C3ISP Innovation Workshop 1 Report:
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 chapter is organised as follows.

- Paragraph 1 – Some workshop preparation and planning information.
- Paragraph 2 – A description of the stakeholder engagement process.
- Paragraph 3 – The objectives, format and content of the workshop.

Outcomes are analysed in paragraph 4 and the next steps described in paragraph 5.

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 A).

- 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 B for list of approached companies).
- Shortlisting of external participants based on interests and alignment with C3ISP (see Appendix C 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 (see Appendix D).
- Table Plan (see Appendix E).
- Worksheets Handouts (see Appendix F).
- Rules of the road (See Appendix G).

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.
- Possesion of a significant Cyber Security Budget or a provider of cyber security services.

See Appendix B for list of approached stakeholders.

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

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

Format

The workshop was held at Digital Catapult Centre, London. It was held under the Chatham House Rule in order to facilitate open and productive discussion (see appendix G), 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

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 L.

Workshop Illustration (see Appendix H)

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).

Dissemination and Communications

- 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 A).
    - Promoted on social media channels and shared with approached stakeholders (see Appendix B).

- An informative C3ISP brochure has been created to better brief and inform external stakeholders (see Appendix I).

- During the workshop, Digital Catapult has retweeted C3ISP tweets from C3ISP official Twitter page (see Appendix K) 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 interviews to participants and partners for promotional matters. The video is available at this link.

Appendix

Appendix A

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

Appendix B

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 C

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 D

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 E

Workshop 1 Table Plan

Table Plan

Table 1
Selina - BT
Mirko - HPE
Cherlaine - DC (Facilitator)
Thanh - CEA
Glen - Huawei
Shadi - Cynation

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

Table 3
Mark - BT
Maria P - DC (Facilitator)
Alex - Thales
Marko - Grid Pocket
Alyn - Clearswift

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

Appendix F

F.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

F.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

F.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)	

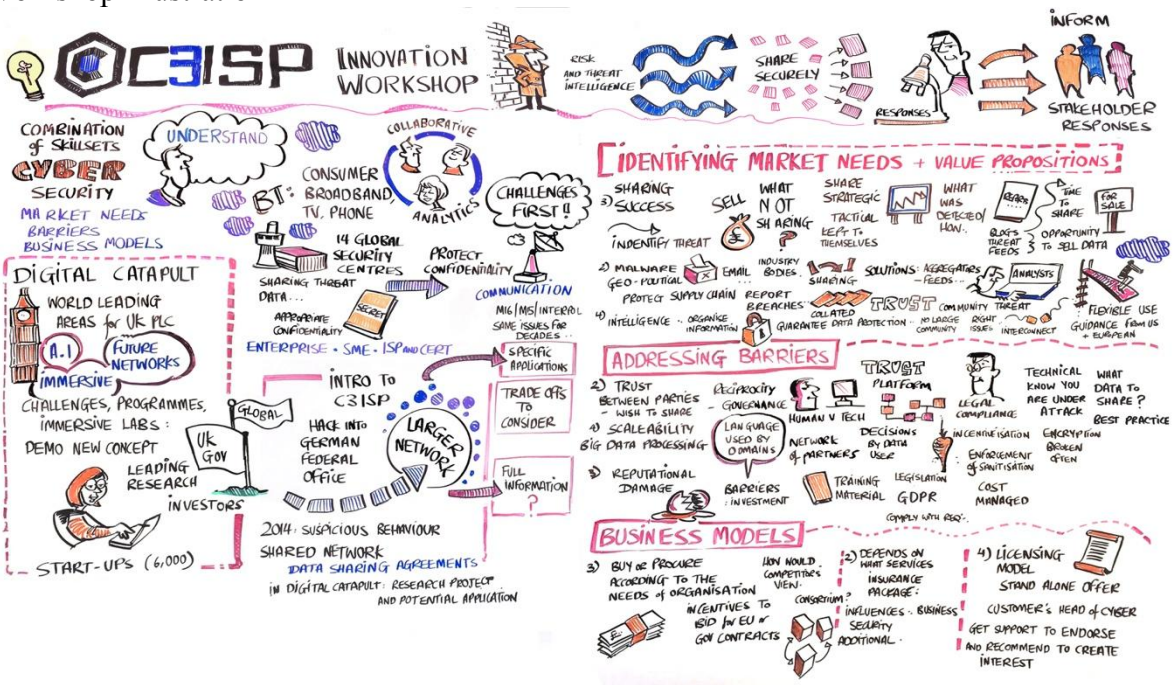
Digital Catapult digitalcatapultcentre.org.uk @DigiCatapult

