D9.2

First Exploitation and Dissemination Report

WP9 – Exploitation, Dissemination, Communication and Standardization

C3ISP

Collaborative and Confidential Information Sharing and Analysis for Cyber Protection

Due date of deliverable: 30/09/2017
Actual submission date: 30/09/2017

30/09/2017
Version 1.0

Responsible partner: HPE
Editor:I.Koparanova
E-mail address:iva.koparanova@hpe.com

Project co-funded by the European Commission within the Horizon 2020 Framework Programme		
Dissemination Level		
PU	Public	**X**
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. Koparanova (HPE), C. Wright (Digicat), G. Costantino (CNR), F. Di Cebro (SAP), I.Matteucci (CNR), A. Saracino (CNR)

Approved by: C. Wong (3D REPO), A. Saracino (CNR)

Revision History

Version	Date	Name	Partner	Sections Affected / Comments
0.1	30.08.3017	I. Koparanova	HPE	Initial draft of ToC
0.2	05.09.2017	I. Koparanova	HPE	Initial draft of plan for partner inputs and review
0.3	19.09.2017	I. Koparanova	HPE	Adding further details from partners
0.4	19.09.2017	C.Wright	DigiCat	Update on the exploitation results
0.5	19.09.2017	I. Koparanova	HPE	Update on the research and IP state-of-the-art
0.6	20.09.2017	G. Costantino	CNR	Update on the ISP Pilot
0.7	25.09.2017	F. Di Cerbo	SAP	Update on the Enterprise Pilot
0.8	25.09.2017	A. Saracino	CNR	Update on the CERT Pilot
0.9	25.09.2017	I. Koparanova	HPE	Further update on the provided contributions. Ready for internal review
1.0	29.09.2017	I. Koparanova	HPE	Update after the review. Final version

Executive Summary

This is the first exploitation and dissemination report for the C3ISP project.

The exploitation and innovation section covers mission statement and business models, exploitation approach and business network, individual exploitation results and research and IP state of the art, IP protection, sustainability and assessments of the added value of the C3ISP project.

The standardization includes contribution to and liaison with standardisation bodies.

The dissemination and communications describe the communication activities, publications, events' schedule and event participation.

This document reviews progress against D9.1 and provides input into deliverables D9.3 and D9.4, which report on the exploitation and dissemination throughout the project.

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), which are machine readable 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.

1.2. Business model

For the set of priority business scenarios, we will develop detailed business models, including strategy for investment and outline roadmaps.

As these business models are refined, it may be possible to identify clusters of characteristics, which will allow of the development of core C3ISP technologies or components.

1) ISP: up-to date monitoring infrastructure will be offered by Regitro.it to all the Italian registrars in order to monitor their Internet ServersEnterprise: The Enterprise Pilot focuses primarily on the interactions among a Managed Security Service Provider (MSSP) and its customers. The business value brought by C3ISP to a MSSP is in the capability to analyse collaboratively cyber threat information that are integrated within each MSSP's operation to enable improved intelligence to be extracted from the aggregated data belonging to the customer enterprises without allowing sensitive data to leak to other enterprises or external parties.

   The primary business model in this scenario is for an MSSP or its platform supplier to integrate the C3ISP components (IAI, ISI and DSA Manager) to create an enhanced version of its cybersecurity platform. Business benefits of this include:

   - increased quality of threat intelligence available to all customers, providing competitive advantage over other MSSPs;
   - opportunity to offer added value/reduced price options tailored to customers' needs and dependent on the terms of their data sharing agreements;
   - reductions in operational costs where the C3ISP technologies allow consolidation of multiple customer-specific platform instances into a single multi-tenanted platform instance.

   This model fits well with the strategy of BT's cybersecurity business.

4) up-to-date ICT attack prevention based on discovered vulnerabilities and attacks which have been discovered on other SMEs' systems.

1.2.1. Exploitation Board

We've started setting-up the Exploitation Board as detailed in D9.1 with selecting the potential board members.

The first face-to-face Exploitation Board meeting is proposed for Q1 2018. The Coordinator will write the minutes of the Exploitation Board meetings, and prepare the implementation of the Exploitation Board's suggestions.

