Safer tools.
Better performance.

Project funded by
European Union

PUZZLE Framework
Technical Concept & Approach

Thanassis Giannetsos

UBITECH Ltd., Digital Security & Trusted Computing Group

agiannetsos@ubitech.eu

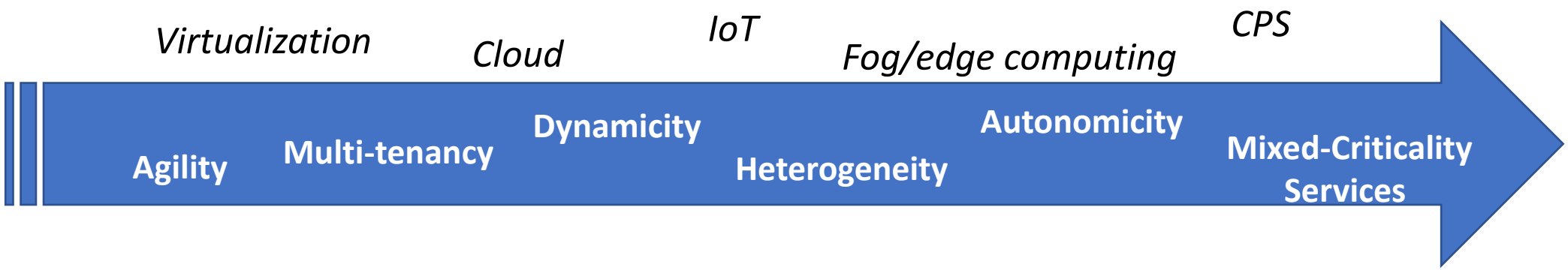
PUZZLE VISION

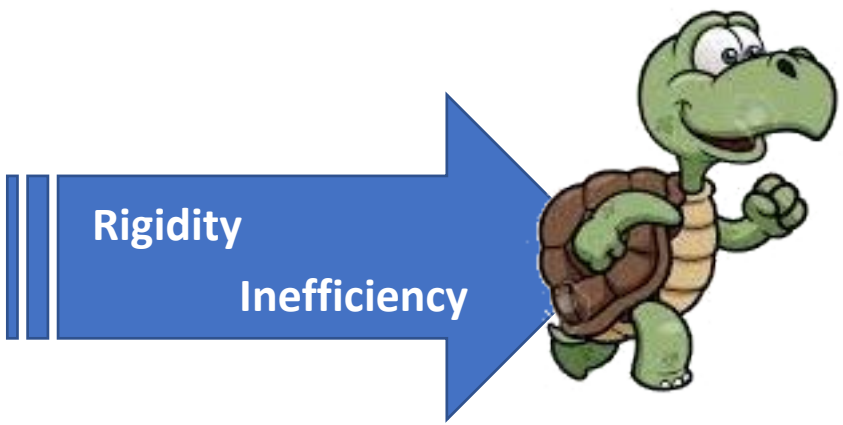
PUZZLE aims to deliver a novel approach of providing cybersecurity services through a marketplace ("As-a-Service"), easy to adopt and deploy within a business ecosystem and computational infrastructure; highly usable cybersecurity, privacy and data protection management framework. Dynamic monitoring and forecasting of threats, identification of optimal security policies and deployment of dynamic PUZZLE Agents for efficient and secure collection of edge and network data. This is also coupled with the creation of a threat intelligence data marketplace through the integration of Blockchains.

- **FOR WHO?** PUZZLE will enable a new mode of security and verification for mixed-criticality services running at various levels in the overall business ecosystem stack
- **WHY?** Turn the business ecosystem into a real-time verified ecosystem governed by security enablers to safeguard the correct state of all assets during the entire lifecycle of operation.
- Safeguard also attestation/verification & threat intelligence data sharing.

PUZZLE

MOTIVATION & 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****.*

ECSO SRIA (June 2019)