Appendix G

Workshop rules of the road

Appendix H

Workshop Illustration



CATAPULT Digital

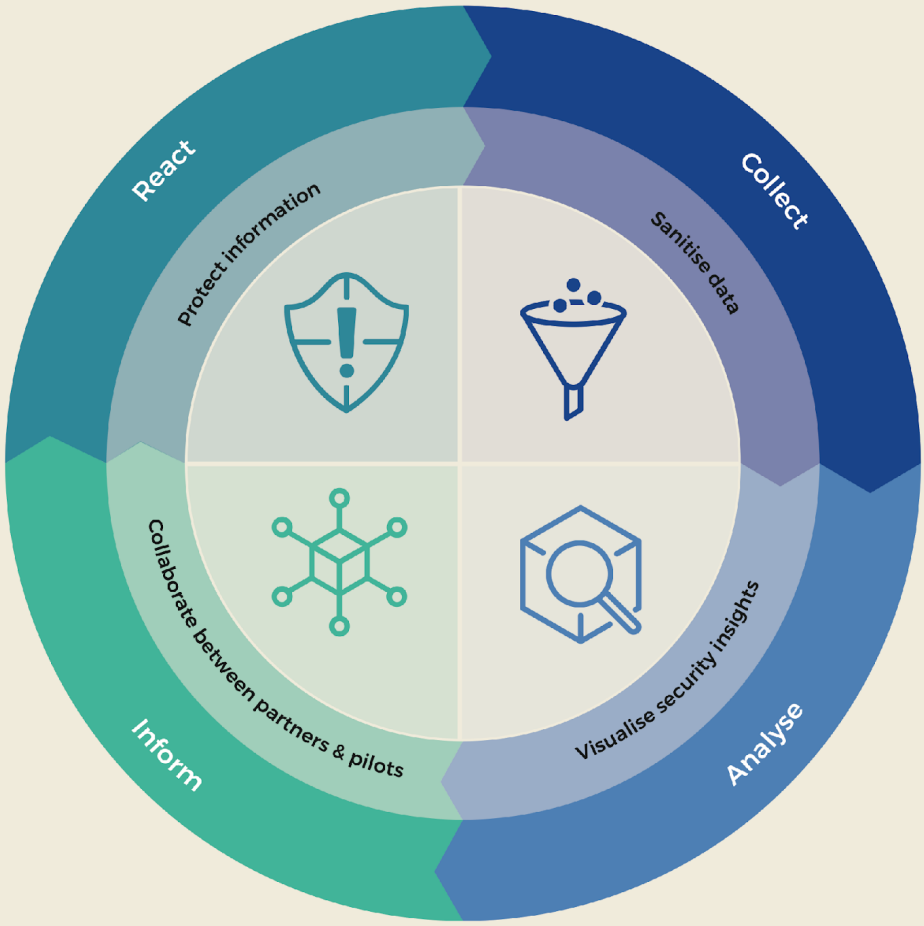
Appendix I

C3ISP Brochure

C3ISP
Collaborative and Confidential Information Sharing and Analysis for Cyber Protection

