D6.5 Commercial actions report V2

Grant Agreement number:	740723
Project acronym:	CS-AWARE
Project title:	A cybersecurity situational awareness and information sharing solution for local public administrations based on advanced big data analysis
Principal author:	Laurentiu Vasiliu, Peracton Ltd, laurentiu.vasiliu@peracton.com
Co-author(s)	Judi Blackmur (Peracton), John Forrester (Cesviter), Thomas Schaberreiter (University of Vienna), Chris Wills (Caris Research), Jerry Andriessen (Wise & Munro), , Adamantios Koumpis (Passau University),
Document version:	2.0
Quality Reviewers	Adamantios Koumpis (Passau University) Georgios Apostolopoulos (OTS)

Table of Contents

Executive Summary

The current deliverable constitutes the second version of the 6.4 report on Commercial Actions as it expands the original V1.0 commercialization analysis, plan and actions to be pursued by the CS-AWARE consortium members.

1 Introduction

This document is an update of the deliverable D6.4.1 Commercial actions report (M6 - February 28th, 2018). The content produced in this deliverable represents the new developments, changes and updates on the commercial positioning received from of all consortium partners, for the period March 1st, 2018 to March 1st 2019.

2 Aimed exploitable results

In the first version of the deliverable when the discussion was focused on the aimed exploitable results, a certain consideration was given towards:

a) the individual analysis of a customer's systems
b) the automation and tool driven detection, as well as the provision of an awareness solution we considered .

As option(a) has been fully detailed in D6.4.1 this update will focus on detailing the awareness solution, currently being built from a commercial presentation perspective.

The CS-AWARE solution - , currently in the implementation phase, aims to be an automatic detection tool for cyber-threats and awareness solution. The unique selling points envisaged are:

- connectivity to any type of internal and external data source
- data analysis of potential suspicious activity that doesn't necessarily appears to be a direct threat
- potential threat identification and correlation with external sources if they are available
- suggestion of possible healing solutions
- implementation of healing solutions
- sharing with cyber community of the threat findings

All these above points are intended to be (semi)automated, part of a ready-to-deploy and run solution

1. Summary and main features of CS-AWARE platform
2. Product

Besides the main exploitable results relating to CS-AWARE as a cybersecurity awareness system, the enhanced understanding of the cybersecurity environment in local public administrations that was gained (especially through the two rounds of systems and dependency workshops in our local public administration piloting partners) has shown the potential for additional exploitation routes that could

be taken with the CS-AWARE technology at its base. Especially two additional aspects have caught the attention of the CS-AWARE consortium and would require little to no modifications to the technological basis of CS-AWARE core technologies:

1. **CS-AWARE as a knowledge management system:** During the CS-AWARE workshops it has become evident that the knowledge asymmetry and the incomplete understanding of the system set-up and their interaction, especially between departments and/or external suppliers, is a major cybersecurity risk factor in LPAs. The holistic socio-technical analysis approach, as well as the capturing of the system interactions (assets and dependencies along with their descriptions) in electronic form has already at this point helped to improve cybersecurity in those LPAs. The CS-AWARE consortium sees a potential to promote the knowledge management aspect of CS-AWARE and integrate it much more in organizational management operations, going even beyond management tasks that are purely cybersecurity related. Both the knowledge capturing element of the CS-AWARE stack as well as the other relevant technology stack would support those concepts.
2. **CS-AWARE as a compliance monitoring tool:** The recently introduced European regulations relating to cybersecurity, especially the NIS directive and the GDPR, are imposing certain measures on system and service owners/operators to ensure the compliance with those regulations. Some of those measures require constant re-evaluation and monitoring in order to ensure legal compliance. CS-AWARE has from the start highlighted its potential for NIS compliance (especially the potential for automating incident reporting), we have identified a great potential for CS-AWARE to be a strong tool for ensuring GDPR compliance. In GDPR, one of the major aspects is to be able to know where data resides within ones systems and how this information flows through the systems. CS-AWARE system and dependency analysis models exactly this behavior, and can based on this model monitor the behavior of this data to e.g. detect data breaches. Furthermore, the information sharing component can assist the data protection officer in reporting of detected data breaches to the authorities, as required by the GDPR. Besides the automated procedures, it was identified that the CS-AWARE system and dependency analysis methodology can easily be adopted to assist in GDPR compliance work for measures that do not require automated monitoring.

Those two additional exploitation routes will be investigated further for their potential and whether they could add additional value to CS-AWARE core exploitation route as a cybersecurity awareness system.

2.1 Goal and features of the solution

The original idea of CS-AWARE solution remains intact & unchanged: offering cybersecurity related services aiming at organizational systems, where big factors influencing securityare the socio-technological relations between technology & its users, as well as the complexity of such organizational set-ups that often neglect to provide an overview of the security situation.

