

C3ISP Innovation Workshop #2 Report: ***Exploitation Workshop***

Held at the National Research Council of Italy in Pisa on 11 October 2018, this was the second of a programme of three workshops and one engagement event. The 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 CR&D project.

The exploitation 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.

1. Preparation and planning for workshop #2

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

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

The preparation and planning included:

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

Several documents were developed to conduct and evaluate the workshop. These documents include (see Appendix):

- Workshop Agenda
- Table Plan
- Worksheets Handouts

2. Commercial Investigation Process

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

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

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

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

Further investigation has taken place at the Internet Festival 2018 in Pisa on October 12th.

See Appendix for the report on the interviews.

3. Objectives, Format and Content

Overall objective

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

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

Particular objectives

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

Format

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

Content and delivery

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

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

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

4. Outcomes

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

In particular, the discussion revealed the following:

Customer Characterisation

Through the first open discussion Digital Catapult wanted to understand the main differences between potential clients in the early market and the mainstream market, their needs and the

way we can address them. Every pilot group has defined early market and mainstream market characteristics.

A. Enterprise

- *Early Adopter Mindset:*
Companies working in military, law enforcement, smart cities and utilities sectors because they are technology leaders in their industries, they have budget allocated for innovative solutions and they tend to be employed in public services.
- *Mainstream Adopter Mindset:*
Companies in the banking, healthcare, shipping and transportation sectors that apply traditional business models and use legacy technology in their core business so they are more business oriented.

B. SME

- *Early Adopter Mindset:*
Early adopters need to gain more customers before taking advantage of C3ISP potential. Early adopters can encounter problems and don't necessarily have ready solutions to apply. Early adopters can pay on the usage to limit the use of resources.
- *Mainstream Adopter Mindset:*
Mainstream adopters rely on their markets and have guarantees in terms of customers. Mainstream adopters address problems with more experience but can also afford to use more resources.

C. CERT

- *Early Adopter Mindset:*
Companies like the Italian telecommunication since we already have 3 of them in the pilot and probably are going to be the first users of C3ISP. Also, CERT in Italy is a public organisation, part of economic development ministry which means easy reach to bank industry. Insurance companies could be early adopters as well.
- *Mainstream Adopter Mindset:*
The use of C3ISP will probably need to be forced for entities like public administrations, considering that they will need to be forced also to use specific security standards. Large manufacturing companies may become natural adopters in the future.

D. ISP

- *Early Adopter Mindset:*
Italian service providers and small companies without great security systems. ISPs companies that do security but not enough, ISPs that outsource all or part of security protections, ISPs that want to increase security for their partners and ISPs that want to protect confidentiality data, in compliance with GDPR..
- *Mainstream Adopter Mindset:*
Large ISPs as they already do similar things internally and they tend not to integrate anything to their internal systems.

Value Proposition

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

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

A. Enterprise

Customer: Company working in the military industry

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

- Solution to aggregate CTI of different origins with different disclosure profiles and analyse them effectively
- Pain relievers
 - Focused investigations on incidents involving assets
 - Focus on critical threats for critical assets (prioritisation)
 - Awareness of ongoing attacks
- Gain creators
 - Early detection may lead to a deterrent effect
 - Reputation gain to improved efficiency
 - Money and effort gain from better reactions to attacks

B. CERT

Customer: Not specified (Italian telecommunication)

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

C. SME

Customer: GPS Case

- Customer Jobs:
 - Software as a service monitoring utility energy consumption

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

D. Internet Service Provider (ISP)

Customer: Not specified

- Customer Jobs:
 - Vulnerability assessment
 - Data confidentiality
 - Discover new security issues, attacks
 - Looking at its customers
 - Providing security guarantees
 - Stable and robust systems against attacks
- Customer Pains:
 - Not quick enough
 - Loss of face and reputation
 - Malfunctioning
 - Financial
 - Difficulties in increasing user awareness
- Customer Gains:
 - Save effort

- Save money and time
- Increase of users
- Being more robust against attacks
- Increase reputation and credibility
- Being more reactive when vulnerabilities are found
- Better service provided
- Product and services:
 - Robust solutions
 - Adaptive solutions
 - Update regularly
 - Assurance of confidentiality and privacy preventions
 - Cutting edge innovation and solution
- Pain relievers
 - Providing more security, confidentiality and privacy in the treatment of customers' data
 - Provide securing solutions to customers in a unique and integrated way
 - Open source solutions
- Gain creators
 - Improve customers' reputation
 - Improve customers' compliance with respect to law
 - Save customers' money
 - Fully adaptive and integrated solution
 - Save money and time

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

5. Next steps

Pilot projects

- Implementation and testing phase 1 complete by October 2018.
- Implementation and testing phase 2 complete by October 2019.