1.2.2. [DRAFT] Email to Exploitation Board Members

Here, we show the DRAFT text of an email to Nominated Exploitation Board Members to be sent as an invitation as described in D9.1.

From: Cherlaine Wright [Cherlaine.Wright@digicatapult.org.uk]
Sent: <date>
To: <name>
Subject: Exploitation Board: C3ISP project

Dear <name>,

I hope you're well.

I'm Cherlaine Wright, the Project Manager for C3ISP here at the Digital Catapult. It's great news that you're able to partake in the Exploitation Board and we are delighted to have your support.

Attached you will find an Invitation and agreement to join the Exploitation Board of the C3ISP Project. Within you will see details of various activities you could be asked to support, but as Kathryn has rightly confirmed all are subject to mutual agreement and availability.

Please can you populate the highlighted fields, scan and return to me at your earliest convenience.

If you have any questions, please don't hesitate to ask.

I look forward to meeting with you in the future

Best Regards,

Cherlaine

Project Manager

M: +44 (0)7796 950995

Digital Catapult Centre | 101 Euston Road | London | NW1 2RA

www.digitalcatapultcentre.org.uk

@DigiCatapult - LinkedIn

1.2.3. [DRAFT] Exploitation Board Agreement

Figure 1 shows the DRAFT text of the Exploitation Board Agreement to be sent to the selected Exploitation Board members as an agreement as described in D9.1.

European Commission | Horizon 2020 European Union funding for Research & Innovation

CATAPULT Digital

C3ISP 700294

For the attention of:
Cherlaine Wright |Project Coordinator
Digital Catapult Centre | 101 Euston Road | London | NW1 2RA

Reference: Invitation and agreement to join the Exploitation Board of the C3ISP Project

Dear Cherlaine,

Thank you for your invitation to join the Exploitation Board of the H2020 C3ISP project.

I understand the main objective of the 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 project is 36 months in duration, and is scheduled to finish in December 2019.

This letter is to confirm that I, [xxxxx], in my current position as [xxx] at [name of the organization xxxxxxx], am willing to contribute to the project as a member of a Exploitation Board.

Against this background I am ready to support this project in the following activities, **subject to specific mutual agreement** between the project coordinator of C3ISP and me (kindly delete or customize below):

- providing a point of view on the market, commercial and exploitation questions the project is dealing with;
- enhancing the visibility of C3ISP towards my network
- liaising the project with other stakeholders (including from the policy making level) ~~and activities~~
- ~~acting as key-note speaker at events of C3ISP~~
- reviewing and commenting on the draft project documents.

Expenses related to participation in the Exploitation Board will be compensated by the C3ISP-project upon prior agreement and up to a limit determined appropriate.

Sincerely,

Name:
Title:
Contact details:

Signature:

Place, Date:

Figure 1: Text of the Exploitation Board Agreement

1.3. Exploitation approach

The project will regularly perform assessments of the added value of C3ISP results against the industry and research state-of-the-art. Candidate items will be raised as a point on the agenda of the first exploitation board meeting. If necessary, or in case of urgent events, they will be considered *ad hoc*.

1.4. Business network

1.4.1. Community building

C3ISP joined the following business communities:

- Consortiums of other Horizon 2020 projects
- TRUESSEC.eu network
- Companies, researchers and individuals specifically selected for open innovation
- Leveraging each Partner's individual communities.

1.5. Individual exploitation results

This section summarises the exploitation results and activities for each Consortium Partner.

1.5.1. CNR

Being a scientific partner, CNR will exploit C3ISP results to take advantage of the technology in their research activities. In particular, the know-how produced within the project about DSA, controlled natural language, mapping and refinement function from high to low specification languages, and access/usage enforcement will be useful to attract new business and scientific partners and collaboration in a twofold prospective: (1) for new European projects, and (2) new business/research collaboration and activities. Indeed, within the C3ISP project, CNR is mainly involved in the DSA management infrastructure, as well as, in the development of the DSA and Usage Adapter components.