2.1.1 Visualisation and decision support

No change from version V1.0

2.1.2 Situational awareness

No change from version V1.0

2.1.3 System self-healing

No change from version V1.0

2.1.4 Customer's (end user's) perspective

No change from version V1.0

2.1.5 An example scenario

No change from version V1.0

2.2 Delineating the CS-AWARE product

The CS-AWARE product provides features such as :

- consultancy services (1) Dedicated analysis of a customer's systems resulting to the spherical understanding of the organizations assets and dependencies . It is critical, within this analysis, to understand the client-set-up and the type of threats specific to its environment , in order to set up the appropriate set of threat patterns in the CS-AWARE platform for real time detection.
- CS-AWARE platform (2) Semi-automatic and tool driven detection and awareness solution.

3 SWOT analysis

Figures 3 next is presenting the updated SWOT analysis for the CS-AWARE envisioned approach:

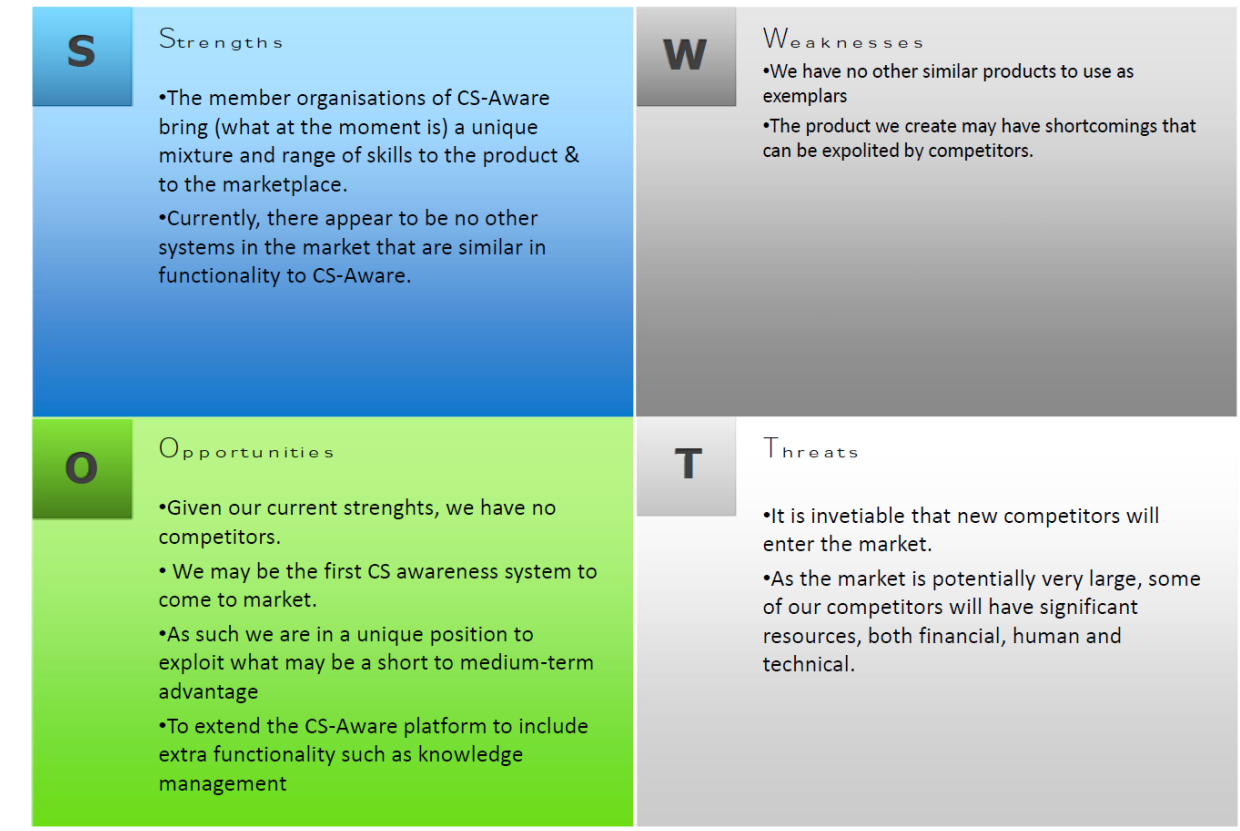

Figure 3 CS-AWARE SWOT analysis (updated)

Strengths

Between them, the member organization comprising the consortium, have an unparalleled, extremely diverse and comprehensive skill set, which we believe to be unique when compared to those of our potential competitors. Moreover, while there are other tools in the marketplace that offer threat intelligence and vulnerability management (such as Recorded Future's *Recorded Future Express),* none offer a solution as comprehensive as that which will be offered by CS-Aware.

Weaknesses

Our product is unique. Therefore, the CS-Aware solution has no other systems that can be used as exemplars. In our considered opinion, we have developed a highly comprehensive solution. However, new competitors entering into the marketplace will seek to identify and develop new or enhanced functionality to surpass CS-Aware's solution. To reduce this risk, the development of the CS-Aware offering must be dynamic, be continually developed and quickly respond to changing market requirements and demand.

Opportunities

Being first to market, we have the opportunity to create a market-leading brand, develop a ubiquitous product that gains rapid market penetration and maintains market dominance. Within the SWOT

analysis a new opportunity has been identified, namely a possible extension of the platform, with knowledge management capabilities. Based on the market feedback, considerations will be made on the extension of development, e.g. ensure just API type connectivity or, create a basic GUI and functionality of knowledge management.

