Proposal No. 830929
Call H2020-SU-ICT-03-2018

Project start: 1 February 2019
Project duration: 42 months

Cyber Security for Europe

D9.19

Exploitation Strategy Report 2

Document Identification	
Due date	31 January 2022
Submission date	31 January 2022
Revision	1.0

Related WP	WP9	Dissemination Level	PU
Lead Participant	TDL	Lead Author	David Goodman
Contributing Beneficiaries	ATOS, JAMK, SINTEF	Related Deliverables	D9.14, D9.27

Abstract: This is the second in a series of three reports identifying the exploitation of the CyberSec4Europe results at consortium and individual partner levels relating to assets developed or enhanced during the course of the project, as well as a sustainability strategy in the context of the establishment of a cybersecurity competence centre and network.

This document is issued within the CyberSec4Europe project. This project has received funding from the European Union's Horizon 2020 Programme under grant agreement no. 830929.

Executive Summary

This is the second in a series of three reports identifying the exploitation of the CyberSec4Europe results at both individual partner and collective levels relating to novel cybersecurity products and services developed or enhanced during the course of the project. These assets may have been exploited either within or during the course of the project, or for which partners plan future exploitation after the completion of the project.

Unlike the first report in which collected responses from individual partners, here we have taken a pro-active approach by looking at the assets primarily in work packages 3 and 5. In parallel, we present the details of a questionnaire/survey which has already been sent to all project beneficiaries inviting them to declare their exploitation plans beyond the end of the project.

Hence the primary objective of this report is to outline the methodology to be adopted after collecting responses to the partner questionnaire/survey. This will involve inviting a set of representatives, drawn from CyberSec4Europe's Associates and consortium partners to comprise and exploitation and innovation board. The initial role of the group will be to validate the value proposition criteria outlined in this report and evaluate the results of the partner questionnaire/survey. The goal is both to highlight all the innovation and societal benefits created during the project as well as to reduce the long list of assets to a small number of key exploitation candidates and to present them in a jury-style competition during the project's final conference.

Finally we provide a timetable of the next steps we intend to take over the coming twelve months.

Document information

Contributors

Name	Partner
David Goodman	TDL
Aljosa Pasic	ATOS
Elina Suni	JAMK
Jani Paijanen	JAMK
Gencer Erdogan	SINTEF
Karin Bernsmed	SINTEF
Per Meland	SINTEF
Shukun Tokas	SINTEF

Reviewers

Name	Partner
Jos Dumortier / Magdalena Kogut	TLEX
Jozef Vyskoc	VAF

History

Version	Date	Authors	Comment
0.1	30 November 2021	David Goodman	First draft
0.2	12 January 2022	David Goodman	Second draft
0.3	13 January 2022	Aljosa Pasic	Atos update
0.3	13 January 2022	Gencer Erdogan	SINTEF update
1.0	27 January 2022	David Goodman	Final draft
1.0	31 January 2022	Ahad Niknia	Final check, preparation and submission

Table of Contents

List of Tables

List of Acronyms

A	**AI**	Artificial Intelligence
B	**BFT**	Byzantive Fault Tolerance
C	**CEF**	Connecting Europe Facility
	CONCORDIA	Cyber security cOmpeteNCe fOr Research anD InnovAtion
D	**DG CONNECT**	Directorate-General for Communications Networks, Content and Technology
	DoA	Description of the Action
	DPI	Dots Per Inch
	DPIA	Data Protection Impact Assessment
E	**ECB**	European Central Bank
	ECB/SSM	European Central Bank/ingle Supervisory Mechanism
	ECHO	European network of Cybersecurity centres and competence Hub for innovation and Operations
	eIDAS	Electronic IDentification And trust Services
	EUPL5	European Union Public Licence
G	**GDPR**	General Data Protection Regulation
H	**H2020**	Horizon 2020
I	**IdM**	IDentity Management
	IDS	Intrusion Detection System
	IoT	Internet of Things
	ISO/IEC	International Organization for Standardization and the International Electrotechnical Commission
J	**JRC**	Joint Research Centre
	JSON	JavaScript Object Notation
	JWT	JSON Web Token
M	**MPC**	Multi Party Computation
	MRL	Market Readiness Level
N	**NIS**	Network and Information Security
O	**OSINT**	Open-Source Intelligence
P	**PSD2**	Payment Services Directive 2
R	**RGCE**	Realistic Global Cyber Environment
S	**SAML 2.0**	Security Assertion Markup Language 2.0
	SDVA	Social Driven Vulnerability Assessment
	SIEM	Security Information and Event Management
	SME	Small to Medium-sized Enterprise
	SOC	Security Operations Centre
T	**TARGET2**	Trans-European Automated Real-time Gross settlement Express Transfer 2
	TRL	Technology Readiness Level
W	**WP**	Work Package

List of Assets

A	**Adaptive Authentication**	Adaptive Authentication
	AIRE	Atos Incident Reporting Engine
	ArchiStar	ArchiStar (aka SECOSTOR)
	ARGUS	Argus
B	**Blockchain Platform**	Blockchain Platform
	BowTie++	BowTie Plus
	Briareos	Briareos
C	**Compliance issues**	Compliance issues
	CORAS	CORAS methodology
	Cryptovault	Cryptovault
	CSA	Cyber Security Awareness
D	**DANS**	Data ANonymization Service
	DP analysers	DP analysers
	DynSMAUG	Dynamic Security Management Framework Driven by Situations
	eABCs	e-attribute-based credentials
E	**EBIDS**	Ensemble Based Intrusion Detection System
	Edge-Privacy	Edge Privacy
	EEVEHAC	End-to-End Visualizably Encrypted and Human Authenticated Channel
	eIDAS Proxy	eIDAS Proxy
	eIDASBrowser	eIDAS Browser
	ENIDS	Edge Network Intrusion Detection System
F	**Fine-granular rewriting on blockchains**	Fine-granular rewriting on blockchains
	FlexProd	FlexProd - Integrity-Preserving Data Analytics
G	**GENERAL_D**	Gdpr-based EnforcemeNt of pERsonAL Data
	Guidelines for GDPR compliance	Guidelines for GDPR compliance
H	**HADES**	Hades
	HAMSTERS	Human – centered Assessment and Modelling to Support Task Engineering for Resilient Systems
	HERMES	Hermes
	HoneyGen	Generating Honeywords
I	**IntelFrame**	A framework for intelligent machine learning-based intrusion detection
	Issuer-Hiding ABCs	Issuer-hiding attribute-based credentials
J	**JUDAS**	Json Users and Device AnalysiS tool
L	**LINDDUN Privacy threat elicitation**	Linkability, Identifiability, Non-repudiation, Detectability, information Disclosure, content Unawareness, and policy and consent Non-compliance privacy threat elicitation

M	**MITIGATE**	Multidimensional, integrated, risk assessment framework and dynamic, collaborative risk management tools for critical information infrastructures
	Mobile p-ABC	Mobile privacy-preserving attribute based credential
	modssl-hmac	mod_ssl hash-based message authentication code
N	**NetGen**	Network Generator
P	**Password-less AuthN**	Password-less AuthN
	PetShop	Petri net workshop
	PLEAK	Privacy LEAKage
	Policy-based reaction tool	Policy-based reaction tool
	PPCTIs	Privacy-Preserving CTI
	PTASC	privacy preserving Trustable Autonomous Secure Communications
	PVS	Protocol Verification Suite (previously OFMC/AIF)
R	**Reliable-CTIs**	Reliable Cyber Threat Intelligence sharing
	RisQFLan	RISk Quantitative Federated Logic analysis
	RoCe	Risk of Compromise estimation
S	**SACM**	Security Awareness Conceptual Model
	SelfSovereign-PPIdM	Self-sovereign privacy-preserving IdM in blockchain
	SEMCO framework	System and software engineering for Embedded systems applications with Multi-COncerns support
	Sharemind MPC	Sharemind multi-party computation
	SOBEK	Sobek
	SPARTA	Security & Privacy Architecture through Risk-driven Threat Assessment
	SPeIDI	Service Provider eID Integration
	SYSVER	CEng System Verifier
T	**TATIS**	Trustworthy APIs for enhanced threat intelligence sharing
	TEE	Trusted Execution Environments
	TIE	Threat Intelligence Integrator
	Trust Monitor	Trust Monitor
U	**UASD**	Unauthorized App Store Discovery
V	**VCUCIM**	Verifiable credential user centric identity management
	VEREFOO	VErified REFinement and Optimal Orchestration
	VTPin	Virtual Table (VTable) Pin