PUZZLE

MOTIVATION & CHALLENGES

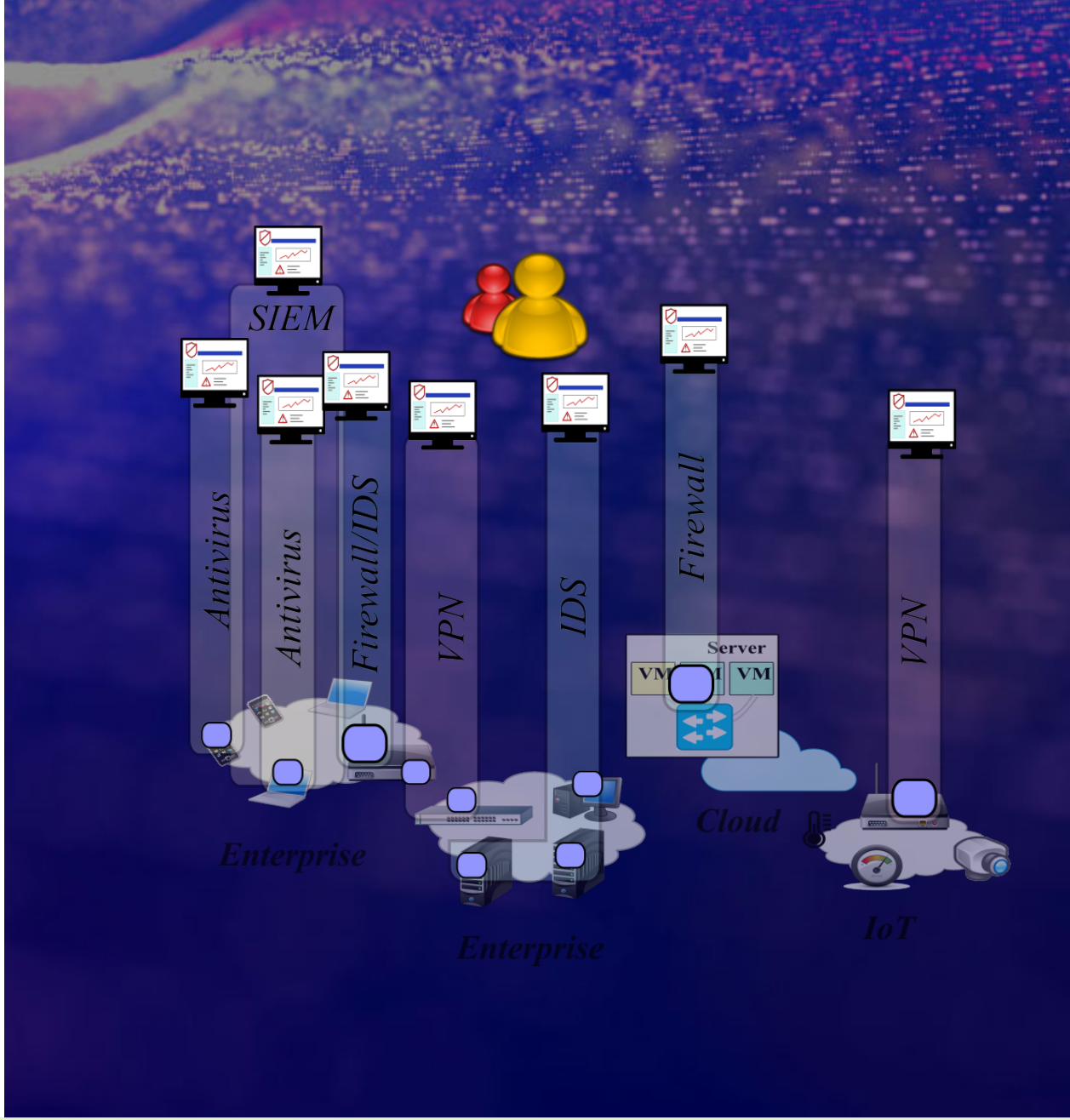
*Cyber-space is effectively **without frontiers** […]. Strategic management of Critical Information Infrastructures has to balance the benefits created through "**ease of connection and remote control**" versus the increased level or risks. […]*

*The externalisation of IT resources to outside providers and new approaches to hardware, such as BYOD make **the notion of perimeter obsolete**. Intrusion Detection Systems need to adapt in order to be able to work in an environment where there is no perimeter.*

PUZZLE

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. More of the decision making authority will need to be devolved to intelligent software, with human analysts taking on a goal-setting, supervisory role and working in co-operation with autonomous software agents.*



PUZZLE

A CROWDED MARKET SEGMENT

Closed verticals vs Open source

PUZZLE

WHY PUZZLE?

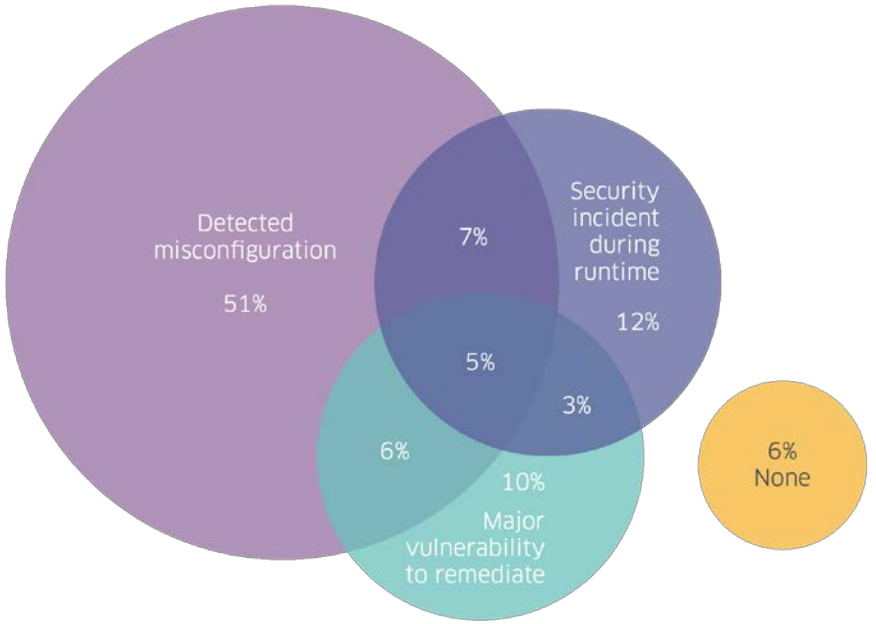
- **Lack of common and uniform Security Service Marketplace**
  - ***"Security-as-a-Service"*** *APIs in SMEs&Mes secure management software*
  - *Monitoring & Introspection, Distributed Firewall, SIEM, etc.*
- **Lack of edge-cloud interoperability met in today's business ecosystems**
  - *Network Security 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

