Collaborative and Confidential Information Sharing and Analysis for Cyber Protection

C3ISP Exploitation Workshop 3 Report

Summary of results and impact on exploitation plan

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

Report Date: 21 May 2019

Activity: 02 April 2019 at CNR, Pisa

Introduction

Held at CNR in Pisa on 2nd April 2019, this was the third 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.

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

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

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

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

In summary

Digital Catapult conducted this workshop in two parts.

The first part of the workshop drew out the positive and negative impacts of various proprietary and open source approaches. Considering both extreme cases (totally open source, totally proprietary) and stepped approaches, with some elements proprietary and others open source.

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

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

Part 1 of the workshop

Key outcomes from part one point toward a more open source over proprietary approach however the hybrid approach (which allowed for a baseline open source platform with proprietary services) also fared well in the assessment.

We have summarised the outcome of the workshop below, the rationalised scores only give limited insight into the potential impact of one selection over another, as it does not interpret the scale of one benefit vs another. If you were to select a scenario which could offer the biggest benefit (regardless of negative impacts) you could argue that a fully proprietary platform would be the winner over the open source approach for exampe.

Therefore to offer greater clarity we have looked into the pros and cons with the heaviest weightings in order to best interpret the results.

Scenario	Pro	Cons	Rationalised score
A: Proprietary platform with free to access services	21	21	0
B: Open core platform with proprietary services	20	18	+2
C: Total proprietary	16	16	0
D: Total open source	18	15	+3

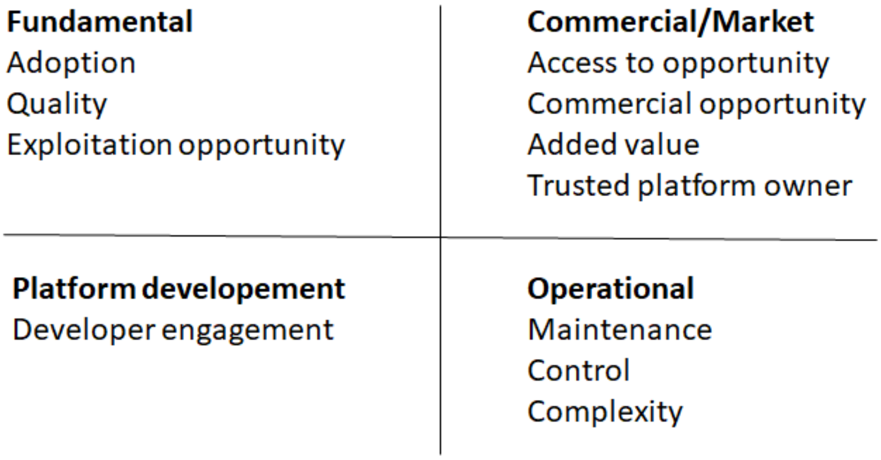
The key considerations (both pros and cons) of the consortium, those scoring the top weighting of 5, are summarised by the list of terms below:

- Access to opportunity
- Adoption
- Trusted platform owner
- Exploitation opportunity
- Developer engagement
- Commercial opportunity
- Added value
- Maintenance
- Complexity
- Control
- Quality

We have selected headings to group these phrases based on undisputable impact areas on an exploitation strategy:

Fundamental EU project objectives: Considerations which impact the way the C3ISP project is perceived by its funders
Operational Effectiveness: Considerations relating to how the C3ISP organisation would need to operate

Platform development: Considerations which are related to how a developer base can be utilised to the benefit of the organization managing the platform and/or services
Commercial and market attractiveness: How will the platform and services be sustained effectively from a commercial standpoint



Fundamental	**Commercial/Market**
Adoption	Access to opportunity
Quality	Commercial opportunity
Exploitation opportunity	Added value
	Trusted platform owner
Platform developement	**Operational**
Developer engagement	Maintenance
	Control
	Complexity

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

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

Note on security
Underpinning discussions was the need for the platform to be trusted and secure to drive adoption in a meaningful way. Particularly the need for both technical security, organisational trust and socio-techical security issues which would need to be priorotised for this to be remotely acknowledged by the community we seek to serve. Security can be achieved in both an open source and protected environment and through the detailed notes on the topics below we have gained a deeper understanding of how this could be best realised for the C3ISP solution.