Threats

While being first to market with a comprehensive tool (encompassing both real-time threat monitoring, visualization, threat intelligence, self healing and knowledge management), is an advantage, it is also likely that being first to market with such a tool will encourage existing providers of threat intelligence tools to develop to meet or surpass CS-Aware's functionality. Indeed, it may provoke emulation on the part of new potential competitors who are as yet are not operating in the market and lead to increased competition in what could become a potentially crowded marketplace.

4 Initial market analysis

No change from version V1.0

4.1 Selected Country profiles

4.1.1 France

No change from version V1.0

4.1.2 Ireland

No change from version V1.0

4.1.3 Italy

No change from version V1.0

4.1.4 The Netherlands

No change from version V1.0

4.1.5 Poland

No change from version V1.0

4.1.6 United Kingdom

No change from version V1.0

4.1.7 Additional market analysis / relevant market information

4.1.7.1 Cybersecurity workforce shortage: building the case for automated solution need:

According to a recently published report by ISC2 (International Information System Security Certification Consortium Inc), the cybersecurity workforce shortage is 22.93 million globally, with demand versus supply of security professionals in Asia-Pacific outpacing all other regions combined. The APAC shortfall is estimated at 2.15 million, attributed to growth in numerous countries and new security and privacy regulations. Research indicates that there is considerable regional variance across the globe. North America has a cybersecurity workforce shortage that is significant, with demand outpacing supply by 498,000, followed by Europe, the Middle East and Africa, with an estimated 142,000 open positions; and Latin America, with 136,000.

4.1.7.2 New EU Cybersecurity act:

The European Parliament, the Council and the European Commission have reached a political agreement on the Cybersecurity Act, which reinforces the mandate of the EU Agency for Cybersecurity. It will better support Member States with tackling cyber security threats and attacks. The Act also establishes an EU framework for cybersecurity certification, boosting the cybersecurity of online services and consumer devices.

Vice-President Andrus Ansip, in charge of the Digital Single Market, said: "In the digital environment, people, as well as companies, need to feel secure; it is the only way for them to take full advantage of Europe's digital economy. Trust and security are fundamental for our Digital Single Market to work properly. This evening's agreement on comprehensive certification for cybersecurity products and a stronger EU Cybersecurity Agency is another step on the path to its completion."(Reference?)

Commissioner Mariya Gabriel, in charge of Digital Economy and Society, added: "Enhancing Europe's cybersecurity, and increasing the trust of citizens and businesses in the digital society is a top priority for the European Union.

"Major incidents such as Wannacry and NotPetya have acted as wake-up calls because they dearly showed the potential consequences of large-scale cyber-attacks. In this perspective, I strongly believe that tonight's deal both improves our Union's overall security and supports business competitiveness." (Reference?)

Proposed in 2017 as part of a wide-ranging set of measures to deal with cyber-attacks and to build strong cybersecurity in the EU, the Cybersecurity Act includes:

- A permanent mandate for the EU Cybersecurity Agency, ENISA, to replace the limited mandate that would have expired in 2020, as well as more resources allocated to the agency to enable it to fulfil its goals, and;
- a stronger basis for ENISA in the new cybersecurity certification framework to assist Member States in effectively responding to cyber-attacks with a greater role in cooperation and coordination at Union level.

In addition, ENISA will help increase cybersecurity capabilities at EU level and support capacity building and preparedness. Finally, ENISA will be an independent centre of expertise that will help promote a high level of awareness of citizens and businesses but also assist EU Institutions and Member States in policy development and implementation.

The Cybersecurity Act also creates a framework for European Cybersecurity Certificates for products, processes and services that will be valid throughout the EU. This is a ground breaking development as it is the first internal market law that takes up the challenge of enhancing the security of connected products, Internet of Things devices as well as critical infrastructure through such certificates.

The creation of such a cybersecurity certification framework incorporates security features in the early stages of their technical design and development (security by design). It also enables their users to ascertain the level of security assurance and ensures that these security features are independently verified.

The new rules will help people trust the devices they use every day because they can choose between products, like the Internet of Things devices, which are cyber secure.

The certification framework will be a one-stop shop for cybersecurity certification, resulting in significant cost saving for enterprises, especially SMEs that would have otherwise had to apply for several certificates in several countries. A single certification will also remove potential market-entry barriers. Moreover, companies are incentivized to invest in the cybersecurity of their products and turn this into a competitive advantage.

Following tonight's political agreement, the new regulation will have to be formally approved by the European Parliament and the Council of the EU. It will then be published in the EU Official Journal and will officially enter into force immediately, thus paving the way for European certification schemes to be produced and for the EU Agency for Cybersecurity, ENISA, to start working on the basis of this focused and permanent mandate.

4.1.7.3 INTERNET ORGANISED CRIME THREAT ASSESSMENT 2018

An Europol Internet Organised Crime Threat Assessment 201:

- Ransomware retains its dominance

Even though the growth of ransomware is beginning to slow, ransomware is still overtaking banking Trojans in financially-motivated malware attacks, a trend anticipated to continue over the following years. In addition to attacks by financially motivated criminals, significant, public reporting increasingly attributes global cyber-attacks to the actions of nation states. Mobile malware has not been extensively reported in 2017, but this has been identified as an anticipated future threat for private and public entities alike.

