SPARTA

D10.6

Commercial Deployment Plan

Project number	830892
Project acronym	SPARTA
Project title	Strategic programs for advanced research and technology in Europe
Start date of the project	1st February, 2019
Duration	41 months
Programme	H2020-SU-ICT-2018-2020

Deliverable type	Report
Deliverable reference number	SU-ICT-03-830892 / D10.6 / V1.0
Work package contributing to the deliverable	WP10
Due date	April 2022 – M39
Actual submission date	29th April, 2022

Responsible organisation	LEO
Editor	Claudio Porretti
Dissemination level	PU
Revision	V1.0

Abstract	This deliverable is a report exploring ways to promote results from SPARTA for commercial deployment
Keywords	Commercial, Exploitation, Stakeholders, Sustainability, IPR, Market, Cyber Security

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 830892..

Editor

Claudio Porretti (LEO)

Contributors (ordered according to beneficiary numbers)

Sebastien Dupont (CETIC)

Martin Zadnik (CESNET)

Mark Ohm (UBO)

Paula Cecilia Fritzsche (EUT)

Mauro Gil Cabeza (IND)

Cristina Martinez (TEC)

Luca Verderame (CINI)

Artsiom Yautsiukhin (CNR)

Šarūnas Grigaliūnas (KTU)

Filipe Apolinário (INOV)

Reviewers (ordered according to beneficiary numbers)

Christophe Slim (CEA)

Armands Meirāns (LMT)

Executive Summary

This deliverable is a report exploring ways to promote results from SPARTA for commercial deployment.

First of all, an overview of the Cyber Security market (based on recent Gartner study) is described in order to provide a reference for a commercial development plan.

Then, the CANVAS business model is introduced, as considered the more suitable business model to use in case a future commercial deployment of products development in a research project such as SPARTA.

It was asked to prototype/tools owners developed in SPARTA programs to fill the Canvas one-page view related to their products.

The result is a number of synthetic business plans that gives a clear idea of how prototypes/tools developers intend to approach a future commercial deployment of their products.

Table of Content

Chapter 1 Introduction 1
1.1 Scope and Document structure 1
1.2 The SPARTA project 1
Chapter 2 Cyber-Security Market Overview 2
2.1 Introduction 2
2.2 Market trend by segment 2
2.3 Market trend by sub-segment 3
Chapter 3 Commercial Plan for SPARTA results 4
3.1 Generalities [3] 4
3.2 The CANVAS business model 4
3.2.1 Introduction 4
3.2.2 The nine building blocks of the Canvas model 6
3.2.2.1 CS - Customer Segments 6
3.2.2.2 VP – Value Proposition 6
3.2.2.3 CH - Channels 7
3.2.2.4 CR – Customer Relationship 7
3.2.2.5 R$ – Revenue Streams 7
3.2.2.6 KR - Key Resources 8
3.2.2.7 KA - Key Activities 8
3.2.2.8 KP - Key Partnership 9
3.2.2.9 C$ - Cost Structure 9
3.3 The CANVAS model applied to SPARTA prototypes and tools 9
3.3.1 Virtual Control Room 11
3.3.2 DDoS backscatter traffic detection 12
3.3.3 Match2FuzzyGroups 13
3.3.4 BP-IDS business process intrusion detection system 14
3.3.5 Business Impact Assessment 15
3.3.6 FingerICS 16
3.3.7 Anticipation of cyber-physical attack on Transport CII 17
3.3.8 Network flow-based threat intelligence 18
3.3.9 Vacsine 19
3.3.10 OpenCert 20
3.3.11 Sabotage 21
3.3.12 Approver 22
3.3.13 SATRA 23
3.3.14 Buildwatch 24
Chapter 4 Summary and Conclusion 25
Chapter 5 List of Abbreviations 26

Chapter 6 Bibliography 28

List of Figures

Figure 1: WW Cyber Market End user spending by segment 3
Figure 2: Canvas model representation 5
Figure 3: Canvas model one-page view 5

List of Tables

Table 1: WW Cyber Market by sub-segment 3

Chapter 1 Introduction

1.1 Scope and Document structure

The aim of this document is to explore ways to promote SPARTA results for commercial deployment purposes.

The document is structured in the following way:

- In this section, a brief description of the SPARTA project is provided.
- Chapter 2 gives an overview of Cyber Security Market
- Chapter 3 describes the business model adopted for commercial plans of SPARTA results and its application to prototypes and tools developed in SPARTA programs T-Shark and CAPE
- In Chapter 4, conclusions are reported
- Chapter 5 includes the abbreviation table
- In Chapter 6 is reported the bibliography

1.2 The SPARTA project

The aim of the SPARTA is to brings together a unique set of experts at the intersection of scientific excellence, technological innovation, and societal sciences in cybersecurity.

The main objective of the project is to create a networked governance for advanced cybersecurity research in Europe, defining and sustaining an EU-wide roadmap at the cutting-edge of cybersecurity research and innovation.

The following four programs are part of the SPARTA project:

1. **T-SHARK** *(Establish a Full-Spectrum Cybersecurity Threat Intelligence Framework by developing comprehensive solutions based on novel technology developments and cross-disciplinary breakthroughs)*
2. **CAPE** *(Continuous Assessment in Polymorphous Environments)*
3. **HAII-T** *(Developing a foundation for secure-by-design Intelligent Infrastructure built on strong formal approaches)*
4. **SAFAIR** *(Investigate approaches to make systems using Artificial Intelligence more reliable and resilient)*

Most of the outcomes of the above programs are prototypes used for demonstrating specific and relevant use cases. They can be exploited in term of commercial deployment.

The following section gives an overview of the actual Cyber-Security market that has to be taken as reference for commercial deployment aspects.

Chapter 2 Cyber-Security Market Overview

2.1 Introduction

The analysis of the cyber security market for 2021-2025 refers to the Gartner Group studies for the civil market [2].

Cyber security market is split into HW and SW products and services, which can be further broken down into:

- HW and SW products aimed at securing a phase of the data transmission chain; include products for network security (transmission), cloud security (storage and processing), identity access management (access control), data security (encryption), application security (security testing SW and vulnerability assessment SW);
- HW and SW products to manage the entire governance process; include Infrastructure protection (SIEM SW, Threat intelligence SW, End point protection SW) and Integrated risk management SW;
- Professional consulting services: advisory, assessment and support services to improve resilience and understanding of risks or to analyse incidents.
- Design & build (Implementation) services: customized services to develop IT security solutions, assets and processes (including cyber security training);
- Outsourced security services, which include both Security Operations - on Premise and MSS (Managed Security Services) - via SOC Provider.

2.2 Market trend by segment

Civilian market analysts predict that the enterprise cyber market (excluding consumer market) will continue to have two-digit growth (CAGR 21-25 at 10.6%), starting from around 147bln$ in 2021 to reach almost 220bln$ at the end of the period.