Fundamental EU project objectives
Adoption: Adoption was discussed as one of the most crucial areas for success, as to some extent the success of a threat sharing platform requires a reasonably large number of threats being collected from multiple sources. However the diversity of these sources is less of a concern. The consortium discussed both the need for broad adoption but suggested success could be found through industry specific focus.

Barriers to Adoption: Pay-walls preventing widespread access was also highlighted as a key issue regarding proprietary approaches..

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

Exploitation Opportunity: Incentives broadly were discussed however clear exploitation opportunities for contributing organisations, either internal or external to the consortium was seen as a fundamental need, as without a clear benefit to adoption of the platform the platform would struggle to gain attention. It was also highlighted as a concern around the impact of organisational control and contributors would need to be confident that any controlling organisation would not make any changes that could adversely impact exploitation opportunities.

Impact of Fundamental section on exploitation plan
When considering these three fundamental concerns the conclusions to test would be:

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

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

Impact of the Platform Development section on the exploitation plan

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

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

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

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

Trusted Platform Owner: Inherent to both the adoption of the platform and the willingness to invest in developing on the platform or deploying the platform, ensuring the market has full belief in the platform owner will be essential to success regardless of the open source vs proprietary nature. However should any of the platform be protected it will be the organisation controlling the protected element that would need to engender trust in their practices most. Trust here equates to Trust in the Security of the service being provided both at the platform IT level and in terms of any personnel and process security if provided as a service offering. This in turn will need to be evidenced by appropriate certifications.

Impact of commercial and market attractiveness on the exploitation plan:

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

Operational effectiveness

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

Control: Highlighted in the mixed groups there was a foreseen challenge in ensuring that any open components could not be modified to negatively impact the proprietary components. Control was an underlying theme as too much control was seen as a negative impact regarding commercial endeavours and lack of control was acknowledged as a fundamental result of open source applications. If providing a service then control over the platform being used to provide the service is key to ensuring the integrity and quality of those services.

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

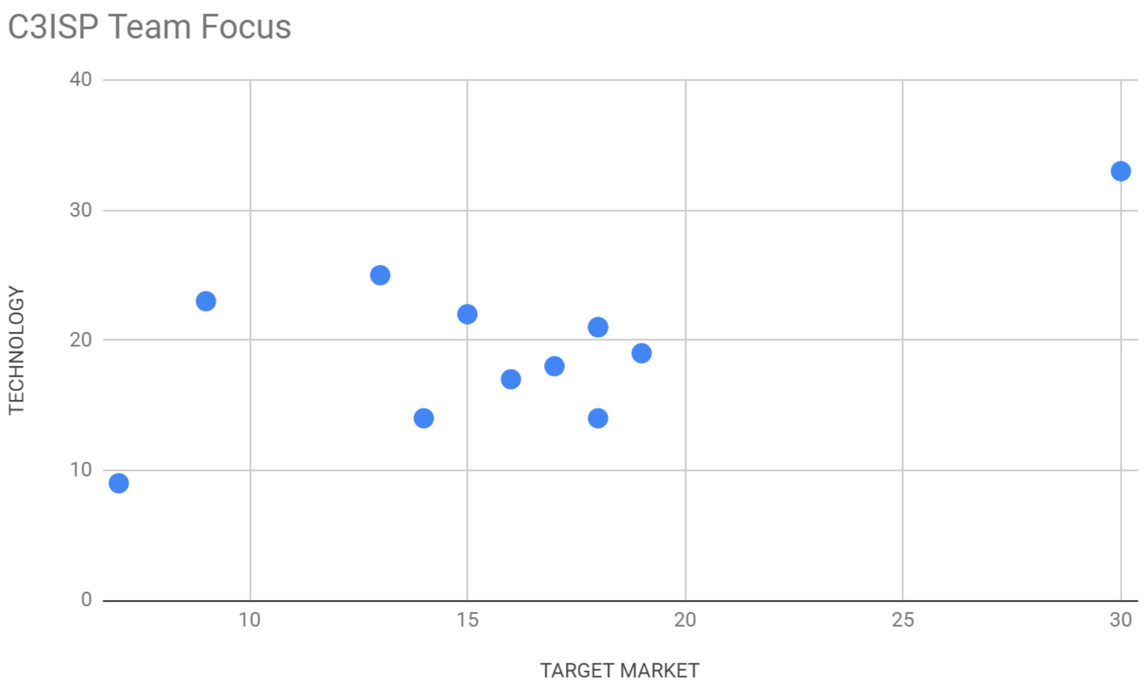
Impact of operational effectiveness on the exploitation plan:

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

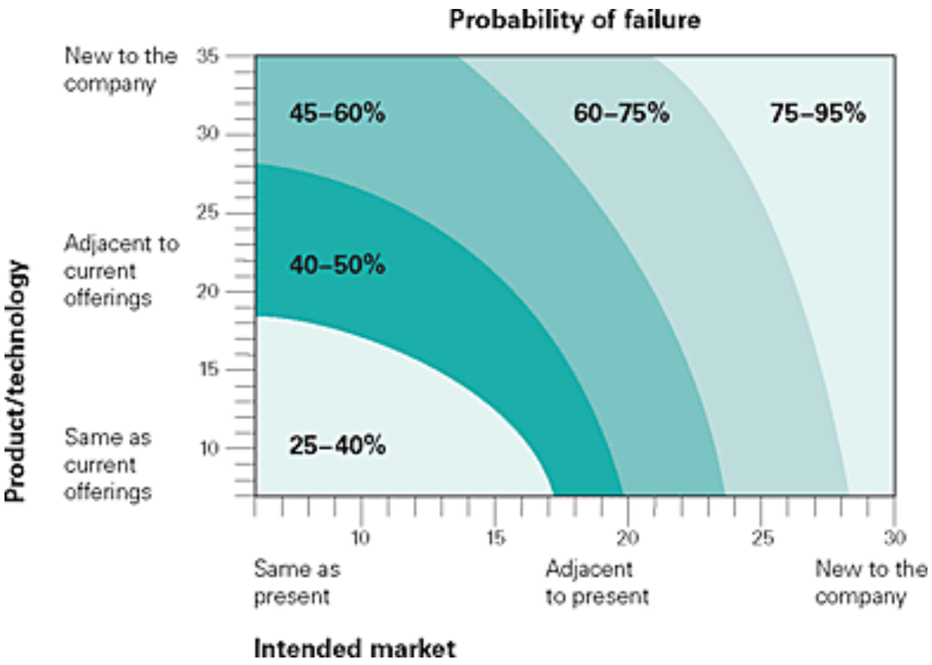
Part 2

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

The outcome is summarised by this chart:



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



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

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

Technology:

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

Market:

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

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

Impact on the exploitation plan

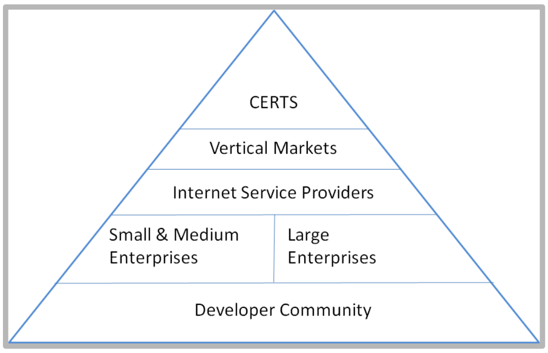
- We will first identify key target market verticals and then look to align with the companies in the consortium which have the most brand equity in that vertical to begin to make traction with a potential customer base
- We will focus in on consortium members with commercial exploitation ambitions to understand how the functionality employed within the solution can best be managed to enable us to reach the highest number of early adopters
- We will look to run activities which engage a customer and user base across all consortium members as this is a key strength across the organisations in response

In conclusion

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

The Key conclusion points are:

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



ANNEX

Full results from workshop 1

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

*Facilitator notes on final score from team working on Scenario A
- the discussions focussed on trust and started from opposite assumptions: paying to be a means to fuel a community VS paying as hurdle to community growth, revenue stream beneficial to run services with added value VS trust in the way services are run
- choosing this option would address the main cons with a convincing approach, better would be to focus on delivering the pros in the way they are formulated. Addressing correctly the cons would automatically end up in fulfilling the pros, leading to a convincing offering.

