Guidelines for applicants.
PUZZLE Validation Contracts Call.

Open date for proposals: 8th February 2022 at 9:00 CET.
Closing date for proposals: 30th June 2022 at 17:00 CEST.

May 2022.

The work described in this document has been conducted within the project PUZZLE. This project has received funding from the European Union's Horizon 2020 (H2020) research and innovation programme under the Grant Agreement no 883540. This document does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of such content.

Table of contents

The work described in this document has been conducted within the project PUZZLE. This project has received funding from the European Union's Horizon 2020 (H2020) research and innovation programme under the Grant Agreement no 883540. This document does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of such content.

List of Abbreviations

Abbreviation	Explanation
PUZZLE	PUZZLE: Towards a Sophisticated SIEM Marketplace for Blockchain-based Threat Intelligence and Security-as-a-Service
CET	Central European Time
EC	European Commission
EU	European Union
SME	Small and Medium-sized Enterprises (including start-ups)
ME	Micro-enterprises
ENISA	The European Agency for Cybersecurity
DSME	European Digital SME Alliance

Table of Figures

The work described in this document has been conducted within the project PUZZLE. This project has received funding from the European Union's Horizon 2020 (H2020) research and innovation programme under the Grant Agreement no 883540. This document does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of such content.

1. Introduction

The aim of the PUZZLE Validation Contracts Call is to provide SMEs&MEs who deal with cybersecurity, privacy and personal data protection a set of tools and solutions of varied sophistication level, to allow them benefit from the innovative targeted solutions that the PUZZLE Marketplace offers, addressing their specific needs and available resources. Through this Validation Contracts Call, the interested parties are invited to present their idea on how the PUZZLE Marketplace could complement the development activities of a product/service they are already providing to their customers, detailing the PUZZLE components and services utilized, to prove the applicability, usability, effectiveness and value of the PUZZLE concepts, models and mechanisms under real-life conditions.

In the following text, a full set of information is provided to the applicants regarding the Validation Contracts for proposals which will be evaluated and selected for Validation Contracts, with a special focus on the technical activities of the PUZZLE project.

PUZZLE project has received funding from the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No 883540.

1.1. Background information on PUZZLE project

PUZZLE's novel approach of providing **cybersecurity services through a marketplace**, easy to adopt and deploy within SMEs&MEs network and computational infrastructure, leads to a bigger picture of improved readiness and responsiveness of SMEs&MEs in the areas of **security, privacy, threats management, and personal data protection**.

The PUZZLE framework is going to identify and track the relationships among the cyber assets of each SME or ME, considering the available network, compute and storage infrastructure and use them to efficiently calculate individual, cumulative and propagated risks, as well as recommend and apply mitigation actions for tackling identified cyber threats.

PUZZLE aims to employ a highly usable cybersecurity, privacy and data protection management framework in two directions: **SMEs&MEs and Cybersecurity providers**.

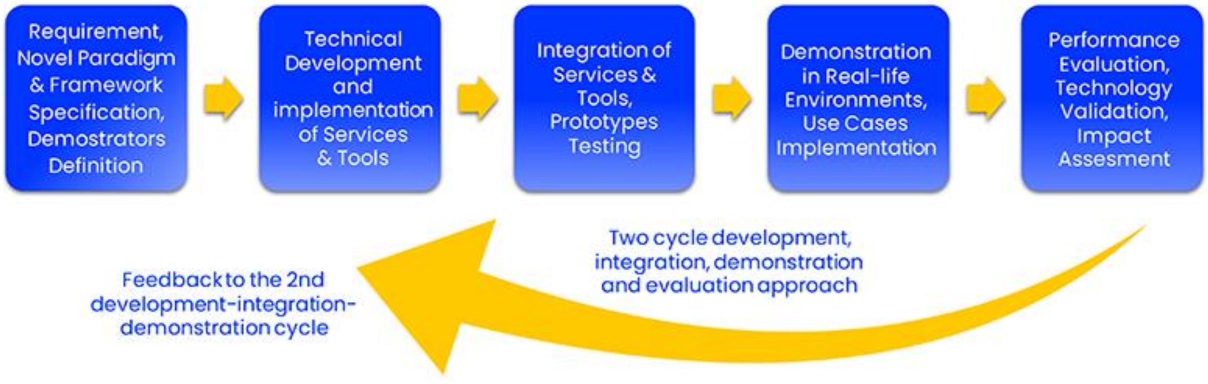
Requirement, Novel Paradigm & Framework Specification, Demostrators Definition
Technical Development and implementation of Services & Tools
Integration of Services & Tools, Prototypes Testing
Demonstration in Real-life Environments, Use Cases Implementation
Performance Evaluation, Technology Validation, Impact Assesment
Two cycle development, integration, demonstration and evaluation approach
Feedback to the 2nd development-integration-demonstration cycle

Figure 1: PUZZLE Methodology and Approach

The work described in this document has been conducted within the project PUZZLE. This project has received funding from the European Union's Horizon 2020 (H2020) research and innovation programme under the Grant Agreement no 883540. This document does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of such content.

What kind of innovations does PUZZLE bring to SMEs&MEs? Through blockchain-oriented technologies, SMEs&MEs will efficiently process information flows and establish online collaboration and knowledge sharing with other SMEs&MEs. Processed data analysis will lead to security insights and threat intelligence reports and, ultimately, increase their cybersecurity awareness.

By simplifying the design, configuration, deployment and management of cybersecurity management and provision services, the PUZZLE project will offer services capable of **providing advanced levels of security, privacy and trustworthiness for SMEs&MEs**. PUZZLE will also facilitate the collection, processing, and exchange of data and knowledge sharing among SMEs&MEs with regards to cyber threats and vulnerabilities.

Compiling a set of mechanisms for secure data exchange based on applied artificial intelligence and blockchain is the chosen way to go. The PUZZLE Marketplace has a special role in the process – to leverage PUZZLE efforts, ascertain optimal deployment plans and support their execution.

1.2 PUZZLE Marketplace

PUZZLE will implement a highly usable cybersecurity, privacy and data protection management marketplace targeted at SMEs&MEs. The PUZZLE project will track the relationships among the cyber assets of each SME&ME, considering the available network, compute and storage infrastructure and use them to efficiently calculate individual, cumulative and propagated risks, as well as recommend and apply mitigation actions.

1.3 PUZZLE Concept

Cybersecurity is a complex and fast-evolving field, thus security professionals and experts working for SMEs&MEs need constant learning. Malicious online activity can **cost enterprises millions**. Resources dedicated to cybersecurity are often scarce with SMEs&MEs, and therefore are of special interest and in the focus of the Project. Opening access to a marketplace of services, with a multitude of cybersecurity tools and processes that can keep corporate systems, networks, and sensitive information secure, is of the utmost importance. The majority of cyberattacks (86%) in SMEs&MEs are targeted, where financial gain (53%) and corporate espionage (47%) are the main motives. In spite of the current cyber threat landscape, 68% of SMEs&MEs have no systemic approach toward ensuring cybersecurity, 60% of those who were victims of cyber-attacks did not recover and thus shut down within 6 months, while less than 3% have cyber insurance. According to Gartner's predictions, 75% of public blockchains will suffer "privacy poisoning" soon.

