2026 ECSCI CLUSTER WEBINAR SERIES · 3RD WEBINAR · 26 OCTOBER 2026

ACT4FOOD: Cybersecurity for Food Supply Chains

AI-driven threat detection, SOC 4.0 and secure information sharing for aquaculture, dairy and retail

Odysseas Kokkinos
Project Coordinator · INNOV-ACTS Ltd

ACT4FOOD

Co-funded by the European Union

ACT4FOOD has received funding from the Digital Europe Programme under grant agreement No 101249720

www.act4food.eu

ACT4FOOD

01 Why food
02 What we build
03 Year one
04 Synergies

www.act4food.eu

Food is now regulated as critical infrastructure

A cyber incident in a food plant ends in unsafe product, empty shelves or a recall — not only in downtime.

NIS2

Directive (EU) 2022/2555

Food is an Annex II sector: industrial producers, processors and wholesale distributors must manage cyber risk and report significant incidents — early warning in 24 h, notification in 72 h, final report within one month.

CER

Directive (EU) 2022/2557

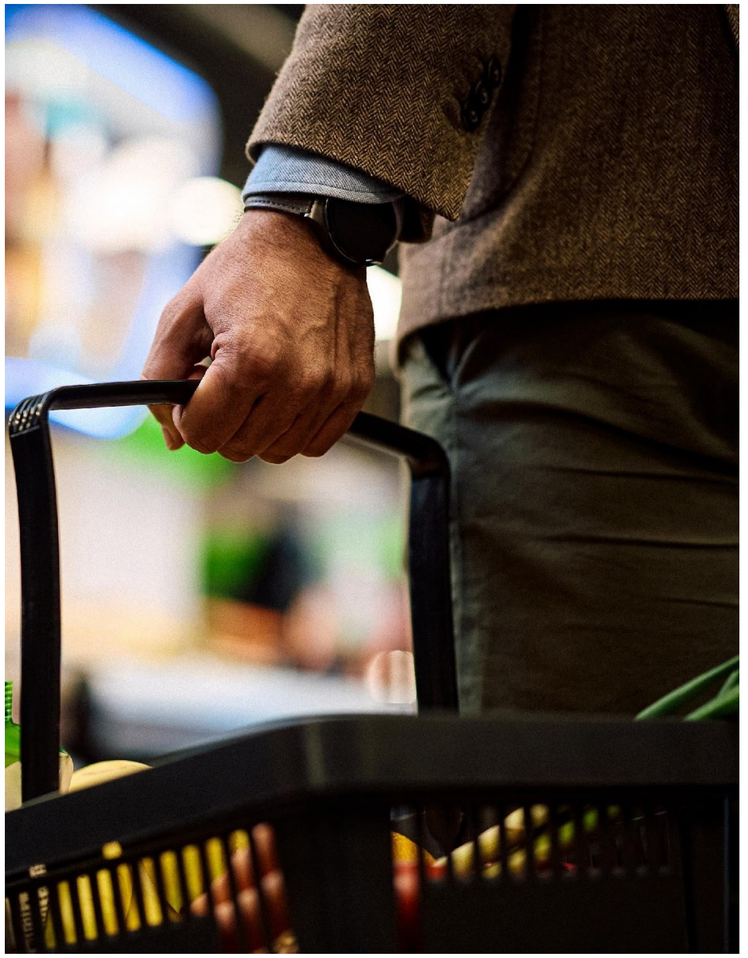
Food is one of 11 sectors: Member States had to identify critical entities by 17 July 2026. Those entities must build all-hazards resilience — and become NIS2 essential entities.

CRA

Regulation (EU) 2024/2847

Connected sensors, controllers and gateways on the line are products with digital elements; manufacturers' reporting of exploited vulnerabilities applies from 11 September 2026.

The gap Food-safety practice (HACCP, TACCP, ISO 22000) has no cyber dimension; cyber practice has no food-safety consequence model.



ACT4FOOD at a glance

12	8	36	3
beneficiaries	countries	months, Dec 2025 – Nov 2028	pilot sectors

Programme	Digital Europe Programme (DIGITAL), managed by the ECCC
Call topic	DIGITAL-ECCC-2024-DEPLOY-CYBER-07-KEYTECH
Grant · budget	No 101249720 · €5.6 M total, €3.7 M EU funding
Coordinator	INNOV-ACTS Ltd (Cyprus)
Pilots	United Aquaculture (BG) · Greek Family Farm (EL) · METRO (EL)

CONSORTIUM

Innov-acts · Gruppo Maggioli · Universidad Politécnica de Cartagena · Creme Global · Montimage · IANUS Technologies · Agritrack · Greek Family Farm · METRO · June · United Aquaculture · BYTE

www.act4food.eu

ACT4FOOD

MISSION

Make cyber risk a food-safety parameter: detect, rank and share cyber-physical threats from farm to shelf.

The gap

01 Consequences are physical

A spoofed temperature sensor or altered set-point ends in unsafe product or a recall. CVSS cannot score that.