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

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

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

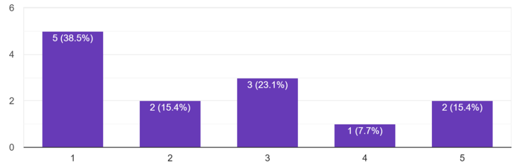
PROS	GROUP	SCORE		CONS	GROUP	SCORE
REVENUE GENERATION	C	1		QUALITY OF OPEN SOURCE	B	1
COLLABORATION	D	3		LICENSE	D	1
QUALITY CONTROL	C	3		COST OF MARKETING	C	2
ENGAGEMENT	B	3		RETURN ON INVESTMENT.1	D	2
TRANSPARENCY	D	3		MONITORING	A	3
OVERHEAD	A	3		COMPLEXITY.2	B	3
ENGAGEMENT	B	3		FORESSEN BENEFITS	C	3
IMPLEMENTATION	C	3		PACE OF DEVELOPMENT	C	3
ADAPTION	D	3		RETURN ON INVESTMENT.2	D	3
COMPETITION	A	4		COMMUNITY	A	4
AVOIDS LOCK-IN	B	4		ADDED VALUE.2	A	4
COMPLEXITY	C	4		EXPLOITATION	B	4
DEPENDENCE	A	4		BARRIER TO ENTRY	C	4
CONSORTIUM SKILLS	D	4		EFFECTIVENESS	C	4
ACCESS TO OPPORTUNITY	B	5		VULNERABILITY	D	4
ADOPTION	A	5		ADDED VALUE.1	A	5
TRUST PLATFORM OWNER	A	5		MAINTENANCE	A	5
EXPLOITATION	C	5		COMPLEXITY.1	B	5
DEVELOPER ENGAGEMENT	D	5		CONTROL	B	5
COMMERCIAL	B	5		QUALITY	D	5

ANNEX

Aggregate results from workshop 2

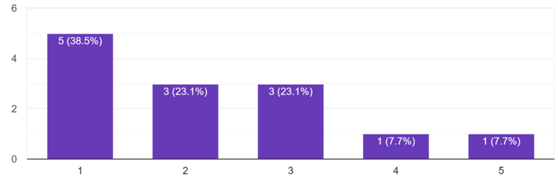
Our current development capability is...

13 responses



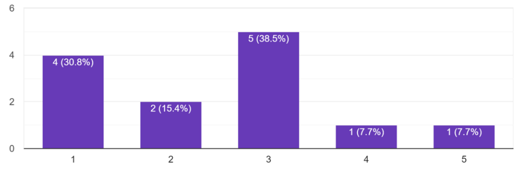
Our technology competency is...

13 responses



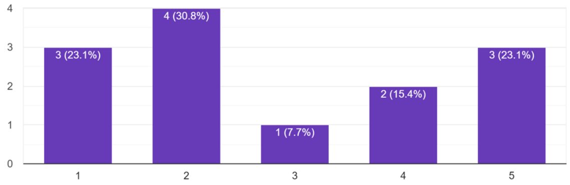
Our data management service is...

13 responses



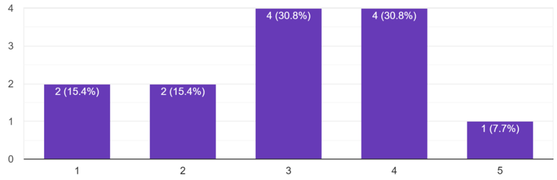
The expected quality standards in delivery are...

13 responses



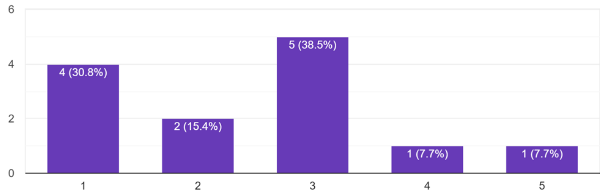
The required knowledge and science base are...

13 responses



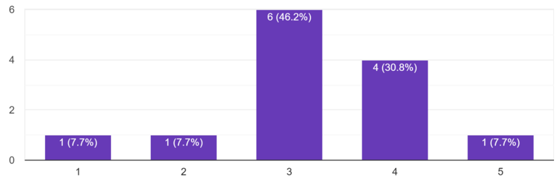
Our digital service delivery system is...

13 responses



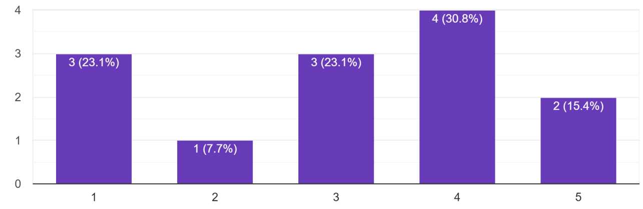
The necessary product and service functions are...