List of CyberSec4Europe Partners

A	**ABI**	ABI Lab
	AIT	Austrian Institute of Technology
	ARCH	Archimede Solutions SARL
	ATOS	Atos
B	**BBVA**	BBVA Group
	BRNO	Masaryk University
C	**C3P**	University of Porto
	CNR	Consiglio Nazionale delle Richerche
	CONCEPT	CONCEPTIVITY
	CTI (P)	Computer Technology Institute and Press “Diophantus”
	CYBER	Cybernetica
D	**DAWEX**	Dawex
	DTU	Technical University of Denmark
E	**ENG**	Engineering Ingegneria Informatica S.p.A
F	**FORTH**	Foundation for Research and Technology Hellas
G	**GEN**	Comune di Genova
	GUF	Johann Wolfgang Goethe-Universität Frankfurt
I	**I-BP**	Informatique Banques Populaires
	ICITA	International Cyber Investigation Training Academy
	ISGS	Intesa Sanpaolo
J	**JAMK**	JAMK University of Applied Sciences
K	**KAU**	Karlstad University
	KUL	KU Leuven
N	**NEC**	NEC Laboratories Europe GmbH
	NTNU	Norwegian University of Science and Technology (NTNU)
O	**OASC**	Open and Agile Smart Cities
P	**POLITO**	Politecnico di Torino
S	**SIE**	Siemens
	SINTEF	SINTEF
T	**TDL**	Trust in Digital Life
	TLEX	Timelex
	TUD	Delft University of Technology
U	**UCD**	University College Dublin & LERO
	UCY	University of Cyprus
	UM	University of Maribor
	UMA	University of Malaga
	UMU	University of Murcia
	UNILU	University of Luxembourg
	UNITN	University of Trento
	UPRC	University of Piraeus Research Center
	UPS-IRIT	Université Toulouse III Paul Sabatier – Institut de Recherche en

		Informatique de Toulouse
V	**VAF**	VaF
	VTT	VTT Technical Research Centre of Finland

1 Introduction

Task 9.5 identifies *'the exploitation of the CyberSec4Europe results at a consortium and participant level relating to the comprehensive suite of novel cybersecurity products and services as well as the implementation of a common cybersecurity research and innovation roadmap also taking into consideration advice from the advisory board'*.[1]

The first Exploitation Strategy report[2] consisted of:

- **Exploitation**: listing responses from all 43 project partners
- **Joint Exploitation**: broken down by work package
- **Sustainability**: based on strategic input, technical collaboration, communications & networking
- **Innovation**: three examples of CyberSec4Europe innovation based on asset maturity and potential real-world impact

We were highly conscious that the information provided would only give an early snapshot of what the eventual outcomes would be. As, at the time of writing, we have moved into the second half of the project and this report will outline the methodology and approaches for capturing the best exploitation and innovation results including criteria for success at the end of the project funding period.

2 Asset Overview

The first Exploitation Strategy report listed the responses from all CyberSec4Europe beneficiaries to questions about their exploitation plans, an exercise which is being repeated now, 12 months later, albeit with a different set of emphases and perspectives given the timing in relation to the duration of the project. As discussed below, we do not expect to have collected and curated the feedback from the partners before March 2022.

In this report we are taking a more proactive approach to identifying potentially exploitable assets developed during the course of the project, specifically those involved in WP3 and WP5. The WP3 assets are used in a specific set of WP3 solutions as well as integrated into some of the WP5 demonstrator use cases.

---

1 CyberSec4Europe Annex 1 Description of the action (part A) p.50

2 Deliverable D9.14: Exploitation Strategy Report 1

2.1 WP3 Demonstrator Assets

The WP3 demonstrators are categorised according the JRC taxonomy:

- Privacy-preservation, TEE and IoT-Edge security (T3.2)
- Software development lifecycle (SDL) (T3.3)
- Security intelligence (T3.4)
- Adaptive security (T3.5)
- Usable security (T3.6)
- Conformity, validation, certification (T3.8)

As in the first report, the partners are listed according to the following categorisation:

- Research Institutes
- Software Vendors
- Universities

2.1.1 Research Institutes

2.1.1.1 Austrian Institute of Technology (AIT)

Research institute, Austria

2.1.1.1.1 ArchiStar (aka SECOSTOR)

Description: Secret-sharing allows one to securely split data into multiple (say, n) shares, such that any subset of size t is sufficient to restore the data, but any smaller subset does not include any information about the data. It can thus be used, for example, for secure outsourcing of sensitive data to untrusted storage providers

Actors: Users wishing to store/retrieve data, and (cloud) storage providers

2.1.1.1.2 eABCs

Description: Anonymous attribute-based credential (ABC) systems allow for strong yet privacy-preserving user authentication. Yet, they are computationally heavy on the user side. eABCs (encrypted ABCs) mitigate this challenge by allowing a privacy-maintaining cloudification of ABC systems.

Actors: Issuers certifiying user attributes; users wishing to authenticate; service providers as relying parties; cloud wallet provider hosting the cloud-based authentication platform

2.1.1.1.3 Fine-Granular Rewriting on Blockchains

Description: Hash algorithm which, when deployed in the blockchain context, allows for fine-granular modifications and upgrades of the blockchain, e.g., in order to satisfy legal requirements

Actors: Applications relying on broadly immutable, yet needing possibilities to correct/update certain fields of information

2.1.1.1.4 FlexProd - Integrity-Preserving Data Analytics

Description: Secure multi-party computation platform based on secret sharing which can be used to perform analytics on shared sensitive data without requiring access to plaintext data.

Actors: Parties who wish or want to carry out joint data analysis on sensitive data, or who wish to offer data analytics "as a service".

2.1.1.1.5 Issuer-Hiding ABCs

Description: Anonymous attribute-based credential (ABC) systems allow for strong yet privacy-preserving user authentication. Yet, upon compromise of the issuing authority, all certificates need to be revoked, posing a practical scalability risk. Issuer-hiding ABCs allow one to use multiple issuers (e.g., one per state in a country) to address this problem, without having to reveal the precise issuer upon authentication

Actors: Issuers certifiying user attributes; users wishing to authenticate; service providers as relying parties

2.1.1.2 Consiglio Nazionale delle Richerche (CNR)

Research institute, Italy

2.1.1.2.1 EBIDS – Ensemble Based Intrusion Detection System

Description: The tool is an ensemble-based approach used to identify anomalous/suspicious activities in networks and computer systems

Actors: The approach can be used in any network or computer system, which need to be protected from external/internal attacks

2.1.1.2.2 GENERAL_D (Gdpr-based EnforcemeNt of pERsonAL Data)

Description: GENERAL-D is an abstract architecture that can be customized with several real tools, methodologies for assisting the development of GDPR-based access control systems. It is composed of three main modules:

(1) GDPR–based access control policies management, which contains the components for (semi)-automatic deriving and testing GDPR-based access control policies;

(2) Access control system, which enforces the access control policies; and

(3) GDPR analytics which logs, stores and analyses collected data.

Actors: Data subject and data controllers

2.1.1.2.3 SYSVER (CEng System Verifier)

Description: The tool supports security administrators of large distributed systems in the verification of correct implementation of the security policies in the actual system possibly affected by (software) vulnerabilities. When problems are detected, the tool leverages the detailed analysis results to investigate possible changes to apply in the system to correct the anomalies (conflict resolution).

Actors: System administrators, security engineers

2.1.1.2.4 UASD – Unauthorized App Store Discovery

Description: UASD can identify unauthorised mobile app stores (black market) in the regular and dark web.

Actors: Brand protection for all enterprises delivering services through dedicated apps

2.1.1.3 Fondazione Bruno Kessler (FBK)

Research institute, Italy

2.1.1.3.1 ENIDS – Edge Network Intrusion Detection System

Description: ENIDS is an intrusion detection/mitigation system based on deep learning (DL) methods and Linux kernel technologies. The output of a DL-based traffic classifier is the input of a Linux kernel-based traffic filter that blocks all the packets classified as malicious. ENIDS has been designed to work on resource-constrained systems such as the nodes of edge computing environments.

Actors: Security and domain experts, system administrators

2.1.1.4 SINTEF

Research institute, Norway

2.1.1.4.1 BowTie++

Description: BowTie ++ was formerly named Bow Tie Plus, but is now being reimplemented under the new name. It is a risk management tool that supports a methodology for modelling causes and effects of unwanted security events using the bow-tie analysis and diagram notation. The tool is also used to identify preventive and reactive barriers to causes and consequences of unwanted incidents..

Actors: Security experts and domain experts

2.1.1.4.2 CORAS

Description: CORAS is a method for conducting security risk assessment. It provides a customised language for threat and risk modelling and comes with detailed guidelines explaining how the language should be used to capture and model relevant information during the various stages of a security risk assessment. The

CORAS method provides a web-based tool designed to support documenting, maintaining and reporting assessment results through risk modelling.

Actors: Security risk analysts, domain experts

2.1.1.5 VTT Technical Research Centre of Finland (VTT)

Research centre, Finland

2.1.1.5.1 Cryptovault

Description: Trusted management environment for blockchain keys with secure key backup using Shamir Secret Sharing protocol. Backup shares are stored in cloud platform and paper

Actors: Allows any Edge/IoT-devices or human user to backup blockchain key used in trusted execution environment to cloud services

2.1.1.5.2 EEVEHAC (End-to-End Visualizably Encrypted and Human Authenticated Channel)

Description: EEVEHAC establishes an end-to-end encrypted channel that is both human authenticable and visualisably encrypted

Actors: Users, AR devices, untrusted terminals, servers / service providers that wish to establish a secure communication channel

2.1.2 Software Vendors

2.1.2.1 Atos Spain

Software vendor/consultancy, Spain

2.1.2.1.1 TIE (Threat Intelligence Integrator)

Description: The Threat Intelligence intEgrator, through a heuristic analysis process called threat score, is enriching MISP events with various parameters such as relevance, accuracy, timeliness, variety and completeness. TIE is able to act as a filtering, processing and prioritisation filter for MISP events that correlate (e.g., in SIEM) with the monitored infrastructure.

