Call: HORIZON-CL3-2025-02-ECCC-01: Generative AI for Cybersecurity applications
Opening: 12 Jun 2025 (tentative)
Deadline(s): 12 Nov 2025 (tentative)
Total budget 40.00 M€ Contribution per project 12.00 to 14.00 Number of project 3

GENAICS – Generative AI for Cybersecurity Solutions- Concept Note

1. Context and Relevance to Call

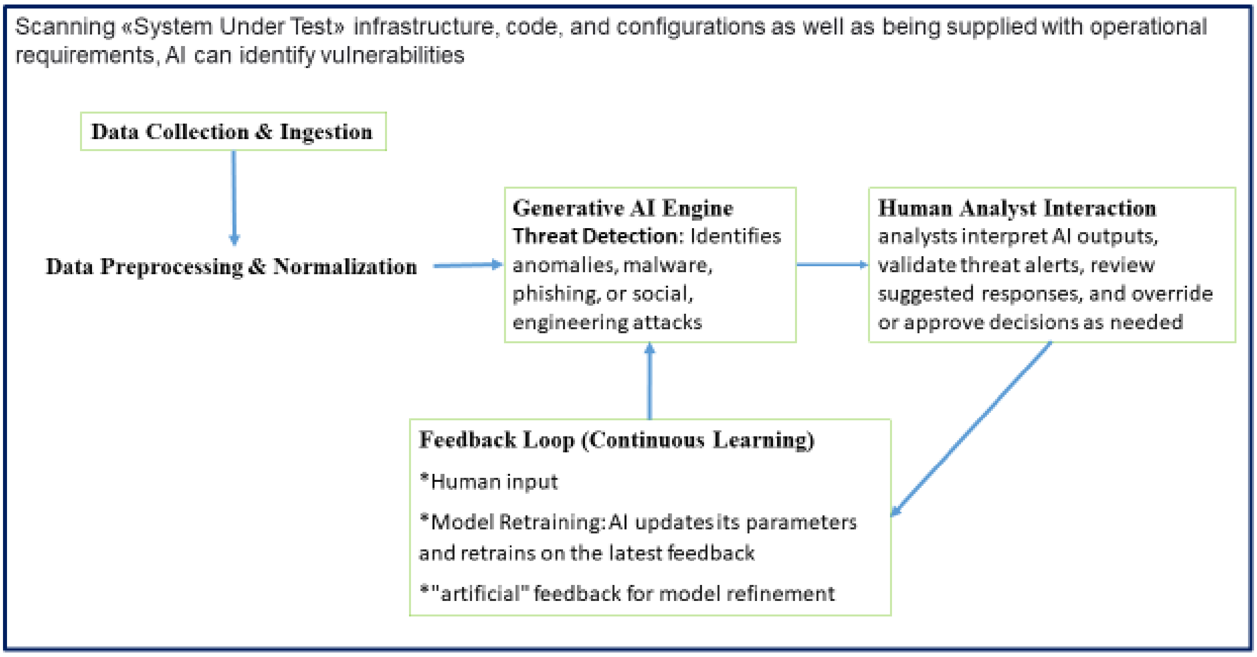
The increasing sophistication and frequency of cyberattacks across Europe threaten digital infrastructures, critical services, and citizens' privacy. While traditional cybersecurity solutions focus on rule-based detection, they are increasingly insufficient against evolving, AI-driven threats. Generative AI holds transformative potential to proactively predict, simulate, detect, and mitigate such threats.

The HORIZON-CL3-2025-02-ECCC-01 call seeks innovative approaches leveraging generative AI to enhance cybersecurity capabilities. GENAICS directly addresses this by developing explainable, secure, and scalable generative AI models specifically optimized for cybersecurity applications, aiming to reinforce the EU's technological sovereignty and resilience.

GENAICS addresses various aspects of cybersecurity. The main functions are::

1. Reduce cybersecurity operational costs: Generative AI helps organizations manage cyber risk more cost-effectively by reducing the time and personnel required to complete security tasks. When implemented well, gen AI tools enhance productivity, optimize security workflows, and reduce response times, ultimately lowering the total cost of cybersecurity operations.
2. Optimize real time threat detection: Threat detection is a top use cases of generative AI today. It allows to identify patterns and anomalies faster, more efficiently filter incident alerts, and reject false positives.
3. Enhance threat intelligence: Previously, analysts would have to use complex query languages, operations, and reverse engineering to analyse vast amounts of data to understand threats. Now, they can use generative AI algorithms that automatically scan code and network traffic for threats and provide rich insights that help analysts understand the behaviour of malicious scripts and other threats.
4. Allows automated security patches: Generative AI can automate the analysis and application of patches. Using neural networks, it can scan codebases for vulnerabilities and apply or suggest appropriate patches using natural language processing (NLP) pattern matching or a machine learning algorithm known as the K-nearest neighbours (KNN) algorithm.
5. Improves incident response: Generative AI can provide security analysts with response strategies based on successful tactics used in past incidents, which can help speed up incident response workflows. Gen AI can also continue to learn from incidents to adapt these response strategies over time. Organizations can use generative AI to automate the creation of incident response reports as well.

