PUZZLE project Overview

A holistic Security as a Service framework for safeguarding cloud-based asets of SMEs & MEs

UBITECH Mellanox netcompany intrasoft montimage AEGIS IT RESEARCH uni.systems FOGUS Suite5 FORTH European DIGITAL SME Alliance VOIVODINA ICT CLUSTER

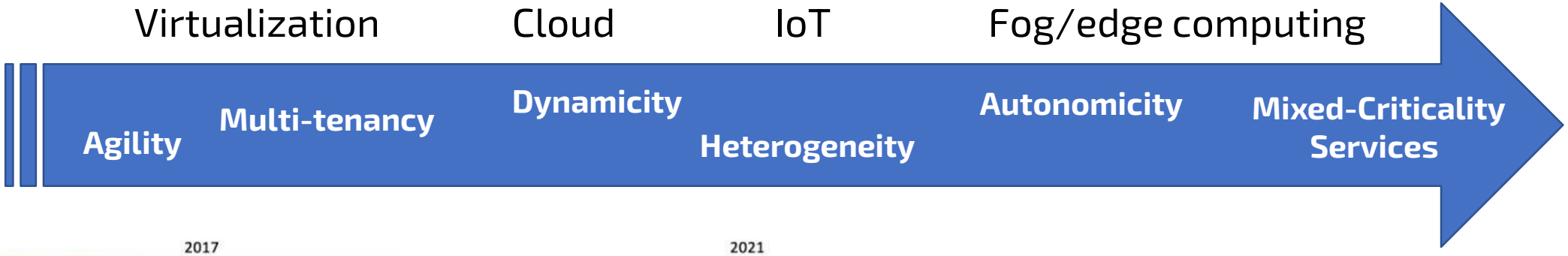
Our Motivation

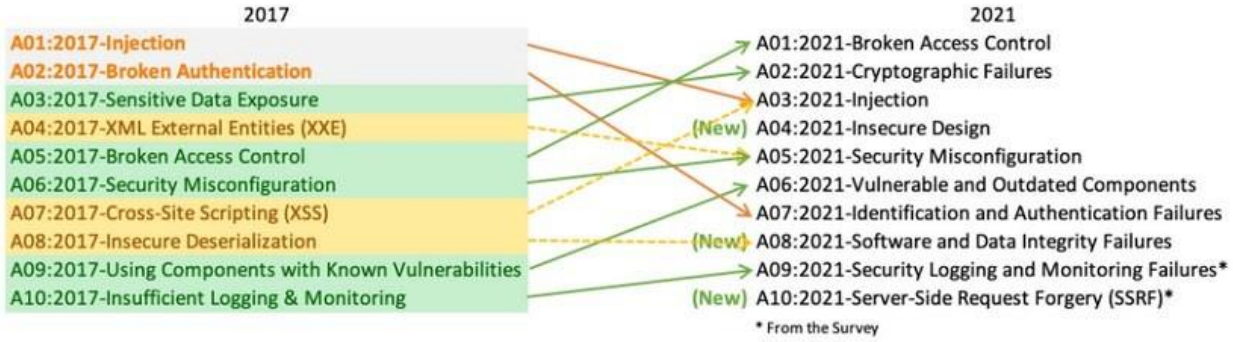
SMEs/MEs (and beyond) must be safe, trusted and secure.
However, they might not have adequate resources to be able to employ the latest trend in security services nor to be able to monitor all (security and attack) advancements;

Compliance with emerging security regulations on security and privacy protection is critical but it is also a challenging task

PUZZLE can help!

