The Call

The DIGITAL-ECCC-2024-DEPLOY-CYBER-07-KEYTECH call aims to facilitate real-time pattern recognition, automate vulnerability scanning, and enhance data privacy through technologies like anonymization. Tools developed under this call will also be made available for National or Cross-Border **Security Operation Centers (SOCs)**. Eligible participants include technology companies, especially SMEs, which may receive funding covering 50-75% of costs for grants between 3 and 5 million euros. The project duration is expected to be 36 months, and the submission window is open from July 4, 2024, until January 21, 2025.

Topic ID: DIGITAL-ECCC-2024-DEPLOY-CYBER-07-KEYTECH
Funding programme: DIGITAL Europe
Destination: CYBER
Call: Deployment Actions in the Area of Cybersecurity Q3 2024
Application Phase: 04.07.2024, 12.00 pm - 21.01.2025, 12.00 pm
Budget: 35M € in total
Type of Action: DIGITAL SME Support Action
Funding quota: 75% for the SMEs, 50% for the others

The Project

The **VANTAGE** project (Vulnerability Assessment aNd Testing Automation for Global Enhancement) is a groundbreaking cybersecurity platform designed specifically for Security Operation Centers (SOCs). The primary goals are two:
1- to enhance vulnerability assessment and penetration testing (VAPT) capabilities and
2 - to enhance incident investigation through advanced automation and AI-driven collaboration
We can do this featuring a sophisticated team of AI agents that operate as a coordinated unit.

Dual AI-Driven Approach

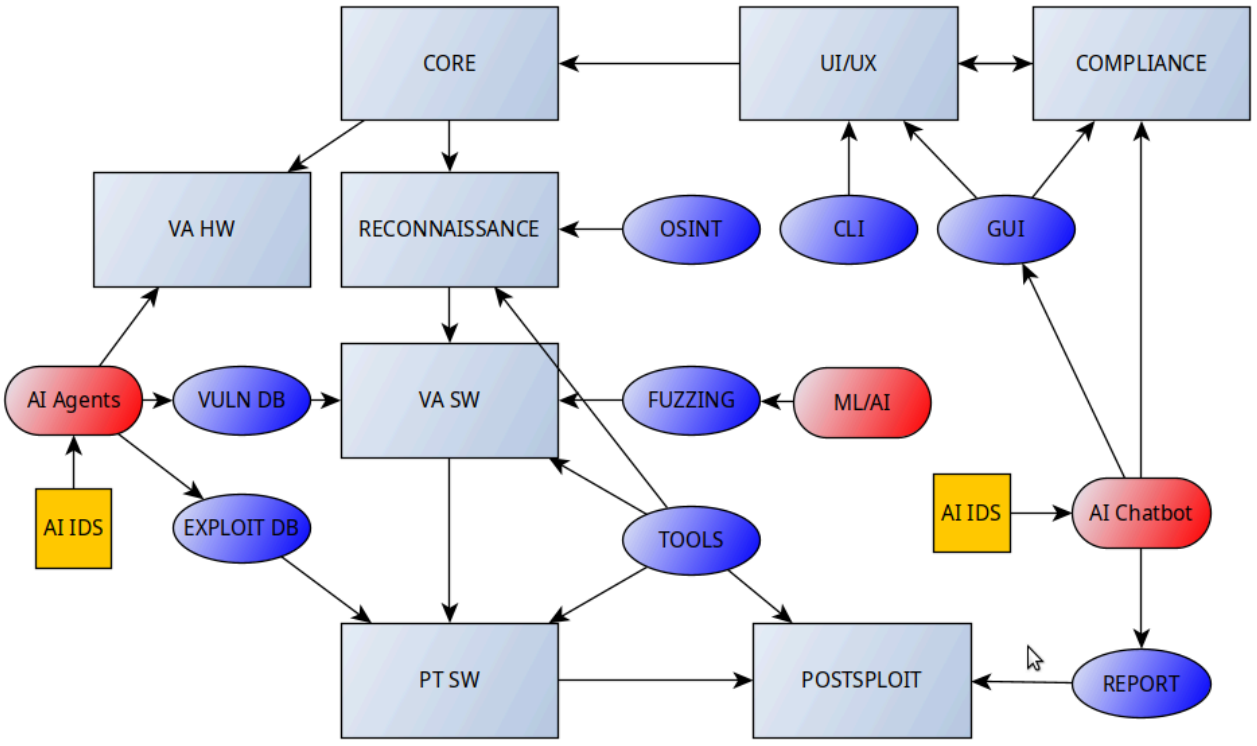
The platform employs a complex and highly efficient **team of AI agents**, working collaboratively to deliver advanced capabilities on two levels:

