TELEMETRY

Find the TELEMETRY tools that fit your needs.

TELEMETRY brings together a set of tools developed by project partners to address different needs across the cybersecurity and IoT ecosystem.

Explore our suite of tools at a glance, with intuitive colour coding that helps stakeholders quickly identify the solutions most relevant to their needs.

Visit our website

www.telemetry-project.eu

The project is funded by the European Union under grant agreement ID 101119747. Views and opinions expressed are, however, those of the author (s) only and do not necessarily reflect those of the European Union or the European Research Executive Agency (REA). Neither the European Union nor the granting authority can be held responsible for them.

WHO CAN BENEFIT?

1 Component Developers
2 System Integrators
3 System Operators
4 Cybersecurity researchers
5 Scientific community
6 Academia
7 Policy makers

Anomaly-Based Component for intrusion detection (BACON) - ENG

BACON is a machine learning-based analysis tool that detects anomalies, threats, and malicious activities on network traffic data leveraging federated learning approach.

Nokia Anomaly Detection (NAD) Pipeline - NOKIA

Enables predictive anomaly detection on IoT time series data using automated machine learning model generation.

Secure Information Event Acquisition (SIEA) Pipeline - NOKIA

Improves security operations by filtering, prioritising and aggregating security indicators from multiple tools.

Trust Analyser (TA) - MTU

A customizable trust analysis solution that integrates easily into existing or new systems and supports flexible trust evaluation.

Auditable Data Infrastructure (ADI) - MTU

Provides tamper proof, auditable and trustworthy data storage and sharing across distributed IoT ecosystems.

Misuse Detection ML Toolkit - i4RI

Detects misuse by learning normal IoT behavior and flagging abnormal sensor patterns in real time.

Access Control Risk Assessment Model (ACRAM) - WRCVE

ACRAM is a fuzzy logic based risk assessment solution that continuously evaluates access control risks and supports adaptive cybersecurity management.

Secure Software Updates - KUL

A lightweight cryptographic library for secure IoT software updates, ensuring integrity, authenticity, and efficient performance on constrained devices.

Software Bill of Materials (SBOM) Generator - SINTEF

The tool identifies software components and known vulnerabilities in firmware, supporting supply chain security for IoT systems.

Network Fuzzer - SINTEF

Increases early detection of network-level vulnerabilities by making fuzz testing accessible to non-expert users.

Digital Twin - SINTEF

Enables cost-effective and repeatable security analysis of IoT firmware without requiring physical devices.

Component & System Risk Analysis Tool - University of Southampton

Enhanced cybersecurity risk awareness and decision-making, especially targeted towards SMEs with limited internal expertise.

Robot Anomaly Detection Tool - ATC

An explainable AI tool that identifies deviations from normal operation patterns & their causes, enabling early failure diagnosis & efficient troubleshooting.

R-Monitoring - ATC

A tool for resource-constrained, diverse-architecture systems, comprehensively monitoring system metrics, processes, and file operations to detect intrusions & malware threats.

Network Anomaly Detection - ATC

An AI tool leveraging machine learning to analyze network traffic against predefined baselines, identify behavior anomalies & malfunctions, and detect security threats.

PROJECT PARTNERS

NOKIA · SINTEF · MTU · Ideas for Research & Innovation · ATC Athens Technology Center · KU LEUVEN · TIM · eng · WRCVE · Antonov Airlines · University of Southampton