Actors: Cybersecurity analysts and SOC analysts that deal with the processing of structured cybersecurity information, risk and trustworthiness assessment, threat intelligence sharing with SIEMs and external trusted partners/organisations

2.1.2.1.2 DANS (Data ANonymization Service)

Description: DANS is an anonymisation service based on the data anonymisation Java tool (ARX) that provides different privacy models (e.g., the *k-anonymity* model) to enable the application of certain privacy criteria over a specific dataset. ARX is under a Apache 2.0 licence. Also available as a java library (jar file)

Actors: DANS is intended to be integrated by data managers (data producers/aggregators) in

scenarios where sensitive personal data is managed, such as big data analytics platforms, research projects or clinical trial data sharing, in order to prevent user data privacy breaches. Being integrated in the COVID-19 data exchange platform.

2.1.2.1.3 SPeIDI (Service Provider eID Integration)

Description: SPEIDI integrates online services with an eIDAS infrastructure for European eID use. This connectivity eIDAS-based solution is intended to provide a hub or proxy service between a private SP domain and the country-level eIDAS nodes for secure access to e-services using the eID issued by any Member State. Based on the building blocks provided by CEF following the eIDAS technical specifications, including signing, encryption and the SAML 2.0 standard. SP connection is based on a simple API based on JWT. SPeIDI is under EUPL licence.

Actors: SPeIDI is intended for integrating digital services to an eIDAS network for authentication scenarios when a user strong authentication is needed for securing access to those services.

2.1.2.1.4 AIRE (Atos Incident Reporting Engine)

Description: AIRE is a tool that will help in the mandatory incident reporting to different supervisory authorities. In particular, the aim of this asset is to address the need to report cybersecurity incidents adapted to different procedures/methods depending on the regulatory bodies. This asset will receive in real-time incidents to be reported. The user, depending on his role, will be able to select them in order to classify them, to confirm the classification (managerial judgement) or to carry out the reporting process to the selected competent authorities.

Actors: In a financial incident reporting scenario, this asset would be used by the following actors: the incident classification team (for classifying the incoming incidents), the controller (to perform the managerial judgement) and the incident reporting team (to monitor the evolution of the incidents and carry out the reporting)

2.1.2.2 Cybernetica

Software vendor/consultancy, Estonia

2.1.2.2.1 CSA (Cyber Security Awareness)

Description: A tool for cybersecurity operations centres. The application is intended for gathering and managing information about assets that require cybersecurity and IT security certification. It is possible to define the assets and the different certification needs and events that have been carried out or are planned in the future. This allows for checking the conformity of assets to certificates, and takes a step towards continuous certification It has been refitted to serve as a continuous monitoring application for validation, conformity and certification.

Actors: Different entities (companies, information systems, hardware) that send information

and alerts about events and incidents

2.1.2.2.2 DP analysers

Description: This PLEAK-based application provides tools for static analysis for differential privacy and guessing advantage in business processes, as well as tools to select the appropriate privacy parameters. The analysers take as their input the description of the processes in some programming or query language, as well as the descriptions and possibly the content of tables of input data. It shows the dependencies between the privacy parameters (ε for differential privacy, or the guessing advantage of the adversary) and the utility parameters (the decrease of accuracy in the output of the process due to added noise).

Actors: Business environment analysis, risk assessors

2.1.2.2.3 PLEAK

Description: PLEAK is used for analysing potential privacy leaks in data flows. Analysis tool for the privacy audit of an existing system and the design of new privacy-aware systems. PLEAK allows modelling business processes using the business process model notation (BPMN) and privacy-preserving algorithms using the SecreC privacy-preserving programming language. PLEAK can then analyse the data flows using cryptographic privacy and differential privacy. PLEAK also supports the inclusion of privacy enhancing technologies (PETs) in the business process models to reduce the leakage of private information.

Actors: Business environment analysis, risk assessors

2.1.2.2.4 Sharemind MPC

Description: Secure multi-party computation platform that works on encrypted data without decrypting them and provides data analytics capabilities on this data.

Actors: Different parties wanting to carry out joint data analysis on sensitive data.

2.1.2.3 NEC Laboratories Europe GmbH (NEC)

Industry, Germany

2.1.2.3.1 Blockchain Platform

Description: Ready-to-use platform for instantiating blockchain protocols and related applications. It also provides a ready-to-use blockchain with a novel BFT consensus algorithm.

Actors: Applications that rely on robust, distributed ledgers.

2.1.2.3.2 TEE (Trusted Execution Environments)

Description: Hardware component enabling secure (confidential and integrous) execution of trusted code, isolated in hardware, on an untrusted host.

Actors: Any scenario envisioning untrusted entities participating in security-critical computations.

2.1.3 Universities

2.1.3.1 KU Leuven (KUL)

University, Belgium

2.1.3.1.1 LINDDUN Privacy threat elicitation framework

Description: LINDDUN framework for elicitation of privacy related threats in the categories of linkability, identifiability, non-repudiation, detectability, information disclosure, content unawareness, and policy and consent non-compliance. This asset contains both methodology and the supporting knowledge bases (threat trees, catalogues of PETs structured in accordance to LINDDUN threat types).

Actors: Software engineers, software architects, requirements engineers

2.1.3.1.2 SPARTA (Security & Privacy Architecture through Risk-driven Threat Assessment)

Description: Based on enrichment of data flow diagrams (DFDs) with security countermeasures, attacker model and assumptions about adversary and its capabilities, risk calculation is automated. SPARTA implements interaction-based threat elicitation and prioritizes large bodies of documented threat in accordance with risk.

Actors: Software engineers, software architects, requirements engineers

2.1.3.1.3 TATIS (Trustworthy APIs for enhanced threat intelligence sharing)

Description: Enhanced open source threat intelligence sharing platform to share indicators of compromise in trustworthy manner on top of the MISP platform

Actors: Security and domain experts, system administrators

2.1.3.2 Norwegian University of Science and Technology (NTNU)

University, Norway

2.1.3.2.1 SACM (Security Awareness Conceptual Model)

Description: Guidelines for enhancement of societal security awareness across critical indicators and targeted societal groups

Actors: General public and professionals

2.1.3.3 Politecnico di Torino (POLITO)

University, Italy

2.1.3.3.1 eIDAS proxy

Description: This component runs a fundamental part of an eIDAS node which is part of an eIDAS network. It interacts with the national eID scheme (identity) providers and service providers, transforming national identity management protocol messages (e.g., SPID in Italy) into/from the eIDAS protocol and handling national specific information to resolve attributes to be transferred through the eIDAS network.

Actors: Security and identity management experts operating an eIDAS node, identity providers notified under eIDAS and the service providers providing eIDAS-enabled services

2.1.3.3.2 NetGen

Description: This tool generates a non-DPI analyzer that can classify any kind of network traffic

Actors: Security and domain experts, system administrators

2.1.3.3.3 Policy-based reaction tool

Description: This tool generates a set of security policies able to mitigate a cyber-threat

Actors: Security and domain experts, system administrators

2.1.3.3.4 Trust Monitor (TM)

Description: TM provides integrity verification of nodes in the target infrastructure leveraging remote attestation

Actors: Security and domain experts, system administrators

2.1.3.3.5 VEREFOO (VErified REFinement and Optimal Orchestration)

Description: Automated refinement of network security requirements (security policies) into virtual security function configurations (e.g. firewall rules) with formal correctness guarantee

Actors: Network security managers

2.1.3.4 Technical University of Denmark (DTU)

University, Denmark

2.1.3.4.1 IntelFrame – A framework for intelligent machine learning-based intrusion detection

Description: This framework allows each IDS node to select an appropriate machine learning algorithms from a pool in a periodic manner, with the purpose of maintaining the

detection accuracy. It can be used to detection external/internal attacks for any type of computer networks

Actors: Software and hardware security engineers

2.1.3.4.2 PVS (previously OFMC/AIF) – Protocol Verification Suite

Description: The PVS consists of several security protocol verification tools that allow for formally proving protocol specifications correctly. In the smart cities scenario, any Internet-connected device will probably communicate using security protocols, and the PVS can provide formal assurances that models of such protocols work as intended. This is crucial since safe communication relies on the correctness of security protocols. Such formally proven guarantees may also be necessary to achieve high levels of certification.

Actors: PVS is intended to be used by designers of security protocols, in order to formally verify their security properties

2.1.3.4.3 RisQFlan

Description: RisQFlan is an Eclipse-based tool for quantitative risk modelling and assessment and is used as a tool for the quantitative analysis of probabilistic attack scenarios based on attack-defense trees. Besides statistical analysis, the tool includes features to perform single simulations of the model and export model in a format used by tools able to perform exact probabilistic analysis such as PRISM and STORM (stormchecker.org).

