This call for projects aims to stimulate collaborative innovation to propose solutions for improving the digital security of small entities, such as SMEs and municipal administrations, from risk assessment to intrusion analysis. It is carried out in collaboration with the Forensic Department of the Vaud Police.

We encourage academics, innovation stakeholders, and cybersecurity experts to join forces to address the scale of developments underway and contribute to the essential protection of small organizations against the increasing threats of cybercrime.

Context and Challenges

The expansion of the digitized scopes in all areas of activity correlates with a meteoric rise in cybercrime. Criminal organizations diversify and professionalize their activities, exploiting the weaknesses of an increasingly vast and complex digital environment (systems architecture, connected devices, supply chain evolution, open-source developments, virtualization techniques, machine learning). To achieve their compromise goals, attack models are becoming highly sophisticated, both technically and socially, due to the enormous financial incentives.

Small organizations, such as SMEs and local authorities, are the DNA of our socio-economic fabric. They are vital. But they often lack the skills and resources to protect themselves effectively, making them particularly vulnerable to cyber threats. The battle is uneven: defenders have limited financial resources to secure all components and systems, while attackers have significant resources to exploit a single vulnerability.

The consequences of a cyberattack on these fragile organizational structures often severely affect their functioning and the confidence of their customers and partners, leading to a cessation of economic activity in the period following the attack, or a loss of efficiency and citizen trust. In addition to the risk of job loss, the human impact is also psychological and social for the victims of a cyberattack, who find themselves helpless in an uncontrolled environment.

In this context, the digital protection of small organizations is a guarantee of competitiveness and even of the survival of our socio-economic fabric. It is essential to promote a culture and encourage a proactive approach to cybersecurity in order to create a resilient and robust cyber ecosystem, taking into account the specific challenges faced by these players.

Objectives

The objective of this call is to contribute to the **development of technology building blocks and the creation of breakthrough methods and tools for security assessment, prevention, detection, and analysis of vulnerabilities and intrusions in systems and computer networks specific to small organizations**.

Type of Projects

Expected projects will take into account the specific characteristics of small organizations, such as limited financial and human resources, organizational systems, and operational processes. They aim for replicable or industrializable results, as opposed to customized solutions.

The projects can be either software-related – involving the development or enhancement of software related to cybersecurity, **or organization-related** – involving the definition of new processes for SME operations.

Software-related projects will involve the **development of new computer tools** or extensions for existing tools. The software falls into three categories:

- **Security-specific software**: firewalls, antivirus programs, intrusion detection or response systems (new heuristics), event or trace harvesting or storage systems (non-repudiation assurance, etc.), information security assessment systems (for a network, a website, etc.).
- **Business-oriented software related to information security aspects**: VPNs, user identification and access management systems, corporate secret management systems (passwords, certificates, etc.)
- **Software that supports the organization's resilience to IT incidents**: data backup and recovery systems, IT service replication, IT asset documentation management systems and monitoring services

New organizational processes can also be created to reduce exposure to security risks or improve the resilience of SMEs to threats. For example, IT security training or awareness programs and related best practices can be established. Lists of vulnerabilities in the traditional SME architectures can be defined to guide or facilitate the evaluation of security components. Various policies, such as a "Policy for the safe use of IT resources" (computers, online services, email, etc.) or a "Policy for the use of personal computers in a professional context" (or vice versa), can be drawn up. Finally, a proposal to standardize the reporting of IT incidents (attacks, data breaches, etc.) to the authorities, such as incident declaration templates, can be developed as a project.

Aeras of Expertise

In particular, the projects focus on the following areas (not exhaustive):

- Interactive methods and tools for human skills assessment and retraining based on cyber-range and simulation technology building blocks (training platforms, attack simulators, etc.).
- Component and system assessment and verification solutions that explore the contribution of artificial intelligence and integrate deep learning, virtualization, and disaggregation technologies
- Techniques for hardening products, services, or systems in a measurable, repeatable, and industrializable manner
- Modular and scalable security components that integrate with existing infrastructures, in particular for remote communication and collaboration tools
- Mechanisms and tools for automated vulnerability scanning and early intrusion detection based on artificial intelligence and machine learning, pentest automation
- Tools for analyzing attack methodologies and behavior models, potentially combining hardware and software (dysfunctional semantic models, reverse engineering techniques, AI-based analysis, system-scale impact analysis algorithms, interactive visualization and navigation techniques, etc.)
- Methods and techniques for digital investigation and forensic analysis, taking into account the relevant legal framework (investigation of hardware vulnerabilities exploitable by software, analysis of system images and memories of embedded systems, analysis on physical devices, etc.)
- Tools to facilitate the standardization of incident reporting and the legal obligation to report cyberattacks