The market is initially divided almost equally between services component and product component; subsequently the trend is different.

Compared to a few years ago, in fact, the products component grows more (around 13%) while services grow at 7.8%. This trend is linked to the fact that some product sub-segments have a particularly positive trend driven by new technological trends (such as cloud security).

The service component sees a very positive trend (about 10.5%) for consultancy services and a slight slowdown for managed services (about 7%), which shows two different trends between management evolved via SOC and in MDR (Managed Detection and Response) and more traditional security operations.

The trend of each segment for the five-year period 2021-2025 is shown below.

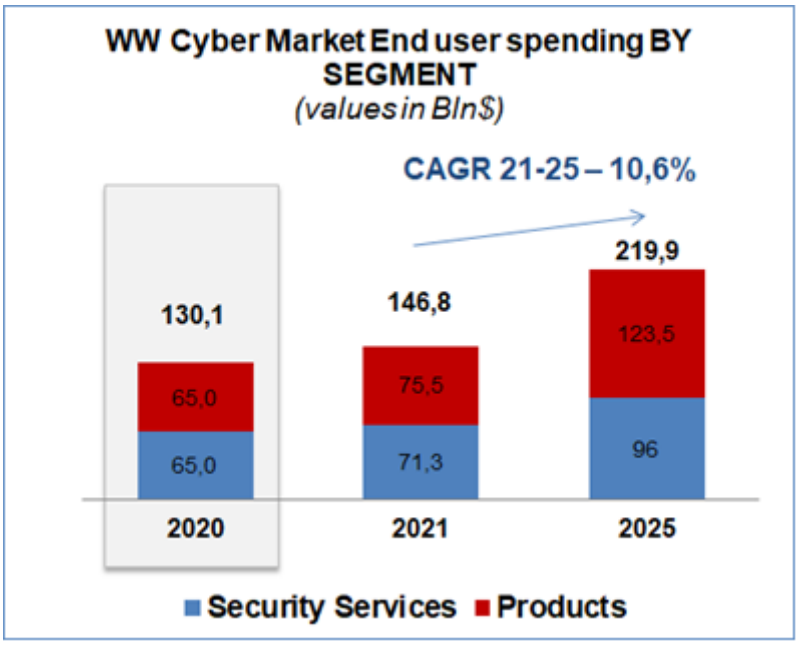


Figure 1: WW Cyber Market End user spending by segment

2.3 Market trend by sub-segment

The market for cyber security products and services is further split into sub-segments shown in the table below:

PRODUCTS	2021 Bln$	CAGR 21-25	Sub-segment
Cloud Security	1,0	32,8%	Cloud Access Security Brokers Software
Infrastructure Protection	25,8	14,6	Endpoint Protection Platform (Enterprise) Software
			Secure E-mail Gateway Software
			Secure Web Gateway Software
			Security Information and Event Management (SIEM) SW
			Threat Intelligence Software
Data Security	3,5	12,9%	Encryption Software
			Enterprise Data Loss Prevention Software
			Tokenization Software
Identity Access Management (IAM)	15	14%	Access Management Software
			Identity Governance and Administration Software
			Privileged Access Management Software
Integrated Risk Management	5,4	7,2%	Integrated Risk Management Solutions Software
Application Security	5,2	23,2%	Application Security Testing Software
			Vulnerability Assessment Software
			Web Application Firewalls Software
Network Security	17	6,9%	Firewall Equipment
			IPS Equipment
Other Information Security SW	2,6	7,5	Other Information Security Software

Table 1: WW Cyber Market by sub-segment

Chapter 3 Commercial Plan for SPARTA results

3.1 Generalities [3]

When companies intend to launch a new product into the marketplace, a commercial plan is needed in order to ensure the planning of operations able to manage distribution and consumer feedback.

Business plans usually include strategic management or planning that involves setting a goal, implementing the strategy, analyzing the business environment, and reviewing the process after it has been implemented.

Business plans are used by companies to help them in creating efficient product placement on the market. Obviously, the plans may require changes before or during the implementation process in order to ensure the company to maximize the sales of released products.

The main inputs for a SPARTA commercial Plan derive from Cyber Security Market overview (reported in Chapter 2). and exploitation KPI's gathered from SPARTA work packages.

Considering that the SPARTA project is categorized as a Research and Innovation Action (RIA) so that results such as prototypes have a maximum TRL of 6[1].is not feasible develop at this stage of readiness level, detailed Busines Plans.

The best way to give an idea of how some SPARTA results can be framed within the perspective of business development, is to adopt the CANVAS busines model, that is a strategic management template that offers a visual chart with nine building blocks in a one-page view.

The following section describes all the segments that compose the CANVAS model.

Then, in section 3.3 the CANVAS model will be applied to SPARTA results that could have future commercial development, i.e. prototypes and tools coming from SPARTA programs T-Shark and CAPE.

3.2 The CANVAS business model

3.2.1 Introduction

Proposed by Alexander Osterwalder's best seller "Business Model Generation", the concept of business model is described as the architecture with which a company creates, distributes and captures value.

The Business Model Canvas is a strategic model built on the logic of visual thinking, universally adopted to describe a business model in a simple and understandable way. Nine segments are highlighted that make up the building blocks of the business model in a one page view.

The business model concept describes the logic of how an organization creates, delivers and captures value (which can be economic, social or other forms).

The 9 blocks allow you to visualize and imagine the constituent elements of each Business Model.

[1] TRL 6: "System / subsystem model or prototype demonstration in a relevant environment"

The following picture gives an idea of what is represented in the Canvas model:

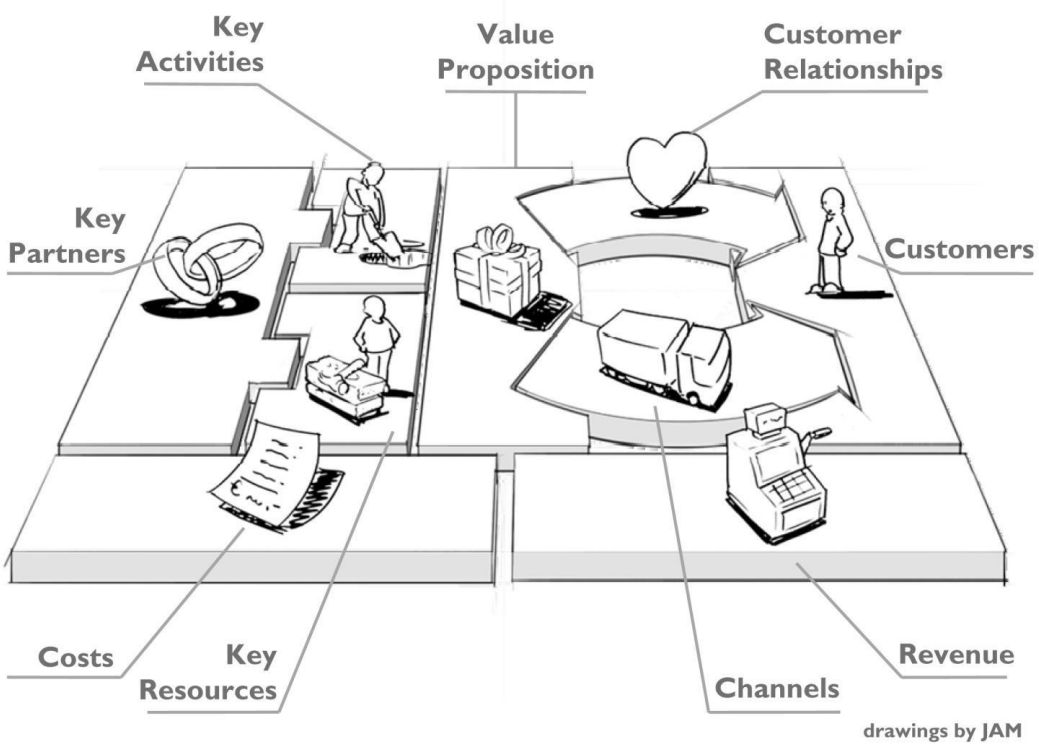


Figure 2: Canvas model representation

while the next picture shows the one-page view of the canvas model

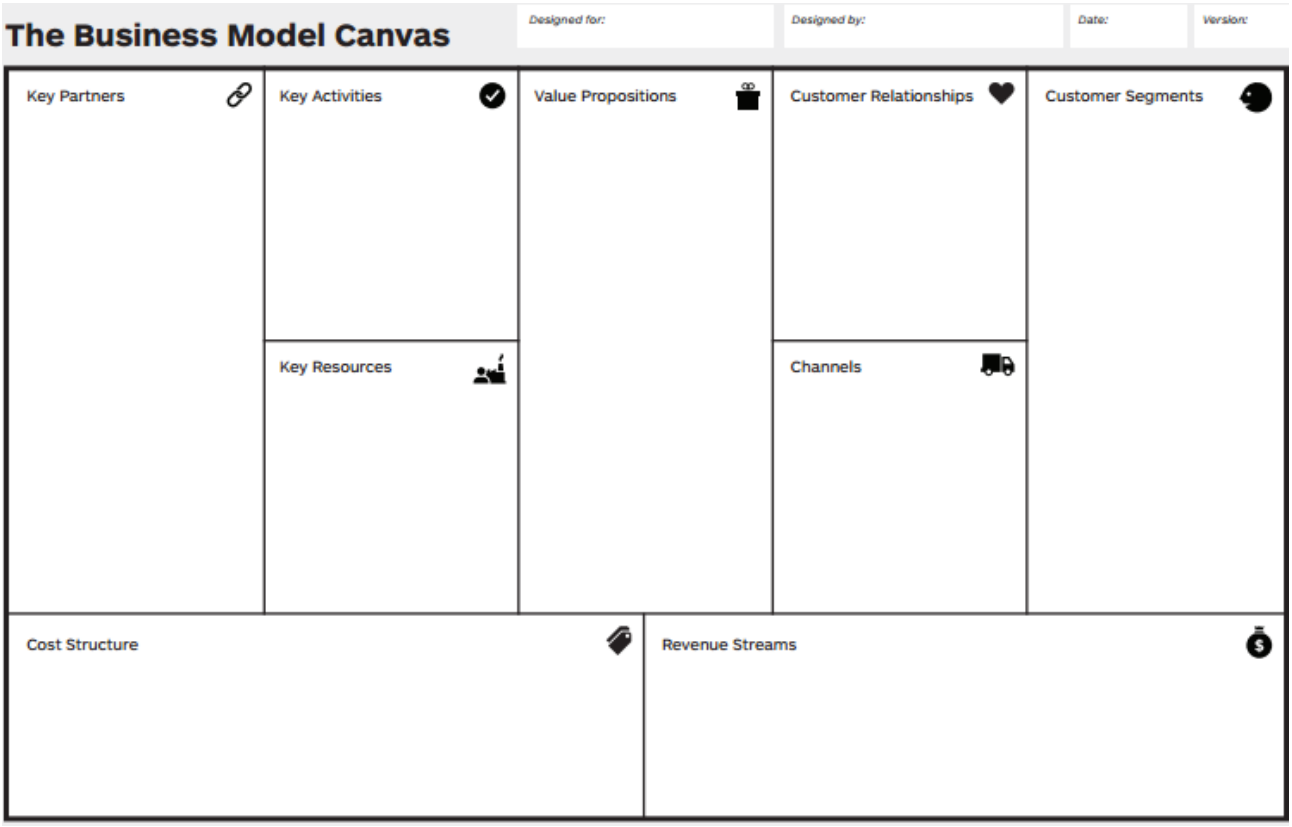
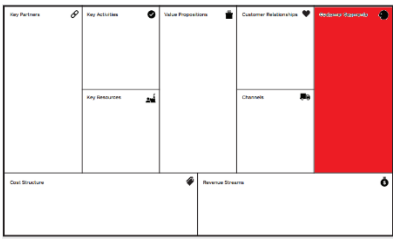


Figure 3: Canvas model one-page view

The following sections describe the nine blocks that forms the Canvas one-page view.

3.2.2 The nine building blocks of the Canvas model

3.2.2.1 CS - Customer Segments

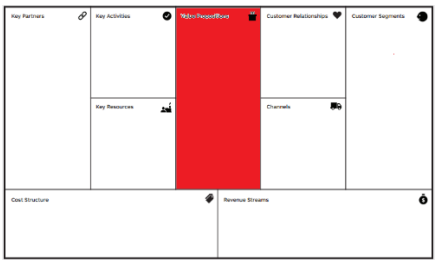


The block of Customer Segments is used to describe the classes of people and organizations with which the company deals.

A customer segment can be related to psychographic factors such as consumption habits, common needs and interests. or through demographic data (age, ethnicity, sex, etc)..

Customer profiling is a key element to plan the market analysis and, consequently, to create a winning business plan: clarifying customer needs allows you to develop a package of targeted products and services, to identify distribution channels more profitable and to direct the company towards the type of market in which it intends to position itself.

3.2.2.2 VP – Value Proposition



The Value Proposition represents the value of products and services that the company promotes and is based on the tangible benefits for a particular customer segment.

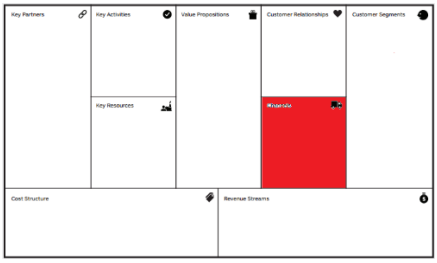
It can be considered the reason why the customer should prefer the company over the competition and, therefore, determines its own sales force. There is no unique way to create a good value proposition.

