



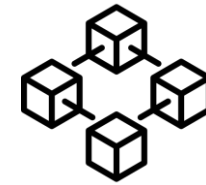
Towards a Sophisticated SIEM Marketplace
for Blockchain-based Threat Intelligence
and Security-as-a-Service



Welcome to PUZZLE

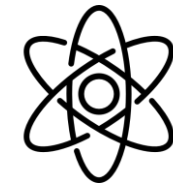
We help SMEs & Micro Enterprises monitor risks to their **digital security, privacy, and data protection**, by analyzing the (hw- and sw-) assets within the SME boundary.

- PUZZLE uses AI data processing to deliver insights and threat intelligence reports so that you are always aware of risk levels.
- PUZZLE builds resilience into your system by offering **cybersecurity management & orchestration services** to prevent danger and mitigate the impact of an attack if it happens. *This means that when something goes wrong - we're there for you.*



About the Project

- **Project title:** Towards a Sophisticated SIEM Marketplace for Blockchain-based Threat Intelligence and Security-as-a-Service.
- **Topic:** SU-DS03-2019-2020 / Digital Security and privacy for citizens and Small and Medium Enterprises and Micro Enterprises.
- **Start:** 01/09/2020. **End:** 31/08/2023.
- **Main Achievements**
 - ✓ Elicitation of privacy and security requirements of the PUZZLE Marketplace
 - ✓ Design of the PUZZLE Conceptual Architecture and building blocks – Defined and detailed MVP of the PUZZLE offering as a whole but also per key technological artefact
 - ✓ Identified unique PUZZLE Value Propositions
 - ✓ Developed the Ethics framework and the Data Management Plan of the Project
 - ✓ Validation Contracts

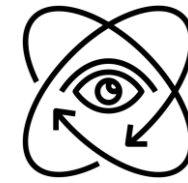


What is the core of PUZZLE?

It is an EU-funded project, a part of the Horizon 2020 programme, set to design and implement state-of-the-art cybersecurity, privacy and data protection management framework.

Marketplace:

PUZZLE is going to provide monitoring and visualisation tools, as well as a dashboard where information regarding sets of assets, vulnerabilities, identified threats and risks is going to be made available to end-users.



The Vision

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

Selected as one of the **most innovative new approaches in cybersecurity by the European Commission**, PUZZLE aims to strengthen cyber-safety also considering post-threat mitigation revolving around optimal security policy recommendation, thus, filling an important security gap for many SMEs, citizens and IT infrastructures on post-threat mitigation.

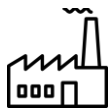
The Mission

FOR WHO?	HOW?	WHY?
<p>PUZZLE will enable a new mode of security and verification for mixed-criticality services running at various levels in the overall SME&ME business ecosystem stack.</p>	<p>Monitoring Agents collect infrastructural (cloud & app servers) and peripheral (edge) information; Risk Assessment provides insights on possible threats to be protected against; Security Recommender & Deployer Manager selects a set of cybersecurity services from the PUZZLE Marketplace; Analysis results are exposed via the Dashboard for advanced awareness; Threat Intelligence Information sharing between SMEs&MEs towards creating a common pool of potential APTs through the use of Blockchain.</p>	<p>Turn the business ecosystem into a real-time, verified ecosystem, governed by security enablers to safeguard correct state of all assets during the entire lifecycle of operation. Safeguard also attestation / verification & threat intelligence data sharing.</p>

Who we are?