PUZZLE aims to increase the cybersecurity awareness of SMEs&MEs through the efficient processing of heterogeneous information flows, the exchange of cyber security information, the knowledge sharing and the establishment of online collaboration with other SMEs&MEs. Enhanced security defence is provided through the PUZZLE "Security-as-a-Service"

The work described in this document has been conducted within the project PUZZLE. This project has received funding from the European Union's Horizon 2020 (H2020) research and innovation programme under the Grant Agreement no 883540. This document does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of such content.

marketplace including risk assessment services, edge analytics and trust assurance services and security situational awareness services.

The **healthcare sector** is going through the **digitalisation process** and continuously **adopting new technologies** to improve patient care, offer new services focusing on patient-at-home care, and reach operational excellence. The integration of new technologies in an already complex IT infrastructure opens up new challenges regarding data protection and cybersecurity. The healthcare sector is one of the sectors most **vulnerable to cyber-attacks**.

Simultaneously, the digitalisation of the healthcare sector is moving forward, and digital solutions or electronic records continuously replace paper-based processes. The transformation affects services along the complete healthcare delivery chain, i.e. medication, appointment scheduling, patient records, inpatient and outpatient care as well as inpatient and remote monitoring or self-management. Digitalisation offers new solutions to **improve patient care** and gain operational excellence in healthcare organisations.

Across Europe, intensive efforts have been made to combat the global spread and effects of the coronavirus (COVID-19) pandemic with various measures to support public health systems, safeguard the economy and ensure public order and safety. At the same time, the outbreak has created an even more fertile ground for **cybercrime**, threatening the safety of citizens and businesses in a challenging operational and financial environment. As businesses and citizens increasingly rely on digital solutions, the nature of the threat is also changing, with cybercriminals exploiting fear, uncertainty and unprecedented situations. The COVID-19 pandemic has created a new reality for the healthcare sector globally testing its limits. Adding to the overwhelming situation it is currently facing, the sector has become a **direct target** or collateral victim of cybersecurity attacks.

Financial technology (FinTech) already plays a key role in the industry, and the EU is well positioned in this subsector: the FinTech market is expected to experience double digit growth in the EU by 2021. Many financial services are data-heavy and fault-prone, thus requiring middlemen for mediation (**trust**) entailing transaction costs. Moreover, information sharing is limited even where obvious synergies can be realized as in the insurance industry (**data sharing**). The size of financing rounds for fintech companies is growing quickly: the mean funding size per round more than doubled in the analysed timeframe, from roughly €11 million in 2018 to €25.5 million in 2019.

SMEs are an important part of the European economy. For the European Union, the average value that SMEs contribute to the economy is around 56 percent. There were estimated to be approximately 22.6 million small and medium-sized enterprises (SMEs) in the European Union in 2021, with the vast majority of these enterprises being micro-sized firms which only employed fewer than nine people. A further 1.3 million enterprises were small firms with between 10 and 49 employees and approximately 201 thousand were medium-sized firms that had 50 to 249 employees. In 2021 SMEs in the European Union employed almost 84 million people. The Finance Sector provides a crucial backbone to the European Economy and -like many other sectors- its increasing dependency on ICT Infrastructures, Providers and their Supply Chain. The **importance of ICT Security and Resilience supporting the Finance Sector** grew considerably and the objective of protecting automated Inter-Banking transactions and more generally all types of Communications is altogether more critical and complex at the same time. A stable Financial System in Europe is however the underlying foundation for Economic stability; and the reliance on IT is now life critical for the entire Sector.

Manufacturing and Industry 4.0. The fourth industrial revolution (Industry 4.0) is closely associated with the topic of cybersecurity. A rapidly increasing number of Industry 4.0 **cybersecurity incidents emerge**, additionally stressing the need to strengthen cyber resilience. Lack of sufficient information security expertise and awareness is a major barrier that hinders the adoption of Industry 4.0 security measures. People involved in deployments of new solutions usually have only knowledge of either IT or OT (Operational Technology) security, while Industry 4.0 and Smart Manufacturing **require expertise over several areas**, e.g. network security, embedded systems, OT and IT security to name a few. It is becoming increasingly difficult to find qualified specialists who are well aware of security issues.

Manufacturers which are at various stages of Industry 4.0 adoption, often do not have appropriate governance structures in place for **secure implementation of new technologies** and secure maintenance of the existing ones.

It is clear that lack of security has the potential to significantly affect business continuity. **Investments in cybersecurity** should not be driven only by fear of losing money. It is equally if not more important, for industries and organisations to not look at cybersecurity only as a cost, but to also start seeing it as an important business opportunity. Cybersecurity can be an important **competitive advantage** for businesses, since it leads to having secure, reliable and trustworthy products and services.

The European **agricultural sector** is transforming from traditional, human labour-intensive work to data-oriented digital agriculture that has great potential for semi- or fully autonomous operation. This digital transformation offers many advantages, such as more precise fact-based decision making, optimised use of resources and big changes in organisation – but it also requires improved cyber-security and privacy data protection.

To feed the world's growing population and compensate for the loss of arable soil, the **agricultural sector** needs to increase efficiency, productivity and food quality, while simultaneously reducing labour costs and environmental impacts. Advanced technologies are becoming essential to increase efficiency in agricultural production while limiting its impact on the environment. The growing global population makes efficiency a necessity in food

The work described in this document has been conducted within the project PUZZLE. This project has received funding from the European Union's Horizon 2020 (H2020) research and innovation programme under the Grant Agreement no 883540. This document does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of such content.

production. This implies that **more data** is being gathered with the new digital solutions and thus there is an increased need for cybersecurity in the sector. The race for solutions has started: fields, crops and livestock are supplied with numerous sensors that monitor the environment. Machines are equipped with intelligent algorithms to perform their daily work with high precision and provide extensive operation status information, enabling a 24/7 availability. The agricultural system infrastructure is composed of numerous networked digital devices. The resulting bulk data can guide precise decision making on the farm and inform product development by machinery manufacturers. However, the colossal data gathering activities are very **attractive for cyber-attacks**, including theft, manipulation and misuse of data. There is a clear need to define cyber-security guidelines for modern Agriculture in the EU.

eGovernment. Cybersecurity threats are almost always **cross-border**, and a cyberattack on the critical facilities of one country can affect the EU as a whole. EU countries need to have strong government bodies that **supervise cybersecurity** in their country and that work together with their counterparts in other Member States by sharing information. This is particularly important for sectors that are critical for EU societies. Cybersecurity has become an **increasingly important** aspect of public policy as internet traffic increases and mounting cyber threats affect the operation of governments and businesses as well as the everyday life of citizens. Mounting cyber-threats are not limited by borders. Network and information systems are globally interconnected, and network-based threats are continually increasing in breadth, volume, and sophistication and represent an existential risk to organizations around the globe; hence, the need for an intervention at EU level, complemented by bilateral and multilateral international initiatives.

The Vision: PUZZLE introduces a novel approach of **providing cybersecurity services through a marketplace**, easy to adopt and deploy within SMEs&MEs network and computational infrastructure, which leads to a bigger picture of improved readiness and responsiveness of SMEs&MEs in the areas of **security, privacy, threats management, and personal data protection**.

1.4 PUZZLE General Requirements and Tracks

Small and Medium-sized Enterprises and Micro Enterprises (SMEs&MEs) who deal with cybersecurity, privacy and personal data protection, can submit proposals at the PUZZLE Validation Contracts contest. Proposals should deliver innovative solutions to increase the knowledge sharing in digital security across SMEs&MEs and between SMEs&MEs and larger providers. The user SMEs&MEs should be supported by democratizing access to tools and solutions of varied sophistication level, to allow SMEs&MEs benefit from innovative targeted solutions addressing their specific needs and available resources (currently reserved to larger organisations, due to their ability to cover such costs and availability of internal expertise).

