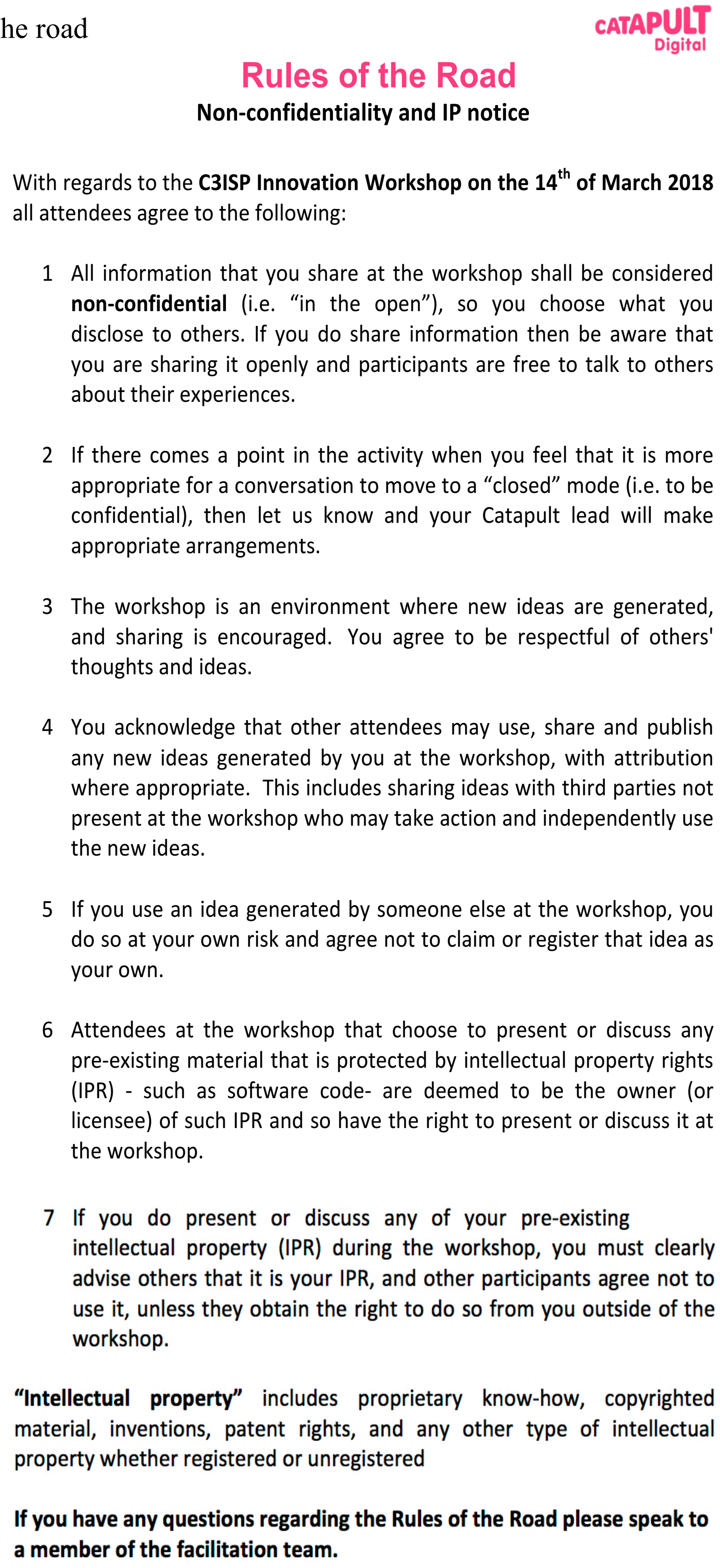
3. Business Models

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)	

Digital Catapult digitalcatapultcentre.org.uk @DigiCatapult

Appendix 8

Workshop rules of the road



CATAPULT Digital

Rules of the Road

Non-confidentiality and IP notice

With regards to the **C3ISP Innovation Workshop on the 14th 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.