Actors: Security analysts who want to model possible attacks to an organization with the goal of studying its vulnerabilities and related risks.

2.1.3.5 University College Dublin & LERO (UCD)

University, Ireland

2.1.3.5.1 Adaptive authentication

Description: A framework and prototype tool to support adaptive authentication which can access different types of information with different sensitivities from different locations and networks. The proposed adaptive authentication mechanisms will be enabled depending on the estimated risk of information exfiltration and also taking into account other requirements, such as security, usability, user preferences and performance. We will provide control methods to adjust the authentication techniques based on the risk level to choose the optimal authentication method and support access control and identity management.

Actors: Software engineers, security engineers

2.1.3.6 University of Cyprus (UCY)

University, Cyprus

2.1.3.6.1 HoneyGen

Description: Password leakage detection mechanism. HoneyGen creates realistic false passwords to be included with each user's real password. As a result, when attackers gain access to the password file F they have to guess which is the real password from a list of 20 sweetwords.

Actors: Developers

2.1.3.6.2 modssl-hmac

Description: An Apache module that uses HMACs instead of hashing for protecting leaked passwords against cracking.

To address the major threat of password leaks, services have started to employ password hardening techniques. Two major families of such hardening techniques exist today. The first one is to use, on purpose, slow cryptographic hash functions, i.e., *bcrypt*. These cryptographic hash functions are designed to adapt to hardware evolution. For instance, *bcrypt* uses a significant amount of CPU cycles, while *scrypt* uses a significant amount of memory for computing a cryptographic digest. This slowdown is designed to slow down the attackers that aim to crack the cryptographic digests off-line. Unfortunately, no matter the slowdown, if the password is weak, it can still be guessed.

The second family of password-hardening techniques is based on using a cryptographic service constructed entirely for the purpose of computing hardened passwords. Hardening here involves several rounds of cryptographic hashing and message authentication codes (MAC). With such a service in place, verifying a password means involving the service. This essentially transforms off-line password cracking to on-line.

Actors: Web developers

2.1.3.6.3 VTPin

Description: VTPin is a representative hardening technique in the form of a utility library that can be pre-loaded to a C++ binary in order to protect it from memory corruption carried out through hijacking of VTable pointers using use-after-free vulnerabilities. In particular, VTPin protects against VTable hijacking, via use-after-free vulnerabilities, in large C++ binaries that cannot be re-compiled or re-written. The main idea behind VTPin is to pin all the freed VTable pointers on a safe VTable under VTPin's control. Specifically, for every object deallocation, VTPin deallocates all space allocated but preserves and updates the VTable pointer with the address of

the safe VTable. Hence, any dereferenced dangling pointer can only invoke a method provided by VTPin's safe object. Subsequently, all virtual-method calls due to dangling pointers are not simply neutralized, but they can be logged, tracked, and patched.

Software hardening against VTable hijacking that requires no source code or binary re-writing.

Actors: Developers

2.1.3.7 University of Malaga (UMA)

University, Spain

2.1.3.7.1 Edge-Privacy

Description: Privacy component for Edge computing

Actors: This asset is expected to be leveraged by Edge end-users as a means to cover sensitive information when accessing services deployed in the cloud. The Pguard component is meant to work as a privacy proxy

2.1.3.7.2 HADES – Automatic analysis of malware samples

Description: HADES is a platform for the orchestration of sandboxes for malware execution. It can send samples to virtual machines, execute them, analyse their behaviour and create reports based on the proof generated.

Actors: Malware analysts

2.1.3.7.3 JUDAS – JSON Users and Device analysis tool

Description: This tool collects the files to be processed, extracts relevant data and correlates them, additionally asking external services to complete the information about the objects generated (e.g. ipapi, VirusTotal, Pipl)

Actors: Digital forensic investigators

2.1.3.8 University of Maribor (UM)

University, Slovenia

2.1.3.8.1 Analysis of interoperability and cross-border compliance issues

Description: Investigation of the compliance for identity technologies interoperability with, for example, the eIDAS regulation, the GDPR, the ePrivacy directive etc. Also to be investigated is the cybersecurity of technologies used with emphasis on authentication, cross-border and cross-sector dimensions and contribute to the design of a common "blueprint", making reference to other regulations relevant for the market.

Actors: Software engineers, security engineers, legal council

2.1.3.8.2 Guidelines for GDPR compliant user experience

Description: GDPR and best practices review with a focus on DPIAs (data protection impact assesment), including a template when and how to perform an assessment.

Actors: Software engineers, security engineers, legal council

2.1.3.9 University of Murcia (UMU)

University, Spain

2.1.3.9.1 eIDASBrowser

Description: Android application implementing a browser that transparently integrates eIDAS authentication via NFC using Spanish ID card (DNIe).

Actors: Service requiring high degree of authentication; Spanish user with the last NFC-enabled version of DNIe

2.1.3.9.2 Mobile p-ABC

Description: Open source privacy-preserving attribute based credential (p-ABC) system for Android, based on the Idemix Anonymous Credential System and the ABC4Trust implementation. It supports minimal disclosure of personal information through zero knowlege crypto-proofs, allowing users holding their smartphone to present those proofs against identity providers.

Actors: Users that employ their smartphones to perform online transactions, which want to authenticate and manage their attributes and personal data in a privacy-preserving way.

2.1.3.9.3 PPCTIs – Privacy-Preserving CTI

Description: This asset will investigate, integrate and adapt privacy preserving solutions, such as attribute based encryption (e.g., cp-abe encryption) and anonymity techniques within cyber-threat intelligence systems. It will allow improving these CTI decentralised platforms and integrate them in different ecosystems, so that security-related information can be shared among organisations in a privacy-preserving way, with selective disclosure of information.

Actors: Security and domain experts, system administrators, belonging to CERT/CSIRTS, companies

2.1.3.9.4 Reliable-CTIs (Reliable Cyber-Threat intelligence sharing)

Description: Enabler leveraging current open threat intelligence platforms such as MISP, to share securely, trusted cyber-threat intelligence data between CERT/CSIRTS, companies and related entities. A multi-dimensional approach to quantifying trust among

involved stakeholders has been devised, combining, for instance, the peer's reputation, the collaboration maturity and membership of federations. The trust model will drive the CTI secure data exchange.

Actors: Security and domain experts, system administrators, belonging to CERT/CSIRTS, companies

2.1.3.9.5 SelfSovereign-PPIdM (Self-sovereign privacy-preserving IdM in blockchain)

Description: This asset will investigate, integrate and adapt privacy-preserving solutions like Anonymous Credentials Systems (e.g. Idemix) in blockchains (e.g. Hyperledger), following an SSI management approach. To this aim, it is envisaged to use, as a baseline, the outcomes from the Decentralized Identity Foundation (DIF). The assets will be aligned with W3C standards on verifiable credentials and decentralized identifiers (DIDs).

Actors: Persons involved in online transactions which want to authenticate and manage their personal data in a privacy-preserving way, and achieve high reliability and provenance of their transactions. IoT devices that want to authenticate and manage autonomously, on behalf or their owners, their digital IoT identities (linked to user) in a privacy-preserving way.

2.1.3.10 University of Piraeus Research Center (UPRC)

University, Greece

2.1.3.10.1 MITIGATE – Evidence-driven Maritime Supply Chain Risk Assessment

Description: MITIGATE is a supply chain risk assessment approach which aims to estimate and forecast the cyber risks of any supply chain service (SCS) that its provision/delivery requires the interaction of various cyber assets from various business partners (cross-partner cyber assets). The multiple objectives of the MITIGATE approach are:

- identify and measure all cyber threats within a supply chain service;
- evaluate the individual, cumulative and propagated vulnerabilities;
- predict all possible attacks/threats paths and patterns within the SC cyber system (which consists of cross-partner cyber assets) based upon specific propagation rules;
- estimate the existence of zero-day exploitable vulnerabilities;
- assess the possible impacts;
- derive and prioritize the corresponding cyber risks of the supply chain cyber assets formulate a proper mitigation strategy.

Actors: Port facility security officers (PFSO), ship security officers (SSO), supervisory control and data acquisition (SCADA)/EMS operators, vessel planners, control room/CCTV operators, infrastructure engineers, infrastructure operators, system engineers, logistics managers, warehouse specialists, supply chain specialists/

analysts, operations managers, ICT administrators etc.

2.1.3.10.2 Password-less AuthN

Description: This asset will replace the traditional username/password paradigm by providing an authentication mechanism that exploits users' biometrics. The password-less authentication system is based on the FIDO Universal Authentication Framework. Later, we are planning to integrate the FIDO server with OpenID Connect to provide user authorisation capabilities.

Actors: Users of the CyberSec4Europe platform. Password-less authentication is intended for integrating the authentication scheme with the CyberSec4Europe services, in authentication scenarios where strong authentication is needed to provide secure access to those services.