Furthermore, being involved in the development in the Pilot about Internet Service Provider, CNR plans to exploit the C3ISP project results to improve the functionalities of providers by allowing them to use collaborative aspects of C3ISP to discover and mitigate security attack.

1.5.2. HPE

HPE manages a Technology Showroom in Milano (Italy), an environment where top Italian customers are invited to experience the most relevant and innovative HPE technology, so we will have the opportunity to include C3ISP in our demonstrations. HPE is also setting up a Demo Centre in Firenze, in collaboration with national academic partners. We plan to include a C3ISP demo environment also in this initiative to showcase to interested customers and partners. Furthermore, leveraging on the high number of community partners of the HPE Cloud28+ initiative (more than 500 worldwide), C3ISP solution also could provide high benefit by enabling the development of cyber security detection services that takes into account the privacy protection of each federated member.

1.5.3. BT

BT features C3ISP progress and innovations at Innovation 2017 in June'17 at its global R&D HQ at Adastral Park. The event had 5000+ visitors, which included external customers, BT market-facing units, technologists, as well Press and Analysts.

1.5.4. Digital Catapult

Digital catapult confirms that the methodology for exploitation innovation has been agreed (as detailed in D9.1, 1.6.2 Exploitation innovation) and planning for the first workshop is underway.

1.5.5. SAP

SAP joined cyber-security intelligence sharing initiatives like CSSA[1] to counter threats by leveraging on the collaboration among different stakeholders, exactly as for the C3ISP vision.

Contacts have been started with the SAP cyber-security team. An interest was demonstrated in the project's ideas and concepts. The same team is also in charge of interacting with CSSA partners. Therefore, and especially with respect to information sharing and acquisition technologies, C3ISP was deemed of strategic interest. To this respect, the initial discussions focussed on reviewing the requirements collected in the Enterprise pilot, which seemed close enough to the actual practice. The cyber-security team demonstrated also interest in the standards used in C3ISP architecture for information encapsulation. The cyber-security team stressed the importance of adopting standards or de-facto standards, with a preference for MISP[2] for its comprehensive tagging and more in general knowledge organisation solutions. The status of the activities involves a review of the C3ISP architecture in order to identify the most effective synergies with the actual practices of the cyber-security team.

SAP Enterprise Threat Detection[3] (ETD) is a tool that can be used to collect security events and context information as well as to monitor and to analyse events and alerts in SAP systems. In such a context, multiple C3ISP concepts find a fertile ground for their reception. An initiative in this direction is represented by a number of proof-of-concepts of the C3ISP-developed differential privacy algorithms to ETD use cases. The interactions with the ETD team continue, taking into account the volatility of the context.

1.5.6. 3D Repo Ltd

3D Repo is a cloud-based 3D Building Information Modelling collaboration tool. The sensitive nature of certain digital assets stored on 3D Repo means that cyber security is a paramount concern for the company and its customers. 3D Repo has previously collaborated with BT on the Trusted Cloud High Impact Initiative project [4]. 3D Repo believe that the results of C3ISP will be directly deployable with some of their largest customers such as Balfour Beatty, Crossrail and High Speed Rail 2.

1.5.7. UKENT

The University of Kent is working closely with BT to add the C3ISP enhancements to BT's cloud systems.

1.6. Research and IP state-of-the-art

The project consortium still believe that the analysis and assumptions made in the proposal with regards to the research and intellectual property state-of-the-art are still valid.

We continue to envision several areas where progress can be achieved and in particular there is the opportunity and need of maturation of the used technologies. We consider:

- Data Sharing Agreements
- Data Usage Control
- Collaborative cyber security information management
- Data analytics techniques
- Anonymisation techniques
- Homomorphic computing
- Visualisation techniques
- Managed Security Services

1.7. IPR protection

At M12, we have just completed the C3ISP design phase. IPR issues will be evaluated during the development activities and reported in D9.3 and D9.4. To date, no Consortium Partners have raised any IPR issues.

1.8. Sustainability plan

The Exploitation Reports (D9.2-4) will describe a sustainability plan for the continued impact from project outcomes, including:

- Summaries of scenarios
- Analysis of options to differentiate and prioritize scenarios
- Approach to technology transfer.