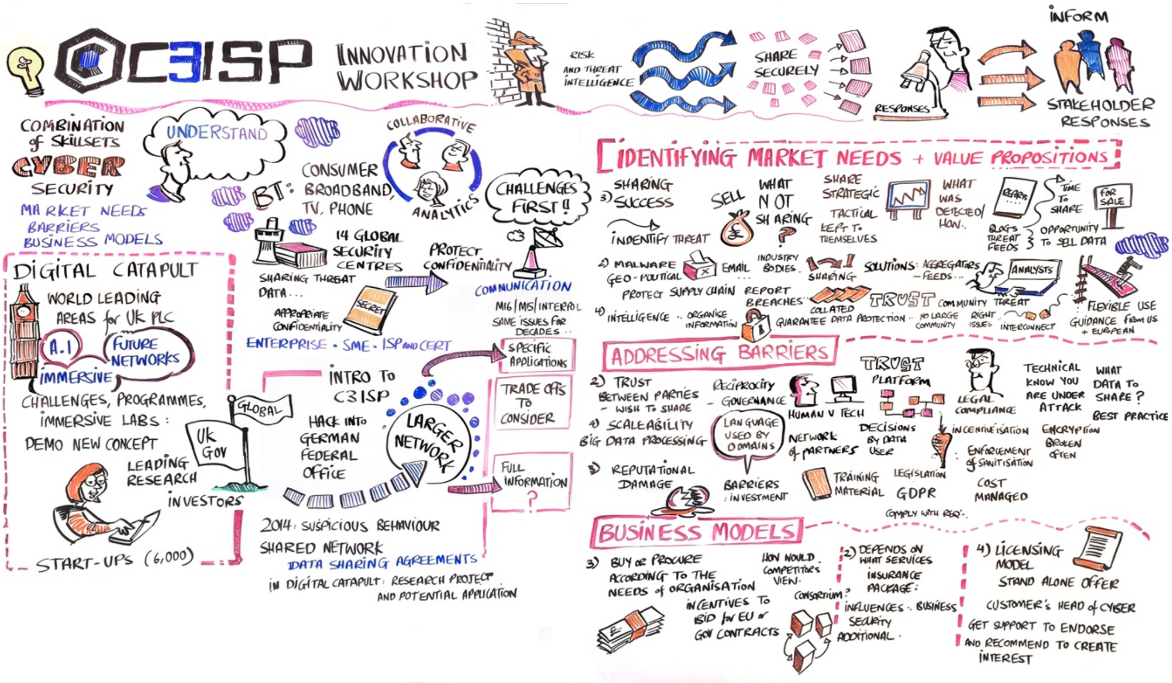
7 If you do present or discuss any of your pre-existing intellectual property (IPR) during the workshop, you must clearly advise others that it is your IPR, and other participants agree not to use it, unless they obtain the right to do so from you outside of the workshop.

"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.