13 responses



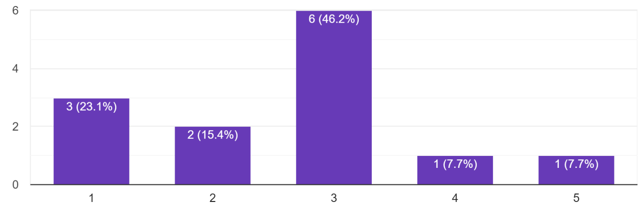
The competitive set (make up of existing or potential competitors) will...

13 responses



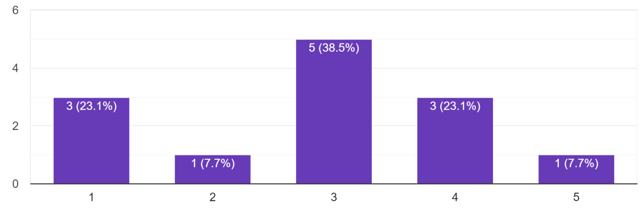
Customer behaviour and decision making processes will...

13 responses



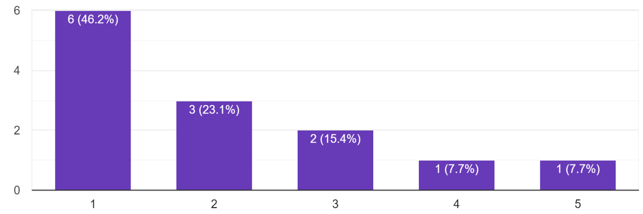
Our distribution and sales activities will...

13 responses



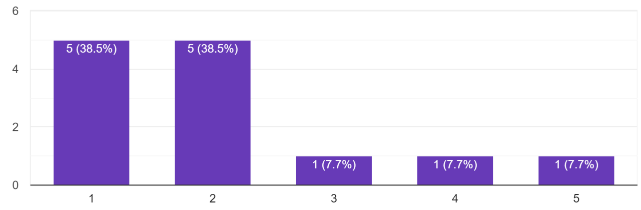
Our brand promise is...

13 responses



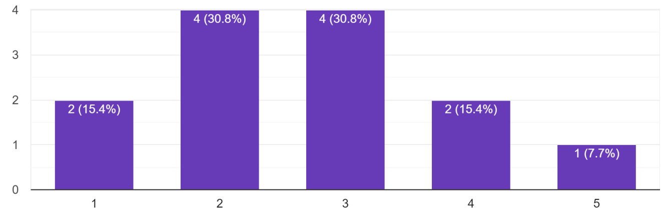
Our current customer relationships are...

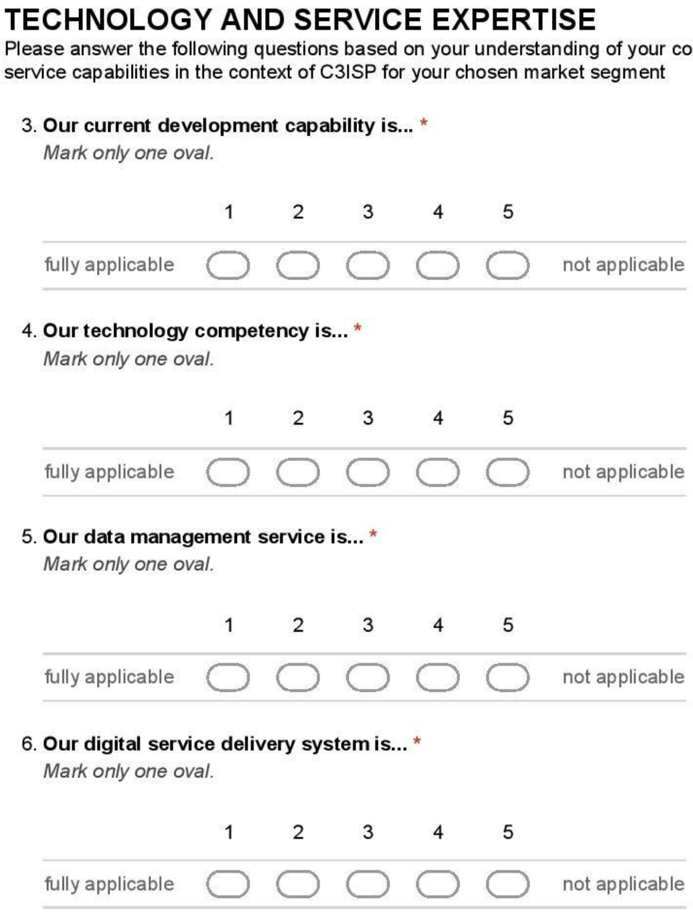
13 responses



Our knowledge of competitors' behaviour and intentions is

13 responses





TECHNOLOGY AND SERVICE EXPERTISE

Please answer the following questions based on your understanding of your companies technical and service capabilities in the context of C3ISP for your chosen market segment

3. **Our current development capability is...** *

Mark only one oval.

