SecOPERA

Secure OPen source softwarE & hardwaRe Adaptable framework

SecOPERA will provide a one-stop hub for complex open-source software and open-source hardware (OSS/OSH) solutions delivering to system designers and operators and OSS/OSH developers and testers the means to analyse, assess, secure/harden, and share open-source solutions. The SecOPERA hub will offer an open-source framework supporting the DevSecOps lifecycle and generate solutions along with appropriate, verifiable security guarantees.

SecOPERA introduces an innovative security-assurance approach based on the decomposition of functionally similar layers (device, network, application, cognitive). The SecOPERA hub will generate a secure flow comprising a sequence of security credentials derived from security audit/testing of open-source components, each belonging to one of the aforementioned layers.

Objectives

Provide a complete security auditing-testing toolbox

Research and develop security hardening and enhancement of open-source solutions

Deliver adaptable security solutions for the open-source community

Establish the SecOPERA hub with a pool of open-source solutions

Develop the SecOPERA framework with tools to support the secure development lifecycle

Validate SecOPERA solution in two industrial pilots across several use cases

Provide a viable, open-source compliant exploitation and business model

Impact

Scientific

Secure disruptive technologies

Societal

Strengthened digital infrastructures, systems, and processes
Enhanced EU cybersecurity capacity and sovereignty in digital technologies
Reinforced awareness and fostering cybersecurity culture

Techno-Economic

Increased software, hardware, and supply chain security
Smart and quantifiable security assurance and certification across the EU
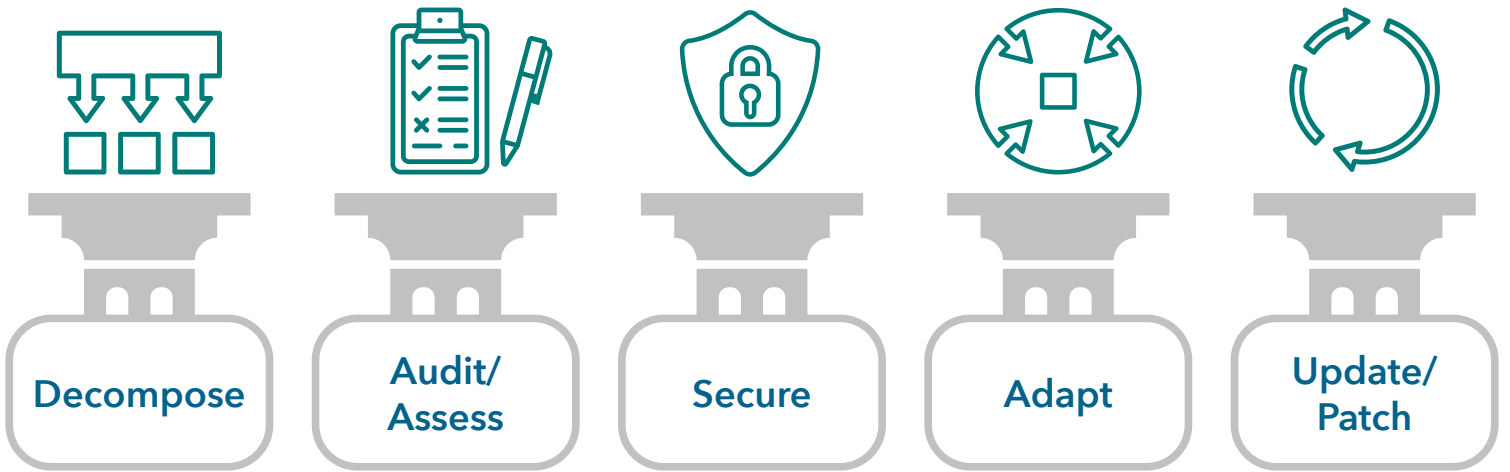
Pilots