1. **Automated VAPT for Vulnerability Detection**: VANTAGE goes beyond traditional VAPT by utilising a team of specialised AI agents that operate together to scan, identify, and assess vulnerabilities across diverse software and hardware environments. Unlike simple AI models, this collaborative AI approach allows the agents to share insights dynamically and perform coordinated actions to uncover even subtle security flaws. The platform's modular architecture supports independent operations of each microservice module, facilitating updates and future scalability with minimal disruptions.
2. **Automated Forensic and Log Analysis for Incident Investigation**: The forensic capabilities of VANTAGE leverage a sophisticated AI agent team that collaborates to provide deep insights into security incidents, such as data breaches, hacking attempts, and malware attacks. Each agent is designed with specialised functions, allowing them to collectively analyse log files, network traffic, and system events to identify indicators of compromise (IOCs) and correlate events across multiple sources (e.g., firewalls, endpoints, servers). This coordinated AI effort enables SOCs to reconstruct the sequence of attacks and efficiently determine the root cause of incidents.

Key Features

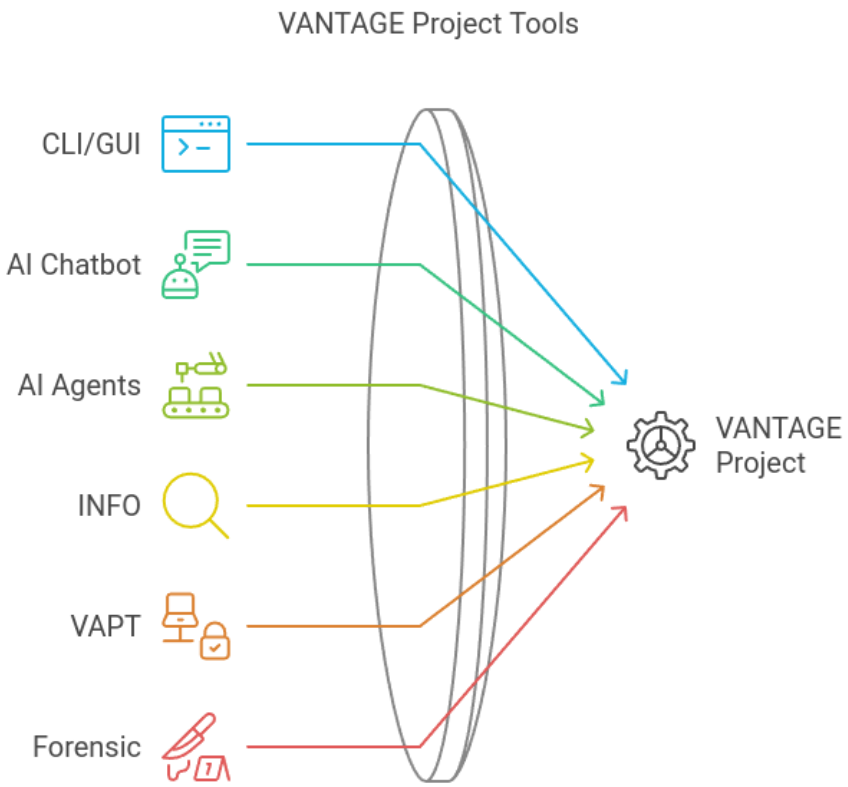
- Coordinated AI Collaboration for Threat Detection and Response: In both VAPT and forensic analysis, VANTAGE's team of AI agents work together to deliver a comprehensive approach to threat detection and incident response. Their joint capabilities facilitate the cross-correlation of events and the identification of advanced persistent threats (APTs), providing a more robust defence than isolated AI solutions.
- Automated and Intelligent Incident Response: The platform's AI agents handle forensic tasks such as log parsing, anomaly detection, and file integrity checks autonomously, allowing human analysts to focus on higher-level strategies. This team-based AI approach accelerates the investigative process and enhances the accuracy of threat assessments.
- Adaptive Learning and Continuous Improvement: VANTAGE uses machine learning techniques across its team of AI agents to continuously evolve and adapt to new threats by learning from fresh data. This enables more intelligent identification of suspicious activities and supports proactive measures to mitigate risks before escalation.

By integrating a coordinated AI-driven approach for both automated VAPT and forensic/log analysis, VANTAGE empowers SOCs to maintain a robust security posture and quickly respond to security events, strengthening their overall cyber resilience. This sophisticated AI agent collaboration sets VANTAGE apart as a comprehensive solution for threat prevention, detection, and investigation.