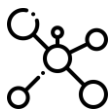
2 Universities



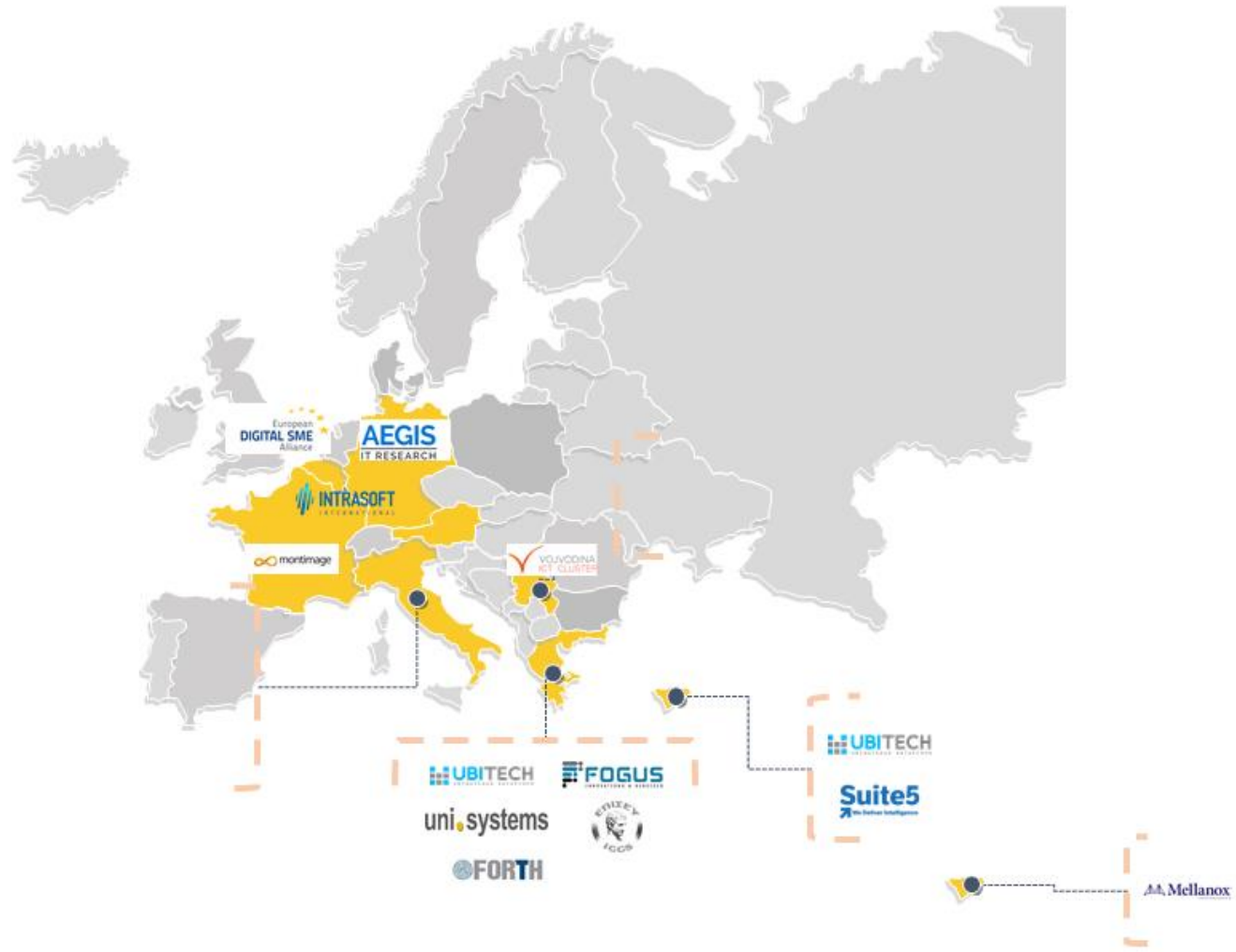
3 Industries



4 RTD SMEs &
2 SMEs as Demonstrators



2 Trade Association Clusters





The partners behind PUZZLE

The PUZZLE consortium contains some of the **strongest European players in cybersecurity**, and brings together **multidisciplinary competences and resources** from the academia, industry and research communities focusing on digital community, multi-dependency cyber-physical risk assessment, edge trust assurance services and remote attestation, distributed processing, programmable networking mechanisms, cybersecurity analytics, deep analysis and distributed machine learning, threat intelligence and blockchain technologies.

