CELTIC-NEXT eureka clusters

Project Achievements

CISSAN

Project ID: C2022/1-3

Start Date: 1 May 2023

Closure date: 31 May 2026

Partners:

Austria
Geodata ZT GmbH

Finland
Bittium Biosignals Ltd.
Bittium Wireless Ltd.
Mattersoft Ltd.
Mint Security Ltd.
Netox
Nodeon Finland Oy
ScopeSensor Ltd.
University of Jyväskylä
Wirepas Oy

Spain
Councilbox Technology S.L.

Sweden
Affärsverken Karlskrona
Arctos Labs Scandinavia AB
Blekinge Tekniska Högskolan
Blue Science Park
Clavister AB
Savantic
Techinova AB

Co-ordinator:

Ilgin Safak

University of Jyväskylä, Finland

E-Mail: ilgin.i.safak@jyu.fi

Project Websites

www.celticnext.eu/project-cissan

https://www.jyu.fi/en/projects/cissan

https://www.bittium.com/about-bittium/technology-innovation/seamless-and-secure-connectivity-program/

https://www.geodata.com/en/project-overview/

https://www.bluesciencepark.se/projekt/cissan-collective-intelligence-supported-by-security-aware-nodes/

https://github.com/markkve/CissanOSTools/

https://www.councilbox.com/en/cissan-en/

Collective intelligence supported by security aware nodes

With the help of CISSAN, organisations can transform their legacy, centralised systems to decentralised ones seamlessly - no need to rely on a single system. Instead, the entire network becomes its own cybersecurity system. Through collaboration, automation, and shared intelligence, organisations can create a new generation of scalable, resilient, and secure infrastructures in Europe.

Main focus

Critical infrastructures are increasingly becoming digitalised and interconnected, including in transportation, smart energy grids, tunnel construction, and manufacturing domains. While this interconnectedness drives efficiency and innovation in these systems, it also poses numerous cybersecurity challenges. Today's systems are largely designed and implemented in isolation from one another, making it difficult to detect and respond to increasingly sophisticated cyberattacks that may affect multiple domains. As a cybersecurity project, CISSAN and its 18 partners across four European countries provide a solution to this problem by introducing collective intelligence for cybersecurity in Internet of Things (IoT) and Operational Technology (OT) networks. In this paradigm, systems and devices collaborate to detect cyber threats locally and share threat information to coordinate incident responses, thereby preventing and mitigating threats in a cooperative manner.

Approach

The main outcome of the CISSAN project is a platform that leverages collective intelligence to enable collaborative information sharing and ensure network cybersecurity. It brings heterogeneous systems together into a unified, resilient environment that enables testing, validation, and cybersecurity improvement. The CISSAN platform incorporates real-world use cases in transportation systems, smart energy grids, tunnel construction systems, and automated disaster recovery scenarios, and enables secure communication among them.