The work described in this document has been conducted within the project PUZZLE. This project has received funding from the European Union's Horizon 2020 (H2020) research and innovation programme under the Grant Agreement no 883540. This document does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of such content.

To prove the applicability, usability, effectiveness and value of the PUZZLE concepts, models and mechanisms in industrial, real-life infrastructures, services and applications, demonstrating and stress-testing the developed PUZZLE artefacts under pragmatic conditions against a set of demonstrators is needed, while the realisation of validation contracts will provide wider participation of third parties in the demonstrators and on-boarding of services provided by vendors and open-source communities.

Validation Contracts for SMEs&MEs Wider Participation will assist in starting the services uptake and testing of the PUZZLE Marketplace towards getting more feedback from interested parties, as well as gaining traction for its utilization right after the end of the project, through the establishment of a community of early adopters.

These **early adopters** will be ten (10) start-ups/SMEs&MEs and five (5) cybersecurity vendors looking for strict personal data and privacy requirements that will be engaged in the project. Selected applicants will be **granted with Validation Contracts** that will allow them to cover expenses for interacting with the consortium, onboarding their own cybersecurity servicesand adopting the PUZZLE Marketplace for the development of a small-scale use case, lasting no more than 10 months.

The Project is issuing the **Validation Contracts Call for the Expression of Interest** on **February 8th 2022,** where interested parties would be requested to present their ideas on how the PUZZLE Marketplace could complement the development activities of a product/service they are already providing to customers, detailing the PUZZLE pieces/services utilized.

After that deadline, applications will be peer-reviewed by an external evaluation committee, resulting in the selection of the 10 highly ranked proposals of SMEs&MEs (maximum 2 proposals per country) and 5 highly ranked cybersecurity vendors.

The draft list of the selection criteria includes:

- innovation character and originality of the idea;
- challenges and relevance of the problem dealt;
- knowledge of technical matters;
- feasibility and construction of demonstrator;
- quality of presentation.

The successful applicants will be granted with a **Validation Contract of 10.000€** that will be used to cover both development costs in order to deliver their proposed cases, as well as 1 trip to one of the project's events, to meet the consortium and improve design of their cases.

It needs to be noted, that the Validation Contract will be redeemed at the end of the successful implementation of each such small case demonstrator, thus guaranteeing that the consortium will collect the appropriate feedback from each use case.

The work described in this document has been conducted within the project PUZZLE. This project has received funding from the European Union's Horizon 2020 (H2020) research and innovation programme under the Grant Agreement no 883540. This document does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of such content.

1.5 PUZZLE Objectives

The purpose of the Validation Contracts Call is to apply the services enabled by the PUZZLE Marketplace in various demonstrators and in the Validation Contracts to assess its architectural soundness, technical excellence and business value.

The overall objective is to evaluate the PUZZLE Marketplace from two perspectives: from the end-user perspective for SMEs&MEs, start-ups in various verticals and domains; and the other is validation from cybersecurity vendors trying to extend and add their services that are existing in the markets, and how its benefits can be used as extra services.

The common objective for SMEs&MEs and cybersecurity vendors is to validate the overall PUZZLE Marketplace and to put the project in the phase that can come up with the validation framework. From this perspective, PUZZLE will be in a position to do user acceptance testing, independent from the predefined use cases or to the extent of the cybersecurity services that will be provided.

The second objective **for participation from SMEs&MEs and start-ups** is to run their own use cases and report how these tests went, what they gained from the process, what are the benefits, and what are the results. Extending the evaluation of the Marketplace by running SMEs&MEs use cases in the Marketplace and providing the results will also help the Project to prove the wide applicability of the PUZZLE marketplace in various vertical domains.

The second objective from cybersecurity vendors, apart from validation, is to add their own cybersecurity services and report on how the PUZZLE Marketplace is evolving these extra services, which is the added value of such an inclusion.

As shown in Figure 2, the Validation Contracts Call selection will follow **funnel approach**, which will help the PUZZLE consortium to focus on the top proposals along the incubation programme.

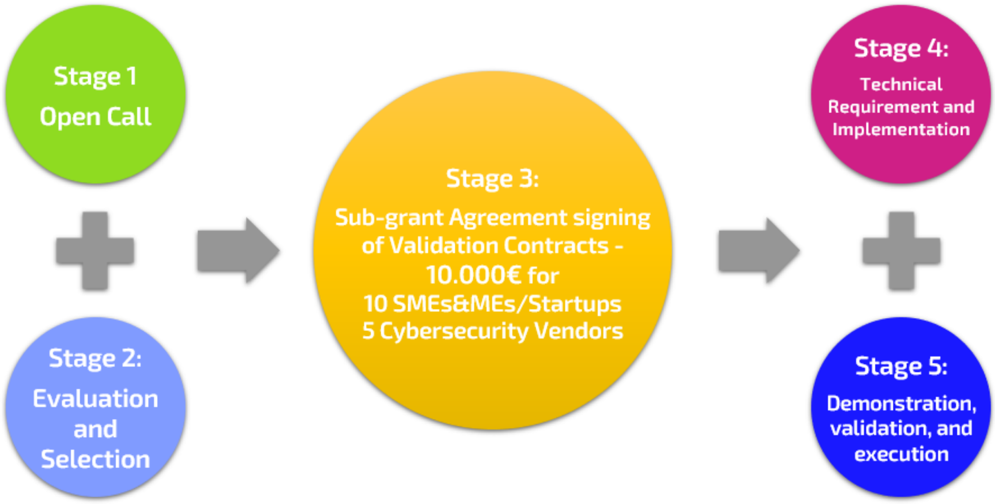
Stage 1
Open Call
Stage 2:
Evaluation and Selection
Stage 3:
Sub-grant Agreement signing of Validation Contracts - 10.000€ for 10 SMEs&MEs/Startups 5 Cybersecurity Vendors
Stage 4:
Technical Requirement and Implementation
Stage 5:
Demonstration, validation, and execution

Figure 2: PUZZLE Overall process

The work described in this document has been conducted within the project PUZZLE. This project has received funding from the European Union's Horizon 2020 (H2020) research and innovation programme under the Grant Agreement no 883540. This document does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of such content.

2. Announcement of the Validation Contracts Call

	Information to be provided by the project consortium
Call title:	PUZZLE Validation Contracts Call for Expressions of Interest
Full name of the EU funded project:	PUZZLE: Towards a Sophisticated SIEM Marketplace for Blockchain-based Threat Intelligence and Security-as-a-Service
Project acronym:	PUZZLE
Grant agreement number:	H2020–883540
Call publication date:	*08 February 2022.*
Call deadline:	*30 June 2022. at 17:00 (Brussels time)*
Expected duration of participation:	*10 months*
Total EU funding available:	150.000€ (10.000€ per proposal)
Submission & evaluation process:	The purpose of the Validation Contracts Call is to apply the services enabled by the PUZZLE Marketplace in various demonstrators and in the Validation Contracts to assess its architectural soundness, technical excellence and business value. The early adopters will be SMEs, MEs and cybersecurity vendors that will be engaged in the project through Validation Contracts where selected applicants will be granted with Validation Contracts that will allow them to cover expenses for interacting with the consortium and adopting the PUZZLE framework for the development of a small scale use case. In particular, ten (10) of the Validation Contracts to be distributed and will be rewarded to end-user **SMEs/start-ups** of varying size, from different industries and countries, to use the PUZZLE marketplace and services evaluating and validating the developed concepts and technologies, while the other five (5) validation contracts will be rewarded to

The work described in this document has been conducted within the project PUZZLE. This project has received funding from the European Union's Horizon 2020 (H2020) research and innovation programme under the Grant Agreement no 883540. This document does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of such content.