It may be an innovation, that is, offering customers something revolutionary, a price reduction that results in economic savings, or an improvement in the design and performance of a product. In any case, the customer is the real protagonist, together with his well-being and the satisfaction of his functional, emotional and social needs.

The following elements can contribute to customer Value Creation:

- Newness,
- Performance,
- Customization
- Design,
- Brand,
- Price,
- Accessibility,
- Convenience/Usability
- Reduction of costs,
- Reduction of Risks,

3.2.2.3 CH - Channels



Channels Building Block indicates the ways in which the value proposition can reach the customer. They involve communication, distribution and sale phases.

The company uses channels to inform potential buyers of the existence and value of its products, to make them accessible and allow their purchase and to ensure adequate after-sales assistance.

The channels can be direct, i.e. owned by the company, or indirect (for example, official distributors and partner stores).

3.2.2.4 CR – Customer Relationship

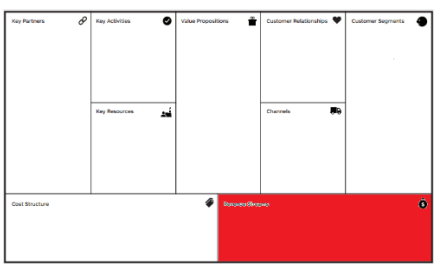
Customer Relationships block describes the type of relationships the company establishes with its customers. This form of communication helps the company to acquire new customers and retain existing ones and is therefore an essential part of a business plan that works.

Questioning the interaction with your target helps to clarify what type of relationship is being built, to support the customer experience and to strengthen the company's image on the market.

Several categories of Customer Relationships may coexist in a company's relationship with a particular Customer Segment:

- Dedicated Personal Assistance;
- Self-service;
- Co creation;
- Automated services;
- Communities.

3.2.2.5 R$ – Revenue Streams



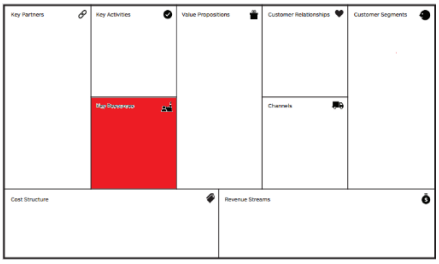
The Revenue Streams block describes the proceeds that the company obtains from the sale of products or services to a specific customer segment.

Payment methods and prices (fixed or dynamic) are the two fundamental aspects that concur to make the business model sustainable. The revenue streams can be of different nature and be generated from varied sources:

- Usage fee,
- Subscription fees,
- Asset sale,
- Licensing,
- Brokerage fees,
- Lending, Renting, Leasing,

In this phase, it is possible to identify the payment system preferred by customers, as well as the added value for which the target is willing to pay.

3.2.2.6 KR - Key Resources



In the Key Resources Building Block are listed the resources a company makes available to run its business. They can be physical (i.e. points of sale, plants, machinery), human (company workforce), intellectual (licenses, software, copyrights) and financial (lines of credit, loans, cash).

The aim is to identify the most effective resources in creating a specific value proposition for a specific customer segment.

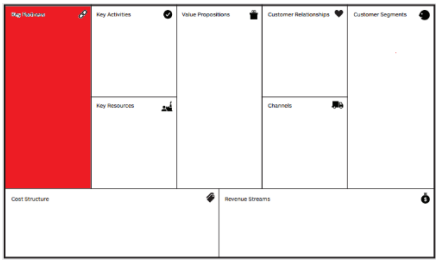
3.2.2.7 KA - Key Activities

The Key Activities block includes the activities that are necessary for a value proposition. These are accompanied by the most efficient processes to reach the target, maintain relationships with customers and, of course, generate revenues.

The categories of key activities can be distinguished as follows:

- Problem solving
- Production
- Platform
- Network

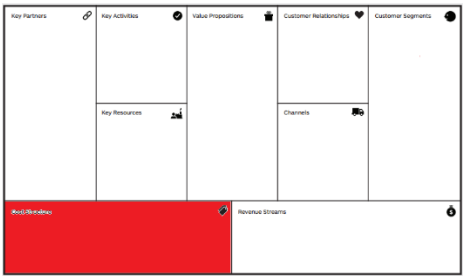
3.2.2.8 KP - Key Partnership



The Key Partners block is populated by the network of suppliers and partners with which the company collaborates to create value to offer to the customer.

A company, in fact, is not a self-sufficient structure, but rather a system that acts within a broader context, supported by external actors. Establishing strategic alliances responds to the company needs to reduce costs, reduce competition risks and acquire particular resources and activities.

3.2.2.9 C$ - Cost Structure



The Costs Structure block defines the fixed and variable costs that the company incurs for activities resources and key partners. For some types of businesses, limiting expenses becomes a central aspect, especially if one of the objectives of the business plan is to keep their prices competitive.

The two main categories of a cost structure are represented by fixed costs (for example, rents and salaries) and variable costs.

The cost structure is dependent on the volume of goods and services produced. In any case, the central objective is to ensure that revenue streams exceed expenses: only in this way can the business be truly sustainable.

Other than Fixed costs, and Variable costs a Cost Structures must take into account the Economies of scale and the Economies of scope.

3.3 The CANVAS model applied to SPARTA prototypes and tools

In following paragraphs some SPARTA partners that developed prototypes in T-Shark program and Tool for certification and validation purposes in CAPE program, have filled the one-page CANVAS view in order to give an idea how their prototypes/tools could have a commercial deployment in the near future after the end of the SPARTA project.

The following prototypes have been analysed, coming from T-Shark program (WP4):

- **Virtual Control Room** (LEONARDO) : This prototype aims to propose a Virtual Control Room that provides situational awareness for the cyber/ physical protection of critical infrastructures, providing operators with a virtual interface. The core system is based on an OSINT platform that will try to identify vulnerabilities and malware related to the protected

critical asset. The information will be captured in real-time and it will be available to the operator in the virtual environment for analysis.