Workshops

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

Dissemination and Communications

- An informative C3ISP brochure has been created to better brief and inform external stakeholders (see Appendix).
- Participation in Cyber Tech in Rome. The C3ISP Pilots were demonstrated in the Exhibition hall on a stand shared with two other Horizon 2020 projects, namely the Protective and Shield projects. Visitors to the stand were given the opportunity to see videos that described the C3ISP capability applied in the context of the various Pilots including the CERT Pilot, the Enterprise Pilot, the ISP Pilot and a video introducing the SME Portal. They were also shown videos that provided a clear visualization of the data analytic capabilities that could be provided on the C3ISP platform. Many of the visitors to the stand took the opportunity to have interactive one to one discussions with the C3ISP / Digital Catapult team as we talked them through the various Pilot scenarios and associated videos.
- Participation in the Internet Festival in Pisa. In this context the Pilot demonstrations exhibited at Cyber Tech in Rome were shown live by the Pilot owners in Pisa. As we did at Cyber Tech, Digital Catapult got audience interaction and participation with our C3ISP Pilot questionnaire which enabled us to achieve our goal of gathering a useful feedback on the C3ISP Pilots from our target audience.
- During the workshop, Digital Catapult has retweeted C3ISP tweets from C3ISP official Twitter page (see Appendix) 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.

Appendix

Appendix A

List of Attending Companies

List of Attendees

BT

HPE

SAP

Digital Catapult

National Research Council

3d Repo

GridPocket

CEA

University of Kent

Chino

ISCOM-MISE

Appendix B

Workshop 1 Agenda

CATAPULT Digital Agenda		C3ISP
14:00	Refresher from the previous workshop	
14:15	Workshop 1: Early Adopter Identification	
15:15	Break	
15:30	Workshop 2: Value Proposition	
16:45	Summary of the workshop and next steps	
17:00	Close	

Appendix C

Workshop 1 Table Plan

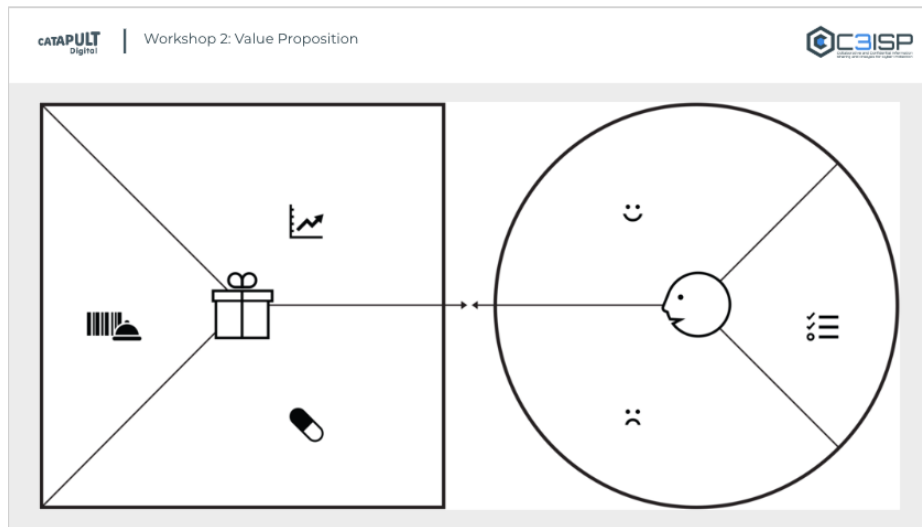
CATAPULT Digital Table Settings		C3ISP	
Table 1: SME Pilot	Table 2: ISP Pilot	Table 3: Enterprise Pilot	Table 4: CERT Pilot

Appendix D


F.1. Worksheet 1: Customer Characterisation

CATAPULT Digital Workshop 1: Customer Characterisation		C3ISP	
CYBERSECURITY INDUSTRY			
EARLY ADOPTER MINDSET		MAINSTREAM ADOPTER MINDSET	