Find out more
www.c3isp.eu

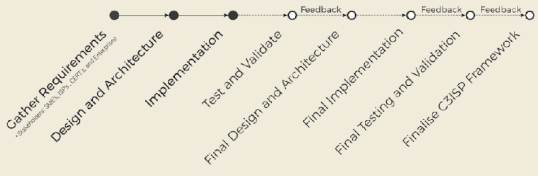
Cyber-Security Framework



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

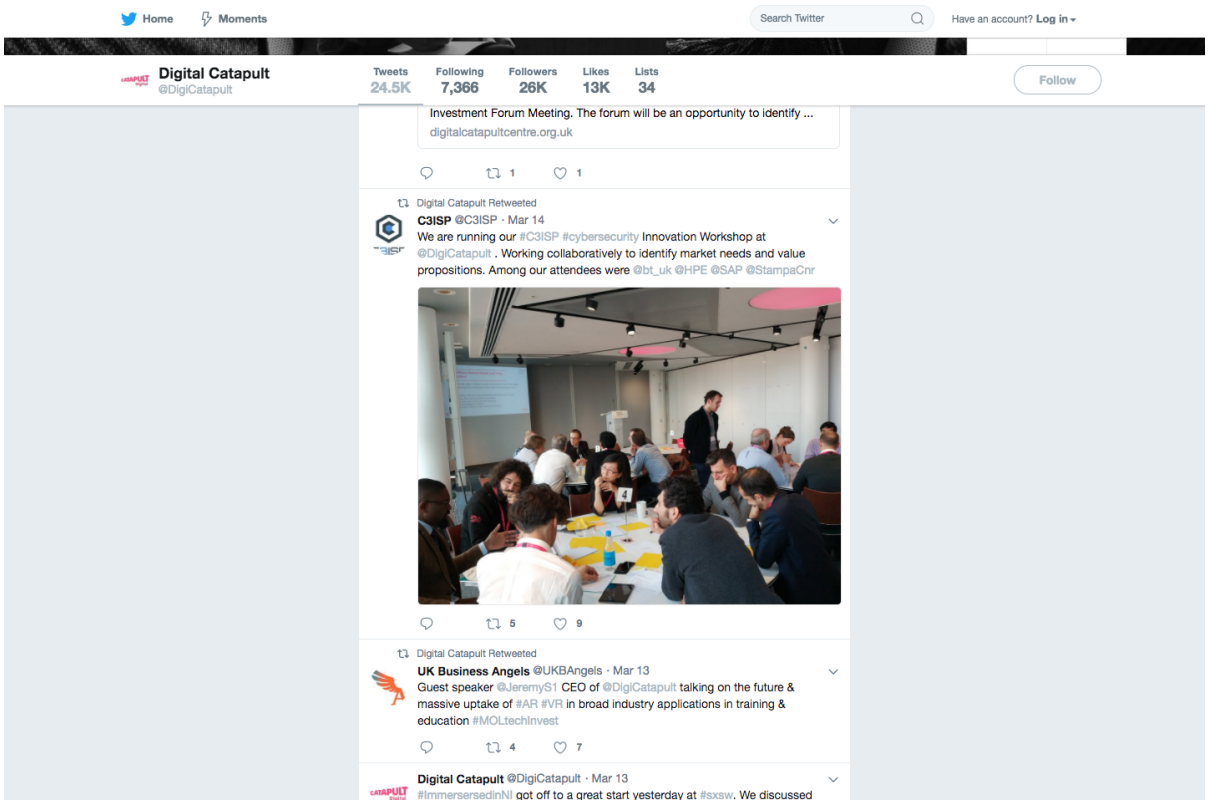


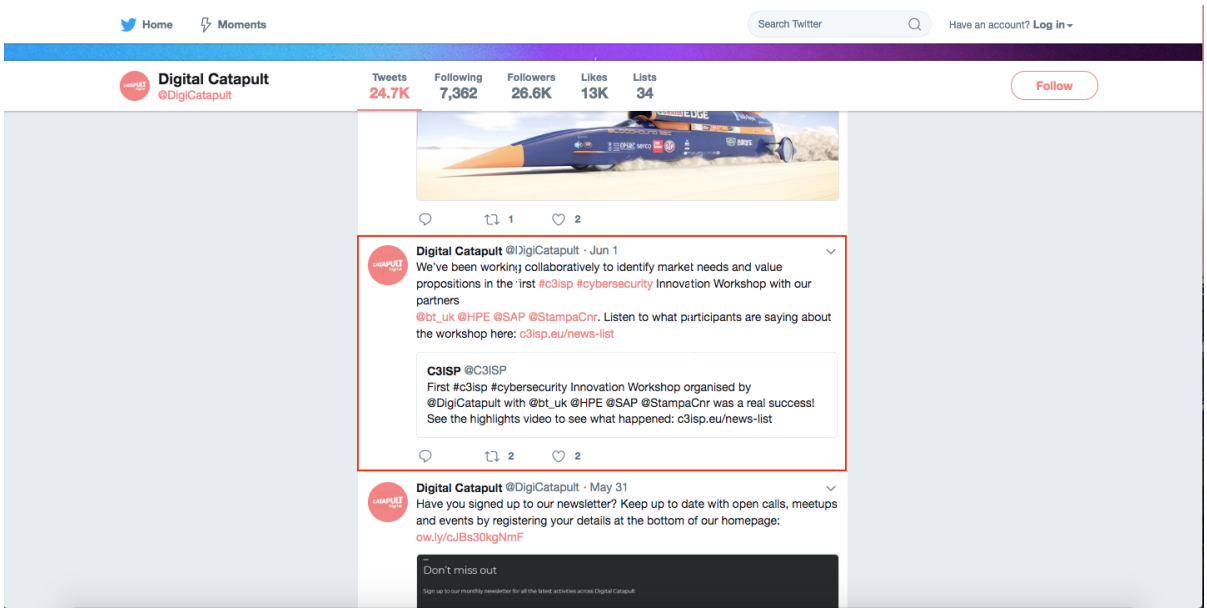
Consiglio Nazionale delle Ricerche · CERT Italia · Hewlett Packard Enterprise · BT · SAP · cea · CATAPULT Digital · University of Kent · GRIDPOCKET · CHINO.IO · 3D REPO

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 K
Workshop Tweets

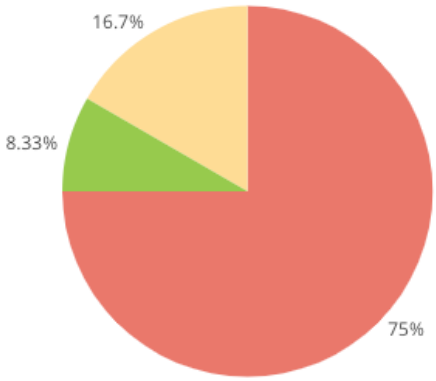




Appendix L

Feedback Form Results

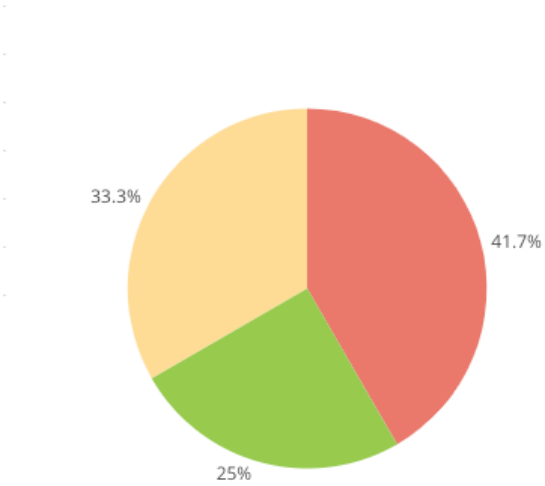
1. Overall, how would you rate your experience at the C3ISP Workshop?