Appendix 9

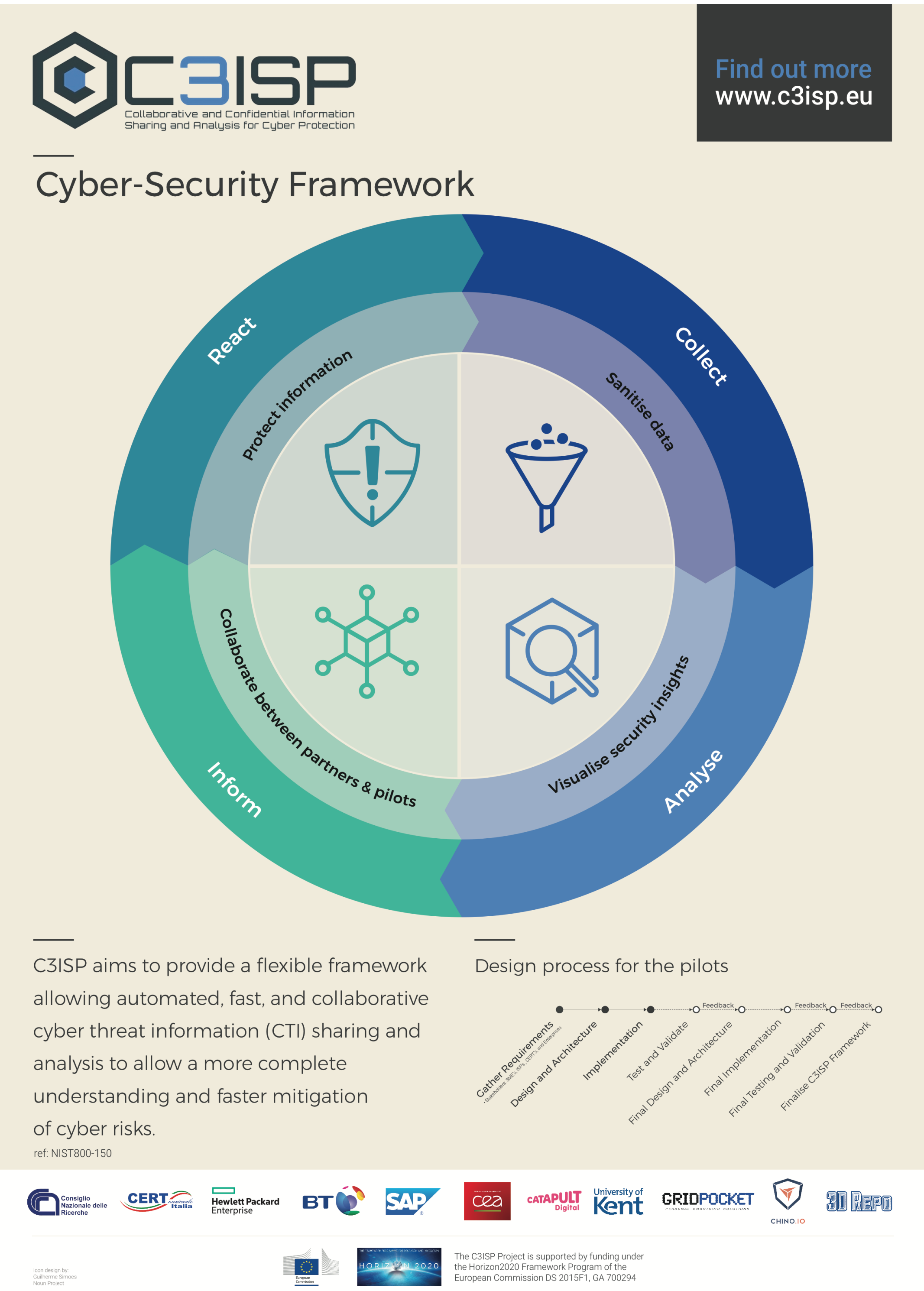
Workshop Illustration



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

Appendix 10

C3ISP Brochure


React
Collect
Analyse
Inform
Protect information
Sanitise data
Visualise security insights
Collaborate between partners & pilots
Gather Requirements
· Stakeholders: SME's, ISP's , CERT's, and Enterprises
Design and Architecture
Implementation
Test and Validate
Feedback
Final Design and Architecture
Final Implementation
Feedback
Final Testing and Validation
Feedback
Finalise C3ISP Framework

C3ISP

Collaborative and Confidential Information Sharing and Analysis for Cyber Protection