F.2. Worksheet 2: Value Proposition

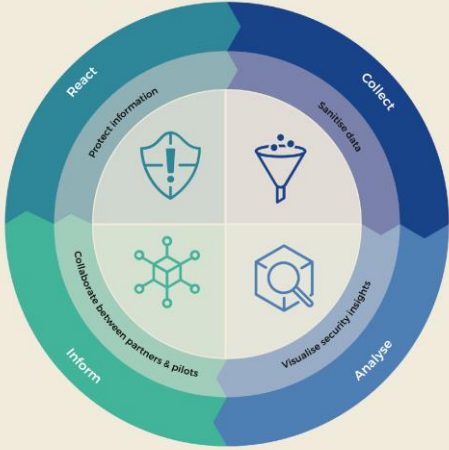


Appendix E C3ISP Brochure



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: 1603100-130

Design process for the pilots





The C3ISP Project is supported by funding under the Horizon 2020 Research Program of the European Commission (641014-01-01-0001)

Appendix F

Workshop, showcasing and investigation process Tweets

 **C3ISP** @C3ISP · Oct 11

Second #c3isp #cybersecurity Innovation Workshop organised by @DigiCatapult with @bt_uk @HPE @SAP @CNR, #Chino.io, #3DRepo, #GPR, #CEA was a success! Follow the latest #C3ISP at c3isp.eu



  1  1 

 **C3ISP** @C3ISP · Oct 11

We are running our #C3ISP #cybersecurity Innovation Workshop at @CNR. Working collaboratively to validate market needs and value propositions. Among our attendees are @bt_uk @HPE @SAP @CNR, #Chino.io, #3DRepo, #GPR, #CEA

   2 



C3ISP @C3ISP · Oct 12

#H2020 #CyberSecurity team #C3ISP, concludes a successful #Internet #Festival. Take a glance of the @C3ISP demos presented at the internetfestival.it here: c3isp.eu/content/pilot-...



1



C3ISP @C3ISP · Sep 27

2nd day at the #CybertechEurope18 and the #C3ISP team is demoing the #SME, #Enterprise, #CERT & #ISP pilots! Visit our stand @ the #CybertechEurope18



2



C3ISP @C3ISP · Sep 26

Getting ready for the CyberTech conference in Rome! Visit the [#C3ISP](#) [#SHIELD](#) [#PROTECTIVE](#) stand and find out more about the latest developments in [#CyberSecurity](#)



1 4 7

Appendix G

Interview Questionnaire

C3ISP PILOT - Interview Questions



Please enter the name of your organisation:

Please enter your email address (optional):

Please enter your job title (optional):

1. Which type of organization do you represent?

- a. SME
- b. Enterprise / Corporate
- c. ISP
- d. Government Agency
- e. CERT
- f. University / Research
- g. Individual
- h. MSSP (Managed Security Services Provider)

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

- a. The C3ISP SME Pilot
- b. The C3ISP Enterprise Pilot
- c. The C3ISP ISP Pilot
- d. The C3ISP CERT Pilot

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

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

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

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

C3ISP PILOT - Interview Questions - Continued



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

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

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

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

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

12. What form of C3ISP procurement model would your organisation find most attractive?
 - a. One off (ready to use)
 - b. Security as a service
 - c. Fixed monthly / Annual license
 - d. Variable license cost depending on number of C3ISP collaborating companies
 - e. Variable license cost depending on volume of CTI data shared
 - f. Other

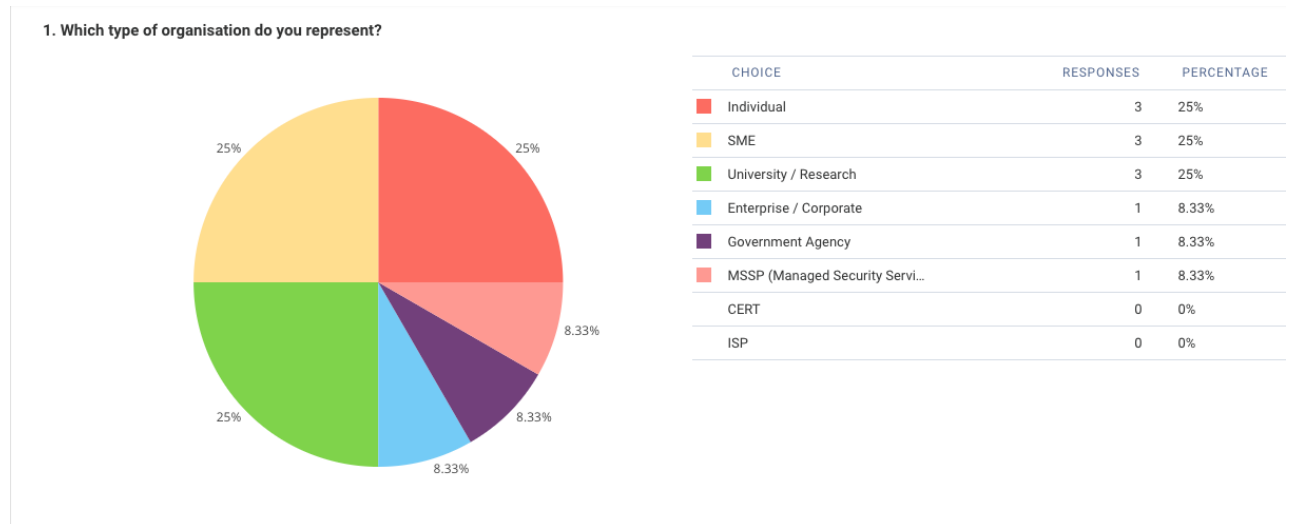
13. What European cyber security events do you normally attend?