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

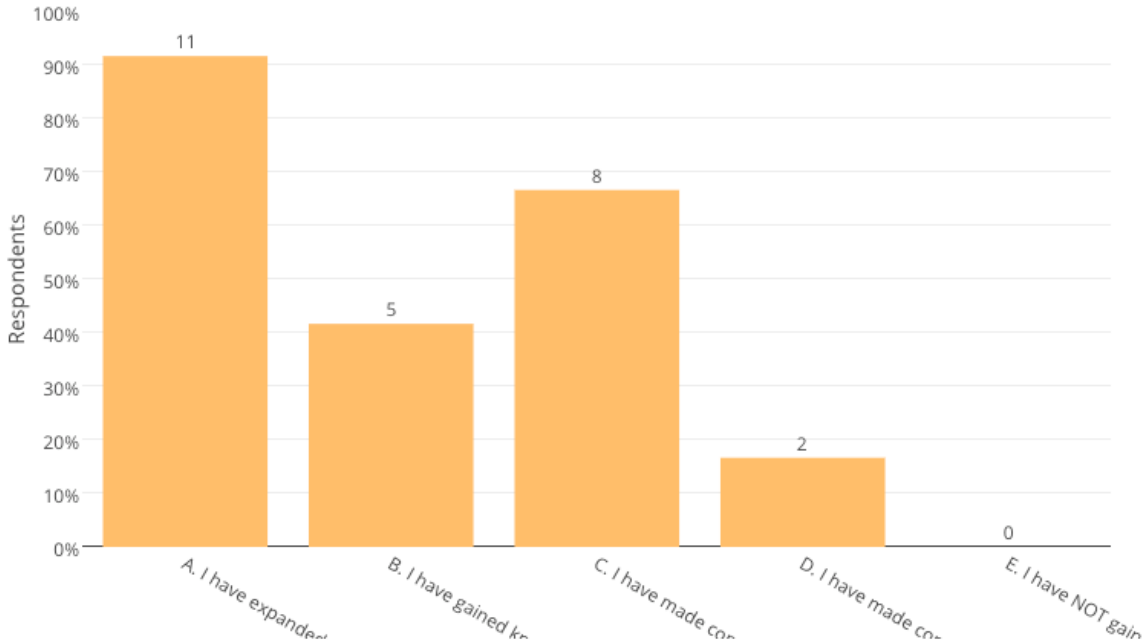
2.

**2. I attended... **

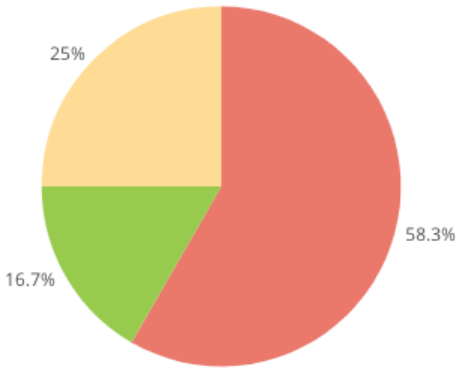


CHOICE	RESPONSES	PERCENTAGE
on behalf of a large organis...	5	41.7%
on behalf of C3ISP Consortium	4	33.3%
on behalf of an small or med...	3	25%
as an academic	0	0%
on behalf of Digital Catapult	0	0%

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

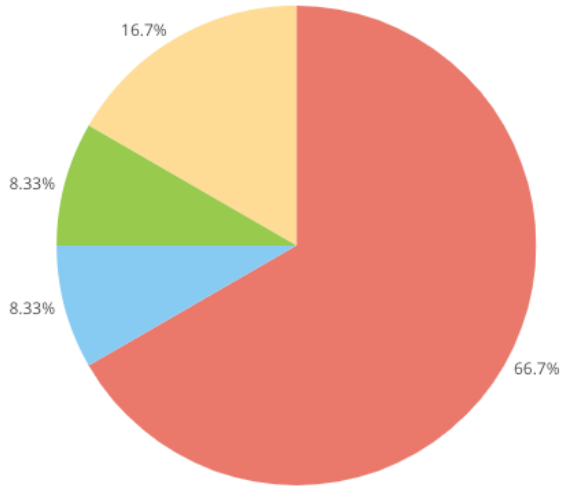


4. Which aspect of the Workshop is of most value for you overall?



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%