To standardize some of C3ISP technologies UNIKENT joined the OASIS standardisation group (2.1.1).

Here, we include the initial assessment of the added value of the C3ISP project.

1.8.1. ISP

C3ISP provides to the ISPs an added value that can be summarised with the possibility to use the collaborative information sharing and the data-analytics to collect and retrieve information related to cyber-security threats. Using C3ISP, ISPs leverage on several services and analytics that help them in mitigating security attacks and avoid future ones. Moreover, ISPs can use powerful, security-targeted and privacy-preserving services that will allow them to analyse their data without losing data-content privacy.

1.8.2. CERT

The added value provided by C3ISP, as discussed can be summarized as the automation of procedures which are currently performed manually inside the CERT, for what concerns data collection and result dispatching, the availability of a larger set of analytics for improved detection of threats and vulnerabilities, and the automatic handling of policies on data, to free the CERT from the burden of ensuring the privacy requirements of providers. Furthermore, the presence of authorisation mechanisms allows a dynamic control on the rights to request specific analysis, publish data and perform other specific operations.

1.8.3. Enterprise

Upon successful validation, the C3ISP technology in the Enterprise pilot would be a crucial contribution for complementing cyber-defence Managed Security Service (MSS) platforms; this would allow, for example, to enhance a MSS provider offerings in this space. The possibility to allow ‘aggregated’ analytics subject to constraints from individual customers’ usage policies, with a high degree of assurance of compliance/preservation of confidentiality would pave the way for new added value services and the associated market opportunities.

1.8.4. SME

The main added value of the C3ISP project in this context is that it allows SMEs to participate and collaborate in federations of information providers/consumers. The benefit for an SME is the availability of the useful cyber threat information shared by other SMEs and also the analyses of a large amount of CTI data, such as might be available to a larger enterprise today. The overarching effect is the barrier of the small size and lesser resources of an SME might be

somewhat overcome or reduced by allowing SMEs to share and aggregate security and threat information.

2. Standardization

2.1. Liaison with standardisation bodies - contribution to & liaison with standardisation bodies

2.1.1. Standardisation body <OASIS OpenC2 TC>

OpenC2's goal is to enable standardised, machine-to-machine response in cyber-relevant time and promote interoperability between domains. As the specification moves to become an international standard, University of Kent, which joined the technical committee, could influence critical decisions around interoperability and procurement. Current OpenC2 TC members include the NSA, Anomali, Bank of America, Cisco, FireEye, Fornetix, Intel, LookingGlass, McAfee, New Context, NC4, NEC, NIST, Phantom Cyber, Symantec, and others.

2.1.2. **British Standards Company**

Digital Catapult is in conversation with BSI (British Standards Company) who have committed to participate as a member of the C3ISP Exploitation Board.

3. Dissemination and Communications

3.1. Communications activities

We targeted the communications objectives described in D9.1 to approach the industry stakeholders and academic researchers as well as standardisation bodies. The primary channels of communication we use are our website and social media (Twitter and LinkedIn).

3.1.1. Communications channels

From January 2017 (M3), the C3ISP project has supported these communication platforms:

- Website - http://c3isp.eu/

Figure 2: Screenshot of the C3ISP website

- Social media - Twitter @C3ISP - https://twitter.com/C3ISP and LinkedIn

Furthermore, in all pages there is a section reporting all the news posted on the project Twitter

Figure 3: Screenshot of the C3ISP twitter account

3.1.2. Brand identity: logo, templates, etc.

By M3, the project established a standard set of branding, which included logo, and document templates that unify and reinforce the branding.

- Project logo
  -  - project logo without text
  - 

 - project logo with text
  - 

 - vertical project logo

- Deliverable's template to be used as a unified format for all deliverables to be submitted

C3ISP_WPz_Dx.y_v1_
YEARMMDD_PARTNE

- Slide's template to be used as a unified format for all presentations created for the C3ISP project

SlideTemplate-c3isp
.pptx

3.1.3. Campaigns

The marketing campaigns were identified to which activities to be aligned. The details of the campaigns have been described in D9.1.