2.1.3.11 University of Porto (C3P)

University, Portugal

2.1.3.11.1 ARGUS (Enforcing Privacy and Security in Public Cloud Storage)

Description: A privacy brokerage system aiming to enhance confidentiality and availability by partitioning encrypted data over multiple public storage providers, solving the problem of trust in public cloud providers, by also leveraring hardware TEEs.

Actors: Users as well as businesses, universities and other large scale institutions

2.1.3.11.2 Briareos

Description: A HIDS (host-based intrusion detection system) capable of launching honeypots in any Linux system extracting information from the filesystem and integration with virtual environments to support Honeypots to diagnose intrusion. A modular framework for elastic intrusion detection and prevention.

Actors: Security and domain experts, system administrators

2.1.3.11.3 HERMES

Description: Hermes (also known as Zermia) is a modular and extensible fault injection framework, designed for testing and validating concurrent and distributed applications. Hermes's principles have been validated by conducting a series of experiments on a distributed applications and a state-of-the-art Byzantine fault tolerant (BFT) library, to show the benefits of Hermes for testing and validating applications.

BFT protocols are designed to increase system dependability and security. They guarantee liveness and correctness even in the presence of arbitrary faults. However, testing and validating BFT systems is not an easy task. As is the case for most

concurrent and distributed applications, the correctness of these systems is not solely dependent on algorithm and protocol correctness. Ensuring the correct behaviour of BFT systems requires exhaustive testing under real-world scenarios. An approach is to use fault injection tools that deliberate introduce faults into a target system to observe its behaviour. However, existing tools tend to be designed for specific applications and systems, thus cannot be used generically. More advanced and powerful tools and frameworks are needed for testing the security and safety of distributed applications in general, and BFT systems in particular. Specifically, a fault injection framework that can be integrated into both client and server side applications, for testing them exhaustively.

Actors: Users as well as businesses, universities and other large scale institutions

2.1.3.11.4 PTASC (Privacy Preserving Middleware)

Description: The IoT middleware platform should aim to (semi-)automatically combine different privacy-preserving techniques to support end-to- end privacy. The middleware platform must also help the user to manage and monetize its data, behaving as a data broker with the existing data consumers. This task aims to design and build the middleware framework.

Actors: Data subjects and data controllers

2.1.3.11.5 SOBEK

Description: Introduction of introspection within Android apps, via code injection using aspect-oriented programming (AOP), to transparently collect metering data that can be used to notify the user or/and sink into a secure backend (for enterprise solutions).

Android users are increasingly aware of private information leakage by third-party apps. SOBEK ensures that any application developed in the scope of smart cities contains the protection mechanisms offered. This way, when interacting with the scenario, the user can manage the behaviour and access policies based on privacy policies defined locally on an Android device or remotely by a smart cities team, maintaining the information privately. The extra underlying feature is the compliance and the capability of a user continually adapting their specific privacy definition when traveling around Europe, without the need for new privacy checks.

Actors: Users as well as businesses, universities and other large scale institutions including smart cities

2.1.3.12 Université Toulouse III Paul Sabatier (UPS) – Institut de Recherche en Informatique de Toulouse (IRIT)

University, France

2.1.3.12.1 DynSMAUG (Dynamic Security Management Framework Driven by Situations)

Description: The framework allows to dynamically enforce security measures based on the current situations of assets to protect. It consists of three sub-assets:

- Security policy specification approach driven by situations. Situation-based policies easily express complex dynamic security measures, are closer to business, and simplify the policy life cycle management.
- Situations description approach using complex event processing techniques.
- A modular event–based infrastructure where a dedicated situation manager maintains active situations allowing one or more command centres to take dynamic situation–based authorisation and obligation decisions.

Actors: Security administrators, security engineers

2.1.3.12.2 HAMSTERS (Human – centered Assessment and Modelling to Support Task Engineering for Resilient Systems)

Description: HAMSTERS is a tool-supported task modelling notation for representing human activities in a hierarchical and structured way, with the intention of supporting modelling consistency, coherence and conformity between user tasks and interactive systems. It provides support to engineers who design and develop usable interactive systems offering a good user experience. The aim is to use HAMSTERS to provide support for systematic assessment of the impact of security policies on usability and user experience. When associated with PetShop (another asset), HAMSTERS provides partly-automated support to ensure consistency between user tasks and system behaviour, as well as training and contextually helping users by showing on task models which user actions are possible according to the interactive system state.

Actors: User interface designers and developers, system and software design engineers

2.1.3.12.3 PetShop – Petri net workshop

Description: PetShop is a high-fidelity formal model-based prototyping environment dedicated to interactive systems. It provides support for modelling the behaviour of interactive systems and running these models along with the user interface as prototypes of the interactive system. It provides support to engineers who design and develop usable and dependable interactive systems. The aim is to use this asset to ensure consistency between user tasks and the behaviour of security policies as they are manipulated by the users through user interfaces. When associated with HAMSTERS, PetShop provides partly-automated support to ensure consistency between user tasks and system behaviour, as well as training and contextually helping users by showing on task models which user actions are possible according to the interactive system state.

Actors: User interface designers and developers, system and software design engineers

2.1.3.12.4 SEMCO framework

Description: SEMCO (System and software Engineering with Multi-COncern) is a methodological tool-support for modelling and analysing multi-concern systems and software architecture. In context, a concern is a requirement, a constraint or an objective a stakeholder has for that architecture. SEMCO consists of a methodology for the creation of a design and analysis framework for handling the composition and integration of architecture and security that semi-automatically supports the analysis of architecture and its security. The approach associates model-driven engineering (MDE) and formal techniques to design a set of modelling languages for specifying and analysing architecture and property models, which allows the reuse of capitalized security-related know-how. The results are provided as a set of complementary artifacts :

(a) modelling and formal languages for the specification of models (system architectures and concerns);

(b) a process of development of reusable (formal) model libraries for the specification and verification of security by a security expert; and

(c) a process of secure architectural design and analysis by an architect reusing the model libraries.

Actors: Pattern developers for populating the repository with patterns (security expert), system and software architects (domain experts)

2.1.3.12.5 VCUCIM (Verifiable credential user centric identity management)

Description: VCUCIM provides a user-centric digital identity system suing FIDO2 and verifiable credentials. It allows anyone to easily benefit from an enriched digital identity made of multi-purpose and multi-origin attributes, increases usability by the elimination of user passwords, makes this digital identity highly trustworthy both for the user (in terms of privacy and sovereignty) and the service provider who requires highly certified information about the user being enrolled to and/or authenticated on its services.

Actors: User interface designers and developers, system and software design engineers

2.1.3.13 University of Trento (UNITN)

University, Italy

2.1.3.13.1 RoCe – Risk of Compromise estimation

Description: RoCe is a methodology for the estimation of risk of compromise of a given network
Actors: Security and domain experts, system administrators

2.1.4 Summary of WP3 Assets

	Partner	Asset	Sub-totals	Totals
Research Institutes	Austrian Institute of Technology (AIT)	ArchiStar eABCs Fine-granular rewriting on blockchains FlexProd Issuer-Hiding ABCs	5	
	Consiglio Nazionale delle Richerche (CNR)	EBIDS GENERAL_D SYSVER UASD	4	
	Fondazione Bruno Kessler (FBK)	ENIDS	1	
	SINTEF	BowTie++ CORAS	2	
	VTT	Cryptovault EEVEHAC	2	14
Software Vendors	Atos Spain	TIE DANS SPeIDI AIRE	4	
	Cybernetica	CSA DP analysers PLEAK Sharemind MPC	4	
	NEC Laboratories Europe	Blockchain Platform TEE	2	10
Universities	KU Leuven	LINDDUN Privacy threat elicitation SPARTA TATIS	3	
	NTNU	SACM	1	
	POLITO	eIDAS Proxy NetGen Policy-based reaction tool Trust Monitor VEREFOO	5	
	Technical University of Denmark	IntelFrame PVS RisQFlan	3	
	University College Dublin	Adaptive Authentication	1	

	University of Cyprus	HoneyGen modssl-hmac VTPin	3	
	University of Malaga	Edge-Privacy HADES JUDAS	3	
	University of Maribor	Compliance issues Guidelines for GDPR compliance	2	
	University of Murcia	eIDASBrowser Mobile p-ABC PPCTIs – Privacy-Preserving CTI Reliable-CTIs SelfSovereign-PPIdM	5	
	University of Piraeus Research Center	MITIGATE Password-less AuthN	2	
	University of Porto	ARGUS Briareos HERMES PTASC SOBEK	5	
	UPS-IRIT	DynSMAUG HAMSTERS PetShop SEMCO framework VCUCIM	5	
	University of Trento	RoCe	1	39
		Total number of WP3 assets		63

Table 1: A summary of WP3 assets

As can be seen, there are a large number of assets involved in the construction of the various WP3 demonstrators, the majority of which come from the universities. It remains to be seen how motivated the knowledge institutes – the research institutes and the universities – are to exploit their assets commercially, either by the individual organisations or jointly with others.