TOP SECURITY PRIORITIES FOR SMEs & MEs

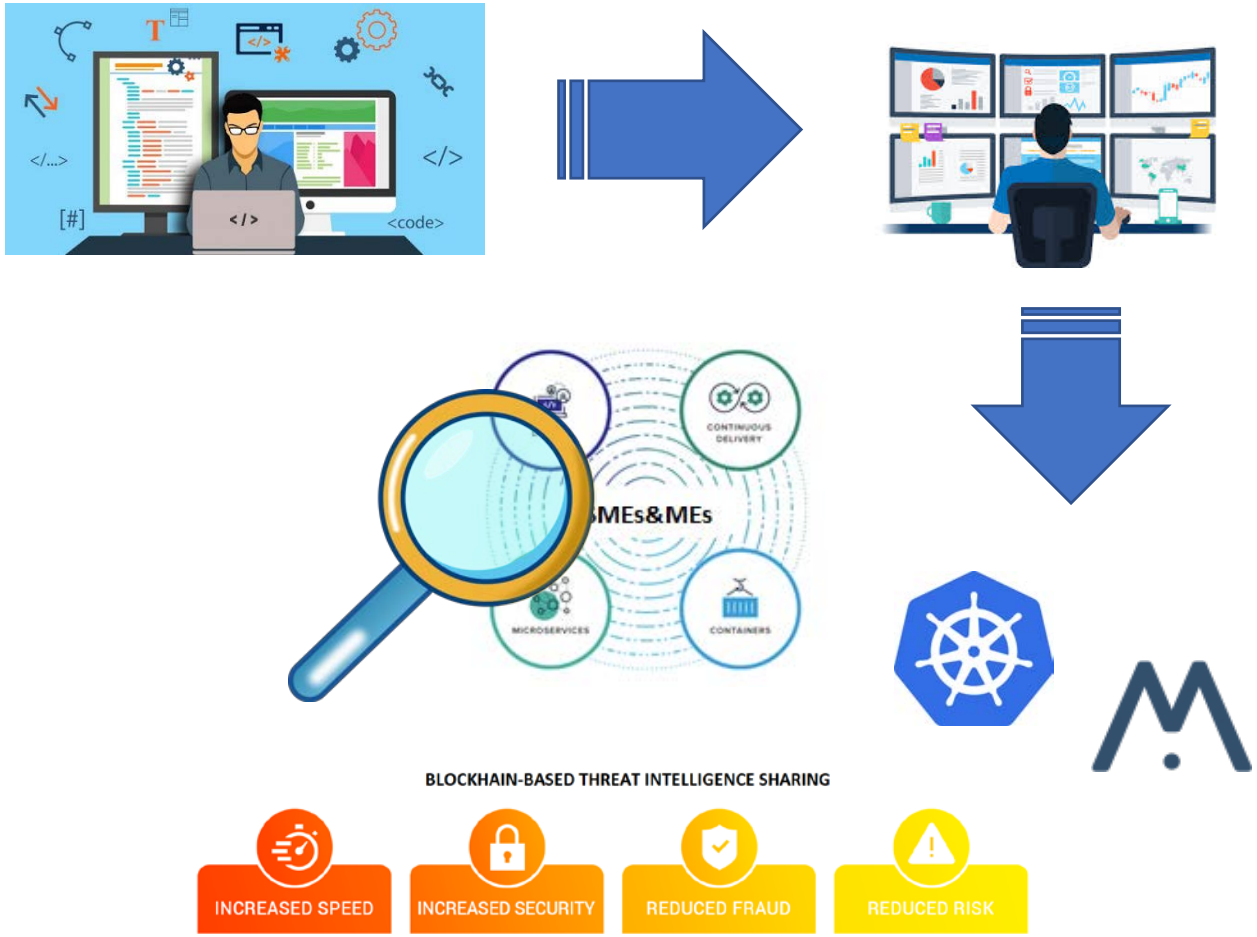
1. Edge-Cloud applications and mixed-criticality services
2. Vulnerability management
3. Configuration management
4. Compliance
5. Runtime threat detection
6. Risk profiling and prioritization
7. Visibility – Threat intelligence sharing

Nearly everyone – 94% of respondents – admitted to experiencing a security incident in the last 12 months.