- **DDoS backscatter traffic detection** (CESNET): This prototype aims to propose an approach for DDoS backscatter traffic detection that can be utilised to improve the situational awareness for national CSIRT/CERTs and stratcom units, allowing them to correlate relevant information with other information sources and create a comprehensive view on large hybrid campaigns as early as possible.
- **Match2FuzzyGroups** (EURECAT): This prototype provides intelligence / knowledge in relation to the potential groups (or group) that may be carrying out a certain attack, novelty of connecting MITER ATT&CK with machine learning, convenience of supporting the decision-making process and attribution of attacks.
- **BP-IDS business process intrusion detection system** (INOV): this prototype provides Cyber-physical incident detection, control processes monitoring of Quality of Service, Customer-specific reporting
- **Business Impact Assessment** (INOV): This prototype provides identification of critical threat propagation on an infrastructure, reporting analysis into CTI platforms, threat propagation analysis, Cyber-threat propagation Reports
- **FingerICS** (INOV): This prototype provides automatic security specifications for identifying cyber-physical incidents, automatic modelling of security policies using understandable business process modelling techniques
- **Anticipation of cyber-physical attack on Transport CII (INDRA**): Considering roads as a critical transport infrastructure, this prototype provides Cybernetic Situational awareness about non-authorised accesses, monitoring of communication (reading and writing attempts), detection of non-authorised permissions
- **Network flow-based threat intelligence** (KTU): This prototype aims to design a network flow-based threat intelligence method for multidimensional visual analytics system. By continually refining network flow-based methods, threat-related data can be identified, and can be used to anticipate technical threats and generate proactive solutions.

and the following tools coming from CAPE program (WP5):

- **Vacsine** (CETIC): open-source security orchestration, automation and response tool that provides adaptive security for distributed systems. It relies on continuous monitoring of Cloud and Edge systems to define, evaluate and apply automated countermeasures such as firewalls, intrusion detection systems, honeypots or quarantining.
- **OpenCert** (TECNALIA): is an assurance/certification management tool to support the compliance assessment and certification of Cyber- Physical Systems (CPS) spanning the largest safety and security-critical industrial markets, such as aerospace, space, railway, manufacturing, energy and health.
- **Sabotage** (TECNALIA): is a model-driven and simulation-based fault injection tool to accomplish an early evaluation dependability evaluation of safety-critical systems. It can be used in different areas such as automotive or robotics.
- **Approver** (CINI): is an automatic toolkit for the in-depth, fully automatic security analysis of mobile applications. It automatically detects, evaluates and provide comprehensive reports explaining the security risks hidden in the mobile applications
- **SATRA** (CNR): provides a simplified way to conduct risk assessment for a software product to be developed. Using SATRA the analyst may: plan security approach for the software; evaluate different security configurations/strategies; estimate the risk of the final product
- **Buildwatch** (UBO): monitors the build, test, and install processes on an operation system call level. detecting malicious software components.

3.3.1 Virtual Control Room

<table>
<tr><th colspan="2" rowspan="2">Business Model Canvas</th><th>Designed for:</th><th>Designed by:</th><th>Date</th></tr>
<tr><th>Virtual Control Room (VCR)</th><th>Leonardo</th><th>27/10/2021</th></tr>
<tr><td>Key Partners

CERT teams</td><td>Key Activities

Development of virtual interfaces

OSINT tool integration

Key Resources

Cyber experts

OSINT platform</td><td colspan="2">Value Propositions

Virtual Control Room provides situational awareness for the cyber/physical protection of a critical infrastructure, providing operators with a virtual interface.

It is based on an OSINT platform able to identify vulnerabilities / malware related to the protected critical asset.

VCR allows remote access by a Virtual Operator allowing him to use all the tools that he would have in the physical structure and support physical operators, making video calls in order to provide remote assistance on specific security issues.</td><td>Customer Relationships

Customer support and training

Channels

Workshops / Demonstration sessions

Web</td><td>Customer Segments

Security Operation Centres who need to create a remote control room.

CERTs that needs to give remote assistance to Physical Operators.

Critical Infrastructures</td></tr>
<tr><td colspan="3">Cost Structure

• Training
• Support
• Licence</td><td colspan="2">Revenue Streams

Usage fee, Subscription fee, Training</td></tr>
</table>

3.3.2 DDoS backscatter traffic detection

<table>
<tr><th colspan="2" rowspan="2">Business Model Canvas</th><th>Designed for:</th><th>Designed by:</th><th>Date</th></tr>
<tr><th>DDoS backscatter traffic detection</th><th>CESNET</th><th>11.10.2021</th></tr>
<tr><td rowspan="2">Key Partners

Key third party components:
• GeoIP database
• Whois service</td><td>Key Activities

Network monitoring
Detection of backscatter
Enriching alerts
Reporting alerts into CTI platforms</td><td rowspan="2">Value Propositions

Situational awareness about DDoS attacks
Customer-specific reporting</td><td>Customer Relationships

Feedback about the data utility</td><td rowspan="2">Customer Segments

Governmental CERT
CSIRT teams</td></tr>
<tr><td>Key Resources

Large network backbone
Monitoring infrastructure
Analysis infrastructure</td><td>Channels

Workshops / Demontration sessions
Web</td></tr>
<tr><td colspan="3">Cost Structure

Reacting to users’ feedback
Management of users
Upgrade of server</td><td colspan="2">Revenue Streams

Public financing
Contracts about specific customizations and filtering of reported alerts</td></tr>
</table>

3.3.3 Match2FuzzyGroups

<table>
<tr><th colspan="2" rowspan="2">Business Model Canvas</th><th>Designed for:</th><th>Designed by:</th><th>Date</th></tr>
<tr><th>Match2FuzzyGroups</th><th>EURECAT</th><th>27/10/2021</th></tr>
<tr><td rowspan="2">Key Partners

CERT teams
Law Enforcement Agencies
Current partners (other sub-cases owners)
Strategic alliances between partners
Strategic alliances with complementary and non-competing organizations and companies</td><td>Key Activities

Research and development
Building of ML algorithms
MISP integration of components and algorithms
Problem solving</td><td rowspan="2">Value Propositions

Provide intelligence / knowledge in relation to the potential groups (or group) that may be carrying out a certain attack
Novelty of connecting MITER ATT&CK with machine learning
Convenience of supporting the decision-making process and attribution of attacks.</td><td>Customer Relationships

Customer support</td><td rowspan="2">Customer Segments

CERT teams
Law Enforcement Agencies
Universities</td></tr>
<tr><td>Key Resources

MITRE ATT&CK matrices (enterprise, mobile, ICS)
MISP Platform & Infrastructure
Analysts and cyber-security specialists for the generation of attack and threat models, providing the required data.</td><td>Channels

Eurecat channel
Partners’ channels
Providing post customer support</td></tr>
<tr><td colspan="3">Cost Structure

Development platform
MISP integration
R&D personal effort</td><td colspan="2">Revenue Streams