Motivation and Challanges





Ensure trusted execution of (insecure) components

Firmware & Software compliance to execution policies

[…] 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****.*

ECSO SRIA (June 2019)

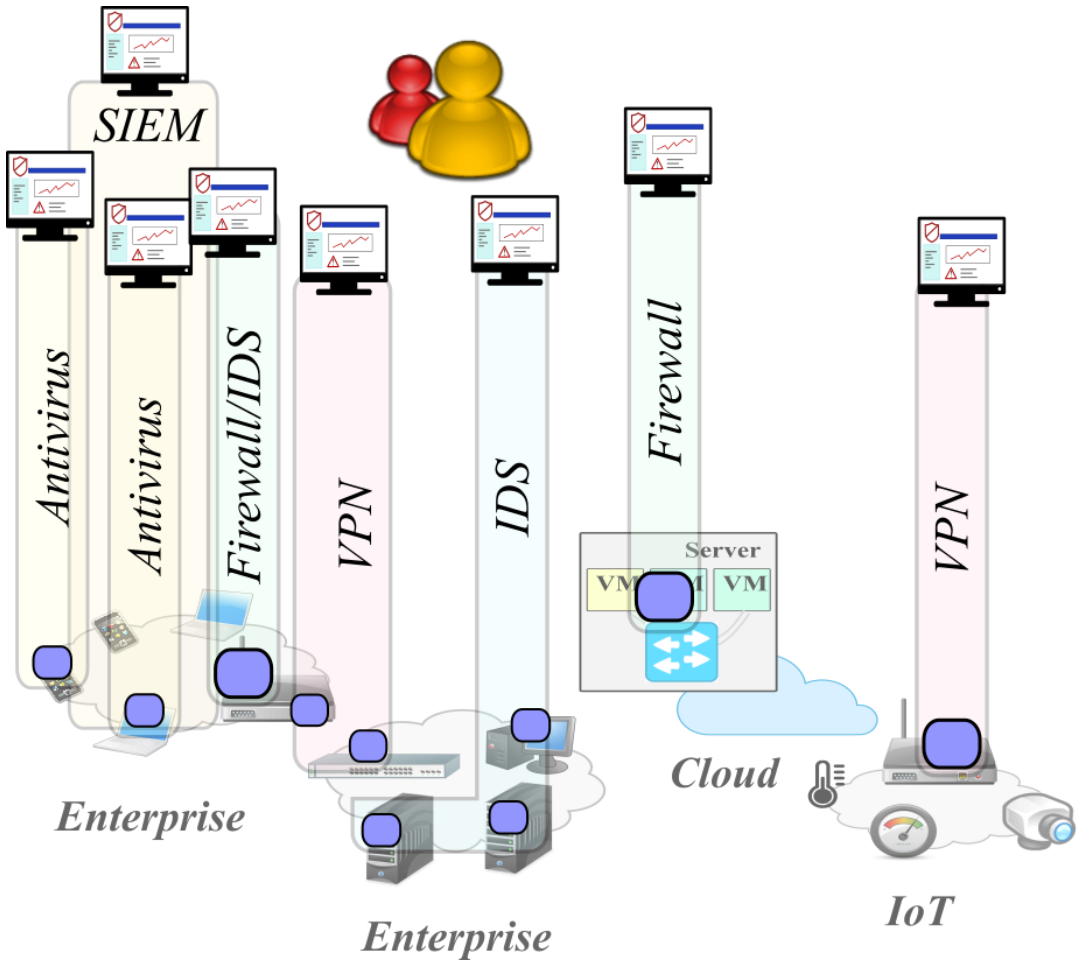
Challanges

- **Long-term security and operational assurance** in SMEs&MEs not easy to achieve due to lack of resources
- New applications and resources are used -> Multiple exploration points for attackers & New Opportunities for cyber-security attacks
- Modern architectures build on distributed services, exposed API endpoints, microservices and containers provide an even bigger attack surface that is not easy to be protected
- Applicability and Usability of security services can be challenging
- Risk-based Classification and Regulatory Compliance is not widely available
- Lack of expertise and trained personnel in SMEs&MEs

Current Landscape

Currently, security operations involves

- Use of **a number of largely independent software tools**, with coordination, decision making and integration being the result of **human cooperative activity**.
- Timely detection and response are already problematic under this arrangement
- **Ever-increasing automation and integration of security operations processes** will be necessary to keep pace.
- Intelligent decision making is required



SMEs also buy security services from third parties – In some cases contradicts privacy requirements