Illegal acquisition of data following data breaches is a prominent threat. Criminals often use the obtained data to facilitate further criminal activity. In 2017, the biggest data breach concerned Equifax, affecting more than 100 million credit users worldwide. With the EU GDPR coming into

effect in May 2018, the reporting of data breaches is now a legal requirement across the EU, bringing with it hefty fines and new threats and challenges.

- DDoS continues to plague public and private organisations

Criminals continue to use Distributed-Denial-of-Service (DDoS) attacks as a tool against private business and the public sector. Such attacks are used not only for financial gains but for ideological, political or purely malicious reason. This type of attack is not only one of the most frequent (only second to malware in 2017); it is also becoming more accessible, low-cost and low-risk.

- Production of CSEM continues

The amount of detected online Child Sexual Exploitation Material (CSEM), including Self-Generated Explicit Material (SGEM), continues to increase. Although most CSEM is still shared through P2P platforms, more extreme material is increasingly found on the Darknet. Meanwhile, Live Distant Child Abuse (LDCA), facilitated by growing internet connectivity worldwide, continues to be a particularly complex form of online CSE to investigate due to the technologies and jurisdictions involved.

As increasing numbers of young children have access to internet and social media platforms, the risk of online sexual coercion and extortion continues to rise. The popularity of social media applications with embedded streaming possibilities has resulted in a strong increase in the amount of SGEM live streamed on these platforms.

- Card-not-present fraud dominates payment but skimming continues

Skimming remains a common issue in most of the EU Member States. As in previous years, this continues to decrease as a result of geoblocking measures. Skimmed card data is often sold via the Darknet and cashed out in areas where Europay, MasterCard and Visa (EMV) implementation is either slow or non-existent.

Toll fraud has received a considerable amount of attention this year, with criminal groups using counterfeit fuel and credit/debit cards to avoid paying toll fees. Many Member States also reported an increase in the creation of fake companies to access and abuse Points of Sale (PoS), as well as profit from compromised information. Meanwhile, CNP fraud continues to be a key threat for EU Member States, with the transport and retail sectors highlighted as key targets within the EU.

- As criminal abuse of cryptocurrencies grows, currency users and exchangers become targets

Previous reports indicated that criminals increasingly abuse cryptocurrencies for funding criminal activities. While Bitcoin has lost its majority of the overall cryptocurrency market share, it still remains the primary cryptocurrency encountered by law enforcement. In a trend mirroring attacks on banks and their customers, cryptocurrency users and facilitators have become victim of cybercrimes themselves. Currency exchangers, mining services and other wallet holders are facing hacking attempts as well as extortion of personal data and theft. Money launderers have evolved to use

cryptocurrencies in their operations and are increasingly facilitated by new developments such as decentralised exchanges which allow exchanges without any Know Your Customer requirements. It is likely that high-privacy cryptocurrencies will make the current mixing services and tumblers obsolete.

- Cryptojacking: a new cybercrime trend

Cryptojacking is an emerging cybercrime trend, referring to the exploitation of internet users' bandwidth and processing power to mine cryptocurrencies. While it is not illegal in some cases, it nonetheless creates additional revenue streams and therefore motivation for attackers to hack legitimate websites to exploit their visitor systems. Actual cryptomining malware works to the same effect, but can cripple a victims system by monopolising their processing power.

- Social engineering still the engine of many cybercrimes

The significance of social engineering for cyber-dependent and cyber-enabled crime continues to grow. Phishing remains the most frequent form of social engineering, with vishing and smishing less common. Criminals use social engineering to achieve a range of goals: to obtain personal data, hijack accounts, steal identities, initiate illegitimate payments, or convince the victim to proceed with any other activity against their self-interest, such as transferring money or sharing personal data.

- Shutters close on major Darknet markets, but business continues

The Darknet will continue to facilitate online criminal markets, where criminals sell illicit products in order to engage in other criminal activity or avoid surface net traceability. In 2017, law enforcement agencies shut down three of the largest Darknet markets: AlphaBay, Hansa and RAMP. These takedowns prompted the migration of users towards existing or newly-established markets, or to other platforms entirely, such as encrypted communications apps.

Athough cybercrime continues to be a major threat to the EU, last year saw some remarkable law enforcement success. Cooperation between law enforcement agencies, private industry, the financial sector and academia is a key element of this success.

- Europol report: Trends in Europe

The majority of cyber threats affecting Europe continues to emanate from within the European Region, either domestically, or from other European countries. The current emphasis on the use of email as an attack vector is clearly demonstrated in some of the trends highlighted by industry. Austria, Germany, Hungary, Italy, Russia, Spain and the UK, had some of the highest global rates of malicious emails containing malware, while Ireland, Norway and Sweden similarly had some of the highest global rates of email containing malicious URLs. Moreover, the Netherlands, Hungary, Portugal and Austria, also suffered from high global rates of phishing emails. In some cases this was exacerbated by some of the world's highest rates of spam.

These attacks also account, at least in part, for the fact that a significant proportion of global attacks originating from compromised IoT devices stem from a number of Europe countries. Moreover, some EU countries, such as France and Germany are significant global sources of spam.