Contracts for services</td></tr>
</table>

3.3.4 BP-IDS business process intrusion detection system

<table>
<tr><td colspan="2" rowspan="2">Business Model Canvas</td><td>Designed for:</td><td>Designed by:</td><td>Date</td></tr>
<tr><td>BP-IDS business process intrusion detection system</td><td>INOV</td><td>22.11.2021</td></tr>
<tr><td rowspan="2">Key Partners
Key third party components:
• COTS sensors</td><td>Key Activities
Network and filesystem monitoring
Detection of cyber-physical attacks
Detection of physical anomalies
Enriching alerts
Reporting alerts into CTI platforms
Modelling of security policies using understandable business process modelling techniques</td><td rowspan="2">Value Propositions
Cyber-physical incident detection
Control processes monitoring of Quality of Service
Customer-specific reporting</td><td>Customer Relationships
1. Customer Acquisition – Pilot demonstration to show product capabilities
2. Customer Retention – Maintenance service
3. Boosting Sales (upselling) – workshops and continuous product improvement with added features</td><td rowspan="2">Customer Segments
Critical infrastructures</td></tr>
<tr><td>Key Resources
Infrastructure communications
Computer logs
Business critical operations and control process specifications</td><td>Channels
Workshops / Demonstration sessions
Academic conferences
Web</td></tr>
<tr><td colspan="3">Cost Structure
Deployment of BP-IDS on a critical infrastructure
Training of critical infrastructure operators to use BP-IDS
Documentation of BP-IDS
Maintenance service for BP-IDS
Case specific customisations needed for integration.</td><td colspan="2">Revenue Streams
Contracts with critical infrastructure owners on a yearly basis</td></tr>
</table>

3.3.5 Business Impact Assessment

<table>
<tr><td colspan="2" rowspan="2">Business Model Canvas</td><td>Designed for:</td><td>: Designed by:</td><td>Date</td></tr>
<tr><td>Business Impact Assessment</td><td>INOV</td><td>22.11.2021</td></tr>
<tr><td rowspan="2">Key Partners

None</td><td>Key Activities

Impact analysis and identification of critical process activities
Identification of critical threat propagation on a infrastructure
Enriching threat propagation visualization
Reporting analysis into CTI platforms
Modelling of threat propagation rules using understandable business process modelling techniques and logic programming</td><td rowspan="2">Value Propositions

Threat propagation analysis
Impact assessment
Cyber-threat propagation Reports</td><td>Customer Relationships

1. Customer Acquisition – Pilot demonstration to show product capabilities
2. Customer Retention – Maintenance service
3. Boosting Sales (upselling) – workhops and continuous product improvement with added features</td><td rowspan="2">Customer Segments

Critical infrastructures</td></tr>
<tr><td>Key Resources

Business critical operations and control process specifications
Infrastructure asset and cyber-threat inventories</td><td>Channels

Workshops / Demonstration sessions
Academic conferences
Web</td></tr>
<tr><td colspan="3">Cost Structure

Deployment of BIA on a critical infrastructure
Training of critical infrastructure operators to use BIA
Documentation of BIA
Maintenance service for BIA
Case specific customisations needed for integration.</td><td colspan="2">Revenue Streams

Contracts with critical infrastructure owners on a yearly basis</td></tr>
</table>

3.3.6 FingerICS

<table>
<tr><td colspan="2" rowspan="2">Business Model Canvas</td><td>Designed for:</td><td>: Designed by:</td><td>Date</td></tr>
<tr><td>FingerICS</td><td>INOV</td><td>22.11.2021</td></tr>
<tr><td>Key Partners

Key third party components:
• COTS sensors</td><td>Key Activities

Identification of critical operations on network communications

Automatic modelling of security policies using understandable business process modelling techniques

Key Resources

Infrastructure communications</td><td>Value Propositions

Automatic security specifications for identifying cyber-physical incidents</td><td>Customer Relationships

1. Customer Acquisition – Pilot demonstration to show product capabilities
2. Customer Retention – Maintenance service
3. Boosting Sales (upselling) – workhops and continuous product improvement with added features

Channels

Workshops / Demonstration sessions

Web</td><td>Customer Segments

Critical infrastructures</td></tr>
<tr><td colspan="2">Cost Structure

Deployment of FingerICS on a critical infrastructure

Training of critical infrastructure operators to use FingerICS

Documentation of FingerICS

Maintenance service for FingerICS

Case specific customisations needed for integration.</td><td colspan="3">Revenue Streams

Contracts with critical infrastructure owners on a yearly basis</td></tr>
</table>

3.3.7 Anticipation of cyber-physical attack on Transport CII

<table>
<tr><th colspan="2" rowspan="2">Business Model Canvas</th><th>Designed for:
Anticipation of cyber-physical attack on Transport CII</th><th>Designed by:
INDRA/IFT</th><th>Date
26.11.2021</th></tr>
<tr><td rowspan="3">Key Partners
Commercial team of Indra in the different geographies.
Communication and social media department.</td><td>Key Activities
Contact with potential clients, starting from current clients.
Proposition of prove of concept.
Execution of real-life demos.</td><td rowspan="3">Value Propositions
Increasing Cybernetic Situational awareness about non-authorised accesses.
Monitoring of communication (reading and writing attempts)
Detection of non-authorised permissions
Alerts to infrastructure operators
Reporting alerts into CTI platforms</td><td>Customer Relationships
Dedicated and personalized deployment for the client based in its expectations.
The solution should be configured based in the feedback provided by the operator after a proof of concept/demo.</td><td rowspan="3">Customer Segments
Public or private infrastructure operators in any domain: transport, energy, public administration, etc.</td></tr>
<tr><td>Key Resources
Transport (or other domain) infrastructure
Monitoring infrastructure
Analysis infrastructure</td><td>Channels
Dedicated meetings with current clients.
Participation in ITS (Intelligent Transport System) congresses
Social media publications.
Press releases.</td></tr>
<tr><td colspan="2">Cost Structure
Personnel cost for configuration and supporting actions
Cloud for hosting the solution.</td><td colspan="3">Revenue Streams
Contracts for services</td></tr>
</table>

3.3.8 Network flow-based threat intelligence

<table>
<tr><td colspan="2" rowspan="2">Business Model Canvas</td><td>Designed for:</td><td>Designed by:</td><td>Date</td></tr>
<tr><td>Network flow-based threat intelligence</td><td>KTU</td><td>30.11.2021</td></tr>
<tr><td rowspan="2">Key Partners

Key third party components:
• GeoIP location
• IP address of attackers and victims
• Risk - how risky is the target (1-10)
• Reliability - how reliable is the rating (1-10)
• Activity - what type of host is it
• Visualisation of cyber threats</td><td>Key Activities
• Count the risks in the information space.