	1	2	3	4	5	
fully applicable	○	○	○	○	○	not applicable

4. **Our technology competency is...** *

Mark only one oval.

	1	2	3	4	5	
fully applicable	○	○	○	○	○	not applicable

5. **Our data management service is...** *

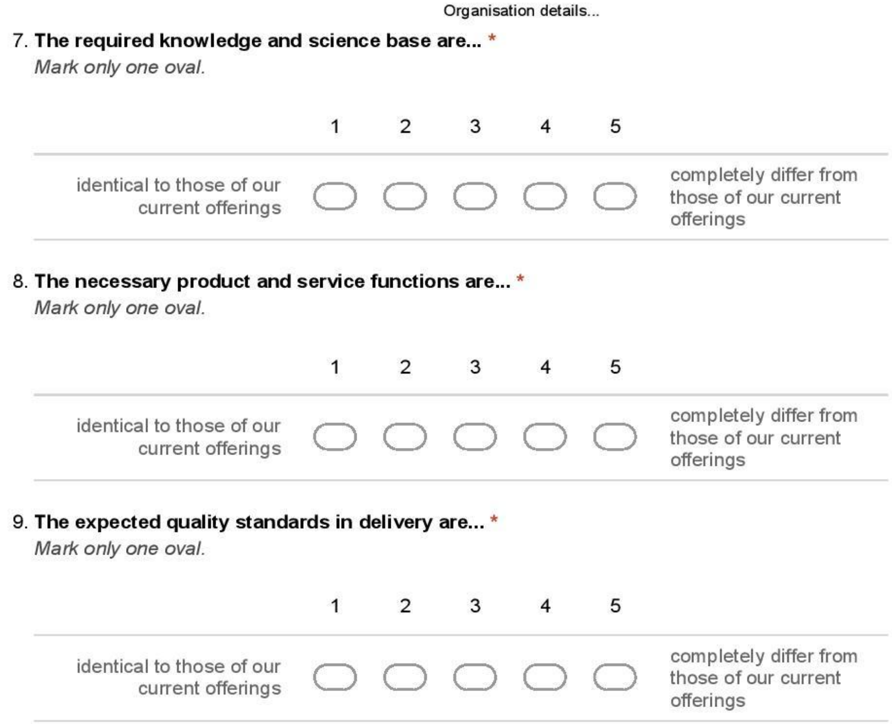
Mark only one oval.

	1	2	3	4	5	
fully applicable	○	○	○	○	○	not applicable

6. **Our digital service delivery system is...** *

Mark only one oval.

	1	2	3	4	5	
fully applicable	○	○	○	○	○	not applicable



Organisation details...

7. **The required knowledge and science base are...** *

Mark only one oval.

	1	2	3	4	5	
identical to those of our current offerings	○	○	○	○	○	completely differ from those of our current offerings

8. **The necessary product and service functions are...** *

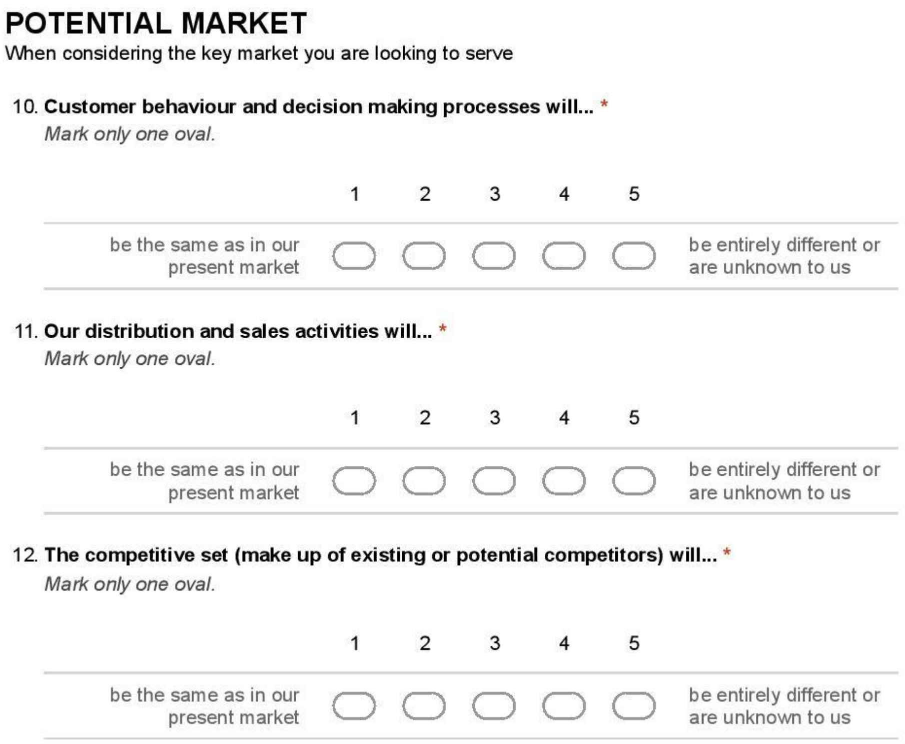
Mark only one oval.