Find out more
www.c3isp.eu

Cyber-Security Framework

C3ISP aims to provide 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

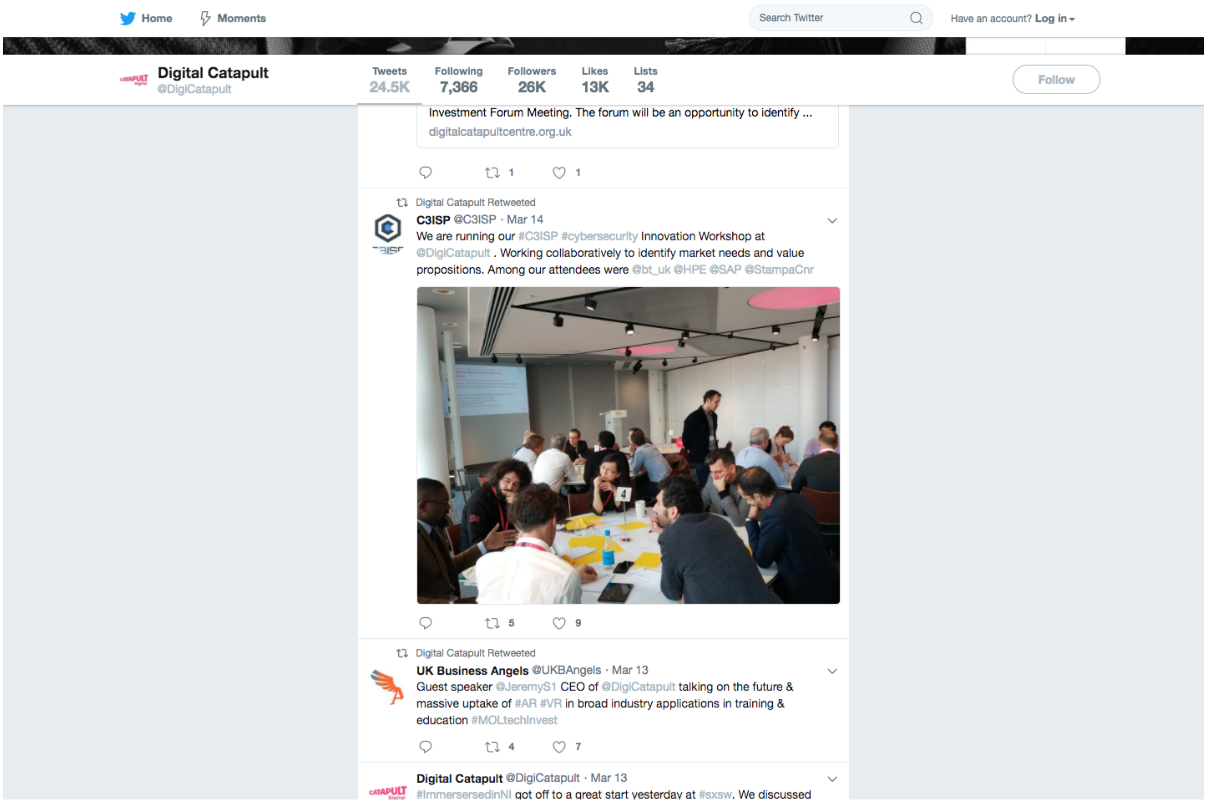
Design process for the pilots

Icon design by:
Guilherme Simoes
Noun Project

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

Appendix 11

Workshop Tweets



Digital Catapult @DigiCatapult

Tweets	Following	Followers	Likes	Lists
24.5K	7,366	26K	13K	34

Investment Forum Meeting. The forum will be an opportunity to identify ...
digitalcatapultcentre.org.uk

1 1

Digital Catapult Retweeted

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

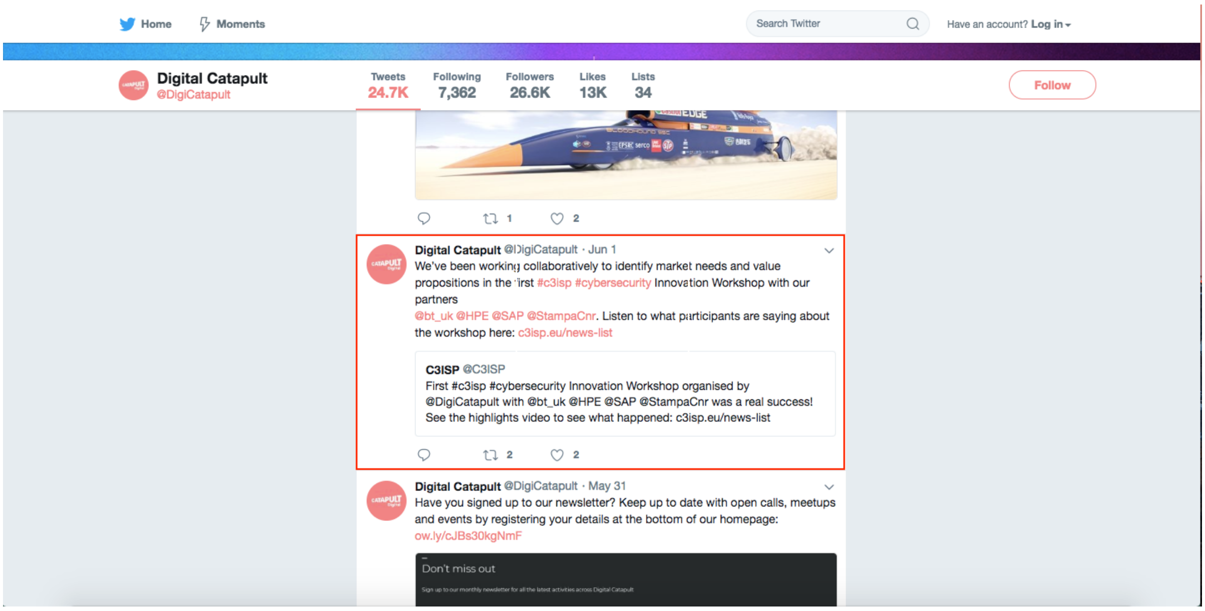
5 9

Digital Catapult Retweeted

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 #MOLtechInvest

4 7

Digital Catapult @DigiCatapult · Mar 13
#ImmersersedinNI got off to a great start yesterday at #sxsw. We discussed