Thank you for completing this questionnaire

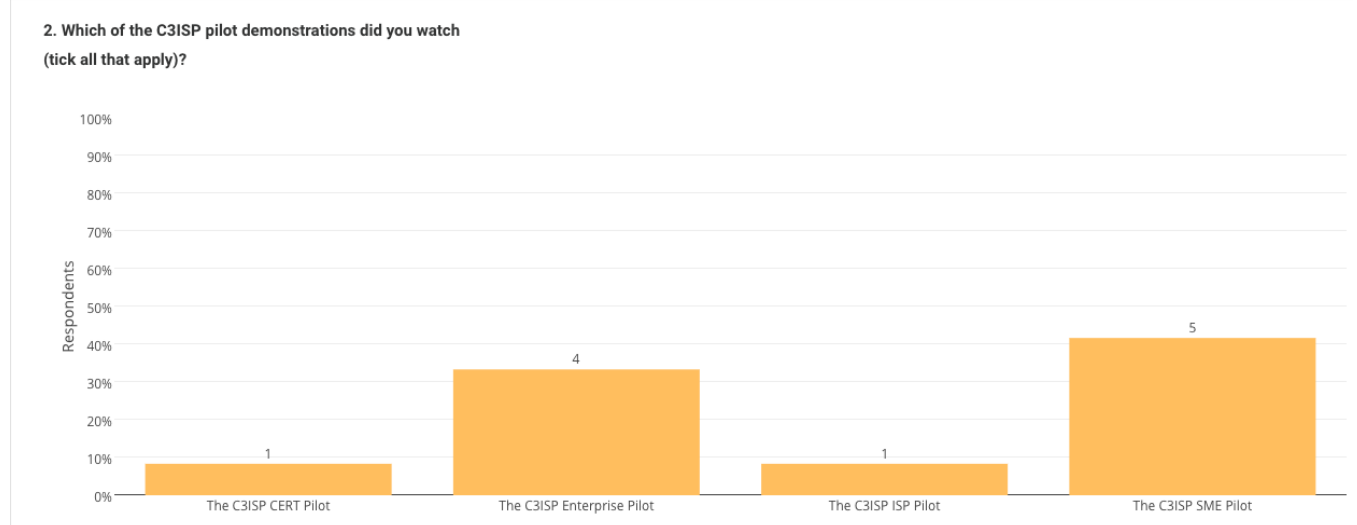
Appendix H

Investigation Report

1. Which type of organisation do you represent?



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



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

- *Type: University/Research*
Personal data, nominative data, sensitive personal identifying information (PII).
- *Type: Government Agency*
NA

- *Type: SME*
Mainly employees data.
Customers data.
- *Type: Enterprise/Corporate*
Yes.
- *Type: MSSP (Managed Security Services Provider)*
Internal network information from customers. Customers' security incidents..

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

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

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

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

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

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

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

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

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

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

- *Type: MSSP (Managed Security Services Provider)*
Being able to jointly analyse and view information from multiple customers.

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

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

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

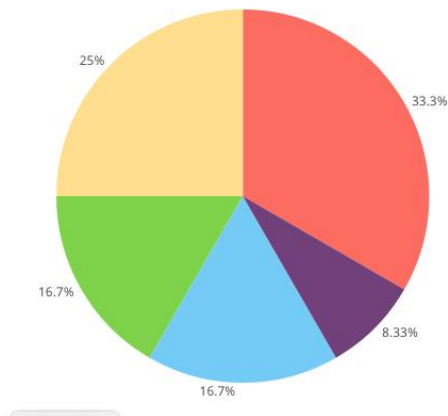
- *Type: Research/University*
Learning and training for employees.
Fundings, government infrastructure.
- *Type: Government Agency*
NA
- *Type: SME*
Additional workload for IT/Security people (severely understaffed). Give awareness of benefits to the management.
There aren't particular barriers at the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

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

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

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

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



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