Key Resources

Data visualization

Monitoring cyber threat activities

Analysis cyber threat activities</td><td rowspan="2">Value Propositions
• Network flow-based threat intelligence method for multidimensional visual analytics system
• Situational awareness about DDoS attacks
• Customer-specific reporting</td><td>Customer Relationship
• Integration with other analytical or data sharing systems

Channels

Workshops / Demonstration sessions

Web</td><td rowspan="2">Customer Segments
• Chief information security officer (CISO)
• Information and communications technology (ICT) officers
• Decision makers - forensics and digital analytics</td></tr>
<tr><td colspan="2">Cost Structure

Visual Analytics System Administration

Server maintenance

API integration</td><td colspan="2">Revenue Streams

Public financing

Free license</td></tr>
</table>

3.3.9 Vacsine

<table>
<tr><td colspan="2" rowspan="2">Business Model Canvas</td><td>Designed for:</td><td>Designed by:</td><td>Date</td></tr>
<tr><td>Vacsine</td><td>CETIC</td><td>28/10/2021</td></tr>
<tr><td rowspan="2">Key Partners
Integration with
• cloud/edge/IoT platforms (hypercloud, FOSS), PaaS platforms
• security services (firewalls, honeypots, antivirus, IDS, SIEM ..)
• use case providers (ex. industrial actors)</td><td>Key Activities
• maintain security services catalogue and support platforms integration through an “as a service ” model where updates are made available to customers</td><td rowspan="2">Value Propositions
Vacsine is an open-source security orchestration, automation and response tool that provides adaptive security for distributed systems. It relies on continuous monitoring of Cloud and Edge systems to define, evaluate and apply automated countermeasures such as firewalls, intrusion detection systems, honeypots or quarantining.
The automated response is triggered by changes to security requirements, indicators of compromise, incidents and vulnerabilities.
The efficiency and speed of countermeasures deployment is evaluated in automatically provisioned sandbox environments that shadow the target Cloud/Edge systems. Those sandboxes provide observability and scalability for the training and maintenance of security response strategies.</td><td>Customer Relationships
Freemium, product is FOSS with paying maintenance and operation service.</td><td rowspan="2">Customer Segments
• cloud/iot/edge solution providers
• Segments: ex. autonomous vehicles or smart industry manufacturers and operators</td></tr>
<tr><td>Key Resources
• software maintenance
• cloud resources for operation and maintenance (artifact repository)
• 3rd party security services licenses
• vulnerability and malware signature databases
• dissemination (ads, tech/doc writers)</td><td>Channels
• Research projects
• Whitepaper/publications
• Open Source available at GitHub: https://github.com/cetic/vacsine
• Showcase website/page
• IT security, edge, industrial events (marketing)</td></tr>
<tr><td colspan="3">Cost Structure
• development human resources - maintenance and operation + new integrations
• compute capacity (Cloud) - fixed baseline + variable needs for scaling purposes
• economy of scope: federated management service</td><td colspan="3">Revenue Streams
• maintenance - update software
• setup - in customer environment
• customization - ex. add 3rd party security service, integrate w/ bespoke customer solution
• tech support
Pricing model: subscription for maintenance and tech support, customization are b case by case basis.</td></tr>
</table>

3.3.10 OpenCert

<table>
<tr><td colspan="2" rowspan="2">Business Model Canvas</td><td>Designed for:</td><td>Designed by:</td><td>Date:</td></tr>
<tr><td>OpenCert</td><td>TECNALIA</td><td>04/11/2021</td></tr>
<tr><td>Key Partners

• Standards organisations
• Tool suppliers
• Manufacturers
• Integrators</td><td>Key Activities

• Development and maintenance of the platform.
• Technical support of the platform, for clients.
• Maintenance of the open source community.

Key Resources

• Software platform.
• Engineers for the development and maintenance of the platform.
• The OpenCert community</td><td>Value Propositions

• Introduce safety & security aspects in the early stages of product development to reduce costs.
• Introduce co-assurance of safety and security.
• Reduce efforts and costs of compliance management with identified standards.
• Reduce efforts and costs of safety & security assurance and certification.
• Reduce efforts to perform safety & security analysis.
• Re-use assurance results for product upgrades and re-certifications.
• Reduce the risk of new developments/certifications.</td><td>Customer Relationships

• Personal attention would be appropriate to facilitate the integration of OpenCert into customer processes.
• Another option is to use the OpenCert open source community for customer interaction.

Channels

• Workshops / Demonstration sessions
• Website
• Social media (Linkedin)</td><td>Customer Segments

• OEM
• Component suppliers (manufacturers)
• Integrators of safety-critical platforms
• Consultancy and service providers
• Tool vendors
• Legislators and Standardisation Groups</td></tr>
<tr><td colspan="2">Cost Structure

• Development and maintenance of the platform.
• Technical support for clients.
• Open source community support and management.</td><td colspan="3">Revenue Streams

• The platform is open source, but revenues are expected for:
  ○ Library of standards and architectural patterns
  ○ Platform customisation and maintenance
  ○ Premium functionalities.
• SaaS version for SMEs.
• OpenCert Premium version to be integrated with other tools (e.g. Papyrus and Cappela are two examples for the design of safety & security critical systems).</td></tr>
</table>

3.3.11 Sabotage

<table>
<tr><td colspan="2" rowspan="2">Business Model Canvas</td><td>Designed for:</td><td>Designed by:</td><td>Date:</td></tr>
<tr><td>Sabotage</td><td>TECNALIA</td><td>04/11/2021</td></tr>
<tr><td>Key Partners
ENISA (European Union Agency for cybersecurity)
Standardisation Bodies
Regulatory Bodies
Road Equipment Manufacturers
System Providers
System Integrators
Operators of Intelligent Transport Systems
Universities</td><td>Key Activities
Development and maintenance of the platform.
Platform technical support.
Key Resources
Physical: Hardware and office equipment
Intellectual: Matlab license, software
Human: engineers for developing, testing and maintenance, marketing specialists.</td><td rowspan="2">Value Propositions
Early safety assessment
High obserbability and controlability
Automatization of fault injection test</td><td>Customer Relationships
Direct and personal support
Channels
Workshops / Demonstration sessions
Website
Social media (Linkedin)</td><td rowspan="2">Customer Segments
Critical systems developers
OEM
Tier 1 and 2 Suppliers
Road Equipment Manufacturers
System Providers
System Integrators
Validation and verification engineers
Operators of Intelligent Transport Systems</td></tr>
<tr><td colspan="2">Cost Structure
Team
Development and maintenance of the platform.
Technical support for clients.</td><td colspan="2">Revenue Streams
Sale of software tool</td></tr>
</table>

3.3.12 Approver

<table>
<tr><td colspan="2" rowspan="2">Business Model Canvas</td><td>Designed for:</td><td>Designed by:</td><td>Date:</td></tr>
<tr><td>Approver</td><td>CINI-Talos</td><td>31/11/2021</td></tr>
<tr><td>Key Partners

• University
• Sales partners</td><td>Key Activities

• Marketing
• Development, maintenance, security and update of the platform

Key Resources

• Approver Platform
• Human resources:
  ○ Developers
  ○ Cybersecurity consultants
• Physical Resources:
  ○ Cloud infrastructure (for SaaS)</td><td>Value Propositions

Help clients to detect, reduce and solve cyber security risks in the field of mobile security</td><td>Customer Relationships

• Customer support
• User-friendly systems

Channels

• Website and Social Media
• Cybersecurity events
• Sales Teams</td><td>Customer Segments

• SMEs
• Public Sector
• App developers</td></tr>
<tr><td colspan="2">Cost Structure
• R&D
• Cloud Infrastructure
• Personnel</td><td colspan="3">Revenue Streams
• Premium Plans (Annual/Monthly Subscription Fees)
• Developer Plans
• Individual Scans
• VA/PT premium services</td></tr>
</table>

3.3.13 SATRA

<table>
<tr><td colspan="2" rowspan="2">Business Model Canvas</td><td colspan="2">Designed for:</td><td>Designed by:</td><td>Date:</td></tr>
<tr><td colspan="2">SATRA</td><td>CNR</td><td>20/01/2022</td></tr>
<tr><td>Key Partners

There are no essential resources and partners for SATRA to operate. An analyst (SATRA user) is assumed to be able to provide all required information.