3.2. Key messages

According to Table 5 in D9.1, the initial set of C3ISP messages, mapped to principle stakeholders, are shown.

Each set of messages applies to a *Phase* of the project. Messages are classified by *Type* which characterises its primary objective.

Stakeholders are grouped by the primary high-level class of influence (or call to action) that the communication associated with message seeks to have, including:

- Encourage the stakeholder to *consume* a C3ISP outcome
- Encourage the stakeholder to *supply* capability or information to support C3ISP outcomes, for example threat information

- *Advise* a stakeholder of C3ISP outcomes that are potentially important to them
- Influence bodies to change how they *regulate* security-related matters.

			Stakeholder								
Phase	Type	Message	consume		supply		advise			regulate	
			Enterprise	SME	enterprise	ISP	ISP	CERT	University	overnment Bo	standard body
Q1...	Mission	*During the initial phase of the project, the key messages echo the project mission statement that appears in Section (1.1).*									
	Mission	improve detection of cyber threats and response capabilities	y		y	y	y	y			
	Mission	facilitate computer interpretable and multi-stakeholder threat intelligence sharing			y	y	y	y		y	
	Mission	improve detection of cyber threats and response capabilities					y	y			
	Mission	preserve confidentiality of shared security information			y		y	y	y		
	Mission	exploit in cyber security management services	y		y	y					
	Mission	regulate by Data Sharing Agreements (DSAs)	y			y				y	y
	Mission	share information inside a collaborative multi-domain environment			y	y	y	y			
Q2...	Exploit	*Communications associated with the exploitation board will echo the terms of the Exploittion Board Agreement that is listed in Section (1.5.5).*									
	Exploit	market is ...	y	y	y	y					
	Exploit	commercial [tbd]									
	Exploit	liase with <organisation>					y	y		y	y
	Exploit	deliver project outcome			y	y		y	y	y	y
	Paper	*Communications associated with research publications will summarise the abstract of the associated paper, poster or presentation.*									
	Paper (n)								y	y?	y?
	Business	*During the second half of the project, messages for industrial stakeholders will reflect the business scenarios, and later the business cases.*									
	Business	Open innovaiton workship <n>			y			y		y	
H2	Business scenario <n>		y	y	y	y					
H2	Business case <n>		y	y	y	y					
Q4	Achievement	*In the last quarter of the project, messages will summarise project findings and achievements*									
	Deliverable <n>										y

Figure 4: Initial C3ISP message by stakeholder

3.3. Publications

3.3.1. Press release

The consortium published a joint press release for the project in June 2017.

Partners may handle their individual press releases independently, using the agreed text.

Consortium assembles to deliver C3ISP project dedicated to help the fight against cyber crime

The Horizon 2020 R&D funded project is dedicated to creating innovations in sharing information to help fight against cyber crime and will also look to develop a protection framework for exploring cyber security management services

XX April, 2017 – [Insert company name] has today announced that it is part of a consortium of industry and research institutions, SMEs and innovation promoters that are working together to help deliver the C3ISP project. Focused on cyber security, the Horizon 2020 R&D funded project has been created to encourage new ways of sharing information in a flexible and controllable manner.

Acknowledging the critical role data sharing plays in the fight against cyber crime, the project will run across a collective multi-domain environment. It is designed to improve detection of cyber threats and response capabilities, while also preserving the confidentiality of the shared sensitive information.

With a mission to develop a protection framework for exploring cyber security management services, C3ISP aims to create an efficient and flexible framework for secure data analytics through the development of a dedicated platform. C3ISP allows data access and analytics operations to be automatically regulated by multi-stakeholders and in addition, the project will facilitate data sharing agreements to ensure access to sensitive data is limited by sophisticated cryptographic and stochastic mechanisms.

In particular, C3ISP will look to address some of the key challenges around the compliant sharing of cybersecurity related information, from threat reports and sensor vulnerability data to systems logs. The project will address the issue from a "compliance by design" approach to ensure regulatory requirements are factored into the early stages of data sharing agreements.