2.2 WP5 Demonstrator Use Case Applications

There are seven application areas each with their own set of one of more demonstrator use cases. Most of the scenarios involve the management of sensitive data in different industry environments i.e., Open Banking, medical data exchange, smart cities and others.

2.2.1 Open Banking

2.2.1.1 Cyber threat intelligence and information sharing (CYTILIS)

CYTILIS is a collaboration between a number of WP3 and WP5 partners, together with 20

representatives from the CONCORDIA project.

This use case highlights issues arising from data sharing between financial entities, national and sectorial CERTs. In particular, it recognises that sensitive data should only be exchanged in a trusted environment with privacy-preserving techniques and ideally in real-time. Over the last few years, while attacks have become more refined and are evolving quickly, the financial sector is incrementing the digitalisation of its critical processes, amplifying the attack surface.

The attackers may hurt several entities without changing their behaviour due to the lack of fast reactions and responses. The demonstrator shows how threat intelligence platforms can be used for sharing and exchanging critical information in real-time, reducing the response time to cyber attacks. However, the usage of these platforms is limited due to a lack of trust by the institutions as well as differences between national and corporate regulations.

CYTILIS is a trusted privacy-preserving network of threat intelligence platforms based on MISP to exchange and process information automatically which it performs in conjunction with OBSIDIAN. Financial entities are thus provided with several channels capable of informing them about cyber attack threats and fraud events they may encounter.

CYTILIS involves several components that, in conjunction, create a trusted privacy-preserving network. The MISP network is accessed through the TATIS asset which includes:

- **Access control solutions** to the information shared based on a CP-ABE cryptographic scheme to empower financial organisations to keep control over what they want to share and with whom.
- **Privacy-preserving solutions** based on the TATIS and Privacy-preserving Cyber Threat Intelligence assets and privacy-enhancing technologies (PETs), techniques which enable the obfuscation of sensitive information related both to stakeholders and organisations in the cyber threat intelligence sharing process, thus protecting their confidentiality and reputation as well as being compliant with the GDPR.
- **Auditing solutions** based on the Blockchain Platform asset ensure the provenance, the integrity and the immutability of shared information during their whole lifecycle. CTI-related transactions recorded on the blockchain allow for auditability between organisations.

Leveraging TATIS and privacy-preserving cyber threat intelligence provides a fully distributed system.

In addition to the MISP network, a federated learning (FL) network is also deployed in order to provide an alternative way to implicitly exchange CTI information. To do so, organisations can implement a FL module (FL client) along with their MISP instance that will communicate with a FL aggregator to collaborate in the training of a machine learning (ML) model built from the CTI information contained in different domains or organisations. Due to the nature of the FL process,

clients will only exchange model parameters with the aggregator, as a result of which, no data is shared and the need to anonymise or encrypt the information is removed.

2.2.1.2 Open Banking sensitive data sharing network for europe (OBSIDIAN)

OBSIDIAN has been developed by Informatique Banque Populaire with the support of Trust in Digital Life and Associate partners CaixaBank, Poste Italiane and more recently Groupe BPCE, La Banque Postale, Crédit Mutuel and BNP Paribas.

OBSIDIAN is a financial fraud data sharing network to counteract the high incidence of repeated frauds. State of the art tehcnologies allow participating financial institutions to keep control of their data and only share data that is fraud relevant. All of this takes place in total compliance with regulations pertaining to both banking secrecy and data protection.

The objective of OBSIDIAN is to address the increase in banking fraud and digital banking cybersecurity challenges by creating a European network for sharing fraud information between open banking players. The role of the proposed network is to enable national and cross-border cooperation between banks to prevent fraud by immediately sharing fraud information (like, for example, an IBAN implied in a transfer fraud) within a secure, trusted network once a fraudulent attack occurs whilst protecting the data in transit. The role of the network is to share fraud information within the network and establish user experience trust levels; and, in so doing, provide network access to data and money laundering information and share terrorist financing information in the network. The core requirements of OBSIDIAN are:

- Bank anonymity
- Regulatory compliance
- Sharing information without transferring underlying data ownership
- Real-time sharing
- Privacy by design

By centralising information exchange flows, the OBSIDIAN server makes it possible for banks to exchange information anonymously. Additional technologies have been studied to improve the anonymity of the data and the banks; for example, by fragmenting TCP packets on the network and making them transit through several intermediate servers.

When a fraud manager (or a system) of a participating bank detects a suspicious transaction and wants to check the beneficiary's IBAN, she will use the OBSIDIAN client to protect it (through pseudonymisation and encryption) and then send a check request to the OBSIDIAN network.

The underlying principle of the trust network is that it is based on secure multi-party computation (MPC) and consists of:

- centralised architecture for exchange flows
- decentralised data storage

- data protection based on hash and encryption mechanism

This is achieved through a central network server that communicates securely to numerous network clients deployed at each node in the network – the participating financial institutions. Key to the trustworthiness of the network is that no sensitive data is stored on the central network server – all fraud-related data is stored locally at each network node, independent of the network server and all the other nodes in the network.

Fraud data – in this use case, IBANs – is encrypted with Elliptic Curve Diffie Hellman (ECDH) used to generate a shared key each time data is transferred between the network clients and the server. The implementation deployed uses Elliptic Curve Cryptography (ECC) implemented in JavaScript to offer a very simple OBSIDIAN client consisting of a web app usable for any fraud manager/banking expert without requiring her to install any software on her workstation.

2.2.1.3 Privacy preserving verifiable credentials

This solution is based on the VCUCIM asset and uses the smartphone as a wallet to store not only the cryptographic means but also to store and manage different VCs. The smartphone interacts with a laptop launching a web browser and the W3C WebAuthn.

At the end of a use case involving an eKYC process to onboard a new bank customer, a user is onboarded as a fully verified and authenticated customer of the bank. Without the client application installed on her smartphone, she would not have been able to submit the required verified credentials and would not have been able to onboard online with the bank.

2.2.1.4 Open Banking API architecture (OBACHT)

ABI Lab developed a shared map of the macro-components and functionalities for an Open API, designed as a model to support API exposure with a view to openness.

This map or architecture identifies five basic areas within the defined macro-components for the Open API:

- **API Security:** Components useful for ensuring the necessary security features for interaction with the Open Banking Architecture including Identity Provider.
- **API Platform:** Components with responsibility for orchestration, policy enforcement, monitoring and aid to the government including an API Gateway, API Manager and an API Portal
- **Knowledge Base:** Collection, organisation and distribution of knowledge through an API Catalogue and Documentation Management
- **Baseline:** Components constituting the reference point on which the implementation of an Open Bank is based
- **Ecosystem:** Open banking implies the use of external services, data and features developed by parties outside a bank.

2.2.2 Supply chain security assurance

Siemens are developing a protocol for secure 'blaming' in case of disputes. In the context of CyberSec4Europe, together with NEC, they are evaluating conflict resolution techniques which are benefitial/required for distributed supply chains. NEC provides the blockchain platform.

2.2.3 Privacy-preserving identity management

The Austrian Institute of Technology (AIT) is extending its existing knowledge and assets on anonymous credentials and secure multi-party computation based on the project results and integrating the increased functionality and higher security guarantees into prototypes and products to be shared with future customers and commercialisation partners.

Issuer-Hiding ABCs is under continuous evaluation for integration. While not directly required for the selected use case, the asset could increase students' privacy in the broader context of the demonstrator, e.g., by allowing them to prove that they are currently subscribed as students at a university, without revealing which one.

Usability is, in general, a necessary concept for most technical solutions, particularly this demonstrator. Hence, Usable Privacy and Identity Management Guidelines is integrated here.

SelfSovereign-PPIdM (Self-sovereign privacy-preserving IdM in the blockchain) is directly integrated and is continuously adapting to meet the evolving requirements, including the integration of Mobile p-ABC.

2.2.4 Incident reporting

The Incident Reporting Platform has been developed between Atos, BBVA and Intesa Sanpaolo.

Depending on the sector and the nature of the incident, incident and compliance reporting can be a complex and costly process. Contacting different competent authorities and users as well as complying with obligations has to be an integral part of any incident response procedure. Comprehensive data is needed, for which workflows and built-in templates could be used to simplify the entire process.

The target audiences are usually the employees of CERT/CSIRT and SOC teams within financial organisations. In some cases these may be identified as follows:

- the **Incident Management** team for collecting information about the incident,
- the **Incident Classification** team for classifying the incoming incidents,
- the **Controller** to perform the managerial judgement; and
- the **Incident Reporting** team to monitor the evolution of the incidents and carry out the reporting.

The data about the security incidents to be reported is gathered through a graphical interface which integrates the GUI provided by the AIRE asset with the GUI provided by the open source tool

TheHive.

AIRE allows the collection of general information about the financial entities, users and regulations (such as templates required, recipients of the reports and communication channels) that will be used by different incidents reported by the same organisation or under the same regulatory framework.

TheHive offers by itself a security incident response platform where information about security incidents can be managed. It supports the registration of new incidents and, with this purpose in mind, the administrator can define templates with the information necessary to report the incident to competent authorities.