SATRA may use verified/ measured values, instead of the ones declared by the analyst. In this case any “tool”/partner providing objectively verified information about implemented security features could be used (after some relations added to the SATRA’s matching database).</td><td>Key Activities

Connect and provide the required values.

Understand/identify/plan security practices (to be) applied

Evaluate the estimated level of possible losses per resource

Key Resources

Internet access (SATRA is a service)</td><td colspan="2">Value Propositions

SATRA provides a simplified way to conduct risk assessment for a software product to be developed (or just developed), re-using the expert knowledge. It helps the analyst (or software security engineer) to conduct risk assessment by answering a set of predefined (Common Criteria-based) questions and receive the estimated risk values per STRIDE threats. In short, our risk assessment method is quick, standardised, less effort- and knowledge demanding (than general risk assessment), and is based on the best practices for secure software development.

Using SATRA the analyst may: plan security approach for the software; evaluate different security configurations/strategies; estimate the risk of the final product.</td><td>Customer Relationships

None

Channels

We establish the channels with our customer segments by dissemination knowledge about SATRA through participation in projects, delivering dedicated presentations, and proving the SATRA service on-line to the wide public (to be done in the nearest future).</td><td>Customer Segments

The potential customers of SATRA are security software engineers, which should plan, manage and assess security of the developed software product.

SATRA does not focus on a specific segment of developed products and is more useful for “generic” type of the assessed software (since highly specialised products may require more specialised approach to risk assessment).</td></tr>
<tr><td colspan="3">Cost Structure

• There no specific costs for the customer to use our tool. The service is
• provided for free. The activities may require some time to understand the
• questions and provide the correct reply.</td><td colspan="3">Revenue Streams

• The service (SATRA) is free of charge.
• There could be some negotiation about possible payment if SATRA is
• more closely integrated with an external tool.</td></tr>
</table>

3.3.14 Buildwatch

<table>
<tr><td colspan="2" rowspan="2">Business Model Canvas</td><td colspan="2">Designed for:</td><td>Designed by:</td><td>Date:</td></tr>
<tr><td colspan="2">Buildwatch</td><td>UBO</td><td>16.11.2021</td></tr>
<tr><td rowspan="2">Key Partners

None</td><td>Key Activities

Maintenance and further development/research to make Buildwatch reliable in detecting malicious software components.</td><td rowspan="2">Value Propositions

Customers will get more insight into their software dependencies and hence increase the overall security of their product, eventually protecting their customers.</td><td>Customer Relationships

Maintenance and refinement of Buildwatch over the time (expensive). Possibly, operation of Buildwatch to be used as service (cheap).</td><td rowspan="2">Customer Segments

Companies that develop software based on third-party libraries that are not reviewed for security concerns (basically everyone).</td></tr>
<tr><td>Key Resources

Developers, researchers, and servers</td><td>Channels

Through GitHub (free) and GitLab (free). Can be easily integrated as CI job.</td></tr>
<tr><td colspan="3">Cost Structure

Main costs are for researchers and programmers to further refine the product.</td><td colspan="3">Revenue Streams

Buildwatch may be self-hosted (possibly licenced) or paid per usage (software as a service).

Currently, Buildwatch is open source and free.</td></tr>
</table>

Chapter 4 Summary and Conclusion

Based on the proposed busines model (Canvas), the partners that developed prototypes and tools during the SPARTA project have indicated in the one-page CANVAS view the main elements that can give an idea how their prototypes/tools could have a commercial deployment in the near future after the end of the SPARTA project.

Using the synthesis capabilities of the CANVAS view, it's quate easy understand which channels, segments and relationships they want to use to promote their products, which cost structure they have in mind, which revenue streams they aspect to have, in relation to key partner, key activities and key resources.

Of course, once their products will reach the correct TRL (8 or 9) that allows them to be commercially deployed, a more specific business plan needs to be worked out.

Chapter 5 List of Abbreviations

Abbreviation	Translation
AI	Artificial Intelligence
ADR	Alternative Dispute Resolution
CA	Consortium Agreement
CAGR	Compound Annual Growth Rate
CAPE	Continuous Assessment in Polymorphous Environments
CERT	Computer Emergency Response Team
CII	Critical Information Infrastructure
CNAP	Cybersecurity National Action Plan
CSIRT	Computer Security Incident Response Teams
Ct&eF	Cyber training & exercise Framework
DESCA	Development of a Simplified Consortium Agreement
ECSO	European Cyber Security Organisation
ENISA	European Union Agency for Cybersecurity
ENLETS	European Network of Law Enforcement Technology Services
EU	European Union
EUFPS	European Union's Foreign And Security Policy
GA	Grant Agreement
HARA	Hazard Analysis and Risk Assessment
HAII-T	High-Assurance Intelligent Infrastructure Toolkit
HW	Hardware
II	Intelligent Infrastructure
IoT	Internet of Things
IP	Intellectual Property
IPR	Intellectual Property Rights

Abbreviation	Translation
JRC	Joint Research Centre
JV	Joint Ventures
LEA	Law Enforcement Agencies
MDR	Managed Detection and Resp
MoD	Ministry of Defence
MoI	Ministry of Interior
MoJ	Ministry of Justice
NCC	National Coordination Centres
NDA	Non-Disclosure Agreement
NIS	Network and Information Security
R&D	Research and Development
RTO	Research and Technology Organisations
SAFAIR	Secure and Fair AI Systems for Citizen
SIEM	Security Information and Event Management
SME	Small Medium Enterprise
SOC	Security Operation Center
SPARTA	Strategic Programs for Advanced Research and Technology in Europe
SW	Software
TARA	Threat Assessment & Remediation Analysis
T-Shark	Establish a Full-Spectrum Cybersecurity Threat Intelligence Framework by developing comprehensive solutions based on novel technology developments and cross-disciplinary breakthroughs
UBO	Université de Bretagne Occidentale
WP	Work Package
WW	World Wide

Chapter 6 Bibliography

[1] Strategic Programs for Advanced Research and Technology in Europe (SPARTA) - (Proposal ID: 830892)
[2] Gartner: GG_Information_Security_Forecast_2Q21
[3] What is a Commercial Plan for a Business? - Osmond Vitez - September 26, 2017 (https://bizfluent.com/info-7742514-uses-marketing-plan.html)