Law enforcement outlined a wide variety of cyber-attacks emanating from other European countries, although there was strong emphasis on various aspects of payment fraud. In this regard, Bulgaria and Romania were highlighted as having a key role.

4.2 Segmentation of customers

This subsection examines the segmentation of potential customers or market segmentation, outlined as the division of prospects in a given market into discrete groups, based upon similarities such as specific needs or buying characteristics. The final version of this report (Version 3) will be based on further market input/interactions gained as the project evolves . Currently, a high level market segmentation is been kept, as a starting point for future market actions.

As CS-AWARE platform will be sold to businesses and will not be a retail solution, the main perspective is to have a B2B Customer segmentation approach.

- Geographic base/reach
  - EU countries
  - North America
- Industry/sub-industry
  - Local Public Administrations
  - Finance/Banking
- Product usage
  - Internal cyber-security monitoring
  - Supply/chain or clients support/monitoring
- Organization size (revenue, number of employee)
  - LPAs size – initial analysis done, the spin-out will focus on the specific LPA size
  - Banks size (to be further detailed)
  - Financial institutions size (to be further detailed)
- Product delivery model
  - SAAS
  - Installed on site, behind organisation firewall

4.3 Competition

An initial in-depth analysis identified one potential competitor and 8 companies that aren't considered direct competitors, but offer functionalities that are part of the CS-AWARE solution

	Potential Competitor	Link	Description
1	Record Future US/UK/Sweden	https://www.recordedfuture.com/	Recorded Future's unique technology collects and analyses vast amounts of data to deliver relevant cyber threat insights in real time. The solution aggregates this rich intelligence with any other threat data sources, empowering security teams to collaborate on analysis and delivering intelligence

			wherever you need it most, including rapid integration with your existing security solutions. Solution follows an individualized approach for each company
2	S21SEC/ Spain/Portugal /Mexico/UK	https://www.s21sec.com/en/cyber-threat-alerts/	Same as above: individualized approach for each company
3	ThreatConnect USA/UK	https://threatconnect.com/solution/government/	government specific solutions, info sharing, security response - actionable insights
4	ThreatQuotient, Inc USA	https://www.threatq.com	tailored, automated service
5	LookingGlass Cyber Solutions, Inc. USA	https://www.lookingglasscyber.com/products/manage-intelligence/	platform to help security teams identify, contextualize, and prioritize threat data, and then transform that information into actionable intelligence. LookingGlass offers three distinctive threat intelligence platforms as part of their end-to-end solutions portfolio.
6	SecureWorks, Inc. USA[1]	https://www.secureworks.com/	compliance management, government specific solutions

However it should be noted that none of them offer exactly the features CS-AWARE will, but each of them covers partly few of them.

Furthermore, according to eSecurity Planet, the following 8 companies are providing technology for cyber-threat detection and analysis. While they are not considered direct competitors, it is worth including them on a short list for future analysis.

[1] With offices also in UK, France, Germany, Romania, The Netherlands, Japan, UAE, Australia and Singapor. Not clear if only for Sales or also for other product and technology development functions.

Vendor	Use Cases	Metrics	Intelligence	Delivery	Pricing
IBM	Retailers, financial services, enterprise	Unlimited queries per month, and up to 5,000 records per month	Machine learning and IBM Watson analytics	Via web browser or through an API interface to interface with existing security solutions	The API is free for 5,000 records/month; the commercial API starts at $2,000 per user/month
Anomali	Financial services, enterprise	Can process millions of Indicators of Compromise (IOCs)	Machine learning and integration with other security platforms	SaaS, on-premises, or hybrid	Pricing varies based on customer environment
Palo Alto Networks	Large enterprises	Receives hundreds of millions of samples per month, and over a trillion artifacts across petabytes of data	Statistical analytics, correlation and machine learning	SaaS-based security services	Licensed as a per-user annual subscription or enterprise-wide
RSA	Financial institutions, governments and oil/gas/energy/telcos	Can ingest 30,000 EPS per system and up to 100k endpoints per system	Automated segmentation and enforcement	On premises, in private clouds, on virtual machines, or public cloud	Tiered throughput or subscription licensing
LogRhythm	Financial services, retail, manufacturing, and government	26 billion messages per day and over 10K gigabytes per day	Pattern matching and advanced correlation to machine learning and statistical analysis	Software and hardware	Pricing begins at $27,000
FireEye	Financial services, government and IT	More than 1,000 experts responding to incidents and researching attacks	Automation enables it to go from alert to fix in seconds	Via API integration, intelligence portal, and email delivery	Subscriptions range from $100,000 to $500,000
LookingGlass Cyber Solutions	Enterprise and third-party risk monitoring	Over 140 sources of threat data gathered	Machine-readable threat intelligence	Hosted or on-premise	Open-source business model
AlienVault	Companies with smaller IT security teams	Receives 10 million indicators of compromise every day	Automation and machine learning	Cloud, virtual or hardware appliance	Monthly subscription; Tiers start at $1,575/month for a 250 GB data volume

5 Go-to-market Analysis

5.1 Business Summary

No change from version V1.0

5.2 Product Strategy

No change from version V1.0

5.3 Marketing Strategy

No change from version V1.0

5.4 Customer Experience

No change from version V1.0

5.5 Technical Requirements

No change from version V1.0

5.6 Evaluation

No change from version V1.0

5.7 Timeline and Execution

No change from version V1.0

5.8 Positioning of the CS-AWARE brand

No change from version V1.0

5.9 Communication Channels

No change from version V1.0

5.10 Sales Channels

No change from version V1.0

5.11 Anticipating difficult market entry in times of austerity and cuts in public spending

No change from version V1.0

6 Risk analysis and mitigation

This section is identifying the various risks related to the usage of CS-AWARE platform and technology. Further it builds the basis for potential solutions and/or mitigation strategies.