What is needed

- Security Marketplace accessible to everyone – "**Security-as-a-Service**"
  - Allowing SMES & ME to keep track of the latest advancements
- Policy based **protection techniques and mechanisms**
  - To allow assets to perform within a predetermined envelope of acceptable behavior
- **Easy to adopt** protection mechanisms with support of the latest IT trends
  - Support modern, distributed application designs
  - Support for cloud, multi-cloud or even cloud-to-edge deployments
- Efficient ways for **certifying the correct behavior** of heterogeneous systems (i.e., ENISA)
  - Usage of trusted service graph chains

Why PUZZLE

- **Lack of common and uniform Security Service Marketplace**
  - "***Security-as-a-Service***" *APIs in SMEs&MEs secure management software*
  - *Monitoring & Introspection, Distributed Firewall, SIEM, etc.*
- **Lack of edge-cloud interoperability met in today's business ecosystems**
  - *Network Security Functions for SMEs&MEs for delivering cost-effective managed security services*
- **Emergence of service-oriented orchestration paradigms**
  - More automation in design, deployment, re-configuration
  - Optimal security policy deployment during run-time

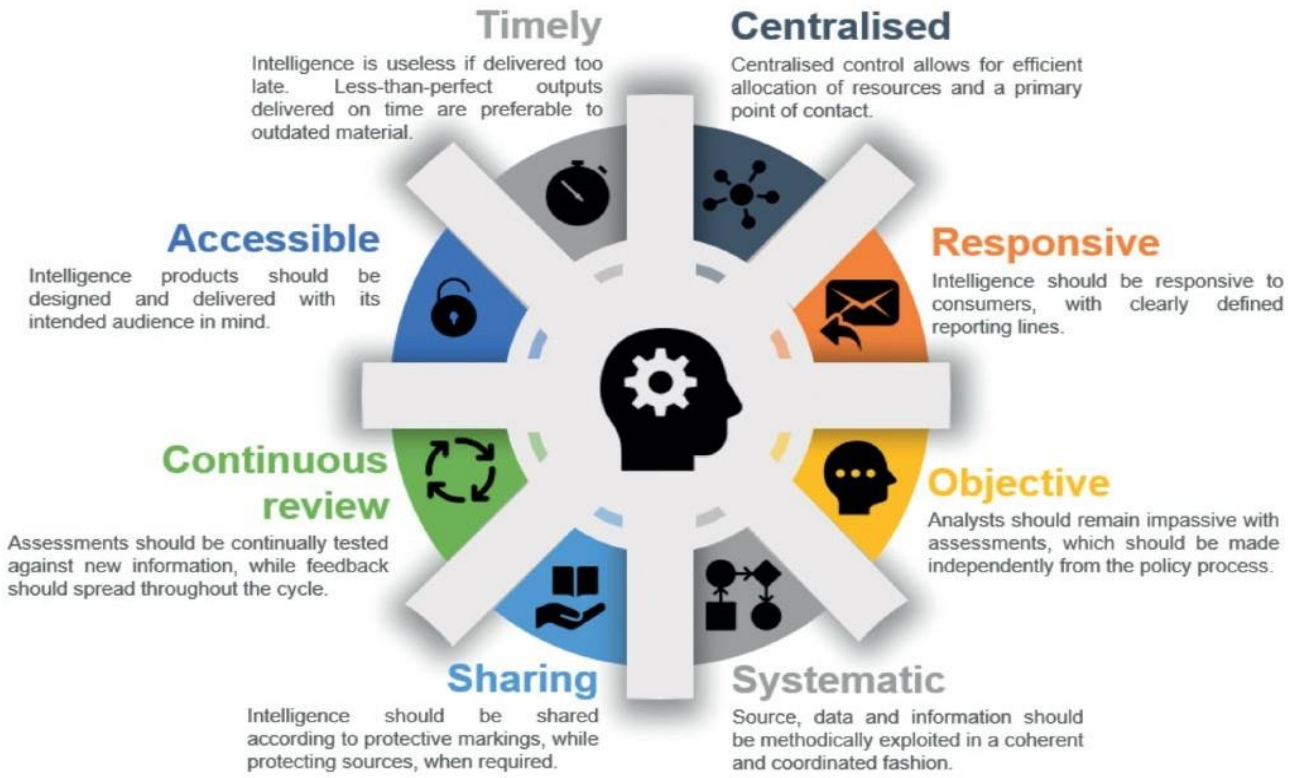
PUZZLE Vision

Reference Project and Catalyst for establishing Trusted Service Graph Chains in SMEs/MEs (and beyond) addressing **Security**, **Safety** and various levels of **Trustworthiness** for mixed-criticality services.