It will then look to validate the framework through four pilots covering distinctive markets; enterprise security, governmental CERTS, Internet Service Providers (ISPs) and SMEs seeking cyber security protection through managed security services.

[TEMPLATE QUOTE: XX from [Insert company name] XXX "Cyber security is a critical issue of our time and the threat landscape is only becoming more complex as our technological capabilities become more advanced. One of the key tools in addressing cyber crime comes from sharing information in a responsible way, not only to enable threat awareness and speed up fixes, but to be able to learn about wider trends in cyber criminal activity, to help everyone to better protect against future attacks. C3ISP will play a vital role in enabling the sharing of critical and sensitive information in a way that will ensure regulatory requirements are met whilst also facilitating the sharing of knowledge that is required to effectively tackle this growing threat."

The project will be co-ordinated by Consiglio Nazionale Delle Ricerche – CNR, with consortium partners including BT, Chino, Digital Catapult, HPE, CEA, GPS, ISCOM-MISE, SAP, UniKent and 3DRepo.

From the scientific to the industrial community and wider audiences, C3ISP is designed to ensure that key learnings from the project can be shared and acted upon by all once it is complete.

For more information on the Horizon 2020 R&D funded C3ISP project, please visit: http://www.c3isp.eu

[Insert company boilerplate]

About Digital Catapult

Digital Catapult is driving the UK economy through digital innovation. Representing a network of centres across the UK, Digital Catapult connects businesses of all sizes with academia, industry experts and the Government to help UK businesses realise sustainable economic growth regionally, nationally and on the global stage.

Digital Catapult delivers a national digital strategy with local impact through its headquarters in London and regional centres in Brighton, North East & Tees Valley, Northern Ireland and Yorkshire. Each centre works with companies of all sizes to transform their businesses through digital innovation.

Digital Catapult deploys its expertise and facilities in sectors where there is the most untapped potential to deliver future economic growth, where digital innovation can make the greatest impact to increase productivity, sustain high value employment opportunities and ultimately grow the UK economy.

To find out more about Digital Catapult, please visit: www.digicatapult.org.uk / @DigiCatapult

Figure 5: Agreed text for the press release

3.3.2. Promotion

All project events and partners activities related to the promotion of the project and its results will be announced throughout the usual project communications channels (the website and the social networks (REF _Ref493252957 \w \h * MERGEFORMAT 3.1.1)).

3.3.3. Brochure

The following brochure has been created to support all partners in the promotion of the project. This brochure contains information on the C3ISP project objectives, information about the Consortium and the C3ISP approach to threat intelligence.

C3ISP
Collaborative and Confidential Information Sharing and Analysis for Cyber Protection

European Commission | Horizon 2020 European Union funding for Research & Innovation

C3ISP is a Horizon 2020 collaborative R&D project which innovates information sharing.

C3ISP aims to provide a flexible framework allowing **confidential** and **collaborative information sharing** and **analysis** in order to ease cyber **protection** among relevant stakeholders.

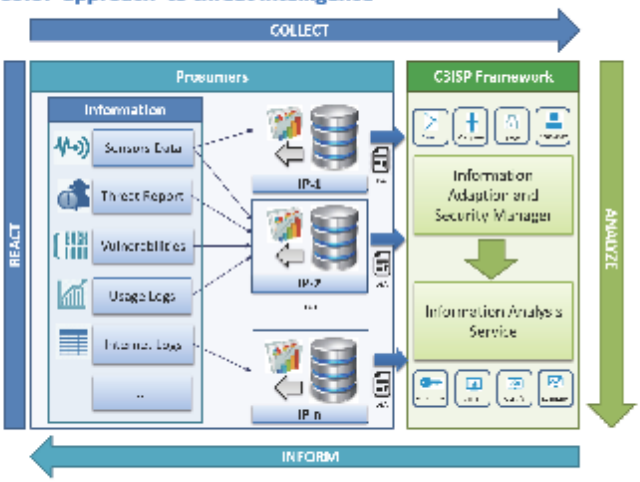
Sharing to protect against cyber-attacks

Cyber-attacks affect every aspect of our lives, targeting our mobile devices, our bank accounts and our vehicles. These attacks can have serious consequences, not only for cyber-security, but also for safety, as the cyber and physical worlds are increasingly linked.