6.1 Technological Risks

No change from version V1.0

6.2 Commercial Risks

	Commercial Risk		Mitigation Strategy
5	Sales cycles longer than initially thought > 1 year after the project ends		Focus on very specific pre-qualified targets, identify possible sale opportunities during the project and secure funding for the spin-out to sustain the sales cycle after the project endsOn this, see Section 6.2.1 below.
6	Getting entrance to decision makers difficult		Target early external partnerships and identify decision makers in sales opportunities
7	Not enough sales experience within the consortium		Identify by M12 specific commercial weaknesses and have a dedicated plan in place; diversify the commercialization approach such as going simultaneously for other type of actions such as licensing and setting up a spin-out company. On this, see Section 6.2.2 below.
7.1	Project finishes and the spin-out doesn't have secured funding		On this, see Section 6.2.3 below.
7.2	Neither Larissa or Rome buy the solution after the project finishes due		On this, see Section 6.2.4 below.

	to unforeseen circumstances		

6.2.1 Secure funding for the spin-out to sustain the sales cycle after the project ends

From experience we have from other projects, it is usual that the result of a project matures to a solution adopted by a customer within a period of at least 3 years. However, we are aware of several funding instruments like the EXIST-Gründerstipendium, a kind of Business Start-up Grant that is offered by the German Federal Ministry of Economic Affairs and Energy and which provides funding for exactly one year. Main purpose is to incentivise graduates build their own start-up, so as a vehicle it is not fitting exactly to our case but is always offering an option, though a rather suboptimal one.

6.2.2 Sales experience within the consortium

Though it is good to identify this as a risk, it should be noted that the consortium exhibits a rather high degree of competence in sales and also in what actually reflects the case of CS-AWARE in terms of pre-Sales expertise.

We mention only that partner OTS is one of the most successful vendors for solutions in LPAs in Greece, while ex-Ancitel and now CESVITER staff have good knowledge of the Italian market as well. Same applies at the corporate level for 3rdplace and at the individual levels for CS-AWARE team members from CARIS, Wise & Munro, PERACTON and UNI PASSAU.

What we actually see as a risk is the lack of mobilising the various partners' resources so that in an organised and sufficiently orchestrated way to create the necessary momentum.

6.2.3 Lack of securing funding for a spin-out

This relates partly to what we mention in 6.2.1 above. What we see as an option here is to employ the Fast Track to Innovation pilot as an alternative means to develop the CS-AWARE market. In this case, and taking into account the nature of FTI pilots, we would reduce the participation in this new scheme we might have as partners:

1. the University of Oulu as representative of the interests of the CS-AWARE consortium and the owner of the CS-AWARE platform,
2. one of the industry partners in CS-AWARE e.g. 3rdplace as CS-AWARE platform provider, who shall be responsible for the maintenance of the platform and its upscaling to meet needs of a future customer installed base,
3. maximum a number of 3 early customers that will use the solution, based on good practices devised within the CS-AWARE project lifetime with our pilot partners Roma and Larissa.

The latter may be also not end users like an LPA but umbrella organisations like an Association of LPAs of a particular region in an EU member country, or at a pan-European level such as the case of the Council of European Municipalities and Regions (CEMR) that represents the interests of Europe's local and regional governments and their associations.

6.2.4 Role of Larissa and Rome after the project finishes

There is no doubt that it would provide us with a good 'seed capital' to have Roma and Larissa paying for having access to the CS-AWARE solution. However, there are two things that have to be taken into account:

1. As contractual partners of the project, they may have the same good reasons to have access to the project outcomes for free. Of course, the case of payment may relate to costs incurred as

result of a services provision from other partners or the CS-AWARE spin-out, so all in all it might still make good sense that Roma and Larissa pay for services after the project finishes but for the access to services and *not* for the access to the solution.

2. However, the most important asset that Roma and Larissa can bring to the post-project commercialisation are their networks and contacts to other municipalities in Greece. In this respect, they might both save the payment costs to the access to services by helping us acquire new customers, while it is not impossible at all that both Roma and Larissa might be able to have revenues from their involvement in the expansion of the CS-AWARE user base.

6.3 IPR/Legal/Ethical risks

No change from version V1.0

6.4 Regulatory Risks

It was identified that GDPR (General Data Protection Regulation) implemented on May 25th, 2018 could create some regulatory risks for the CS-AWARE technology execution, if not correctly followed and implemented. However, the risk here resides only in not observing correctly the GDPR regulation requirements and implementing them rather than set-up and model execution incompatibilities. Currently there is an ongoing GDPR compliance and procedures review done by University of Vienna. Once concluded it will be added to this section in the next deliverable version.

