Service ID S00196

Location Poland, Remote

Testing security and robustness of AI systems

Provider service

Poznan Supercomputing and Networking Center (PSNC)

Link to content

https://agrifoodtef.eu/catalogue-of-services/testing-security-and-robustness-ai-systems

Type of Sector

Arable farming, Food processing, Greenhouse, Horticulture, Livestock farming

Accepted type of products

Physical system, Software or AI model

Type of service

Cybersecurity, Performance evaluation, Test design, Test execution, Test setup

Description

Our service offers comprehensive testing for the security and robustness of AI products, tailored to meet the specific requirements of our customers across various operational fields, technological processes, and communication systems. We specialise in conducting thorough security audits, penetration tests, vulnerability scans and code reviews to identify and mitigate potential security threats. By leveraging advanced testing techniques such as automated and manual pentesting, fuzz testing or hybrid source code reviews, we ensure that AI products are robust against cyber threats and/or adversarial attacks before they go to market. Our adaptable approach allows us to customise each service to align with the unique security needs of each customer, providing them with a high level of protection and confidence in their AI technologies.

How can the service help you

This service provides comprehensive testing for the security of AI products. Through acquiring the service, the cybersecurity level of your product will be maximised, you will be able to remove or mitigate the identified security vulnerabilities and/or additionally harden the product and possibly learn additional best practices for the future releases. Criteria of verification comply with practices described in the ISO 42001 standard. Early identification of security vulnerabilities helps to minimise the cost of deploying and maintaining the product and also increase the level of user trust towards the product.

How the service will be delivered

Service is allowed to be customised to fulfil particular customer needs.

Service customisation

The service can be provided any time. Service execution time depends on the complexity and specific needs of the customer and the AI product (usually it is between 2 and 12 weeks). The service is done remotely. However, if customers need it, it could be performed at the user's premises. The customer must provide an AI product and answer a set of organisational and technical questions to appropriately adjust the service scope and parameters.

The service output is usually an extensive technical report (with executive summary) that contains the description of identified vulnerabilities, related threats, risk levels and suggested mitigation measures. Remote consultations, status and summary meetings may be agreed to. The service will be executed under the requirements of the ISO 9001 standard.