Providing effective **cyber-security** requires cooperation and collaboration among all the entities involved. Increasing the information available for analysis allows better prediction, prevention and mitigation of cyber-attacks.

However, concerns that sensitive and confidential information may be revealed currently deters organisations from sharing data.

C3ISP approach to threat intelligence



The mission of the C3ISP project is to define an exploitable collaborative and confidential information sharing, analysis and protection framework, delivered as a cyber security management service.

We collect risk and threat intelligence from various sources, and share securely to analyse responses that inform stakeholders reactions.

The C3ISP framework can share information inside a collaborative multi-domain environment to improve detection of cyber threats and response capabilities, while appropriately protecting the confidentiality of the shared information using a range of privacy-preserving techniques, regulated by Data Sharing Agreements that are computer interpretable and multi-stakeholder.

This is aligned with the main guidelines of the **European Cyber Security Strategy.**

HORIZON 2020

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

Figure 6: C3ISP brochure

3.3.4. Videos

SAP and BT are currently working on creating a promotional video for the project that is still in production.

The video is being elaborated as follow-up of a successful demonstration jointly held by BT and SAP at the BT Innovation Days 2017 in Ipswich.

It will show a relevant use case for the C3ISP Enterprise pilot.

The video will show how C3ISP data manipulation operations may successfully be applied to lower the sensitivity of cyber threat information collected by an actor, in order to permit their disclosure but at the same time, retaining valuable details for further analysis. The information being considered is that of a dataset of possible attackers to a set of targets belonging to the same entity. The application of the C3ISP anonymization tool with the geo-indistinguishably and IP manipulation functionalities still allows to disclose a dataset that permits to see:

- nationality of the attackers
- patterns and strategies of their attacks

3.3.5. Research papers

In the following, we list all publications submitted, accepted and presented at peer-reviewed international conferences that acknowledge the C3ISP project:

1. *Fabio Martinelli, Francesco Mercaldo, Andrea Saracino* BRIDEMAID: An Hybrid Tool for Accurate Detection of Android Malware ACM Asia Conference on Computer and Communications Security (ASIACCS)
2. *Fabio Martinelli, Ilaria Matteucci, Paolo Mori, Andrea Saracino* Concurrent History-based Usage Control Policies MODELSWARD 2017
3. *Gianpiero Costantino, Fabio Martinelli, Ilaria Matteucci, Marinella Petrocchi* Analysis of Data Sharing Agreements International Conference on Information Systems Security and Privacy (ICISSP 2017)
4. *Mario Luca Bernardi, Marta Cimitile, Fabio Martinelli, Francesco Mercaldo* A Fuzzy-based Process Mining Approach for Dynamic Malware Detection IEEE International Conference on Fuzzy Systems
5. *Mario Luca Bernardi, Marta Cimitile, Fabio Martinelli, Francesco Mercaldo* A Time Series Classification Approach to Game Bot Detection 7th ACM International Conference on Web Intelligence, Mining and Semantics (WIMS)
6. *Mario Luca Bernardi, Marta Cimitile, Fabio Martinelli, Francesco Mercaldo* Game Bot Detection in Online Role Player Game through Behavioural Features 12th International Conference on Software Technologies (ICSOFT)
7. *Fabio Martinelli, Francesco Mercaldo, Vittoria Nardone, Antonella Santone* How Discover a Malware using Model Checking ACM Asia Conference on Computer and Communications Security (ASIACCS)
8. *Mina Sheikhalishahi, Fabio Martinelli* Privacy Preserving Clustering over Horizontal and Vertical Partitioned Data The 22nd IEEE Symposium on Computers and Communications
9. *Mina Sheikhalishahi, Fabio Martinelli* Privacy-Utility Feature Selection as a Privacy Mechanism in Collaborative Data Classification The 26th IEEE International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE 2017)