7 Commercial actions

As mentioned in the previous deliverable, this update is focusing on concrete commercial actions done by consortium members as follows:

Wise & Munro:

Wise & Munro is planning to liaise with a number of organisations in the Netherlands, at national level, who are involved in cybersecurity. The first one is the NCSC (National Cyber Security Center) from the Ministry of Justice. Their platform invites for collaboration to increase digital resilience (https://www.ncsc.nl/english/cooperation). Also, the company has already established good contacts with ICTU, the national think-tank and advising center for technology in government. They organise regular meetings on various topics (e.g. https://www.ictu.nl/evenementen/ictu-cafe-13-november). Both contacts will be more elaborated when demos will be produced.

Wise & Munro also contacted the IBD (Intelligence Safety Service), which is linking municipalities around cybersecurity issues. Their role is to interface between proposed solutions and the municipalities, so they can be an important contact. They responded that the state of knowledge of most municipalities is not yet up for international exchange at this stage. A contact will be made again at the beginning of piloting activities (https://www.informatiebeveiligingsdienst.nl).

Furthermore, Wise & Munro have included (anonymously) an example analysis of stories from one of the pilot sites, in a book on collaboration that was written and completed recently. The analysis serves as an example of technology that actually requires collaboration in order to manage the issues that are caused by using technology.

Peracton ltd,:

Peracton had a series of f2f meetings in London and Paris during Q4 2018 and Q1 2019 with companies in the finance and banking space that represent Peracton's market. These were introductory meetings where the CS-AWARE concept platform was presented and the main ideas highlighted. While no demonstration was made as no prototype was available for this period, the discussions were aimed towards understanding the cyber-security requirements, needs and appetite of solutions within the banking and financial industry. The meetings in London were with Browns Brother Harriman, MAN AG, EzeCastle, Citi and Credit Suisse. In Paris there were f2f meetings with ATOS and Mastercard. Also Peracton attended FintechConnect2018 event in London where discussions on site with various companies were imitated. From all this early stage discussions it appeared across companies the obvious interest in advanced cybersecurity solutions, not only for their own business but also for solutions to encompass and monitor their relation with their clients or, for their clients needs too. It has been agreed to continue discussions once there is a demonstrable CS-AWARE software. Finally, Peracton was driving the open source initiative for developing the STIX2.0 Java library in GSON that was delivered in January 2019 and made available on github. https://github.com/cs-aware/stix2

University of Passau:

University of Passau has established in collaboration with the City of Passau INN.KUBATOR an incubator for new businesses (start-ups) (https://www.innkubator.de). As of today, the main focus has been in the support of graduates of the university to bring their ideas into action and help them finance their first year of operations through the use of some appropriate entrepreneurship support initiatives like the EXIST-Gründerstipendium (https://www.exist.de/DE/Programm/Exist-Gruenderstipendium/inhalt.html). One working meeting has been held with the people of Inn.Kubator on 18 October 2018,where the CS-AWARE project was presented and worked together on some initial scenarios of how a common line of synergies could be developed that might be mutually beneficial for Inn.Kubator and for the UNI PASSAU CS-AWARE project team.

Currently and given the change that has taken place internally (now the project is under the Data Science Lehrstuhl of the University of Passau), new opportunities appear in the form of a repositioning of the main strengths and intellectual assets that can be provided from our side and on a continuing basis for any start-up that would come as result of the project and would involve members of the UNI PASSAU CS-AWARE project team. Of specific importance in this case will be the continuing access to technical know-how that the Data Science Lehrstuhl may provide for the start-up, under some agreement that would involve participation to a new company as a shareholder with a 10% or 15% from the side of the University of Passau. To this extend, there is no experience as of today . There is a need on know-how increase by means of getting in contact with other universities participating in the project (Oulu and / or Vienna) that have more experience, so that they will establish contacts with the respective departments or units (e.g. for technology Commercialisation, Entrepreneurship Support, etc.).

This might possible mean that the initial focus of the project only to local public administrations (LPAs) may change to include also other business focus areas such as the Internet of Things with its ever increasing number of internet-connected devices, possing substantial threats to cybersecurity. .Additionally consideration should rise on how CS-AWARE technologies may respond to needs stemming from the dissemination of cybercrime-as-a-service business models as enabler for crime and significant challenges (: threats) to security.

Municipality of Larissa:

The Municipality of Larissa, as pilot of the CS-AWARE program, will use it in order to be aware of potential threats against its data and to take the necessary precautions. However, cyber-attacks are threatening with the same dangerous way smaller LPAs that are offering equivalent services and administrate personal data (financial and identity data). These LPAs don't have the necessary staff, the infrastructure and the know-how to protect their systems and confront external as well internal "enemies".
The Municipality of Larissa as the biggest municipality in its region has already taken the initiative to communicate the CS-AWARE initiative. It participated in conferences-forums relevant to public administration and presented the progress that has been achieved. The Municipality of Larissa has allreadyinformed its"neighboring" smaller LPAs about the benefits that the implementation of the final product would bring to their organization. Furthermore, it could assist those smallest LPAs be prepared as future possible end users of the product. This includes helping them perform the necessary analysis of the existing infrastructure, the different software they are using, the flows and procedures that are executed during a citizen's transaction with the Municipality. This way it will be easier to detect possible vulnerabilities and "weak-points" of the systems.