PUZZLE comprises **13 partners** representing research institutes, universities, technology providers, infrastructure providers (and users), and industrial partners (including eight SMEs&MEs) **from 8 EC member states and associated countries.**

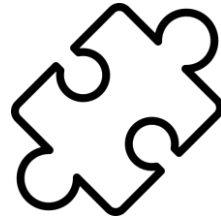


Safer tools. Better performance.



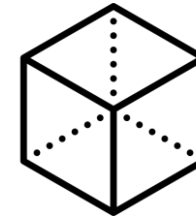
Cybersecurity

Cybersecurity is a complex and fast-evolving field, security professionals and experts working for SMEs & MEs need constant learning.



Challenges

Malicious online activity can cost enterprises everything. Protecting organisations is the paramount for the PUZZLE project.

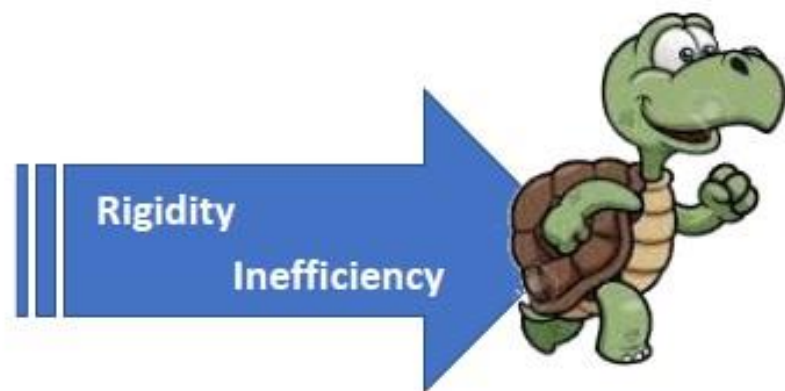
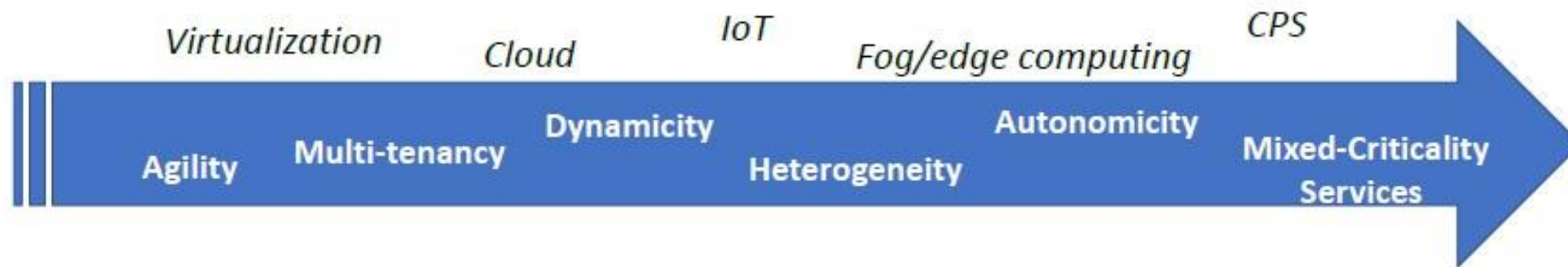


Innovation

Through state-of-the-art technologies including AI, trusted computing and Blockchain, SMEs & MEs will enhance their security and efficiently process information flows and online collaboration knowledge sharing.

Innovative. Reliable. Empowering. Trustworthy.