	SMEs/start-ups that are **cybersecurity solutions/services vendors** and would like to provide their offerings through the PUZZLE marketplace. Each one of the 15 validation contracts to be distributed will amount to 10.000€.
Further information:	Details available at https://puzzle-h2020.com/
Task description:	To increase PUZZLE awareness and ensure its sustainability throughout and after the project ends, PUZZLE will start testing and innovation activities by establishing a community of early PUZZLE framework adopters. This community will provide PUZZLE with highly-valued feedback, as well as help PUZZLE gain traction – from the utilisation of the framework right after the end of the project.

In Validation Contracts, there will be no personal data collection and processing and the PUZZLE functionalities will be tested by the Validation Contracts Call Participants in the secure framework provided for this purpose.

We note that through the Validation Contracts, PUZZLE will seek use cases from **IT-based and non IT-based SMEs not only in the areas of Healthcare, FinTech, Manufacturing, Agrifood, E-Government**, but also in **manufacturing, retails, construction, farming, education, logistics** (with strict security, privacy and operational assurance requirements), targeting SMEs/MEs offering services such as (indicatively):

- electronic **healthcare** records and patient support program services and solutions through the enablement of on-site patient training, medication delivery, reminders via different communication channels, laboratory results management;
- accessibility **to health tracking services** for the disabled, elderly and citizens in remote locations through the enablement of cloud computing and the Internet of Things;
- **mobile e-government** services targeting increasing citizen participation in nation- and EU-wide decision-making processes related, but not limited to, heath, culture preserving, education, and media policies through innovative communication channels;
- **e-Payment** services through the enablement of trusted mobile wallets for providing consumers with the capability to pay any co-operating merchant through several secure methods of the wallet; and

The work described in this document has been conducted within the project PUZZLE. This project has received funding from the European Union's Horizon 2020 (H2020) research and innovation programme under the Grant Agreement no 883540. This document does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of such content.

- promote **education and economic empowerment** throughout EU Member States by encouraging the development of apps, websites and online services that provide real value for EU youth.

3. Calendar

3.1 Stage 1: Proposals Validation Contracts Call

- Call opening on European Digital SME Alliance (DSME) platform [https://puzzle.digitalsme.eu/] on 08/02/2022.
- Deadline for submission via DSME Platform 30/06/2022, 17:00 (Brussels time)
- Evaluation from 01/07/2022 to 31/07/2022.
- Communication of results to applicants from 01/08/2022 to 31/08/2022.
- Negotiation and sub-grantees signature of contracts from 01/08/2022 to 31/08/2022.
- Execution of Validation Contract activities from 01/09/2022 to 30/06/2023 (ten months).

3.2 Stage 2: Criteria, evaluation, and selection

The selection will be performed by an evaluation committee. Applications will be peer-reviewed by 2 members of the consortium and 1 external evaluator (to be chosen by the consortium), resulting, at the end, in the selection of the 10 highly ranked cases of SMEs&MEs (maximum 2 cases per country) and 5 highly ranked cybersecurity vendors.

3.3 Stage 3: Sub-grantees signatures of Validation Contracts

The successful applicants will be granted a Validation Contract of 10.000,00€ each, to be used to cover both development costs in order to deliver their proposed cases, as well as one trip to one of the project's events, to meet the consortium and improve design of their cases.

It needs to be noted, that the Validation Contract will be redeemed at the end of the successful implementation of each such small case demonstrator, thus guaranteeing that the consortium will collect the appropriate feedback from each use case.

Negotiation and sub-grantees signature of contracts from 01/08/2022 to 31/08/2022.

The subcontracting process will be implemented in line with the national procurement procedures and with the art. 13 of H2020 MGA.

3.4 Stage 4: Technical requirements and Implementation

Start-ups/SMEs&MEs should propose and develop **a cybersecurity analytics solution focusing on edge and/or cloud analytic algorithms by devising ML/DL/AI or statistical computation methods** on top of their domain-specific infrastructure monitoring data samples, network or system flows (e.g., collected by edge proxy servers, production-level cloud application logs, data filtering and re-direction to the analytics systems, filesystem verification, etc.). The proposed **cybersecurity analytics solution** will be evaluated for its **novelty, efficiency and accuracy** as it will allow to intercept network data from a variety of

The work described in this document has been conducted within the project PUZZLE. This project has received funding from the European Union's Horizon 2020 (H2020) research and innovation programme under the Grant Agreement no 883540. This document does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of such content.

sources (i.e., eBPF flow logs, network traffic logs, etc.), perform analytics and extract insights by providing to users and central teams a better view about their cloud or edge applications.

An overview of the PUZZLE Logical Reference Architecture that the applicants have to consider during the preparation of their proposals is presented below. As highlighted in Figure 3, the PUZZLE technical components which should be considered by the applicants are mainly the PUZZLE Marketplace, the PUZZLE Dashboard, the Edge and Cloud Analytics. Their details are as follows:

1. The **PUZZLE Marketplace** encapsulates the central reference point where "templated" security services are offered, packaged, and advertised as Extended Berkeley Packet Filter (eBPF) programs/services. **Novel eBPF security programs should be part of your proposal**. **This should be the focus of Cybersecurity solutions providers / Cybersecurity services vendors.**
2. The Administrative and Operational Dashboard, hereafter **PUZZLE Dashboard**, which assists in instantiating some of the "templated" security services that are hosted on the **PUZZLE Marketplace**. The PUZZLE Dashboard will be the supportive front-end to upload, author and instantiate your services.
3. The **PUZZLE Security Orchestrator** which takes care of the entire deployment lifecycle of the cybersecurity services, as well as the required runtime adaptations upon the execution of the security services. The **Orchestration Worker** which incorporates the "local control plane" components of PUZZLE, i.e., the components that materialize the business logic that is "close" to the monitored and running service. Both the Orchestrator and the Worker will take care of the lifecycle of the developed eBPF security programs.
4. **Edge and Cloud Analytics with focus on cybersecurity insights should be part of your proposal**. **This should be the focus of Start-ups/SMEs&MEs proposal.** The analytics should incorporate selected Machine Learning, Deep Learning and Statistical Analysis algorithms from the family of Artificial Intelligence library that undertake "offline or online analytics" tasks, and assist on performing network data interception, traffic classification, malicious behaviour detection, network logs analysis and forecasting, packet indexing and data manipulation (i.e., replication, offloading, dropping, etc.), over the running cloud services of their domain-specific applications.

The work described in this document has been conducted within the project PUZZLE. This project has received funding from the European Union's Horizon 2020 (H2020) research and innovation programme under the Grant Agreement no 883540. This document does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of such content.