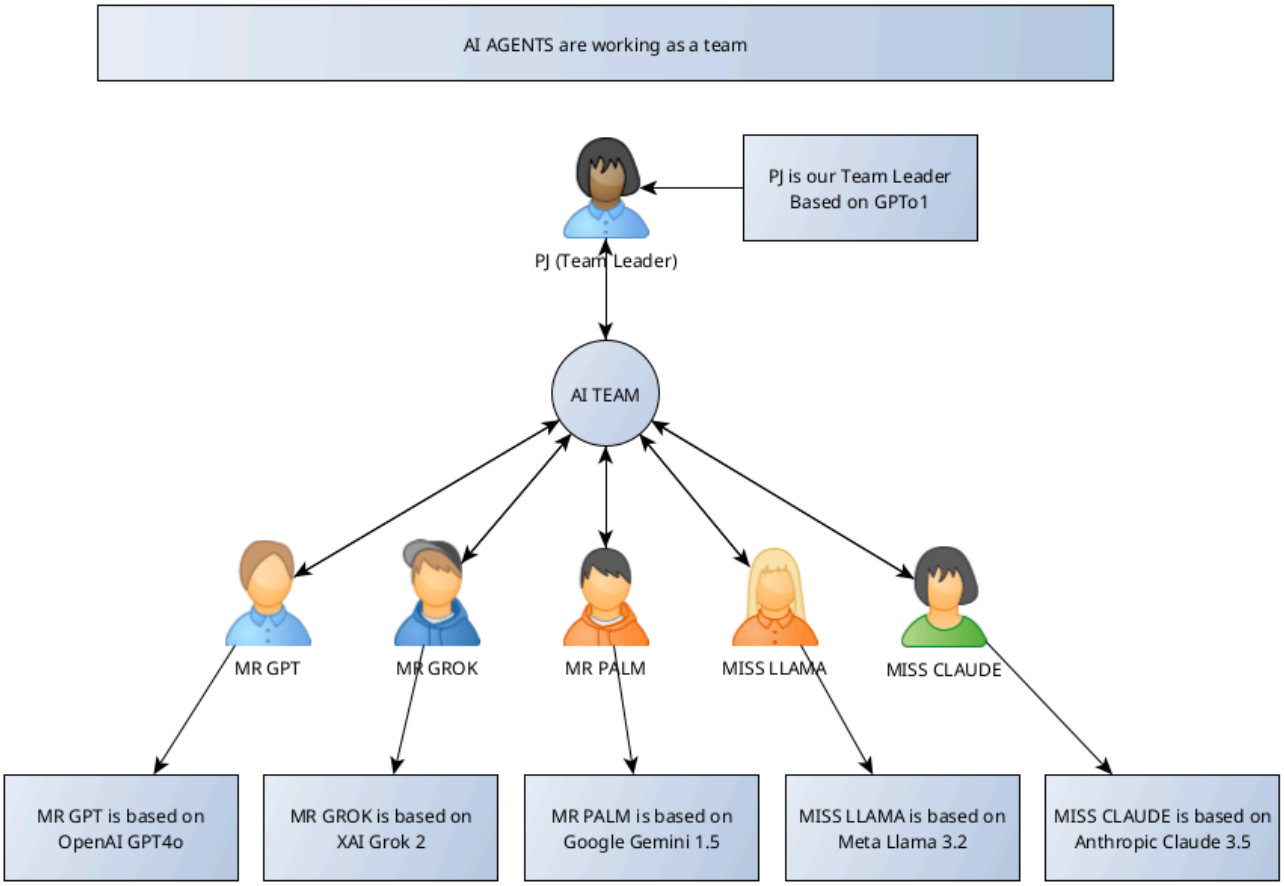


All the core modules (grey) are based on tools (blue) to be developed or to be integrated, as well they are supported by Artificial Intelligence (red) to operate.

MAIN TOOLS in VANTAGE project



- **CLI/GUI**
- **AI Chatbot**
- **AI Agents**
- **INFO**
- **VAPT**
- **Forensic**
- **AI LOGs analyzer**
- **AntiVirus**



