Test and validation

2025WP3_Hortivation_002
Status: In progress

Technical functionality
TF-2 Testing interoperability, standardisation and compatibility

Problem Owner:
Hortivation

Involved:
TNO, Plantfellow, LetsGrow, 30MHZ TomatoWorld, InnovationQuarter

For more information:
Liesbeth Leurs / Bart Luijten TNO

Exploring cybersecurity threats

An exploration of cybersecurity threats in greenhouse horticulture when exchanging data through a cross-company data hub.

Broad knowledge question
What specific cybersecurity threats does greenhouse horticulture face when exchanging data through cross-company data hubs in the context of interoperability and autonomous solutions in the greenhouse?

Approach
Together with experts, a system overview will be developed to identify potential cybersecurity threats and analyse real-world risks. A cybersecurity expert, who is yet to be selected, will then analyse this overview in greater detail and identify potential solutions to address these threats:

1. Generic solutions to address the identified threats.
2. Identification of the remaining specific threats.

The first phase of the project will run for six months. The exploratory work started on 1 January 2025. The outcome of this phase will be a first version of an Overview of cybersecurity threats in the horticulture sector and potential solutions for improving security.

Objective
To identify the cybersecurity threats associated with cross-company data exchange, using the Robocrops data hub of NXTGEN UC19 (IP2) as a concrete example.

Results and reflection
An initial overview of cybersecurity threats in the horticulture sector and potential solutions to address them.