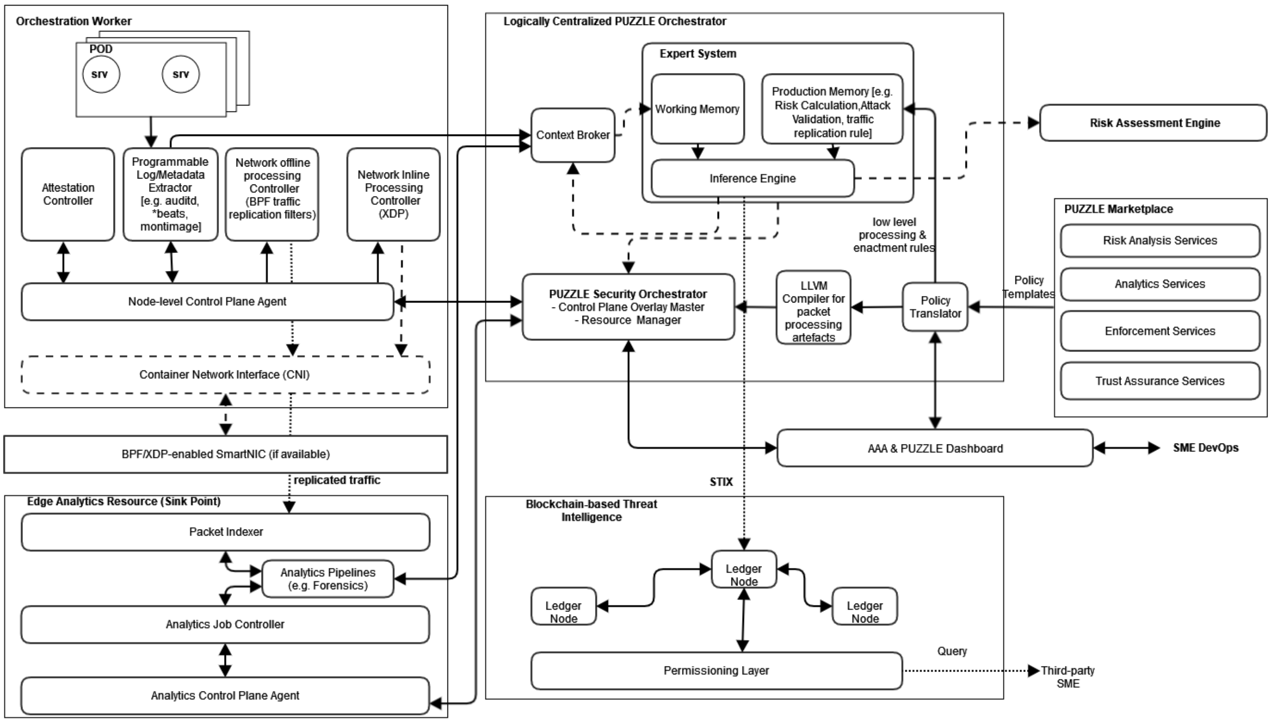
Orchestration Worker
POD
srv
srv
Attestation Controller
Programmable Log/Metadata Extractor [e.g. auditd, *beats, montimage]
Network offline processing Controller (BPF traffic replication filters)
Network Inline Processing Controller (XDP)
Node-level Control Plane Agent
Container Network Interface (CNI)
BPF/XDP-enabled SmartNIC (if available)
replicated traffic
Edge Analytics Resource (Sink Point)
Packet Indexer
Analytics Pipelines (e.g. Forensics)
Analytics Job Controller
Analytics Control Plane Agent
Logically Centralized PUZZLE Orchestrator
Expert System
Working Memory
Production Memory [e.g. Risk Calculation,Attack Validation, traffic replication rule]
Context Broker
Inference Engine
low level processing & enactment rules
PUZZLE Security Orchestrator - Control Plane Overlay Master - Resource Manager
LLVM Compiler for packet processing artefacts
Policy Translator
Policy Templates
Risk Assessment Engine
PUZZLE Marketplace
Risk Analysis Services
Analytics Services
Enforcement Services
Trust Assurance Services
AAA & PUZZLE Dashboard
SME DevOps
STIX
Blockchain-based Threat Intelligence
Ledger Node
Ledger Node
Ledger Node
Permissioning Layer
Query
Third-party SME

Figure 3: PUZZLE Logical Reference Architecture

Cybersecurity solutions providers / Cybersecurity services vendors:

The proposals presented and developed by the cybersecurity solutions / services providers should be **eBPF compliant and be applicable to the areas of interest** that are presented below. The Linux kernel is useful for implementing networking, observability, and security features. Whether adding modules or modifying kernel source code, developers have typically found they need to deal with abstracted layers and intricate infrastructure that are hard to debug. Extended Berkeley Packet Filter (eBPF)[1] is a kernel technology. It lets programs run without needing to add additional modules or modify the kernel source code. It can be conceived as a lightweight, sandboxed virtual machine (VM) within the Linux kernel. It allows programmers to run Berkeley Packet Filter (BPF) bytecode that makes use of certain kernel resources.

Inspiration about eBPF programs and services can be found in the L3AF Marketplace[2]. The L3AF Marketplace is an ongoing effort in the community and is similar with the PUZZLE Marketplace. L3AF provides eBPF based networking and observability solutions with the help of an advanced control plane. In the realm of networking, L3AF enables Kernel Function as a Service by providing complete lifecycle management of eBPF programs that instrument, inspect, and interdict traffic. These eBPF programs use low-level network hooks (e.g., XDP and TC) to give an ultra-high performance programmable network data plane that executes prior to the higher

[1] https://ebpf.io/

[2] https://l3af.io/

and slower layers of the Linux networking stack. eXpress Data Path (XDP) [3],[4] is a further step in evolution and enables to run a specific flavor of BPF programs from the network driver with direct access to the packet's DMA buffer. This is, by definition, the earliest possible point in the software stack, where programs can be attached to in order to allow for a programmable, high performance packet processor in the Linux kernel networking data path. On the observability side, L3AF provides a list of curated metrics by collecting and aggregating custom information generated at the source of the event in the kernel. These metrics provide detailed insight about cluster/node utilization and downstream/upstream network performance as well as traffic distribution across multiple clouds. L3AF provides deeper visibility into the system performance when compared with other programs, which rely on static counters and gauges exposed by the operating system (like /proc). L3AF also offers out-of-the-box integration with Prometheus[5] by maintaining full compatibility.

The proposal will be evaluated for its **novelty, diversity, efficiency and coverage on eBPF programs** while in this Validation Contracts Call, the areas of focus for cybersecurity solutions providers / cybersecurity services vendors are as follows:

Security: Extending the basic capabilities of seeing and interpreting all system calls and providing packet and socket-level views of all networking operations enables the development of revolutionary approaches to **system security**. Typically, entirely independent systems have handled different aspects of **system call filtering, process context tracing, and network-level filtering**. On the other hand, eBPF facilitates the combination of control and visibility over all aspects. This allows to develop security systems that operate with more context and an improved level of control.

Networking & Packet Processing: The combination of efficiency and programmability makes eBPF a good candidate for all **networking solutions' packet processing requirements**. The programmability of eBPF provides a means of adding additional protocol parsers, and smoothly programs any forwarding logic to address changing requirements without ever exiting the Linux kernel's packet processing context. The effectiveness offered by the Just-in-Time (JIT) compiler offers execution performance near that of natively compiled in-kernel code.

Tracing & Profiling: The ability to attach eBPF programs to trace points in addition to kernel and user application probe points enables visibility into the **runtime behavior of applications as well as the system**. By providing introspection capabilities to both the **system and the application side**, both views can be combined. This gives unique and powerful insights to troubleshoot **system performance issues**. Advanced statistical data structures let extract useful visibility data in an effective way, without needing the export of huge amounts of sampling data that is typical for similar systems.

[3] https://www.redhat.com/en/blog/capturing-network-traffic-express-data-path-xdp-environment

[4] https://github.com/iovisor/bpf-docs/blob/master/Express_Data_Path.pdf

[5] https://prometheus.io/

The work described in this document has been conducted within the project PUZZLE. This project has received funding from the European Union's Horizon 2020 (H2020) research and innovation programme under the Grant Agreement no 883540. This document does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of such content.