VALUE PROPOSITIONS & AMBITION

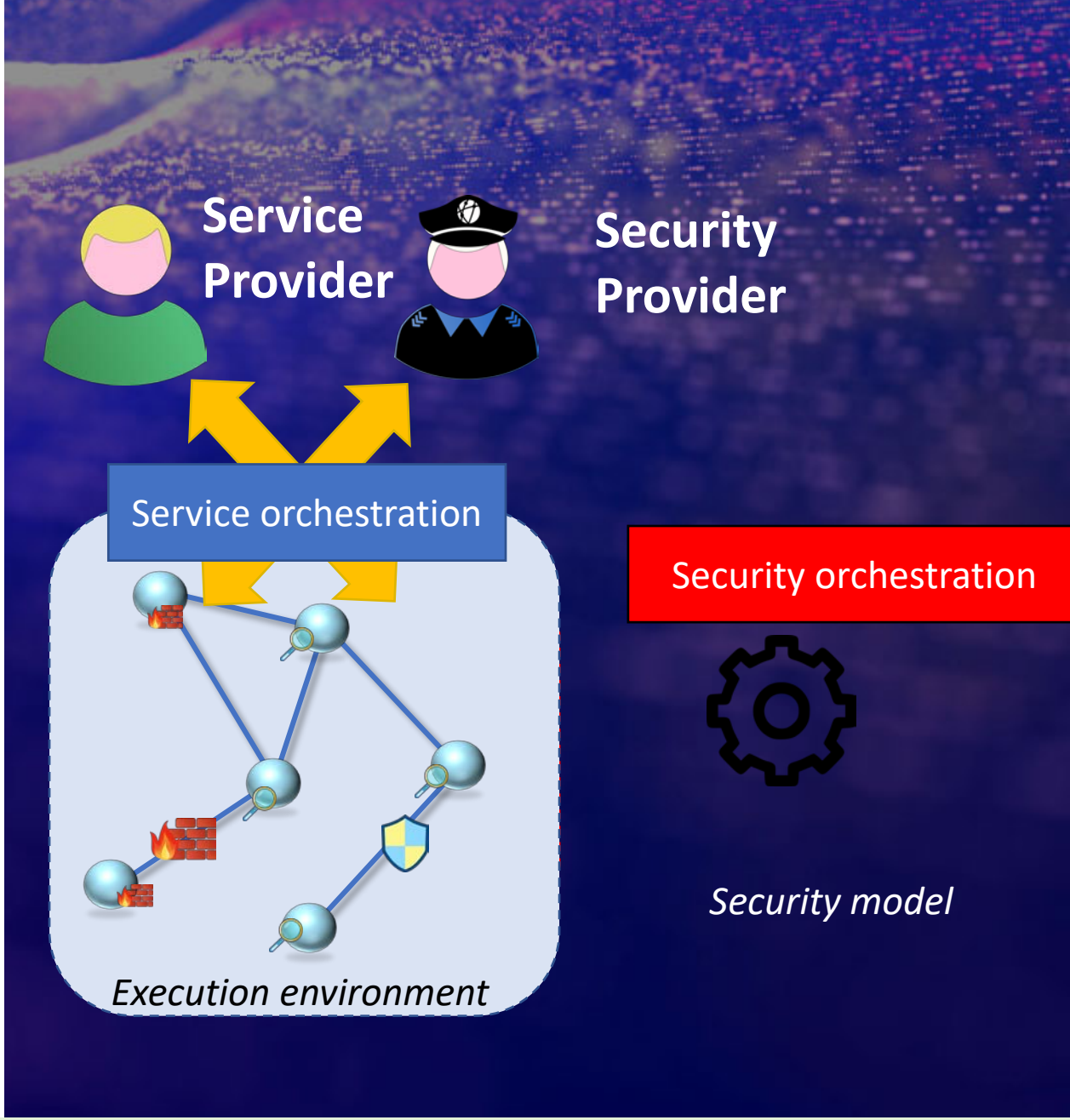
- ✓Security-a-a-Service Marketplace
  - Externalization of security processes
- ✓Edge-cloud Applications and Services
- ✓Optimal Security Policy Recommendation
- ✓Programmatic Inspection and Monitoring
- ✓Portability
- ✓Service Orchestration
- ✓Threat Intelligence Sharing
- ✓On-boarding of Innovative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