Secure Supply Chain in Automotive Industry

Establish a highly secure operation between Pierer Innovation (OEM) and VoXel (Tier 1) that safeguards customer privacy and ensures adherence to current cybersecurity standards throughout the entire development pipeline.
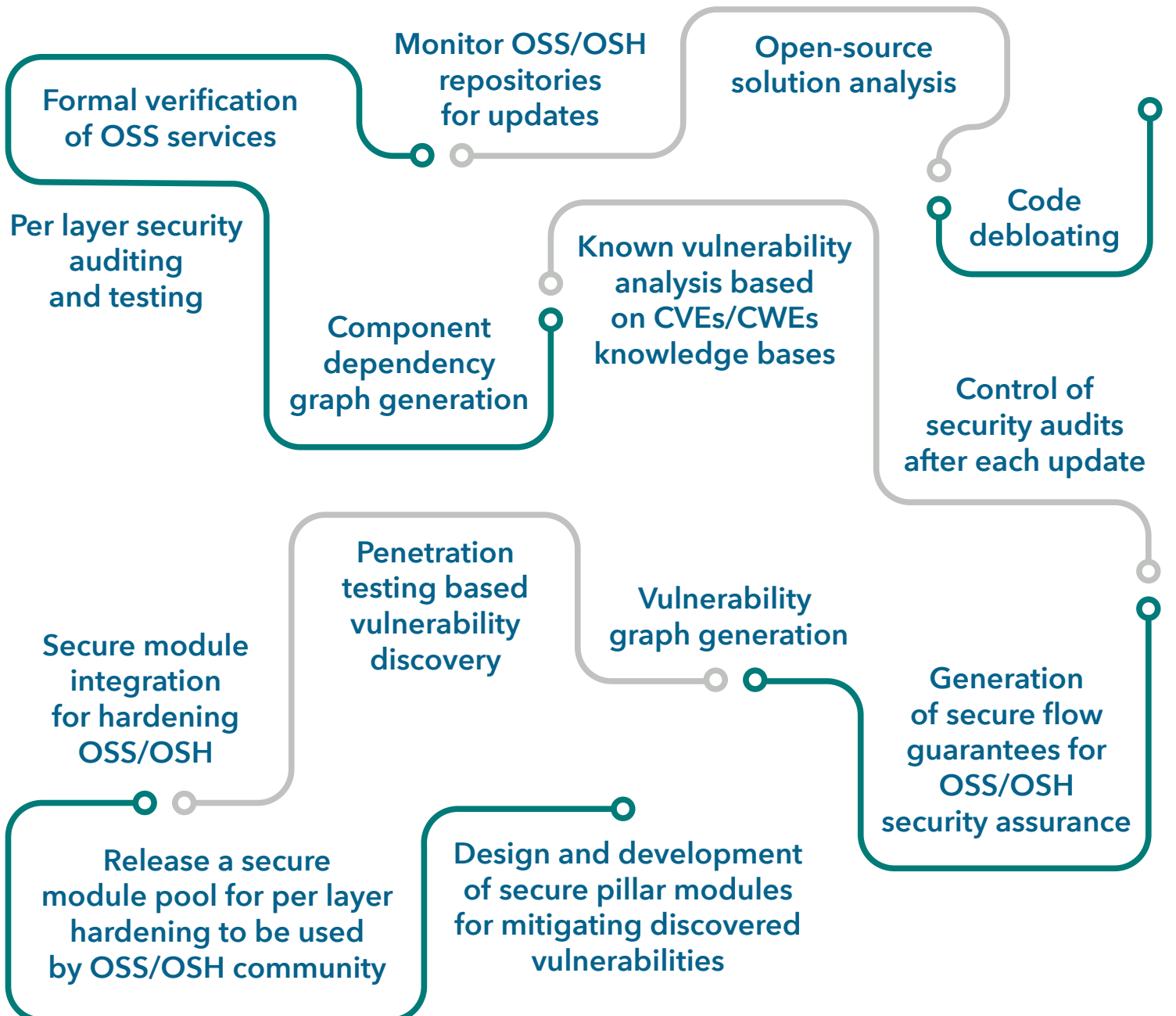
Water Management IoT Critical Infrastructure

Construct high-standard security solutions for the Greencityzen's IoT water-management environment in line with the EU Cybersecurity Act.

Pillars

Decompose	Audit/Assess	Secure	Adapt	Update/Patch

Functionalities

Formal verification of OSS services

Monitor OSS/OSH repositories for updates

Open-source solution analysis

Code debloating

Per layer security auditing and testing

Component dependency graph generation

Known vulnerability analysis based on CVEs/CWEs knowledge bases

Control of security audits after each update

Secure module integration for hardening OSS/OSH

Penetration testing based vulnerability discovery

Vulnerability graph generation

Generation of secure flow guarantees for OSS/OSH security assurance

Release a secure module pool for per layer hardening to be used by OSS/OSH community

Design and development of secure pillar modules for mitigating discovered vulnerabilities

Consortium

ΠΟΛΥΤΕΧΝΕΙΟ ΚΡΗΤΗΣ
TECHNICAL UNIVERSITY OF CRETE

AEGIS
IT RESEARCH

AΘΗΝΑ
Έρευνα & Καινοτομία
Τεχνολογίες Πληροφορίας

University of Cyprus

ATHENS UNIVERSITY OF ECONOMICS AND BUSINESS

PIERER INNOVATION

THALES
Building a future we can all trust

cea

VoXel
Interaction Design

ITML

Green CITYZEN

Sphynx Technology Solutions

Project Coordinator
Prof. Sotiris Ioannidis
Technical University of Crete
✉ sotiris@ece.tuc.gr

Start: 01.01.2023
Duration: 36 months
Participating Organisations: 13
Number of countries: 7
Call: HORIZON-CL3-2021-CS-01
EU Contribution: € 4,581,135.00

Learn more

🌐 https://secopera.eu/   ✉ info@secopera.eu

Follow us

in company/SecOPERA   🐦 @SecoperaP

▶ SecOPERA Project   zenodo /communities/secopera