Observability & Monitoring: Rather than relying on gauges and static counters exposed by the operating system, eBPF allows for the generation of **visibility events and the collection and in-kernel aggregation of custom metrics** based on a broad range of potential sources. This increases the depth of visibility that might be attained and decreases the overall system overhead dramatically. This is achieved by collecting only the required visibility data and by producing histograms and similar data structures at the source of the event, rather than depending on the export of samples.

eBPF with Cilium [6], [7]**:** Cilium is an open-source project that provides eBPF-powered networking, security and observability. It has been specifically designed from the ground up to bring the advantages of eBPF to the world of Kubernetes and to address the new scalability, securit yand visibility requirements of container workloads. Cilium operates at Layer 3/4 to provide traditional networking and security services as well as Layer 7 to protect and secure use of modern application protocols such as HTTP, gRPC and Kafka.

Start-ups/SMEs&MEs:

As enterprises start serving live traffic out of private or public clouds, it is increasingly important for them to export network traffic flow data to serve security solutions that support advanced cybersecurity awareness on incidents, sophisticated threat protection, intrusion detection and reporting across the extended network, edge and cloud applications. Therefore, analytics solutions derived by network traffic logs can operate on the data streams or historical network logs and provide the needed analysis. However, the cybersecurity edge and cloud analytics require a set of preliminary steps to collect and prepare the data, train a model via Machine Learning or Deep Learning, extract useful insights or even detect malicious behaviors out of network logs. With the number of micro services growing by the day, without understanding and having visibility into an application's dependencies and data flows, it is difficult for both cloud service owners and centralized teams to identify **systemic or security issues**.

3.5 Stage 5: Demonstration, validation, and execution

Execution from 01/09/2022 to 30/06/2023.

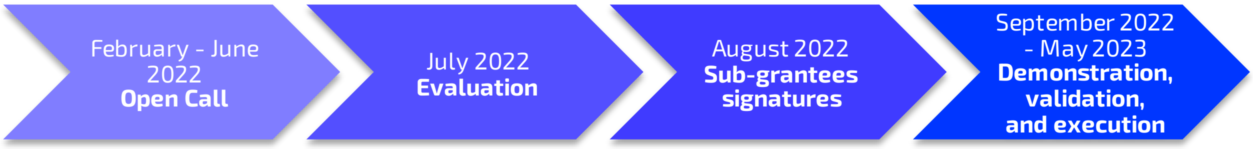

Figure 4: Timeline of the stages

[6] https://cilium.io/

[7] https://github.com/cilium/cilium

4. Beneficiaries

4.1 Types of Beneficiaries

PUZZLE Validation Contracts Call will accept applications with use cases from IT-based and non IT-based SMEs in the areas of Healthcare, FinTech, Manufacturing, Agrifood, E-Government, but also in different sectors and industries from **manufacturing, retails, construction, farming, education, logistics** etc. with strict security, privacy and operational assurance requirements.

4.2 Definition of SME & MEs

A SME will be considered as such if complying with the Commission Recommendation 2003/361/EC and the SME user guide. As a summary, the criteria which define a SME are:

- Headcount in Annual Work Unit (AWU) less than 250.
- Annual turnover less or equal to €50 million or annual balance sheet total, less or equal to €43 million.

4.3 Eligible Countries

Only applicants and End-users legally established and working as SME in any of the following countries will be eligible:

- The Member States (MS) of the European Union (EU), including their outermost regions;
- The Overseas Countries and Territories (OCT) linked to the Member States;
- H2020 Associated countries: according to the updated list published by the EC at https://ec.europa.eu/info/funding-tenders/opportunities/docs/2021-2027/common/guidance/list-3rd-country-participation_horizon-euratom_en.pdf
- Entities from Overseas Countries and Territories (OCT) are eligible for funding under the same conditions as entities from the Member States to which the OCT in question is linked.
- UK entities remain eligible for grants and procurement procedures as if the UK was a member state for the entirety of the Horizon 2020 framework programme, being this is also applicable to financial support to third parties according to Article 204 FR (cascading grants)

5. General Information

5.1 Means of Submission

The European Digital SME Alliance (DSME) platform will be the entry point for all proposals accessible at web location: https://puzzle.digitalsme.eu/. Submissions received by any other channel will be automatically discarded.

Documents required in subsequent stages will be submitted via dedicated channel, which will be indicated by PUZZLE consortium during the sub-granted projects execution.

The work described in this document has been conducted within the project PUZZLE. This project has received funding from the European Union's Horizon 2020 (H2020) research and innovation programme under the Grant Agreement no 883540. This document does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of such content.

5.2 Language

English is the official language for PUZZLE Validation Contracts Call. Submissions done in any other language will not be evaluated. English is also the only official language during the whole execution of the process. This means any requested submission of deliverables will be done in English in order to be eligible.

5.3 Documentation Formats

Any document requested in any of the stages must be submitted electronically in PDF format without restrictions for printing.

5.4 Data protection

In order to process and evaluate applications, PUZZLE will need to collect Personal and Industrial Data. UBITECH Ltd., as the Project Coordinator will act as Data Controller for data submitted through the European Digital SME Alliance (DSME) platform for these purposes. The DSME platform's system design and operational procedures ensure that data is managed in compliance with the General Data Protection Regulation (EU) 2016/679 (GDPR). Each applicant will accept the DSME terms to ensure coverage.

Please note that PUZZLE requests the minimum information needed to deliver the evaluation procedures or the Validation Contracts Call processes. The Bank account information, and Sub-grant Agreement templates, will be provided for reference and will only be requested if the SMEs&MEs/Cybersecurity Vendors are accepted in the Validation Contract process.

The Sub-Grant Agreement will introduce provisions concerning joint ownership of the results of the selected projects, if applicable. This will be assessed and negotiated case by case.

Please refer to https://www.digitalsme.eu/about/privacy-policy/ to check DSME platform data privacy policy and security measures.

All applicants must comply with ethical principles and relevant national, EU and international legislation such as the Charter of Fundamental Rights of the EU, the European Convention on Human Rights and the EU General Data Protection Regulation. At the stage of submitting a proposal for PUZZLE Validation Contracts Call all applicants are obliged to fill the ethically and security relevant issues Checklist offered by the DSME platform. If the applicants specify ethically relevant issues in the ethics issues checklist above, they must demonstrate how these issues will be considered and handled in the envisaged project by completing the Ethics Self-Assessment.

Applicants can read further practicalities in the EU official guide in *"How to complete your ethics self-assessment"*.[8] A proposal which contravenes ethical principles or any applicable

[8] Horizon 2020 Programme: Guidance: https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-self-assess_en.pdf

The work described in this document has been conducted within the project PUZZLE. This project has received funding from the European Union's Horizon 2020 (H2020) research and innovation programme under the Grant Agreement no 883540. This document does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of such content.

legislation, or which does not fulfil the conditions set out in Decision No 2013/743/EU, in the work programme, in the work plan or in the open call for proposals may be excluded from the evaluation, selection and award procedures at any time.

5.5 Origin of the Funds

Any selected proposer will sign a dedicated Sub-Grantee Funding Agreement with the members of the PUZZLE consortium. The funds attached to the Sub-Grantee Funding Agreement come directly from the funds of the European Project PUZZLE, and the consortium is managing the funds according to the grant Agreement Number 883540 signed with the European Commission.