AIRE also integrates libraries like Camunda (https://camunda.com/), while specific add-ons have been made with scripts for an event classifier responder specific to regulations such as NIS, PSD2, TARGET2, eIDAS, ECB/SSM. This asset will receive in real-time incidents to be reported to trigger an incident reporting workflow and generate the mandatory reports adapted to the applicable regulations. The user, depending on their role and the current stage in the workflow, is able to select from the reports in order to introduce information about the incidents and classify them, to confirm the classification (based on managerial judgement) or to generate the reports for the selected competent authorities.

Currently, there is a lack of solutions in the market focused on the management and generation of mandatory incident reporting according to different regulatory frameworks, in spite of a "report incidents" feature included in many of them. Most SIEM (Security Information and Event Management) solutions available in the market, such as IBM QRadar, Alienvault USM or Splunk, provide the generation of reports about the security incidents detected. However, these reports do not follow any common template and the information included in them does not cover what is required for mandatory incident reporting to the different supervisory authorities.

The objective of the Incident Reporting Platform is to enable financial institutions to fulfil the mandatory incident reporting requirements according to the different procedures and methods specified by the applicable regulation or regulatory bodies (such as PSD2 and ECB Cyber Incident Reporting Framework).

The platform covers reporting from the collection of the data related to a detected security incident until the generation of the mandatory reports that have to be sent to the competent authorities. One of the most important features is the ability to connect to diverse stakeholders: EU and national competent authorities, LEAs, sector regulators, individual organisations and clients. Other features include the possibility to adapt collected information relating to the needs of the notification scheme, the use of different communication modalities and channels, the maintaince of statistics and the establishment of feedback loops.

2.2.5 Maritime transport

SINTEF has developed a PKI demonstrator for the 'Trust Infrastructure for Secure Maritime

Communication' use case. Such a PKI is fundamental in order to provide certificates and associated mechanisms for maritime communication solutions. The demo shows how the PKI is used for ship enrollment and visualises real-time ship-to-ship AIS communication (avoiding collissions).

Cybernetica, together with Atos and the University of Piraeus, has further enhanced their privacy-enhanced business process models performing leakage analysis on use cases in maritime transport as well as medical data exchange.

PLEAK is used to model the use cases using privacy enhanced business process model notation (PE-BPMN) and to perform leakage analysis.

Bowtie++ has been used to identify risks for the maritime PKI.

A significant focus is on how assets can be adopted to support the adaptive security activities of the MAPE (Monitor-Analyze-Plan-Execute) adaptation loop architecture which have been used to showcase different application scenarios of the maritime transport use cases. MAPE is traditionally considered to be the reference architecture to engineer adaptive systems. It monitors (M) the protected sub-system and its operating environment and maintains an updated representation of the protected sub-system and its operating environment at runtime (knowledge - K). The protecting sub-system uses this representation to analyse (A) security threats and assess security risks, and plan (P) and execute (E) counter-measures aimed to prevent or thwart the threats discovered during analysis. The protected subsystem (e.g., maritime transport system) is the system to be protected, which interacts with the cyber, physical, and social spaces characterising its operating environment. The assets integrated using the MAPE loop as follows:

- SPARTA asset is used for requirement analysis.
- Adaptive Authentication, MITIGATE and SYSVER are used in the analysis and planning phases.
- AIRE and DynSMAUG are used in the execution phase.
- GDPR compliant user experience asset guidelines are used to discuss the GDPR compliance issues in adaptive security.

2.2.6 Medical data exchange

Dawex are developing a new service based on the the DANS asset developed by Atos to be provided to Dawex clients before they commercialise or exchange data on the Dawex medical exchange platform.

In some sectors, such as the health sector, data providers hold vast amounts of private information, that could be used by other organisations (data consumers). Anonymisation of datasets and avoidance of re-identification are key business enablers for this.
Besides the data exchange platform, services can also be used in similar settings or on similar platforms including:

- **Data Lake** is understood as a vast pool of data, for which the final purpose is typically not defined. Here there is a need for data scientists or those with the appropriate skills or tools to understand the nature of the data and translate it to a specific business use. Access is more open than on the data exchange platform.
- **Data Marketplace** is understood as equivalent to data trading or data commerce platforms, usually referring to a repository plus added value services such as data processing (e.g., aggregation, filtering), matching, trading, contracting, payment and distribution (one to many, many to many etc).
- **Data Sharing** platforms are similar to those in the previous category, but without trading and payment services. Contracts are replaced with data sharing agreements, codes of conduct, adhesion MoUs or similar documents. Payment can be replaced by reputation or feedback mechanisms and services
- **Data Warehouse** is understood as a kind of a data repository, used to store structured, filtered and processed data that has been treated for a specific purpose. In principle it is outside the main scope of exploitation, as data management operations usually remain within a single or small number of organisations.

The target audience for the exploitation of the assets used in this pilot are data owners (e.g. hospitals), data unions (e.g. associations) and data intermediators (e.g. brokers, markeplaces).

The main asset, DANS, uses the ARX library, but does not change its code, therefore supporting data pipeline engineer/integrator. For the Java version wrapper is done in Java, while the version which uses delivery as a service (DANS-as-a-Service), Atos also made the Java-based API and user interface in Angular Javascript. DANS (partially) eliminates the need for specific domain knowledge (e.g. disease taxonomy), therefore supporting data scientists in configuring anonymisation logic.

Another asset used in this pilot is SPEIDI which is based on the CEF eID DSI building blocks following the eIDAS technical specifications, including signing, encryption, the SAML 2.0 standard and the results of the LEPS project, including an API to decrease the integration cost of a private online service provider at the Spanish eIDAS node. For this medical data exchange pilot, an extension was made with support for more protocols; for example, the OpenID Connect protocol for the French eIDAS node. In addition, an adaptation to eIDAS 2.0 was implemented.

Guidelines for GDPR Compliant User Experience is also used here. The goal of the demonstrator is to take the data and processes used to create a data protection impact assessment (DPIA) for this specific scenario. This should allow anybody else looking to perform a DPIA to use this demonstrator as an example of how to use the DPIA template provided in this asset.

Finally, in relation to this pilot and exploitable assets, a further segmentation of target customers will be carried out for the individual partner exploitation plan: namely according to the type of service, the data flow models, the technology they use, as well as the type of organisation and

alternative business models.

2.2.7 Smart cities

Engineering, parterning with the Comune di Genova, have expanded the scope of their cybersecurity offering through the inclusion of additional services based on the prototypes validated through their work in CyberSec4Europe. The evolution of the outcomes of the project are leading to a fully-fledged social driven vulnerability assessment (SDVA) and thus enlarging its assessment and management of the cybersecurity risks service.

ARGUS, Briareos and PTASC havev been tested and deployed in the Porto Data Hub. The main focus of the integration is to ensure that:

- users can trust the Porto data Hub platform to store private information using public cloud storage (ARGUS);
- the detection of vulnerabilities can take place at an early stage, allowing the system's vulnerabilities to be understood and analysing requests from the environment (Briareos);
- devices can communicate end-to-end using the Porto Data Hub platform to reveal information to external entities through a marketplace (PTASC).

General_D is being integrated to manage citizen access control and consent.

SYSVER and SelfSovereign-PPIdM (self-sovereign privacy-preserving IdM in the blockchain) are being directly integrated into the demonstrator.

Reliable CTI and Privacy-Preserving CTI bring privacy-preserving methodologies to cybersecurity sharing.

2.3 Other Innovative Applications

2.3.1 Flagship 1 & 2

From 12-13 January 2021, as part of CyberSec4Europe WP7, JAMK University of Applied Sciences conducted Flagship 1, a two-day cybersecurity exercise that required no previous experience and was (uniquely) only accessible online rather than as an in-person event. The event, the first of its kind, was open to representatives from CyberSec4Europe partners although future events may be made available to others. Part of the exercise, which simulates a potential real-world cyber attack and demonstrates new cyber range concepts, was published as an open online course. A similar second cybersecurity exercise, Flagship 2, took place on 25-26 January 2022, involving not only representatives from CyberSec4Europe partners, but also individuals from other organisations who took part in a parallel exercise as cybersecurity analysts examining the output from the main exercise and providing expert feedback.

During the exercise, participants were provided with guidelines concerning a fictional organisation they were working for. With the available documentation, participants were able to examine and analyse a cyber attack and seek to mitigate the damages. The short duration of the exercise

provided an interesting challenge: one of the key questions was what to expect participants to learn in a complex learning situation in such a short time. It was a technical cyber exercise, but was also fun, educational and inspiring as well as offering purposeful roles for attendees with varying technical and non-technical backgrounds.

In the exercise, the fictional organisation's internal and external communication representatives are alerted. A video setting the scene for Flagship 1, which is also applicable to Flagship 2, is available at JAMK's video sharing service.