PUZZLE

PUZZLE OBJECTIVES

- ✓Decouple the service business logic from the security management
- ✓Automate security management and response to threats, security incidents, attacks
- ✓Optimal security deployment plans per target business ecosystem
- ✓Reduce the run-time overhead of security processing



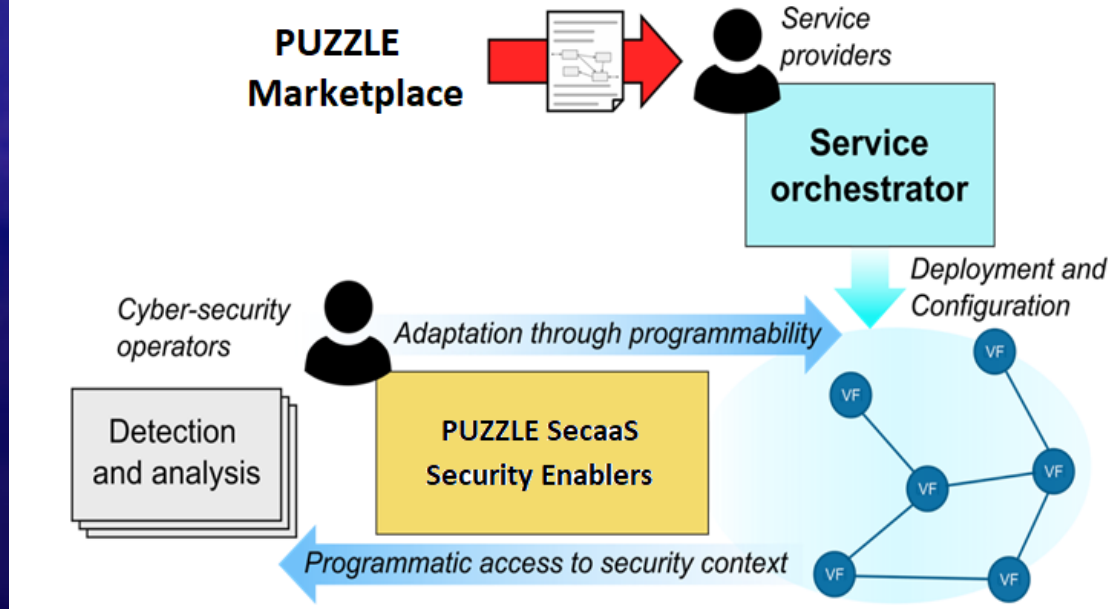
PUZZLE

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"*

⇩

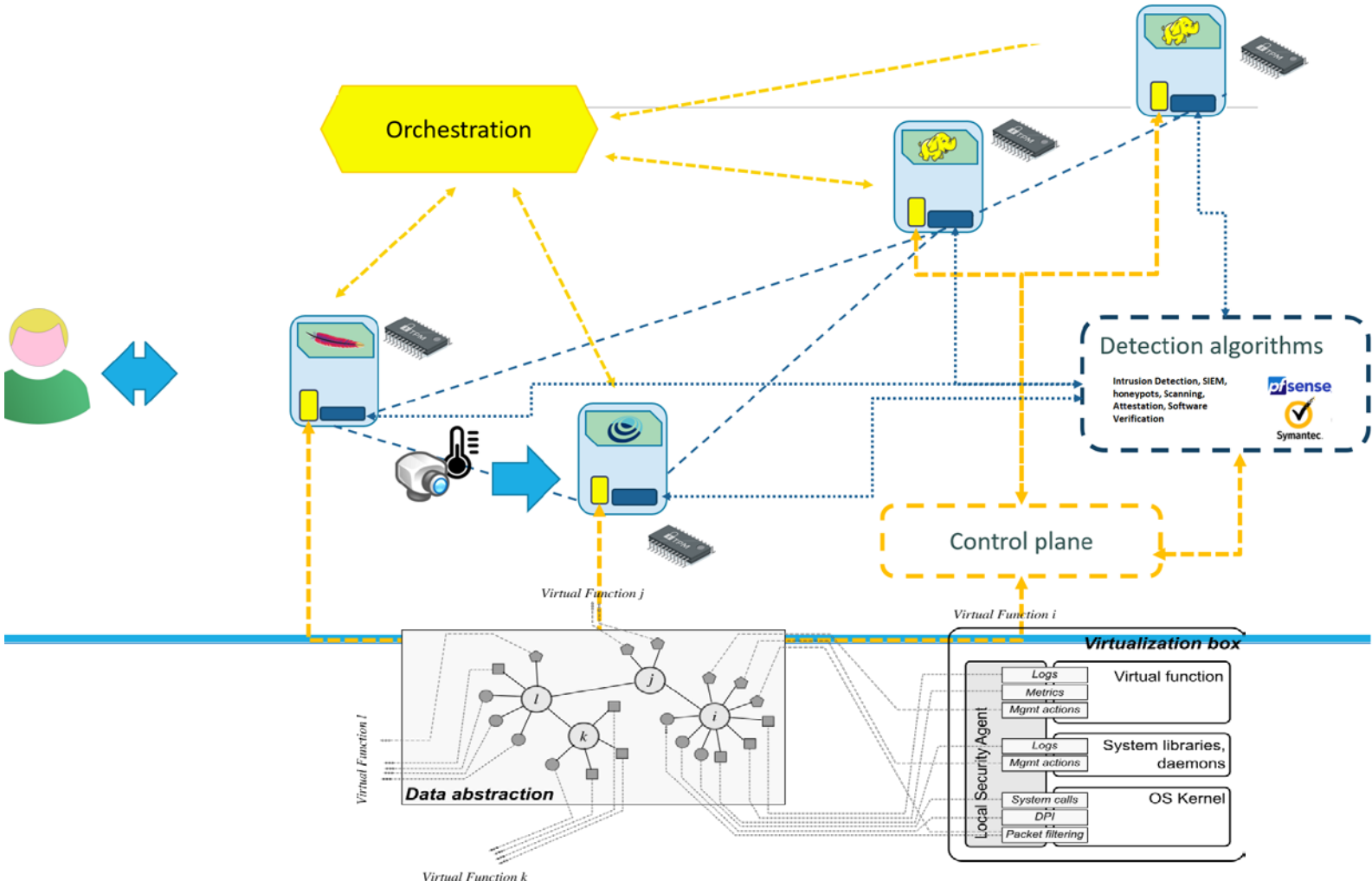