10. *Mina Sheikhalishahi, Fabio Martinelli* Privacy-Utility Feature Selection as a tool in Private Data Classification 14th International Conference on Distributed Computing and Artificial Intelligence (DCAI 2017)
11. *Antonio La Marra, Fabio Martinelli, Paolo Mori, Andrea Saracino.* Implementing Usage Control in Internet of Things: A Smart Home Use Case, , IEEE Trustcom 2017
12. *Giacomo Giorgi, Antonio La Marra, Fabio Martinelli, Paolo Mori, Andrea Saracino* Smart Parental Advisory: A Usage Control and Deep Learning-based Framework for Dynamic Parental Control on Smart TV, STM 2017 (ESORICS)
13. *Antonio La Marra, Fabio Martinelli, Paolo Mori, Athanasios Rizos, Andrea Saracino*. Introducing Usage Control in MQTT for IoT, CyberICPS 2017 (ESORICS).
14. *Ian Herwono and Fadi Ali El-Moussa.* Collaborative Tool for Modelling Multi-Stage Attacks. 3rd International Conference on Information Systems Security and Privacy - ICISSP 2017", 19-21 February 2017, Porto, Portugal.

3.4. Event schedule

3.4.1. Industry workshop to validate business models [mid-project]

In consultation with the whole consortium we will identify which market sectors/business scenarios present the biggest need and commercial opportunity for further development of the C3ISP protection framework. In addition, we will validate those market sectors and business scenarios identified during the 'understand' phase, with a specially selected target audience to ensure the propositions meet the needs of the market.

3.4.2. Industry workshop to disseminate results [near end of project]

The aim of this workshop is to involve potential framework users and their ecosystems, along with members of the Exploitation Board to refine findings and raise awareness about the framework benefits and identify opportunities for commercial exploitation.

3.4.3. PhD school

CNR researchers will utilise significant experience of running summer schools (one of the oldest PhD summer schools in computer security) and organize the PhD school of C3ISP jointly with the one of NeCS. This is planned to be held in 2018 in Trento.

3.4.4. Conferences, seminars and industry events

Table 1: Schedule of past Conferences, seminars and industry events

Date	Type	Title	Location
June 2017	conference	Innovation 2017	BT R&D HQ, UK
September 2017	workshop	3rd International Workshop on TEchnical and LEgal aspects of data pRIvacy and SEcurity	Trento

3.5. Events participation & organisation

Innovation 2017 in June'17 was held at BT's global R&D HQ at Adastral Park. The event had 5000+ visitors, which included external customers, BT market-facing units, technologists, as well Press and Analysts.

Both BT and SAP collaboratively demonstrated C3ISP progress and innovations at this event, including in the area of Differential Privacy using a demo created specifically for the purpose.

The 3rd International Workshop on TEchnical and LEgal aspects of data pRIvacy and Security (TELERISE 2017) has been organised by CNR in conjunction with the International Conference of Computer Safety, Reliability, and Security (SAFECOMP2017) the 12th of September (http://www.iit.cnr.it/telerise2017/). It was located in Trento. The topics of the workshop cover some of the main problems addressed by the C3ISP project. The workshop has been attended by around 20 persons.

The keynote speaker is Francesco Di Cerbo (SAP), partner of the project. The talk is well focused of the project.

4. References

This section lists the references used throughout the document:

[1] Cyber-Security intelligence sharing initiative(CSSA) - https://www.cssa.de/en/index.html

[2] Open Source Threat Intelligence Platform & Open Standards For Threat information Sharing - https://misp-project.org

[3] SAP Enterprise Threat Detection - https://help.sap.com/viewer/p/SAP_ENTERPRISE_THREAT_DETECTION

[4] 3D Repo. 3D Repo in a Secure Cloud Environment; a Case study, Retrieved 17 August 2017 - http://3drepo.org/projects/3d-repo-in-a-secure-cloud-environment-a-case-study/

Appendix 1. Glossary

Table 2 - Glossary

Acronym	Definition
SME	Small and Medium Enterprise
DSA	Data Sharing Agreement
CSSA	Cyber Security Sharing & Analytics
ETD	Enterprise Threat Detection

1.