Digital Catapult @DigiCatapult

Tweets	Following	Followers	Likes	Lists
24.7K	7,362	26.6K	13K	34

1 2

Digital Catapult @DigiCatapult · 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

C3ISP @C3ISP
First #c3isp #cybersecurity Innovation Workshop organised by @DigiCatapult with @bt_uk @HPE @SAP @StampaCnr was a real success! See the highlights video to see what happened: c3isp.eu/news-list

2 2

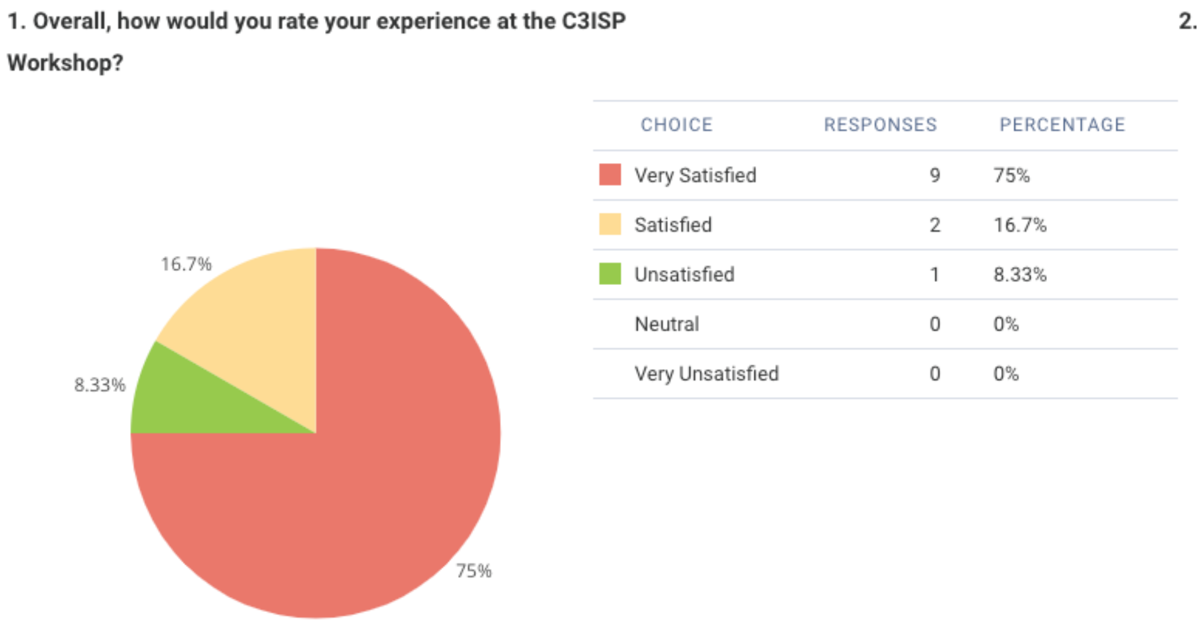
Digital Catapult @DigiCatapult · May 31
Have you signed up to our newsletter? Keep up to date with open calls, meetups and events by registering your details at the bottom of our homepage: ow.ly/cJBs30kgNmF

Don't miss out

Sign up to our monthly newsletter for all the latest activities across Digital Catapult