Additionally, the Municipality of Larissa, keeping in mind the good connection with the educational institutions of its region (University of Thessalia, Technological Education Institution) can contribute to the engagement of the scientific community regarding CS-AWARE. By communicating the whole attempt, it is possible to attract the interest for further research and development as regards the protection against cyber-threats. Moreover, information data and statistics from our experience on the subject could be presented to IT Master courses of the aforementioned institutions. We could in this way awaken the students' interest and attention towards this direction.

CESVITER S.R.L.:

The following actions have been taken / are in progress:

- Working on establishing contacts with 1-3 regions like Campania and Toscana
- Working on identifying associations of municipalities and their administrators
- Discussions with a group of municipalities in the South
- Will seek to work with University of Salerno on possible integration of past European project "Route-to-PA"
- Will develop a mailing list and newsletter to propose for people interested and possibly even early adopters.

OTS SA:

The following actions have been made / are in progress, since the last report:

- Organization of two major conferences in Greece, with the participation of more than 80 different LPAs and more than 330 participants, upon which the CS-AWARE project was introduced
- A scheduled third conference (11th OTS Forum) in which the estimated number of participant LPAs will be in the area of 100 and a dedicated workshop on Cybersecurity & Data protection will take place
- Communications and meetings with 10 Greek municipalities where the CS-AWARE concept platform was presented the and the main ideas highlighted. A demo is expected
- Discussions with 2 municipalities & 2 public legal entities to become early adopters.

8 Conclusions and future work

There are two main 'modalities' that have not yet been utilised and the consortium shall concentrate its interest for the forthcoming second period of the project: the Demo and the Knowledge Repository areas under the project's official Website. For both the considerations are :

8.1. Demo

The idea is to offer in this section of the Website access to any interested party to have a *live* or a *pre-cast demo*. Both cases are worth to consider and also could be offered concurrently. More specifically, while a live demo might make sense for the case of a member of the project team or a member of the Marketing or Sales unit of one of the consortium members, offering access to functionality offered by the CS-AWARE system, it is also exhibiting some demands for prior training and familiarization with the features and the functionality of the system. This means that a live demo will be ideal for instance for a sales consultant from OTS that has a meeting with potential customers from an LPA like the municipalities of Veria or Katerini in Greece. For this only a prior course for the use of the system would be required since and the access codes (user name and passwords) to enter their individual demo 'showroom'. This can be customized not only for the language aspects, but also for some predefined scenarios, but at the same time leaving space for the sales consultant to customise the demo to the needs of the potential customer.

For pre-cast demos, alternative options of short videos that provide answers to anyone interested are considered, spanning from an overall presentation of the CS-AWARE concepts, to more specific presentations on how certain threats are recognised and 'neutralised'. The risk with videos are that though they are expected to be informative, usually they end up providing unworthy information , offering very little or actually negative value to the subject they present. For this, a concept that has to avoid these 'elementary' mistakes is of an imperative importance assisting people understand the concepts and the value the solution offers. In discussions with members of the Marketing and Media departments of the participating companies and the universities respectively, it was clear that these videos should not last for more than 5 minutes, while ideally, they may not need more than 3 minutes to provide answers in a FAQ-like fashion e.g.

- "What is a cyberthreat for an LPA?",
- "How can an LPA protect itself from a cyberthreat?",
- "How does CS-AWARE technology work?",
- "How can we use the CS-AWARE technology in our LPA?",
- "How much will the CS-AWARE technology cost to us?",

- ...

Answers to the above questions should be informative and not open-ended, as in the latter case will be anything than convincing or motivating for future potential customers.

8.2. Knowledge Repository

The knowledge repository is - same as the Demo section - still one of the inactive parts of the CS-AWARE Website. It is the consortium's intention to populate the knowledge repository with all necessary information that might be of use to the various people who will be engaged in the future market development and exploitation activities. This means that not only business-relevant information has to be included, but also technical information that will help the different parties involved in a purchase to get access to all necessary information. It should be mentioned that no information included in the knowledge repository will be of confidential nature, so no data sets or other content that might raise issues related to privacy or ownership will be included. The main role of the repository is to act as a complimentary source of content to the demo.

Both the demo and the knowledge repository are planned to become operational on 1st October 2019. A first preliminary version, however, of the functionality and the features and the content to be communicated will be ready for discussion by 1st of June 2019.

References

eSecurity Planet, Eight Top Threat Intelligence Platforms, accessed 22/02/2019 https://www.esecurityplanet.com/products/top-threat-intelligence-companies.html

http://www.ecs-org.eu/documents/uploads/the-ecso-cybersecurity-market-radar-high-resolution.pdf

new EU cybersecurity act: https://www.openaccessgovernment.org/europes-cybersecurity-act/55598/

Europol Internet Organised Crime Threat Assessment 2018: https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018