Implement the transition to **Zero Trust** concept with the principle *"Never Trust, Always Verify"* for assuring vertical trust for all assets comprising the target business ecosystem

Furethermore… Threat Intelligence Sharing

- *Different levels of threat intelligence*
- *Secure, privacy-preserving and accountable information sharing*
- *Use of Blockchain-Market*
- *Strengthen European Digital Solutions by the creation of such an enhanced threat intelligence market*



PUZZLE Performs Cutting-Edge Research in „Security-as-a-Sevice Orchestration, Vulnerability Analysis, Policy Management

Enhanced Operational Assurance

Increase trust to a network by detecting misbehaviours without impeding performance in a Zero Trust paradigm – **Multitude of security enablers covering a wide spectrum of attack vectors**

Risk Assessment

Identity risk interdependencies in a service graph chain that can affect the safety of the system

Threat Intelligence Information Sharing

Secure and auditable sharing of operational and attestation data only to authorized & authenticated devices & users – **Useful for Certification**

Policy Management & Enforcement

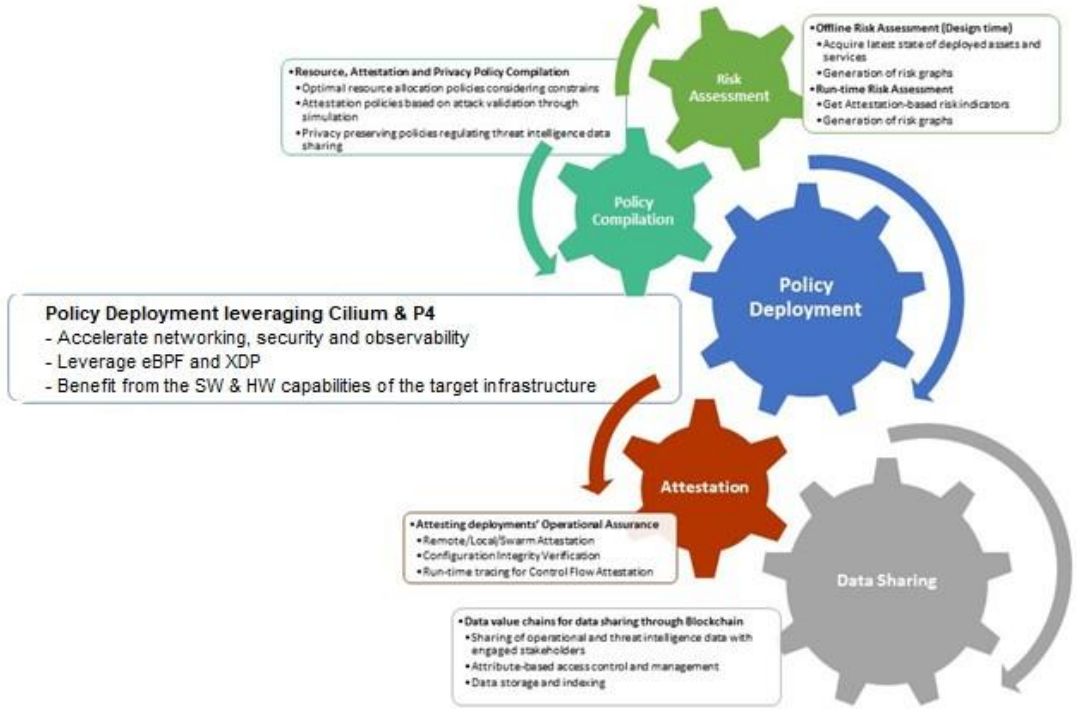
(Re-)Calculation and deployment of network, service and traffic integrity security policies – **Security Worker agents working in tandem enhancing Usability**

Tracing & Monitoring Capabilities

How to efficiently monitor and extract "knowledge" from both network traffic but also from the execution of assets – **Leverage the new technology of eBPFs & XDPs**

Security Awereness

"Security-as-a-Service" approach encompassing a wide range of features including security service discovery, service authentication, observability, vulnerability analysis, etc.