Motivation and Challenges



*[...] give all European SMEs&MEs access to comprehensive security operations solutions that are appropriate to their circumstances, are affordable, and are evolvable to **keep pace with escalating threats and innovations in technology and practice.***

ECSSO SRIA (June 2019)

PUZZLE Overview

1. Development of an **“easy-to-onboard”** and **“easy-to-deploy”** cybersecurity **services marketplace** for enterprises.
2. Conceptualization and development of **cyber threats data modelling and risk assessment models**.
3. Personalized cybersecurity functions per business.
4. Enhanced operational assurance and detection capabilities.
5. Automated orchestration of advanced security deployments.
6. Configurable incentives for new and existing enterprises to join the PUZZLE Marketplace.
7. Tools and mechanisms for continuous cyberwarfare training and cybertechnology development.



Main Goals

The PUZZLE framework envisions to offer the following value propositions:

- Develop a cybersecurity, privacy & data protection **management framework**
- **Facilitate the collection, processing & exchange** of data & knowledge sharing among SMEs respecting cyber threats & vulnerabilities
- **Provide** a set of network & edge cybersecurity functional primitives as a service
- **Suggest optimal** mitigation strategies and policies & support their enforcement
- **Increase cybersecurity** situation awareness & preparedness of SMEs&MEs, through an innovative set of monitoring tools

Approach

The key technologies applied in PUZZLE to enhance the security & privacy posture:

- Marketplace for cybersecurity solutions & services
- Programmable Network Security Mechanisms
- Advanced Cybersecurity Analytics
- Dynamic Real-time Risk Assessment
- Edge Trust Assurance Services based on the use of trusted computing technologies
- Blockchains for enhanced threat intelligence knowledge sharing
- Deployment of Optimal & Adaptable Security Policies
- Decouple the service business logic from the security management
- Automate security management and response to threats, security incidents and attacks
- Optimal security deployment plans per target business ecosystem
- Reduce the run-time overhead of security processing

Value Proposition & Ambition

- **Security-as-a-Service** Marketplace
Externalization of security processes
- **Edge-cloud** Applications and Services
- **Optimal** Security Policy Recommendation
- **Programmatic** Inspection and Monitoring
- **Portability**
- Service **Orchestration**
- **Threat Intelligence Sharing**
- **On-boarding** of Innovative Security Services to the Marketplace