Proposed system intends to study and implement all the cited improvements integrating different SW/framework modules in order to obtain all the advantages allowed by the Gen AI.



Scanning «System Under Test» infrastructure, code, and configurations as well as being supplied with operational requirements, AI can identify vulnerabilities

Data Collection & Ingestion

Data Preprocessing & Normalization

Generative AI Engine
Threat Detection: Identifies anomalies, malware, phishing, or social, engineering attacks

Human Analyst Interaction
analysts interpret AI outputs, validate threat alerts, review suggested responses, and override or approve decisions as needed

Feedback Loop (Continuous Learning)
*Human input
*Model Retraining: AI updates its parameters and retrains on the latest feedback
*"artificial" feedback for model refinement

2. The threath

The market witnessed a surge in AI models specifically optimized and trained for malware development:

WormGPT	Malware, phishing, code generation
Jailbroken LLMs	Obfuscation, variant generation
GAN-based models	Synthetic malware generation (research)
AI-powered malware kits	Automated malware creation, phishing

Malware creation traditionally required substantial technical expertise, advances with Large Language Models (LLMs) have drastically lowered this barrier=> Basic ransomware script generated with Python and ChatGPT API + FraudGPT, etc….

3. Objectives

- Develop novel generative AI architectures tailored to cybersecurity, including threat simulation, anomaly detection, and automated response generation.
- Ensure explainability, traceability, and trustworthiness of generative models applied in sensitive cybersecurity contexts.
- Enhance cyber threat intelligence by generating realistic synthetic attack scenarios for training and preparedness.
- Deploy privacy-preserving federated learning frameworks to secure sensitive data during model training.
- Validate and demonstrate solutions in real-world use cases, including critical infrastructure protection, SOC operations, and zero-day threat detection.

4. Methodology and Approach

Work Packages include:
WP1 – Project Management and Coordination (Ensure effective coordination across partners+Monitor project progress, risks, ethics, and compliance.
+Facilitate communication with the EC and stakeholders).
WP2 – Requirements Analysis and System Architecture Design (Define technical, security, and ethical requirements. +Design system architecture for malware detection and response.)
WP3 – Data Collection, Curation, and Adversarial Dataset Generation (Collect and label datasets for malware detection. + Generate adversarial examples using Generative AI ??? Evaluate ethic issues.)
WP4 – Development of AI/ML/GenAI Models for Detection and Classification (Build models for static and dynamic malware detection. +Use GenAI to evolve malware signatures and test robustness.)
WP5 – Malware Signature Generation and Library Management System (Design of malware signature extraction framework. + Integration of AI-based mutation prediction models.+ Real-time updating and distribution mechanism for signatures.+ Evaluation of backward compatibility and false positives)
WP6 – Runtime Monitoring, Detection, and Self-Healing Engine (Instrumentation of system call tracing and behavior monitoring. + Real-time anomaly detection and malware classification. + Autonomous self-healing and response strategies (e.g., process isolation, rollback). + Performance optimization and latency analysis.)
WP7 – Integration, Testing, and Validation (System integration in testbed environment. + Testing scenarios for both static and runtime analysis. +Stress tests with adversarial inputs and APT simulations. + User feedback, robustness, and usability assessments.)
WP8 – Exploitation, Dissemination, and Communication (Dissemination plan, conferences, journals, workshops. + Exploitation strategy and business models.+ Open-source release strategy (where applicable).+ Stakeholder workshops and community engagement.)

GENAICS actively contribute to EU cybersecurity standards and policy frameworks, ensuring project outcomes are leveraged beyond the project’s lifespan.

5. Innovation and Impact

- First EU-driven generative AI cybersecurity framework with integrated explainability and privacy features.
- Enable early detection and mitigation of novel attack types, including zero-day and AI-generated threats.
- Support EU cybersecurity autonomy by reducing dependency on non-European AI technologies.
- Contribute to EU skills development through training materials and open datasets/tools.

6. Consortium and Expertise

Lead Partner:

- Cybersecurity R&D Company/Institute with expertise in AI, threat detection, and critical infrastructure protection.

Key Partners:

- AI research center specializing in generative models and explainable AI.
- European CERT/SOC providing real-world validation environments.
- SME developing cybersecurity software solutions.
- Partner expert in the HW/FW aspects (development of firmware integrity monitoring solutions, possibly integrated within FPGAs or ASICs)

- Legal and ethics partner ensuring compliance with GDPR (General Data Protection Regulation), AI Act, and ethical AI guidelines.

7. Requested Budget & Duration

- Budget Requested: Approx. €12 million
- Project Duration: 36 months

8. Alignment with Horizon Europe and EU Priorities

GENAICS advances Europe's capacity to counter evolving cyber threats using cutting-edge AI technologies, aligning with the EU's Digital Strategy, Cybersecurity Act, and the forthcoming AI Act.