Appendix 12

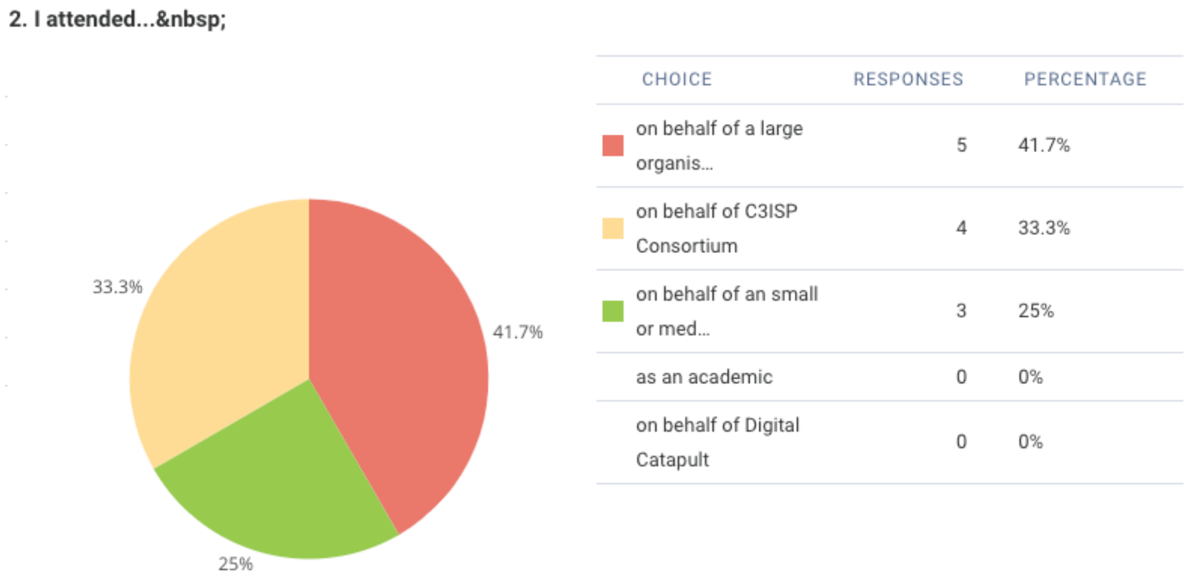
Feedback Form Results



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%

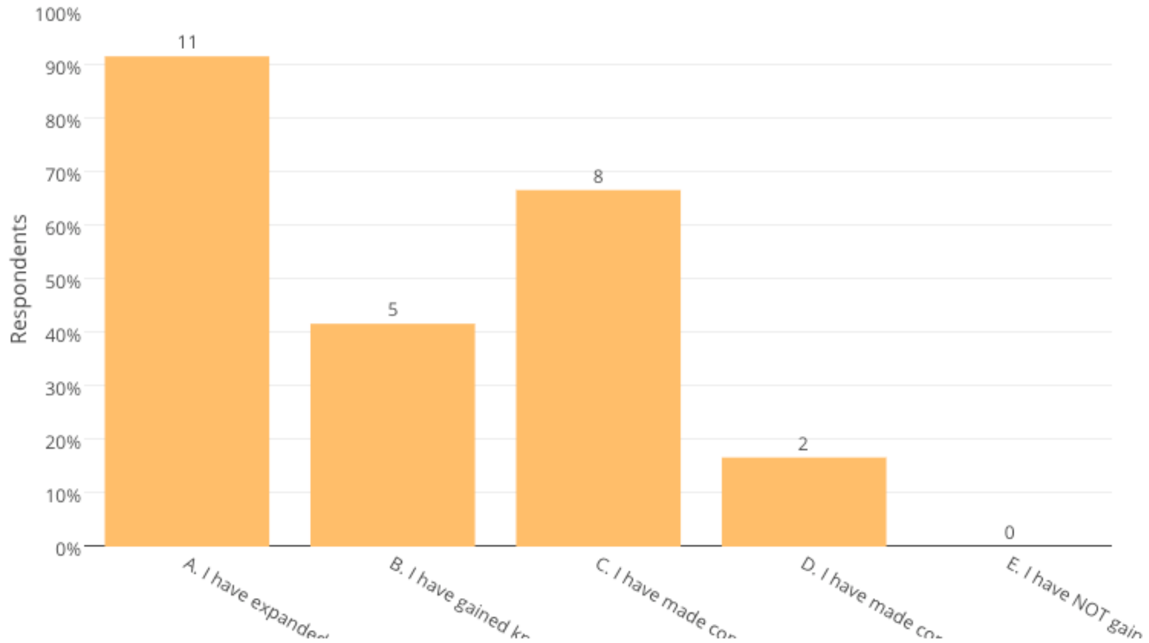


2. I attended...

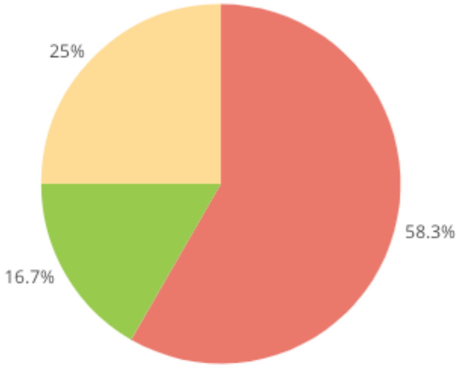
	CHOICE	RESPONSES	PERCENTAGE
🟥	on behalf of a large organis...	5	41.7%
🟨	on behalf of C3ISP Consortium	4	33.3%