Orchestrate security processes



PUZZLE

PUZZLE CONCEPTUAL ARCHITECTURE

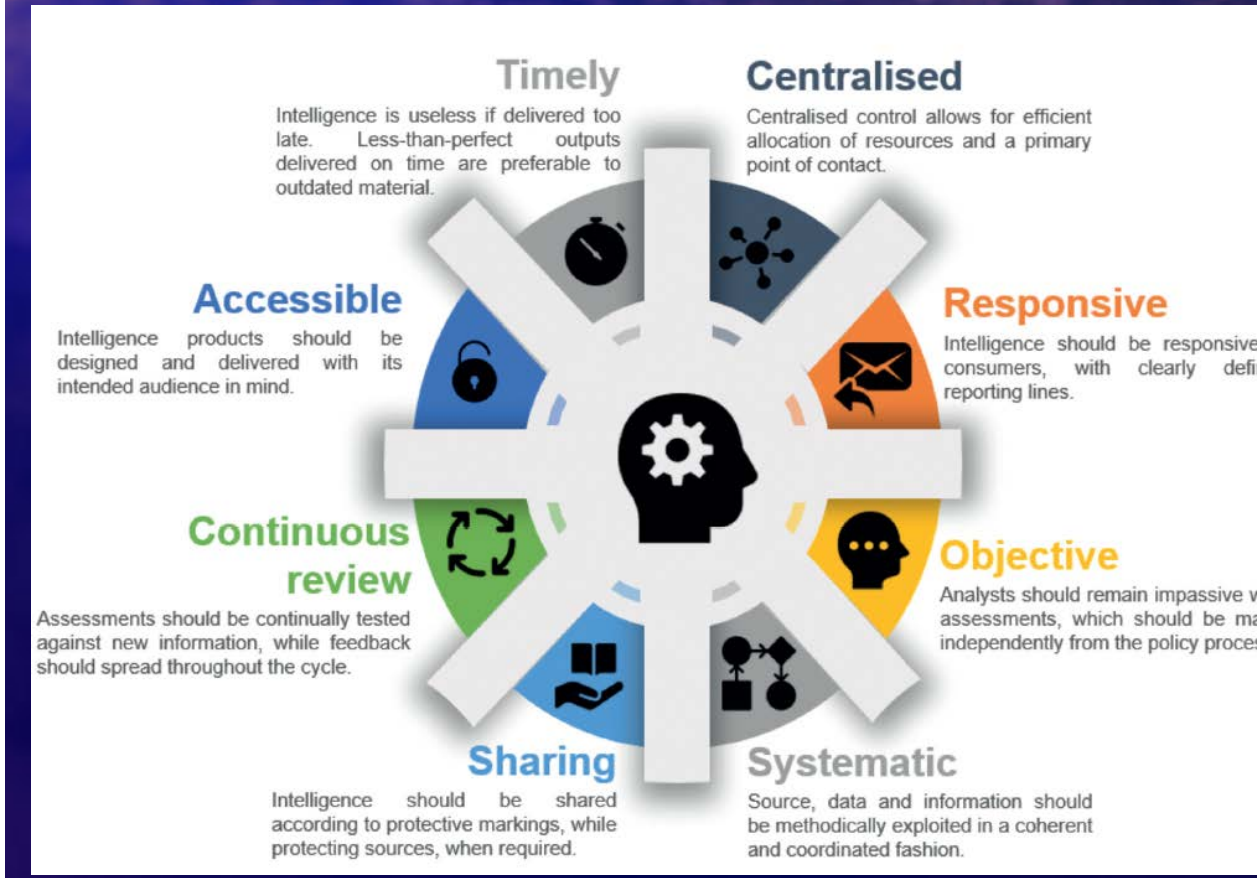
- ✓ Development of PUZZLE's ecosystem cyber threats data and risk model
  - ✓ **Risk Management**
  - ✓ **Risks, Threats, Assets, Attack Types, Vulnerabilities, Control Elements**
- ✓ Optimal Security Policy Recommendation
  - ✓ **Constraint Solver**
- ✓ Advanced Intrusion Detection, continuous RA, SIEM,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