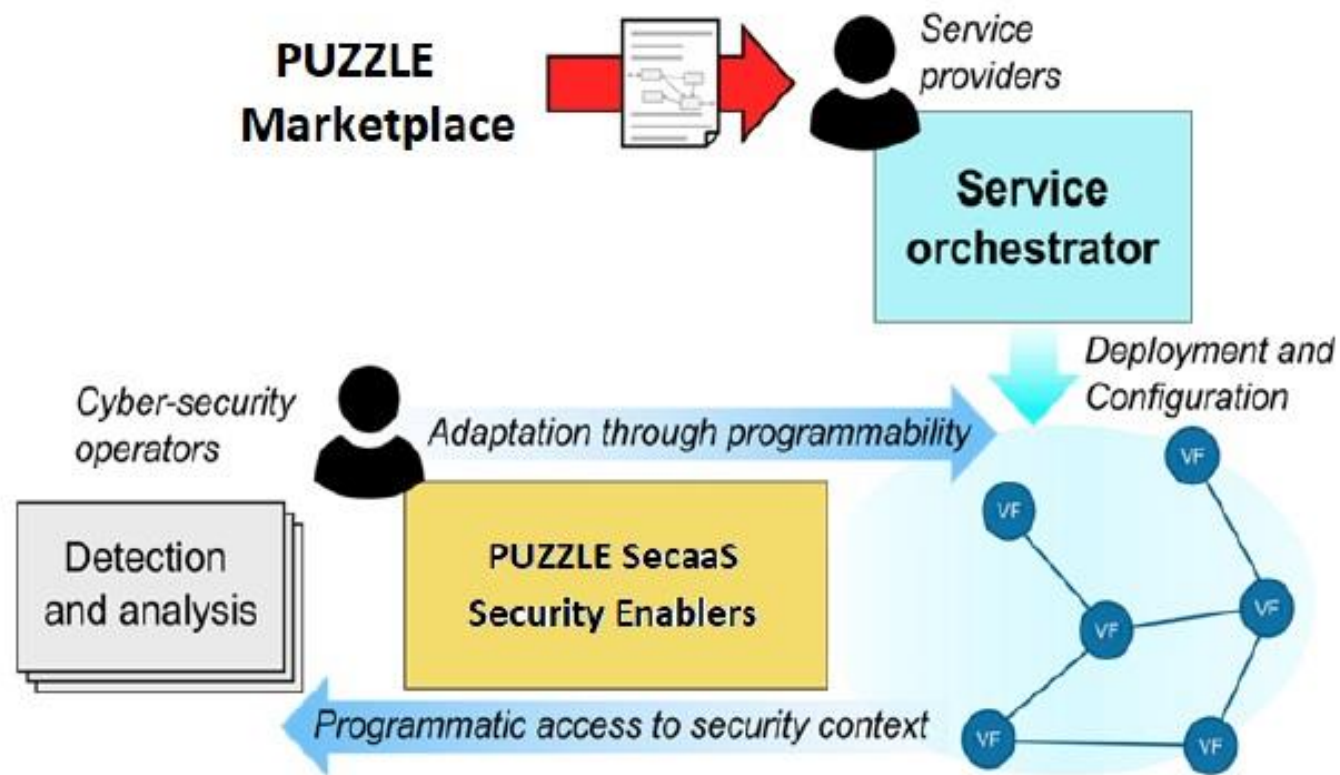


Concept

“A flexible platform that **runs a number of complementary security services** (for detection and analysis) and **feeds them with the appropriate context** from a dynamic and evolving system”