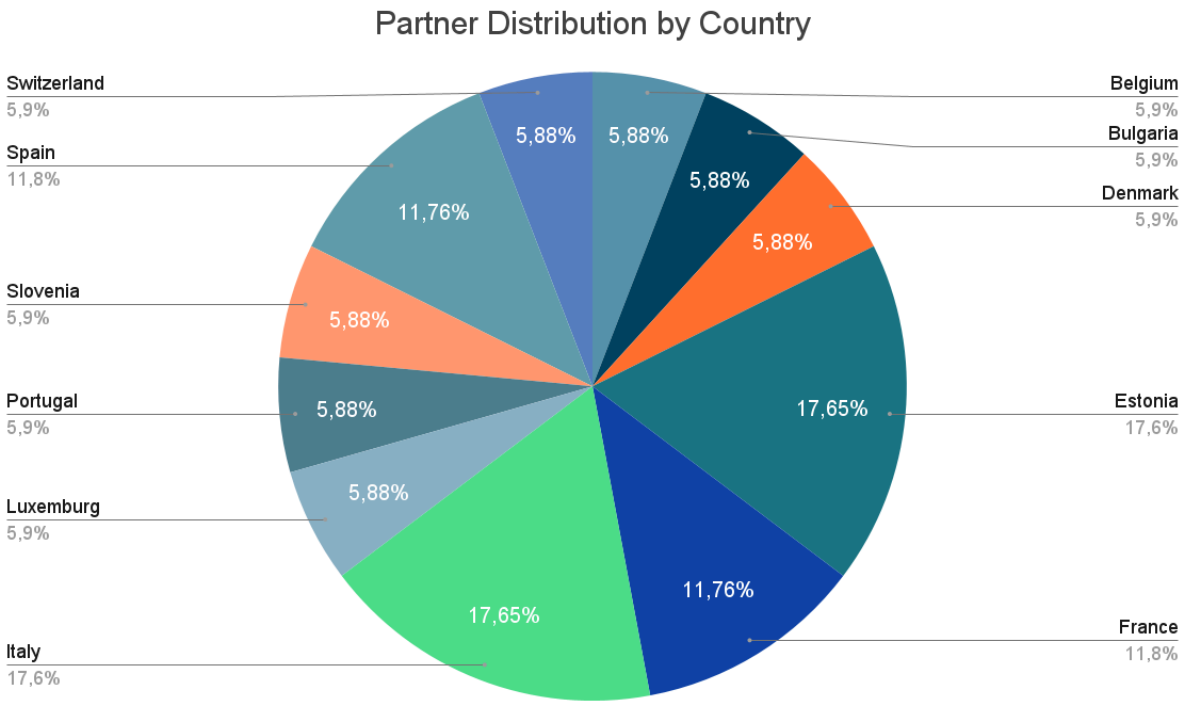
AI Agents using different models are partnered as a team instead of a simple LLM to better elaborate the information.

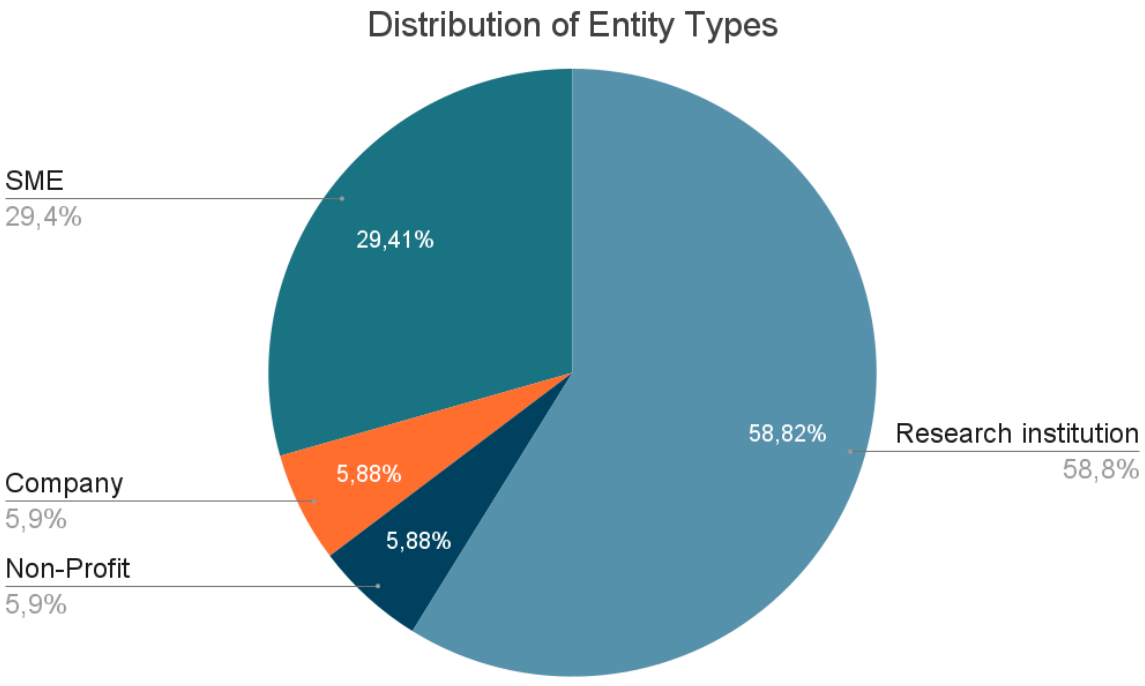
Other Parts
Ethics of AI and Hacking
Videos and Manuals
VMs and Containers

Partner Organisations:

The project is coordinated by The Lisbon Council, one of Europe's leading coordinators with over 100 successfully completed Horizon projects.
(17 partners from 11 countries including Research Institutes, SMEs, Non-Profits).