PUZZLE

FURTHERMORE…THREAT INTELLIGENCE SHARING

- ✓ Different levels of threat intelligence
- ✓ Secure, privacy-preserving and accountable information sharing
- ✓ Use of Blockchain-Market



PUZZLE

KEY TECHNOLOGY ARTEFACTS

- ✓ Runtime Risk Assessment, Forecasting & Compliance
- ✓ Edge Trust Assurance Services
- ✓ Network Security Management
- ✓ Orchestration of “Security-as-a-Service” Enablers
- ✓ Efficient Data Monitoring, Querying and Processing
- ✓ Collective threat Intelligence & DLTs

UBITECH Mellanox TECHNOLOGIES INTRASOFT INTERNATIONAL montimage AEGIS IT RESEARCH uni systems FOGUS Suite5 DTU FORTH INSTITUTE OF COMPUTER SCIENCE European DIGITAL SME Alliance VOJVODINA ICT CLUSTER

PUZZLE

CLOUD-BASED ACTIVITY TRACKING & PERSONAL DATA MONITORING SERVICES

- Use of **S5 Tracker** application as a testbed developed by **SUITE5 Data Intelligence Solutions, CY**
- **Data Anonymization** and **Privacy Preservation**

- **Privacy**, confidentiality and security both at the cloud and edge
  - Direct Anonymous Attestation
- **Data Integrity**
  - Digital Signatures & Integrity Verification
- **Secure Data Sharing**
  - Data sharing, privacy, confidentiality and security considerations, both **at the cloud** based infrastructure as well as **at the edge level**
- Data Volume Handling and Scalability Issues

PUZZLE

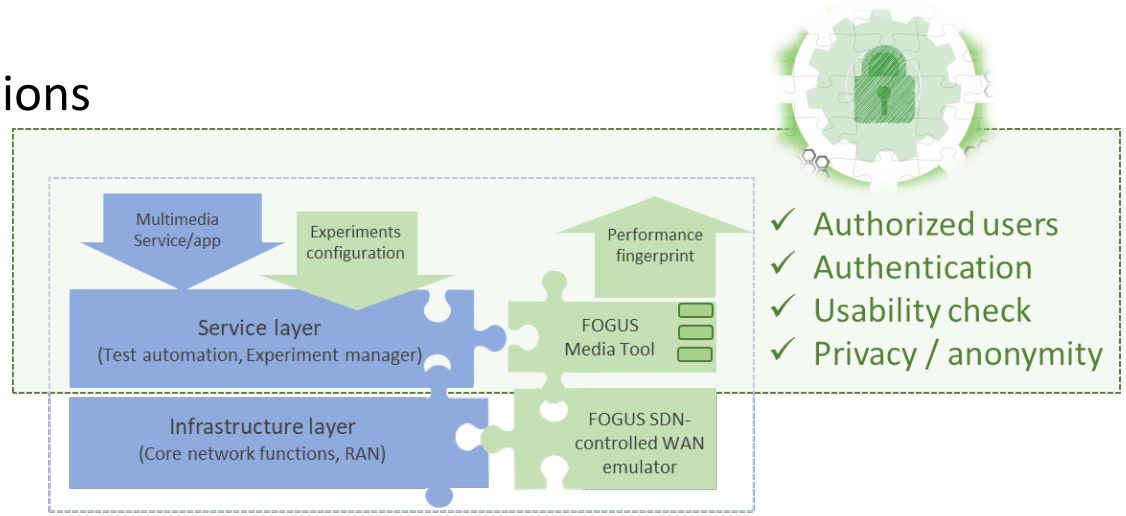
CLOUD-BASED NETWORK MEDIA INFRASTRUCTURE & MANAGEMENT PLATFORM

✓ **FOGUS Media tool:** user's experience management platform for multimedia services