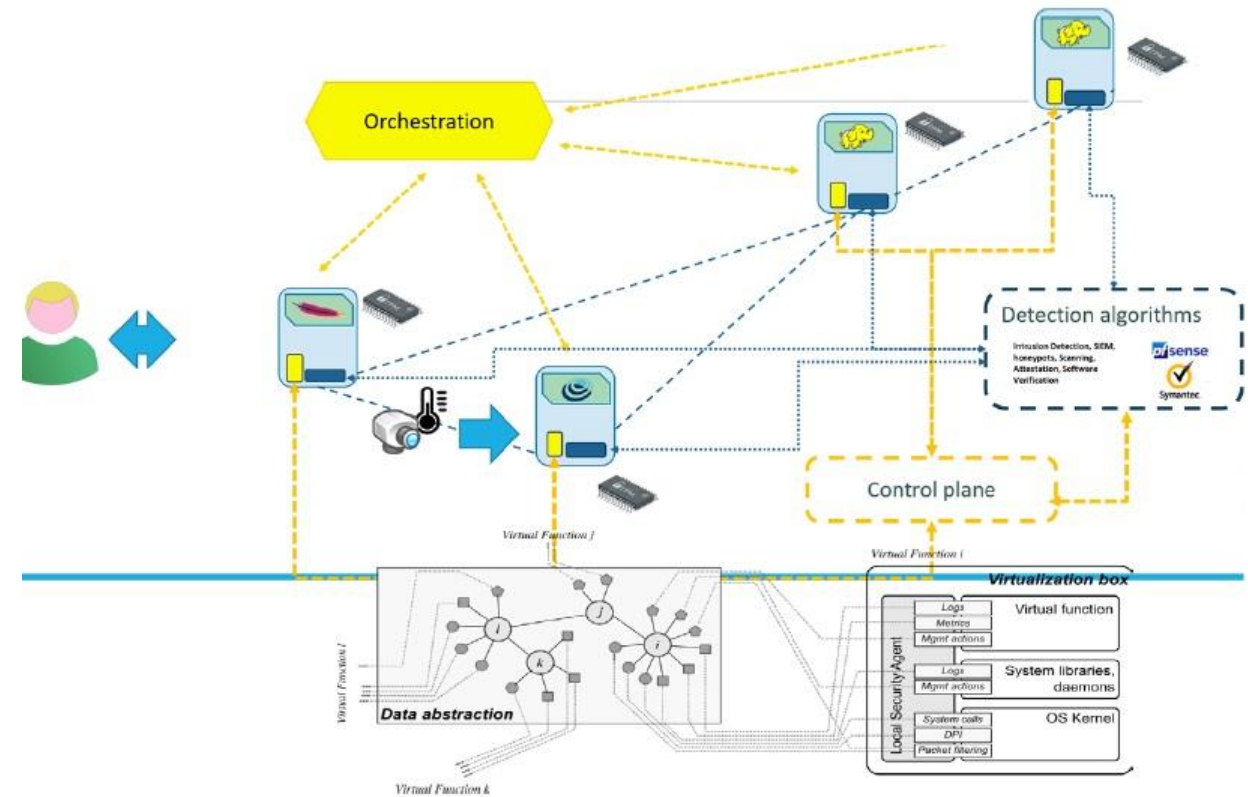


Orchestrate security processes



PUZZLE Conceptual Architecture

- Development of PUZZLE's ecosystem cyber threats data and risk model
 - **Risk Management**
 - **Risks, Threats, Assets, Attack Types, Vulnerabilities, Control Elements**
- Optimal Security Policy Recommendation
 - **Constraint Solver**
- Advanced Intrusion Detection, continuous RA, SIEM, honeypots, etc.
- **Trusted Computing**–Attestation and Verification Methods
- Cyber-security Analytics
- Threat Intelligence Information Sharing



OPEN CALL LAUNCHED

CLOSED



APPLY NOW

VALIDATION CONTRACTS OF **€10.000**
FOR **10** HIGHLY RANKED SMEs & MEs
AND **5** HIGHLY RANKED CYBERSECURITY VENDORS.

What is the PUZZLE Validation Contracts?

“ To open up the services uptake and **testing activities** 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**.

PUZZLE project came up with **Validation Contracts** concept. The aim is to provide SMEs&MEs who deal with cybersecurity, privacy and personal data protection a **set of tools and solutions** of varied sophistication levels, to allow them to benefit from the innovative targeted solutions that the PUZZLE Marketplace offers, **addressing their specific needs and available resources**.

What is the PUZZLE Validation Contracts?

Through Validation Contracts (*Contest/Open Call*) the interested parties were invited to present **their ideas** 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**.

“ PUZZLE aims to employ highly usable cybersecurity, privacy and data protection management framework in two directions:

- **SMEs&MEs and Cybersecurity providers.**

Validation Contracts of €10.000

In the Open Call, the project sought use cases **from IT-based or non-IT-based SMEs&MEs** with the overall objective to evaluate the Marketplace from two perspectives:

- from the **end-user perspective** for SMEs&MEs in various verticals and domains
- 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 PUZZLE Validation Contracts will award selected applicants with a grant of 10.000€!

The selection process was performed by an evaluation committee, peer-reviewed by 2 members of the consortium and 1 external evaluator.

Validation Contracts Partners

- ✓ **Advanced Cyber Security**
- ✓ **Advanced Microturbines**
- ✓ **Enthec**
- ✓ **HOP Ubiquitous SL**
- ✓ **Level7**
- ✓ **Positive Ltd**
- ✓ **Quadible**
- ✓ **R2C System**

Through a series of Innovation Workshops to be held with the participants in the Contracts, the PUZZLE project will also deliver cybersecurity awareness training and share best practices for SMEs, so that along technical improvements in their cybersecurity, companies are also able to implement a better cybersecurity culture within their organisation.

Validation Contracts: Objectives

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** 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**.



Safer tools. Better performance.



www.puzzle-h2020.com

Newsletter? Get started! info@puzzle-h2020.com

Follow us on Social Media [@H2020Puzzle](https://twitter.com/H2020Puzzle)



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883540. The sole responsibility for the content of this presentation lies with the author(s) and in no way reflects the views of the European Union.