🟩	on behalf of an small or med...	3	25%
	as an academic	0	0%
	on behalf of Digital Catapult	0	0%

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

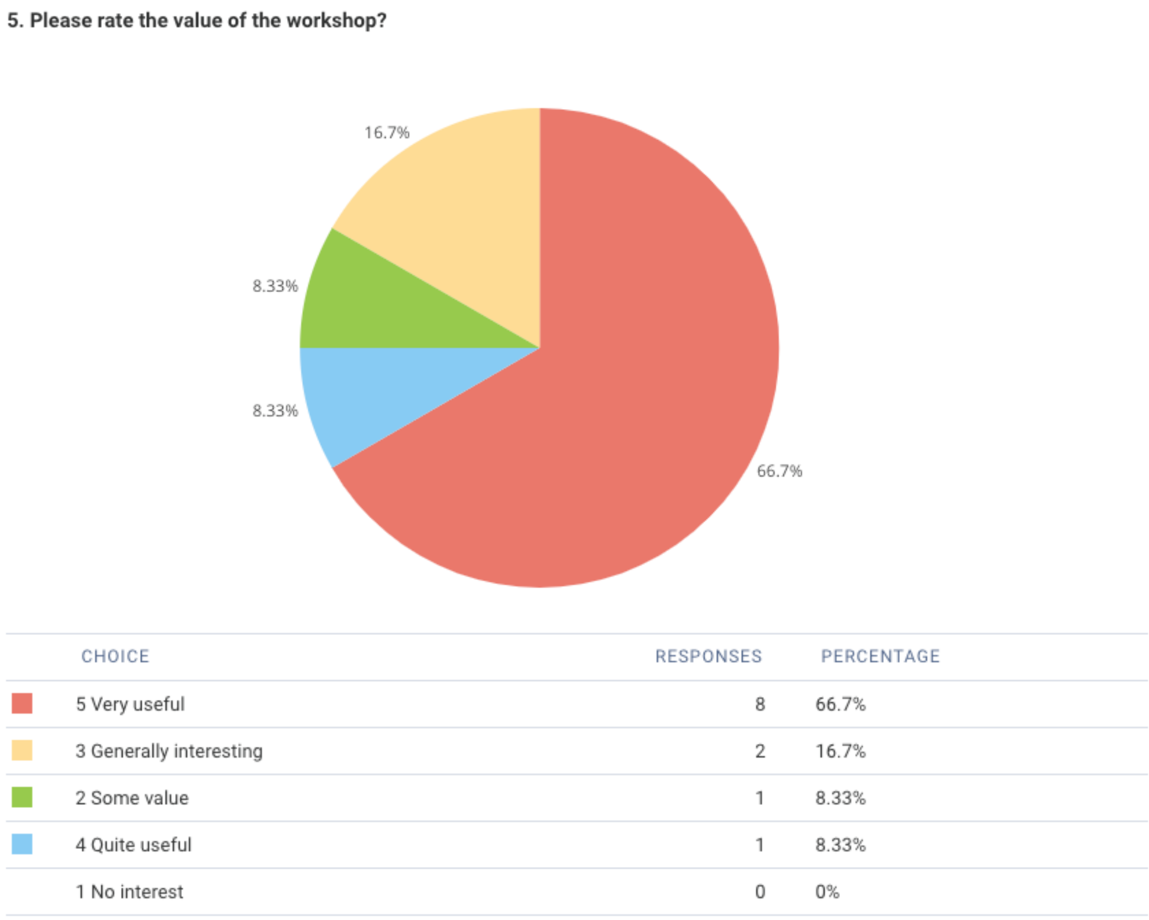
**3. Which of the following statements do you agree with? **



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%