02 Telemetry is heterogeneous

ICS/SCADA, IoT gateways, ERP, quality records, POS and logistics — different owners and formats.

03 Two alert systems never meet

RASFF warns about food hazards, CTI about cyber threats. Neither sees a cyber-physical incident.

What ACT4FOOD adds

→ TACCP 4.0 risk ranking

Every alert scored by food-safety and economic severity, not by asset criticality alone.

→ SOC 4.0 across OT, IoT and IT

One correlation hub over AI-based, rule-based and pentest-driven detection.

→ Food-aware CTI, shared safely

Sector threat intelligence and confidential exchange that does not expose the victim.

02 · WHAT WE BUILD

Four outcomes, one deployable system

ACT4FOOD

TACCP 4.0

Food-defence threat assessment extended to cyber-physical threats, with AI-assisted risk ranking.

SOC 4.0

AI anomaly and intrusion detection, automated pentesting, forensics and food-defence toolkit.

CTI feed & IEP

Food-specific threat intelligence and a blockchain-backed, privacy-preserving exchange platform.

Cyber Arena & training

Live attack simulation and sector training for aquaculture, dairy and retail staff.

17

modules in one integration registry

3

operational pilots, farm to shelf

55+

food-industry professionals to train

1

TACCP 4.0 Guidebook, as a pre-standard

Four layers, one orchestration hub

Reference architecture (draft): every module integrates against a declared interface, not against another module's internals.

Data collection & integration

DCP · data collection | DAL · aggregation | IL · integration layer

IoT, ICS/SCADA, ERP, quality and logistics sources

Detection & intelligence

MAIP | ATD | WaSur | MMT-Pentester | CTI4BC | STIX/CPS | TACCP 4.0 | IEP

Integration & orchestration

SOC 4.0 hub | Blockchain traceability | AI IoT cold chain | Dashboard | Forensics

Validation

Aquaculture | Dairy | Retail | Cyber Arena

Three live environments and a cyber range

DESIGN RULES

Interface-first

Modules from different partners progress in parallel against declared interfaces.

Incremental

Each module is built and connected independently; no big-bang integration.

Compliant by design

NIS2, GDPR and AI Act constraints encoded in the workflow.

Pilot-validated

Continuous validation in live plants and in the Cyber Arena.

TACCP 4.0: triage by what happens to the food

Classic food-defence assessment, extended to cyber-physical threats and fed back into SOC prioritisation.

HACCP hazards to food safety → **TACCP** intentional threats: food defence → **TACCP 4.0** cyber-physical threats, AI-assisted ranking

Likelihood

Incident history, system vulnerabilities, attack feasibility, live CTI

Safety severity

Contamination risk, product integrity, public health

Economic severity

Production loss, supply disruption, recalls, penalties

→

OUTPUT TO SOC 4.0

A ranked cyber-physical risk attached to each alert, so the analyst triages on food outcome — and the food-safety manager agrees with the order.

WORKED EXAMPLE · DAIRY

Milk pasteurisation: map each critical control point to the sensors that monitor it and their known vulnerabilities. New cyber-physical control points appear — a manipulated temperature reading is a food-safety hazard, not an IT event.

Now

Expert weighted scoring (MCDA, AHP)

As data accrues

Machine learning refines the weights

Continuously

Live CTI and STIX/CPS context re-rank

Sharing threat knowledge without exposing the victim

Detection is local; warning has to travel. Three mechanisms make it safe for competing operators to share.



Common language

A cyber-physical extension of STIX 2.1 lets an alert carry the affected process, batch and food-safety impact — exchanged over TAXII and bridged to MISP.

Confidential exchange

Anonymisation and privacy-preserving aggregation let operators share indicators without disclosing who was hit — RASFF-style alerting for cyber-physical events.

