MIRANDA

A framework for collaborative cyber-security operations over service supply chains

Form hypotheses, perform analyses and predict what may happen in complex, heterogeneous, and interconnected systems

Beyond the software: digital services

96% of organsations expect their vendor ecosystem to grow

97% of organsations were negatively impacted by at least one breach in their supply chain

45% of organisations are working directly with partners to remediate issues

Source: BlueVoyant, The State of Supply Chain Defense – Annual Global Insights Report 2025

Software

Devices

Infrastructures

API

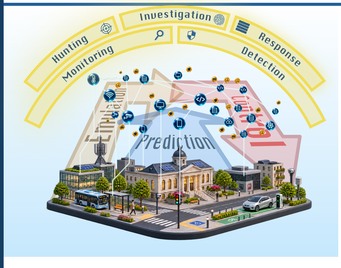
Data

Multi-ownership digital service chains

- Compose across the computing continuum
- One service, many owners
- Dependencies you cannot see
- Fragmented end-to-end cyber-security
- An evolving, unpredictable attack surface



Cybersecurity Digital Twins



- See what is happening — and what may happen next
- Connect runtime context with threat intelligence
- Detect vulnerabilities before they are exploited
- Adapt security as services change
- Turn insight into effective response

Benefits

Investigate with Context

Enriched alerts, service context and prioritised attack paths.

Test Before Acting

Safely emulate attacks and mitigation options before changing live services.

Integrate Existing Operations

Connect SIEM, SOAR and CTI through open interfaces and standards.

Built for Complex Ecosystems

Coordinate protection across domains while retaining local control.

Adaptive by Design

Stay effective as services and threat landscapes evolve.

Anticipate Attack Paths

Identify likely attack paths and lateral movement before an attack escalates.

Consortium

Consiglio Nazionale delle Ricerche
SPACE
ONESOURCE
security technology law research Stelar
Logstail
Politecnico di Torino
NASK
AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
Sphynx
Plaixus
UBITECH ubiquitous solutions
WOBCOM
MINDICITY
GRUPPO TIM
CITY OF ATHENS (o.o) DAEM

Project factsheet

Start date: 1 September 2024
Duration: 36 months
Budget: 7 308 925.00 €
Programme: HORIZON-CL3-2023-CS-01-01

Project coordinator:
Matteo Repetto (CNR/IMATI)

Technical coordinator:
Georgios Koutsimpiris (Space Hellas)

info@mirandaproject.eu

Follow us

@mirandaprj

https://www.mirandaproject.eu

MIRANDA EU project

@MIRANDA-Project

The project funded under Grant Agreement No. 101168144 is supported by the European Cybersecurity Competence Centre