Fundamentals of the FOGUS Media tool

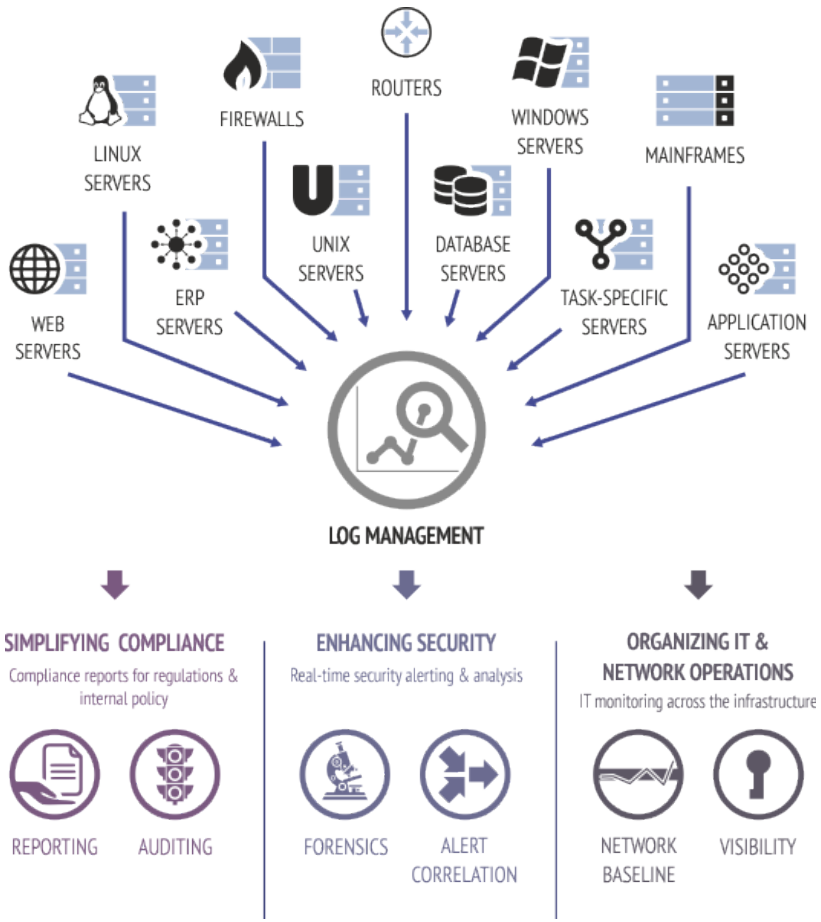
- Twofold Scope
  - Quality of Experience (QoE) subjective assessment of multimedia services
  - Automated QoE evaluation tests of multimedia services

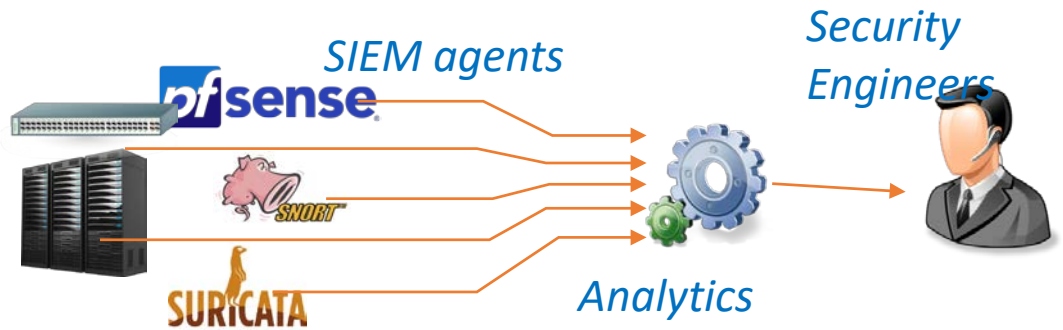
- A core QoE component with three interlinked functions
  - Reliable, secure and passive **QoE monitoring**
  - Efficient, dynamic and objective **QoE estimation**
  - Robust and real-time **QoE-driven service management**



PUZZLE

MARKET POSITIONING





- Beyond bare metal servers and static service architectures:
  - ✓ *virtualization, multi-tenancy, cloud-native applications, software repositories, elastic and dynamic topologies*
- Beyond rigid appliances and services for cybersecurity
  - ✓ *programmable agents, flexible streaming and pipelining, fast offloading, security enablers and trust anchors*

PUZZLE

EXPECTATIONS

- **Help us identify additional needs and functionalities to be supported by such a marketplace**
  - Go beyond the scenarios already identified in the context of our use cases;
  - Priority in the type of assets to be protected;
  - Security or Privacy (or both) a consideration;
- **Online Questionnaire**
  - https://ec.europa.eu/eusurvey/runner/PUZZLE
- **Feel free to contact us for any further feedback/comments**
  - Christina Stratigaki, Project Coordinator (cstratigaki@ubitech.eu);

PUZZLE

Questions?