This relation between the sub-grantees and the European Commission through PUZZLE project carries a set of obligations to the sub-grantees with the European Commission, and will be seen in the Sub-Grantee Funding Agreement template. The task of the sub-grantees will be to accomplish them, and of the PUZZLE consortium partners to inform about them.

5.6 Number of Proposals per Applicant

Only one proposal will be accepted for funding per SMEs&MEs, startups, Solution Vendors.

Given the fact this call is a competitive one, and the solutions will focus on a specific challenge or project, only one proposal per SMEs&MEs will be evaluated. In the case of a multiple submission by a SMEs&MEs, only the last one received (timestamp of the system) will enter our evaluation process, the rest being declared as non-eligible.

If the applicant is legally established and working as SMEs&MEs under the same name in any of the countries that are listed in this document will be considered valid for proposal and evaluation for the open call for the Validation Contracts.

If the last submitted proposal is declared non-eligible or fails to reach the thresholds of the evaluation, the other proposals submitted earlier will not be considered for evaluation in any case.

6. Submission of proposals

The submission will be done through the DSME platform (https://puzzle.digitalsme.eu) which is directly linked from the PUZZLE website (www.puzzle-h2020.com). This means the applicants can submit proposals as a guest, or register a profile at DSME to be able to submit a proposal. In order to be able to save their application and return to it at a later point, the applicants must create a profile.

If the applicant discovers an error in the proposal and provided that the deadline for the call has not passed, the applicant has the opportunity to take a step back, save each version and page of the application, edit as needed only if is logged-in. After the completion of the filling

The work described in this document has been conducted within the project PUZZLE. This project has received funding from the European Union's Horizon 2020 (H2020) research and innovation programme under the Grant Agreement no 883540. This document does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of such content.

process, it is necessary to submit the proposal by clicking the button. Only the latest, submitted version received before the call deadline will be taken into account in the evaluation.

It is strongly recommended not to wait until the last minute to submit the proposal. Failure of the proposal to arrive in time for any reason, including communications delays, automatically leads to rejection of the submission. The time of receipt of the message as recorded by the submission system will be definitive.

PUZZLE offers a dedicated support channel available for proposers at info@puzzle-h2020.com. Requests or inquiries about the submission system or the call itself, received AFTER the closure time of the call will neither be considered nor answered.

The documents that will be submitted are:

- Guidelines for Applicants
- Declaration of Honour
- SMEs&MEs Declaration
- Proposal Supplement

7. Evaluation Process

The Project is issuing the PUZZLE Validation Contracts Call for Expressions of Interest on February 8th, 2022. where interested parties would be requested to present their idea on how the PUZZLE Marketplace could complement the development activities of a product/service they are already providing to customers, detailing the PUZZLE parts/services utilized. PUZZLE's goal is to provide a transparent, fair, and equal evaluation process to all of participants. Submitted proposals will be evaluated as demonstrated in the figure below:

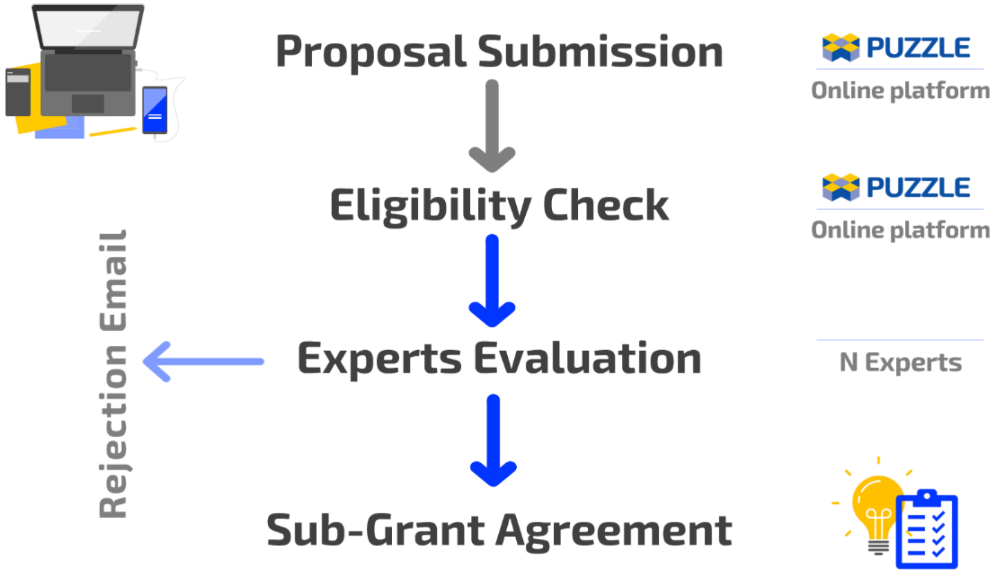

Figure 5: Validation Contracts Call submission and evaluation process

The work described in this document has been conducted within the project PUZZLE. This project has received funding from the European Union's Horizon 2020 (H2020) research and innovation programme under the Grant Agreement no 883540. This document does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of such content.

After that deadline, applications will be peer-reviewed by an experts evaluation committee resulting, in the end, in the selection of the 10 highly ranked cases of SMEs&MEs (maximum 2 cases per country) and 5 highly ranked cybersecurity vendors.

Applications will be peer-reviewed by 2 members of the consortium and 1 external evaluator (to be chosen by the consortium), resulting, in the end, in the selection of the 10 highly ranked cases of SMEs&MEs (maximum 2 cases per country) and 5 highly ranked cybersecurity vendors.

7.1 Eligibility Check

The eligibility check will be done on all proposals submitted before the deadline. All criteria are listed in section 6 of this guide for applicants and are also embedded in the online proposal submission platform offering applicants a real-time eligibility check monitoring. The provided platform also will inform the applicants in case their proposals fail to comply with one or more criteria and automatically requests from the proposers to make the corresponding modifications in order to meet them.

7.2 Experts Evaluation

In this phase, applications will be peer-reviewed by the experts' evaluation committee composed of 2 members of the consortium, proficient at IoT and cybersecurity fields, as well as 1 external independent evaluator with extensive know-how in the abovementioned domains, resulting, in the end, in the selection of the 10 highly ranked cases of SMEs&MEs (maximum 2 cases per country) and 5 highly ranked cybersecurity vendors.

Each project will be evaluated by the experts according to the following award criteria:

7.2.1 Excellence

The objectives of the application must be SMART (specific, measurable, assigned, realistic, time-bound) and must demonstrate a clear vision from the defined start to finish. The use of idea/product/service needs to suit the objectives and needs to support the path towards the marketplace deployment. TRL Level must be demonstrated to be, at least, between 7-9.

Weight: 1, Threshold: 3/5.

7.2.2 Impact

The potential impact of technical contributions or business cases should be based on realistic scenarios and should demonstrate how they can improve their services or products to test, enrich and assess the PUZZLE Services and, as an outcome –open the PUZZLE solution to a wider community. Applicants should also provide a brief plan for communicating with the public so that the community can monitor the progress and impact of the project.

Weight: 1, Threshold: 3/5.

The work described in this document has been conducted within the project PUZZLE. This project has received funding from the European Union's Horizon 2020 (H2020) research and innovation programme under the Grant Agreement no 883540. This document does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of such content.

7.2.3 Implementation

SMEs&MEs, startups, Solution Vendors that will receive the funding will have to prove that they have a team with management and leadership skills, and the ability to take a concept from ideas to a highly changing and evolving market. The team must be balanced and cross-functional, with a strong management background and skills-based.

