Service ID S00289

Location Remote, Spain

Vulnerability scan of agrifood-related AI or robotics software systems

Provider service

GRADIANT

Link to content

https://agrifoodtef.eu/services/vulnerability-scan-agrifood-related-ai-or-robotics-software-systems

Type of Sector

Arable farming, Food processing, Greenhouse, Horticulture, Livestock farming, Tree Crops, Viticulture

Accepted type of products

Software or AI model

Type of service

Cybersecurity

Description

Software systems (like AI and robotics systems developed for agrifood environments) are usually developed using third-party libraries. Regular updates on both proprietary and third-party libraries are strongly recommended to address potential vulnerabilities in the code. The vulnerability scan for agrifood software systems makes it possible to find out if the developed system has cybersecurity vulnerabilities in its code before its production deployment. In case vulnerabilities are found, the customer receives information about each one, including the level of criticality and location in the code. Thus, the customer can solve the issues and prevent possible future security problems in the system.

How can the service help you

From the time a software system is developed until it is put into production, several testing steps are necessary to ensure the effectiveness and reliability of the system. With the vulnerability scan service, the customer can perform the vulnerability analysis phase of the developed code to detect and fix the security issues before putting the system into production.

How the service will be delivered

As an example, a company that has developed a crop irrigation forecasting application is interested in selling a professional AI software system free of cybersecurity issues. The company has a lot of experience in machine learning algorithms but lacks some knowledge of how to find out if its software is secure, so it requests a vulnerability scan for agrifood software systems service.The vulnerabilities report is delivered in file formats JSON or YAML by default. If the customer is interested in using a graphical user interface, we can add this to the service execution.

Service customisation

The service is delivered remotely. The expected duration of the service is approximately two weeks, depending on the customer's needs.

The service is delivered remotely. The expected duration of the service is approximately two weeks, depending on the customer's needs. It is expected that the customer will provide an OCI image of the software system through a REST API. If the customer does not have an OCI image, we can offer another service (S00307) to create this image from the source code. After the service execution, the customer receives the vulnerabilities report, including useful information about each one. This report is in a JSON or YAML format file unless the customer is interested in a graphical user interface. In this case, the execution would take two more weeks. This service can be replicated for each new version of the system to be developed, with instant execution.