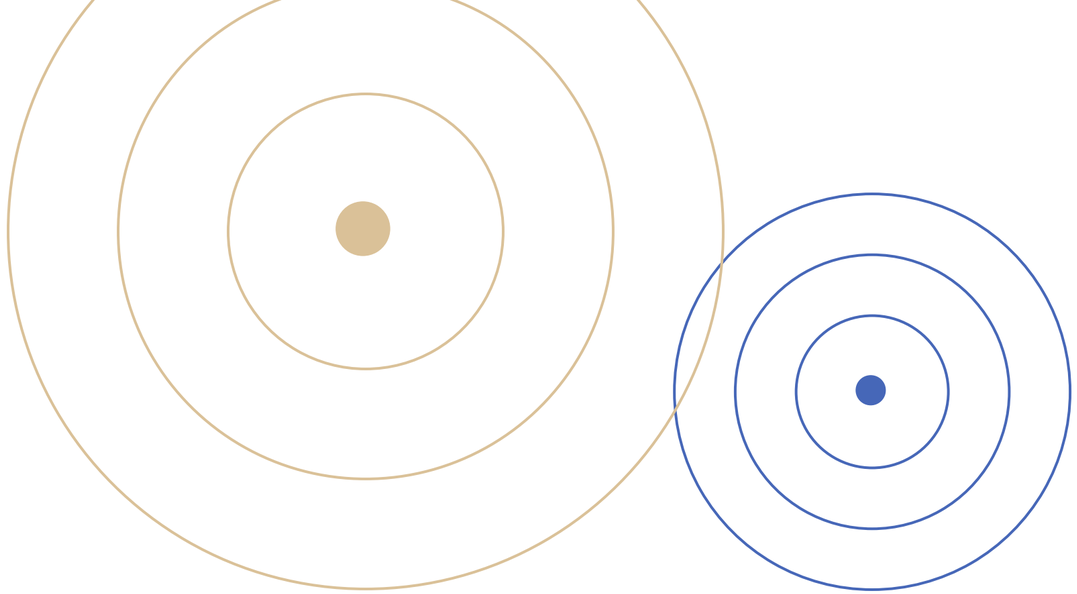
Tamper-evident evidence

Validated SOC events are anchored in a tamper-evident ledger, so an incident report rests on evidence an auditor will accept.

Policy fit Designed to feed NIS2 incident reporting and voluntary information-sharing arrangements (Art. 29), and to plug into the cross-border SOC model promoted by the Cyber Solidarity Act.

Three pilots, one cyber range

Producer, manufacturer and retailer: three operators at three stages of the chain, with three different data realities — plus a cyber range where staff rehearse real incidents.



ACT4FOOD

Aquaculture

United Aquaculture · BG

Trout producers: water-quality and environmental IoT, feeding systems, remote sites.

Dairy

Greek Family Farm · EL

Sheep and goat dairy: automated milking, pasteurisation and refrigeration control.

Retail

METRO · EL

Cold chain, inventory, logistics and POS — the widest attack surface.

Cyber Arena

Cyber range & training

Live attack simulation fed by real pentest findings and SOC playbooks.

Year one done; the build starts in December

Plans, threat landscape and draft architecture in place; integration and demonstration brought forward a year.

ACT4FOOD

SO FAR

Dec 2025
Project start

Jan 2026
Kick-off, Nicosia

Mar & Jul 2026
Two joint webinars, 135 participants

Sep 2026
SOC 4.0 architecture at ESIF, Bucharest

Oct 2026
Pilot co-creation launched; IEEE CloudCom paper

NEXT

Nov 2026
Threat landscape & regulatory report (public)

Dec 2026
Detection, integration and demo work start

Feb 2027
Requirements & reference architecture

May 2027
TACCP 4.0 Guidebook (pre-standard)

2027 – Nov 2028
Pilots, demos, unified SOC 4.0 validated

Work plan streamlined in 2026 A consolidated set of deliverables, and integration and demonstration starting at month 13 instead of month 24 — so pilots meet the system earlier.

Four lessons from the first architecture cycle

Offered to the cluster: what we would tell a consortium starting now.

ACT4FOOD

01 Define interfaces before components

Interface-first work let 17 modules from different partners move in parallel. Where a component led, its interface arrived late and the dependency stalled.

02 Safety severity is not economic severity

Collapsing them into one impact score hid exactly the cases we exist for: cheap incidents with serious food-safety consequences.

03 Heterogeneity is the requirement

Three pilots with three data realities forced generalisation into the design at the start, instead of retrofitting at deployment.

04 Compliance framing earns operator access

NIS2 obligations opened doors that a security pitch did not. Aligning with reporting duties is a deployment strategy, not paperwork.

What ACT4FOOD brings to ECSCI

Food joins the cluster's critical sectors. Our offer, mapped to the cluster's five objectives:

Scientific collaboration	TACCP 4.0 and consequence-weighted risk ranking: joint papers, cluster book chapters, a CEN Workshop Agreement route.
Technical collaboration	Food-sector CTI and a cyber-physical STIX extension to align with other CTI models; cyber-range scenario exchange.
Communication & dissemination	Joint webinars and workshops, cross-promotion of results, and our public threat-landscape and regulatory report.
Stakeholder alliance	A bridge to food operators and the food-safety and food-defence community, alongside our sister projects.
Marketplace	SOC 4.0 modules, the CTI feed and the Cyber Arena as exploitable assets for critical-infrastructure operators.

WHERE WE WOULD VALUE THE CLUSTER

1. **Confidential indicator exchange**

   How are other projects sharing indicators between competing operators?

2. **Consequence-weighted triage**

   Is anyone else ranking alerts on physical outcome rather than asset criticality?

3. **Shared scenario library**

   Interest in pooling attack scenarios across project cyber ranges?

ACT4FOOD

www.act4food.eu

Thank you

Questions, and ideas for working together, are welcome.

Odysseas Kokkinos
Project Coordinator · INNOV-ACTS Ltd
okokkinos@innov-acts.com

contact@act4food.eu
linkedin.com/company/act4food.eu

Co-funded by the European Union

ACT4FOOD has received funding from the European Union's Digital Europe Programme under grant agreement No 101249720. Views and opinions expressed are those of the author(s) only.