- **The exercise in general:** The background story for the exercise was opened for the participants before the exercise. At a generic level, the exercise modeled a situation "at the office" where the exercise organisation did not know what kind of incident it might face, from whom, what the motivation behind it was, and how the incident started.
- **Role of the participants:** A separate survey was sent to enquire about individuals' preferred role in the exercise which varied from hands-on technical roles to more managerial or leadership roles, or an observer role with no hands-on activities. Most of the participants were assigned to an employee, a consultant, or service provider role in the fictional organisation. There could be several fictional organisations in the exercise.
- **The exercise environment** realistically modeled the Internet and its services. For example, there were ISPs (Internet Service Providers) who provided connectivity and services for the exercise organisations. The organisations had environments realistically modelled, both technically and operationally.

The technology behind Flagship is based on Realistic Global Cyber Environment (RGCE), a cyber arena developed in JAMK's cybersecurity research, development and training centre, JYVSECTEC. The platform development started in 2011 and the first national cyber exercises were held in 2013. Since then, RGCE has been used in various realistic cybersecurity exercises and in cybersecurity masters' level cybersecurity education at JAMK. Flagship demonstrates proof of an open-source SD-WAN interconnection requirement specification, which is used for interconnecting various cyber range internal and external services and endpoints.

3 Individual & Joint Exploitation Plans

In parallel with the composition of this report on methodology, in December 2021 a Powerpoint document was circulated to each of the CyberSec4Europe beneficiaries asking them to provide as much information as they can about any expoitable and/or innovative assets developed during the project. They were invited to imagine they were looking for funding for their asset, which they might indeed be, and to consider how they would convince a set of investors.

The questions are:

1. **Asset Overview:**

- What are the needs and challenges, the burning business problems, your asset is addressing?
- Who are the target audience?
- Who owns the asset: is it individually or jointly owned and are there any licence considerations?

Tips:

- *Avoid long stories: a couple of sentences, preferably with keywords*
- *Identify at three levels: (1) sector (2) teams (3) specific name(s)/role(s)*
- *Avoid confusing ownership and licensing!*

2. **Project Dividend:**

- As a result of your participation in the project have there been any noteworthy innovations and / or improvements to the asset?

Tips:

- *Did you start from an existing asset?*
- *Don't be concerned to state that your asset is based on an open source licence?*

3. **Network:**

- Is there a connection with any other tools either from within CyberSec4Europe or beyond?
- Is the asset associated with a particular demonstrator or other use case?

Tips:

- *No need to provide a complete market analysis. You could possibly use a SWOT analysis (cf. the ones in deliverable D4.4)*
- *List all inputs and outputs. This is not necessarily business relevant, but it's important to indicate possible dependencies.*

4. **Market:**

- What market segment does the asset fit?
- How would you position your asset in this market?
- Are there potential competitors who you are aware of?

Tips:

- *Again, you don't have to provide a fully-fledged analysis, just a few bullets will do indicating, for example, whether your asset is available standalone or as a service?*

5. **Business Model:**

- The key elements of a business model that have not been addressed already.

Tips:

- *The key words here are 'key elements' – many aspects of a business model will already have been covered by your answers to the previous questions*

- *One option is to use the Business Model Canvas template – but only if you wish to do so. If nothing else, it could be used for guidance.*
- *Be sure not to add any (business) confidential information!*

The intention of the survey is to make it brief and painless to complete but to provide sufficient information for the task team to proceed with the next steps. The ambition is to collect the project partners' exploitation plans during January and February 2022, and to have this part of the exercise completed by the end of March.

The results will be showcased on the project website and eventually published in deliverable D9.27. In parallel, the output will be forwarded to the proposed Exploitation and Innovation Board (see below).

4 Value Proposition Planning

In the first exploitation strategy report, we introduced the exploitation objectives and strategy with a focus on the scale up and use of community-based collaboration and cooperation to improve the transition from research to market. The nature of CyberSec4Europe was described, with particular emphasis on the procedures and operational setup for the better exploitation of cybersecurity research, one that could later serve the Cybersecurity Competence Centre and Network.

In the first phase of the project, partners were offered a pre-defined set of headings to describe their plans and to maintain them independently throughout the course of the project, together with a list of anticipated benefits that could also serve to derive early value propositions. Although the concepts of value and benefits are not the same thing, they are clearly related. In addition, there might be many definitions or understandings of value, depending on the perspective. While for many commercial assets, value proposition is often related to commercial considerations – for example, the time, cost and effort that a cybersecurity solution might save – whereas public administrators or academic stakeholders might have a different understanding.

This is also why the identification and validation of value propositions by different stakeholders is desirable and beneficial for the wider community, and why procedures for the joint building or ranking of project assets can also be used to improve the initial value proposition.

The initial value proposition is usually created in the concept phase of a project, or even during the proposal, when the business case is still vague or only limited to a single use case. As a matter of fact, one of the objectives of any project should be testing not only of technical feasibility, but also of related value generated for the end user. This initial proposition is often not stated with clarity and in a measurable form. On other occasions, it is linked to technical differentiators or features, proposed therefore from a supply and not a demand side perspective. Only when a prototype is delivered, can more information on the value proposition be gleaned. This is also because a big chunk of value is unique to each end user or consumer, as it is determined by the size and significance of the problem the asset or innovation is addressing for them.

There are numerous parameters that could be used to assess project results and, in so doing, to determine priorities for exploitation and promotion. In order to assess the pecking order of CyberSec4Europe's assets, we have identified a set of value proposition parameters for filtering purposes

- **Technology and market readiness levels (TRL/MRL)** are well-established first call criteria for making decisions on future investments and product roadmaps. (25)
- **Novelty or innovation levels** are important in positioning versus competitors or potential partnerships. (20)
- **Reusability and transferability** across sectors impact scalability, customisation and potential market diversification. (10)
- **Affordability**, needless to say, is a significant factor, especially but not exclusively for SMEs. Large organisations, from corporates to universities, generally have heavy internal competition for any unbudgeted expenditure, particularly if there is no demonstrable or perceived short or even medium term return on investment. (15)
- **Sustainability** includes the available information about future investment, for example, for the evolution or maintenance of code, beyond the initial go-to-market (GTM) outlay. (10)
- **Policy priority** or alignment with policies might be particularly important in the case of EU-funded projects. (5)
- **Green credentials** include how the asset might benefit climate or, for example, whether it relies on a disproportionate use of electric power. Other types of credentials could be derived from an asset's contribution to, say, EU cybersecurity certification or other policy objectives. (5)
- **Power of community** builds on the idea of the strength of the positive impact of networking or what might be called the "community exploitation" of a shared but separate endeavour, such as threat intelligence sharing. The implication is that there is a perceived increase in value if an asset or rather the asset owner is an active member of a consortium where externalities, such as a certification scheme, play a role. (10)

The numbers in brackets after each criterion suggest a possible "weighting of the value proposition" which we would prefer to consider as asset ranking, positioning or clustering. For example, a group of assets with low TRLs would be recommended for technology maturation or pilots with early adopters. Assets with a good score on affordability would be suggested for SMEs and so on. These granular criteria are to be reviewed by exploitation and innovation board.

5 The Exploitation and Innovation Board

As the next part of the process, it is intended to populate an exploitation and innovation board, comprising an invited mixed group of representatives from industry and knowledge institutes.

Representatives would be selected from CyberSec4Europe's consortium partners as well as Associate partners, who would bring a more external perspective. We would start to invite individuals to the Board during March 2022.

The role of the Exploitation and Innovation Board would be to assess the list of assets presented to them and to score them based on the value proposition parameters outlined above. We have tentatively provided a weighting to each of the identified categories: the first task of the Board would be to review the categories and validate or amend the respective weightings.

The overall intention is to reduce the long list of assets to a small number of key exploitation candidates. The Board will complete this objective by July 2022.

6 Event/Workshop

In order to raise the visibility of this initiative, we would like to organise an event – perhaps a half-day workshop – towards the end of the project at which the most successful exploitation candidates identified by the Exploitation and Innovation Board would be invited to present or demonstrate their assets in front of a panel of jurists and an invited audience. The prize for the eventual 'winners' or set of winners of this competition, based on rules agreed with the Board in advance, would be the opportunity for further showcasing by the project to prominent stakeholders in the wider cybersecurity community.

There is a prospect of good synergy or alignment of this event with the CyberSec4Europe final conference, which is tentatively targetted for November 2022.

7 Conclusion and Next Steps

As we move into the final twelve months of CyberSec4Europe, we are well positioned to assess what the exploitable results and innovations derived from the partners' work in the project may be exploitable, either commercially or through the contribution of enhancements to further cybersecurity research.

The next steps are:

- To collect and collate the results of the survey sent to all beneficiaries as described in the section Individual & Joint Exploitation Plans by the end of March 2022;
- To invite representatives from the Associate partners and the project beneficiaries to an exploitation and innovation board as described in the section Exploitation and Innovation Board in March / April 2022;
- To review the value propositions and weightings laid out in section Value Proposition Planning with the exploitation and innovation board during May 2022;

- To work with exploitation and innovation board in assessing the results of the survey with a shortlist of best candidates by the end of July 2022;
- To organise and event/workshop in conjunction with the project's final conference in November 2022 as suggested in section Event/Workshop;
- To report on all of the above in deliverable D9.27 Exploitation Strategy Report in M48.