PUZZLE Key Technologies

Risk Assessment

- Identification & Calculation of risk interdependency graph
- Based on definition of hw- & sw-assets from the system administrator
- Prerequisite for the calculation of optimized set of security policies

Innovation

- Consider both security & privacy related vulnerabilities
- Attack Path Calculation

Modes Of Operations

- Design & Runtime

Policy Recommendation & Management

- Calculation of the optimized set of security policies
- Leverage SW- and HW-capabilities of the target infrastructure
- Security and Context Awareness

Innovation

- Different dimensions – convergence of security, safety, and resource
- Enhancing Usability
- Adoption of latest trends in policy definition – Cilium and P4

Modes Of Operations

- Design & Runtime

Attack Validation Component

- Virtual representation of the physical devices
- Processing of real-time system raw traces for attack path identification
- Simulation & Emulation of various attack vectors

Innovation

- Device Behavioral Analysis
- Mutation Fuzzing & Concolic Testing

Modes Of Operations

- Design & Runtime

Security Services

- Detect both network- and host-based misbehavior
- AI-based Analytics
- Attest both the correct configuration & execution of target system
- Different type of security enablers depending on identified risks

Innovation

- ML-based Traffic Classification
- Lightweight attestation capabilities
- System real-time monitoring through the use of eBPFs

Modes Of Operations

- Runtime

PUZZLE Key Technologies

Security Service Orchestration

- Orchestrate the deployment of both ML- based analytics and attestation enablers depending on risks
- Enhanced applicability and usability through the adoption of Kubernetes orchestration
- Easy to consider additional security services

Innovation

- Applicability & Usability
- Kubernetes-based Orchestration
- Automatic (re-) deployment of security controls

Threat intelligence Information Sharing

- Blockchain-based threat intelligence information exchange
- Auditability of all data transactions
- Secure information exchange & data sharing

Innovation

- Certification Capabilities
- Privacy preservation
- Decentralized Threat Intelligence Information Marketplace

Security Marketplace

- Centralized platform for finding additional security services
- Allowing SMEs & MEs to be up to date with latest security services
- Services can be added by third-parties, content moderated by PUZZLE consortium

Innovation

- Policy based marketplace
- Easy to integrate to private PUZZLE security orchestration setups

Real-time Monitoring & Tracing Capabilities

- Real-time monitoring and tracing of both network- and host-based behavior
- SW-based
- Lightweight enough to operate in constrained environments

Innovation

- Does not affect application performance
- Non-intrusive
- eBPF and XDP

Time for Demo!

UBITECH Mellanox netcompany intrasoft montimage AEGIS IT RESEARCH uni.systems FOGUS Suite5 FORTH European DIGITAL SME Alliance VOJVODINA ICT CLUSTER

Current Status

- Puzzle Platform **up and running**
  - Under development the 2nd release
    - Final release of the tools
    - Final Integrated PUZZLE platform will be provided in the next few months
- Demo **Kubernetes cluster** for testing available
  - Or you can bring your own Kubernetes Cluster
- Instructions available online
  - Online Documentation www.puzzle-h2020.readthedocs.io
  - Demo usage videos also available
- Different testing scenarios onboarding:
  - Policy providers
  - Policy users
  - Custom integration stories

PUZZLE

Safer tools. Better performance.

Website	**www.puzzle-h2020.com**
Newsletter	**office@puzzle-h2020.com**
Social Media	**@H2020Puzzle**

UBITECH · Mellanox · netcompany intrasoft · montimage · AEGIS IT RESEARCH · uni systems · FOGUS · Suite5 · FORTH · European DIGITAL SME Alliance · VOJVODINA ICT CLUSTER