Participants should also demonstrate the quality and effectiveness of the work plan, including the extent to which the resources available for the project activities are in line with their objectives and results. An important aspect is that you make it clear in the proposal that what you are proposing can be developed using the proposed AI solutions.

Finally, all applicants should describe in detail the targeted objectives (KPIs) and expected results of the project and identify the overall structure of the work plan to achieve them.

Weight: 1, Threshold: 3/5.

7.2.4 Added value contribution in terms of data provision

To prove the applicability, usability, effectiveness and value of the PUZZLE concepts, models and services in industrial, real-life infrastructures, and applications, selected PUZZLE artefacts will be made available for demonstration and testing under pragmatic conditions against a set of newly defined Use Cases.

The common objective for SMEs&MEs and cybersecurity vendors is to validate the overall PUZZLE Marketplace and put the project in the phase that can be aligned with its evaluation framework. Extending the evaluation of the Marketplace by running SMEs&MEs Use Cases and providing the results will also help the Project to prove the wide applicability of the different PUZZLE Services in various vertical domains. The objective from cybersecurity vendors, apart from validation, is to add their own cybersecurity services and report on how the PUZZLE Marketplace is evolving these extra services, and what is the added value of that inclusion.

Weight: 1, Threshold: n/a.

7.2.5 Scoring rules

The first three criteria will be scored with the following scale:

- 0: Proposal fails to address the criterion or cannot be assessed due to missing or incomplete information
- 1 (Poor): The criterion is inadequately addressed or there are serious inherent weaknesses
- 2 (Fair): The proposal broadly addresses the criterion, but there are significant weaknesses
- 3 (Good): The proposal addresses the criterion well, but a number of shortcomings are present
- 4 (Very good): The proposal addresses the criterion very well, but a small number of shortcomings are present

The work described in this document has been conducted within the project PUZZLE. This project has received funding from the European Union's Horizon 2020 (H2020) research and innovation programme under the Grant Agreement no 883540. This document does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of such content.

- 5 (Excellent): The proposal successfully addresses all relevant aspects of the criterion. Any shortcomings are minor.

Each evaluator will rank the proposal by assigning a score from 0 to 5 for criteria 1 to 3 and will prepare an individual evaluation report. The threshold for individual criteria will be 3. The overall threshold, which applies to the sum of the three individual scores, will be 10. The final score will be calculated as the average of the individual evaluations provided by the evaluators. If the scores on a project show a significant discrepancy between the three evaluators, a fourth evaluator will be assigned to provide an additional evaluation of this proposal.

For criterion 4, proposals that contribute to the added value of the PUZZLE framework will receive 1 extra point to the overall score. Candidates who do not expect to contribute will receive a score of 0.

Ties will be solved using the following criteria, in order:

- Impact score
- Implementation score
- Excellence score
- Date of submission: earlier submitted proposals go first.

Prior to making the decisions public, draft call results will be shared with the PUZZLE Project Officer at EC services. Feedback on the final evaluation will be managed through PUZZLE's website. All selected proposals will receive a brief summary evaluation report, either accompanied by a letter of rejection or an invitation to enter into an agreement.

Evaluation process from 01/07/2022 to 31/07/2022.

8. Additional Information

8.1 Validation Contracts Call Additional Material

Supported material:

- **Annex 1: Guidelines for Applicants**, this document, which provides the scope and objectives of the Validation Contracts Call,
- **Annex 2: Proposal Template,** an online application form, available at DSME platform (https://puzzle.digitalsme.eu/)
- **Annex 3: Proposal Supplement,** a word document providing information on proposal schedule, timing, Ethical & Security details
- **Annex 4: Declaration of Honour,** a word document, which declares that all conditions of the Validation Contracts Call are accepted by an SME legal representative.
- **Annex 5: SME Declaration**, a word document, which evaluates the status of the SMEs participating at an Validation Contracts Call
- **Frequently Asked Questions** & answers will be published at the DSME platform (https://puzzle.digitalsme.eu/).

The work described in this document has been conducted within the project PUZZLE. This project has received funding from the European Union's Horizon 2020 (H2020) research and innovation programme under the Grant Agreement no 883540. This document does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of such content.

9. Points of Contact

The PUZZLE consortium will provide information to the applicants via PUZZLE website, so that the information (question and answer), will be visible to all participants.

No binding information will be provided via any other mean (e.g. telephone or email).

More info at: https://puzzle-h2020.com/marketplace/validation-contracts-call/

Apply via: https://puzzle.digitalsme.eu/

PUZZLE support team: info@puzzle-h2020.com.

10. Disclaimer

This document may contain material that is copyright of certain PUZZLE beneficiaries and may not be reproduced or copied without permission. All PUZZLE consortium partners have agreed to the full publication of this document. The commercial use of any information contained in this document may require a license from the proprietor of that information.

The PUZZLE Consortium is the following:

PUZZLE consortium			
Number	**Participant organization name**	**Short name**	**Country**
1	UBITECH LIMITED	UBITECH	CYP
2	MELLANOX TECHNOLOGIES LTD	MELL	IL
3	INTRASOFT INTERNATIONAL SA	INTRA	LU
4	MONTIMAGE EURL	MONT	FR
5	AEGIS IT RESEARCH GMBH	AEGIS	DE
6	UNI SYSTEMS SYSTIMATA PLIROFORIKIS MONOPROSOPI ANONYMI EMPORIKI ETAIRIA	UNIS	GR
7	FOGUS INNOVATIONS & SERVICES P.C.	FOGUS	GR
8	SUITE5 DATA INTELLIGENCE SOLUTIONS LIMITED	SUITE5	CYP
9	UBITECH GIOUMPITEK MELETI SCHEDIASMOS YLOPOIISI KAI POLISI ERGON PLIROFORIKIS ETAIREIA PERIORISMENIS EFTHYNIS	UBI	GR
10	INSTITUTE OF COMMUNICATION AND COMPUTER SYSTEMS	ICCS	GR
11	IDRYMA TECHNOLOGIAS KAI EREVNAS	FORTH	GR
12	EUROPEAN DIGITAL SME ALLIANCE	DSME	BEL
13	POSLOVNO UDRUZENJE VOJVODJANSKI IKT KLASTER	VOICT	RS

The work described in this document has been conducted within the project PUZZLE. This project has received funding from the European Union's Horizon 2020 (H2020) research and innovation programme under the Grant Agreement no 883540. This document does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of such content.

The information in this document is provided "as is" and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

Moreover, it is clearly stated that the PUZZLE consortium reserves the right to update, amend or modify any part, section or detail of the document at any point in time without prior information.

The PUZZLE project, co-funded from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883540, foresees as an eligible activity the provision of financial support to third parties, as a mean to achieve its own objectives.

LEGAL NOTICE

Neither the European Commission not any person acting on behalf of the Commission is responsible for the use, which might be made, of the following information.

The views expressed in this report are those of the authors and do not necessarily reflect those of the European Commission.

Funding Scheme: Innovation Action (IA) ● Theme: SU-DS03-2019-2020 - Digital Security and privacy for citizens and Small and Medium Enterprises and Micro Enterprises
Start date of project: 01 September 2020 ● Duration: 36 months

The work described in this document has been conducted within the project PUZZLE. This project has received funding from the European Union's Horizon 2020 (H2020) research and innovation programme under the Grant Agreement no 883540. This document does not represent the opinion of the European Union, and the European Union is not responsible for any use that might be made of such content.