	1	2	3	4	5	
identical to those of our current offerings	○	○	○	○	○	completely differ from those of our current offerings

9. **The expected quality standards in delivery are...** *

Mark only one oval.

	1	2	3	4	5	
identical to those of our current offerings	○	○	○	○	○	completely differ from those of our current offerings



POTENTIAL MARKET

When considering the key market you are looking to serve

10. **Customer behaviour and decision making processes will...** *

Mark only one oval.

	1	2	3	4	5	
be the same as in our present market	○	○	○	○	○	be entirely different or are unknown to us

11. **Our distribution and sales activities will...** *

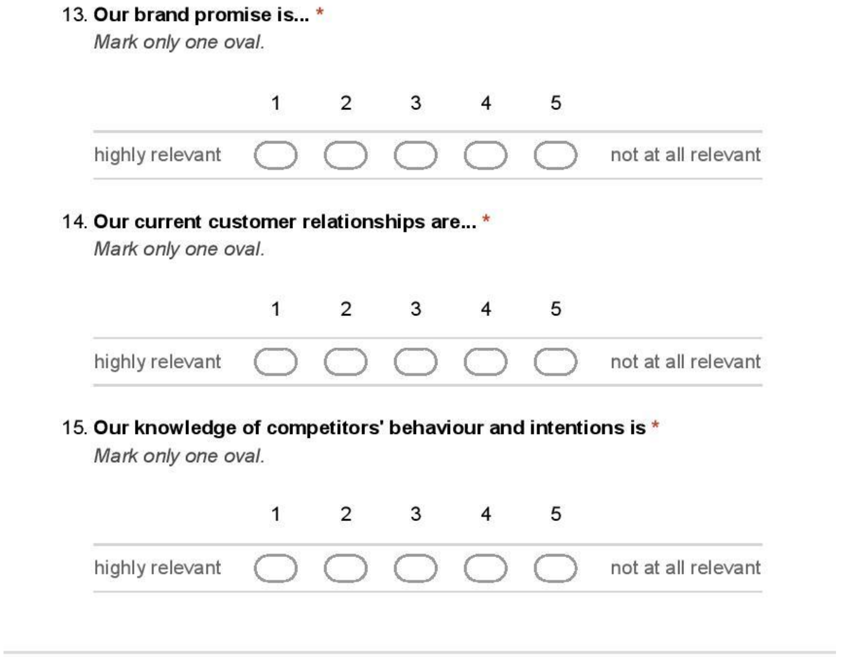
Mark only one oval.

	1	2	3	4	5	
be the same as in our present market	○	○	○	○	○	be entirely different or are unknown to us

12. **The competitive set (make up of existing or potential competitors) will...** *

Mark only one oval.

	1	2	3	4	5	
be the same as in our present market	○	○	○	○	○	be entirely different or are unknown to us



13. **Our brand promise is...** *

Mark only one oval.

	1	2	3	4	5	
highly relevant	○	○	○	○	○	not at all relevant

14. **Our current customer relationships are...** *

Mark only one oval.

	1	2	3	4	5	
highly relevant	○	○	○	○	○	not at all relevant

15. **Our knowledge of competitors' behaviour and intentions is** *

Mark only one oval.

	1	2	3	4	5	
highly relevant	○	○	○	○	○	not at all relevant