1. Belgium - Non-Profit - The Lisbon Council - **TLC** (coordination)
2. Bulgaria - SME - **Yameveo** (backend/full stack programming)
3. Denmark - Public research institution - **SDU**, ML/Fuzzing
4. Estonia - SME - **INFRA** (AI, VAPT automation)
5. Estonia - SME - NG Cybersecurity - **NGC** (OSINT/SOC)
6. Estonia - SME - **Haxor** AI (AI, AI Agents)
7. France - Public research institution - **IRIF** (malwares)
8. France - Public research institution - **LYON2** (piece, graphs)
9. Italy - Public research institution - **UNICA**, (Code Quality)
10. Italy - Public research institution - **UNIPI** (Code Security)
11. Italy - SME - **Stackhouse** (front end programing)
12. Luxembourg - Company - **NetCompany** (AI Agents)
13. Portugal - Private research institution - **INOV**, AI IDS
14. Slovenia - Public research institution - **JSI**, AI chatbot
15. Spain - Public research institution - **UPV**, AI guidance
16. Spain - Public research institution - **UPF**, Ethics
17. Switzerland - Public research institution - **UNIGE** (blockchain)


Partner Distribution by Country
Switzerland
5,9%
Spain
11,8%
Slovenia
5,9%
Portugal
5,9%
Luxemburg
5,9%
Italy
17,6%
Belgium
5,9%
Bulgaria
5,9%
Denmark
5,9%
Estonia
17,6%
France
11,8%
5,88%
5,88%
5,88%
5,88%
11,76%
5,88%
17,65%
5,88%
5,88%
11,76%
17,65%

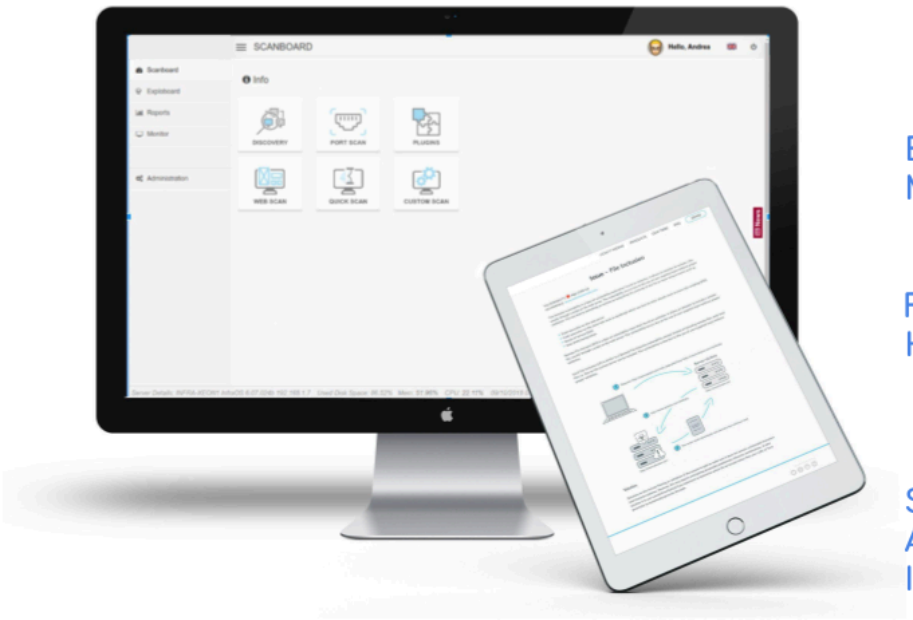

Distribution of Entity Types
SME
29,4%
Company
5,9%
Non-Profit
5,9%
Research institution
58,8%
29,41%
5,88%
5,88%
58,82%

We put AI everywhere

AI/ML for Finding

AI agent for Hacking

AI for Interactive Report



EASY TO USE
Executive
Multi Language

AUTOMATED
Fuzzing
Hacking

MULTI
TARGET
Servers
Applications
IoT and OT

Andrea Bodei 2024