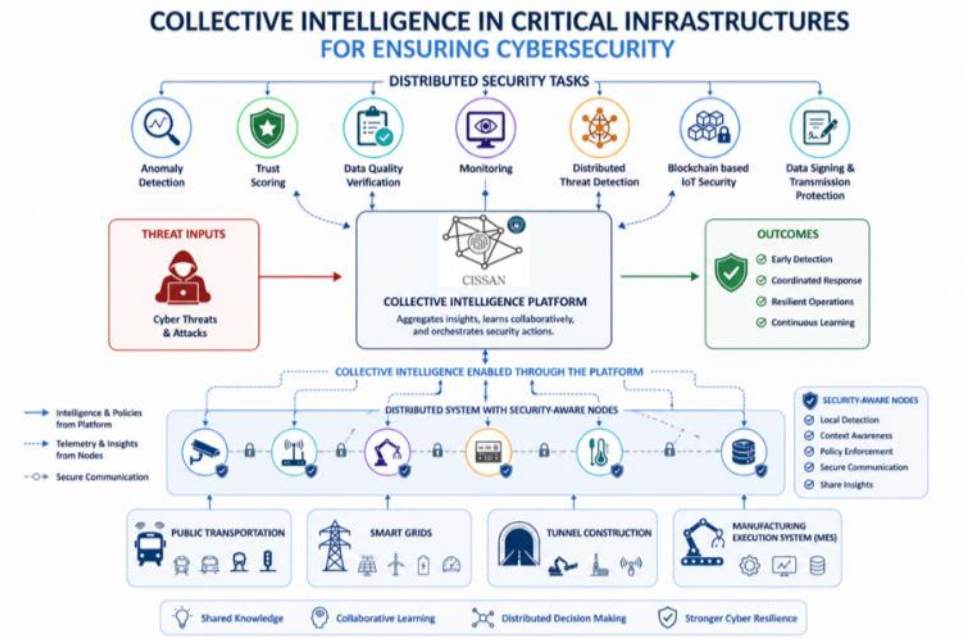

Figure 1. *The CISSAN platform and its use case solutions*

By developing this platform, CISSAN has shown that security events can be detected locally on devices, that information exchange between systems is possible using structured threat intelligence, that trust between systems can be dynamically evaluated, and that automatic and cooperative responses to cyber threats are achievable across multiple domains.

Achieved results

As a cybersecurity project, the main achievements of CISSAN include an innovative platform and its use case solutions, demonstrating clear improvements in security, performance, scalability, and efficiency compared to existing approaches in realistic transportation, smart energy grids, tunnel construction and manufacturing execution system environments, even against multi-domain critical infrastructure attacks. It combines anomaly detection, data quality verification, trust scoring, STIX-based threat sharing, blockchain-based logging and record retrieval, optimal security-task distribution, and automated recovery orchestration across these scenarios. It is interoperable and compliant with existing cybersecurity standards and regulations, enabling them to integrate seamlessly with heterogeneous systems across domains through standardised interfaces and data exchange mechanisms.

One of the main innovations of CISSAN is its potential to allow a gradual evolution of traditional centralised infrastructures towards more distributed and collaborative models. This is particularly important in critical infrastructures, as it is not possible to completely redesign them. Through an extensible architecture and open-source software framework built on WebAssembly technology, it is now possible to enable collective intelligence on any system without disrupting current operations, making it a practical solution.

The project contributed to 18 scientific publications presented at international conferences and workshops and published in peer-reviewed journals and books. In addition, the project generated exploitable results that form the basis for further development, including patent filings and an open-source CISSAN framework. CISSAN contributes to standards with its suggestion for extending the STIX threat report standard, which is a standardised way to describe cyber threats, so organisations can easily share, understand, and use that information to detect, prevent, and mitigate attacks faster.

The results are expected to deliver long-term value through continued use in research, innovation activities, and industrial applications, supporting competitiveness, technological advancement and digital sovereignty of the EU in the cybersecurity domain.

Impact

The CISSAN project delivers innovation by incorporating collective intelligence mechanisms into cybersecurity. It brings significant advances in the state of the art in cybersecurity through the incorporation of trust scoring, anomaly detection, data quality verification, optimal security tasks execution, disaster recovery orchestration, and the ability to share structured threat intelligence in a unified and interoperable manner. This is expected to provide a competitive advantage by enabling organisations across different domains and sectors to offer more scalable, robust, and flexible cybersecurity solutions in the European region.

The impact of CISSAN can be considered in terms of Europe's future:

1) Better security of critical infrastructures
2) Better resilience against cyberattacks in IoT and OT networks
3) New business opportunities in terms of cybersecurity solutions
4) A push towards European digital sovereignty

The project has had an impact on research, innovation, and knowledge sharing through 18 publications, six patent applications, 16 industry events and eight websites.

About CELTIC-NEXT

CELTIC-NEXT is the EUREKA Cluster for next-generation communications enabling the digital society. CELTIC-NEXT stimulates and orchestrates international collaborative projects in the Information and Communications Technology (ICT) domain.

The CELTIC-NEXT programme includes a wide scope of ICT topics based on new high-performance communications networks supporting data-rich applications and advanced services, both in the ICT sector and across all vertical sectors.

CELTIC-NEXT is an industry-driven initiative, involving all the major ICT industry players as well as many SMEs, service providers, and research institutions. The CELTIC-NEXT activities are open to all organisations that share the CELTIC-NEXT vision of an inclusive digital society and are willing to collaborate to their own benefit, aligned with their national priorities, to advance the development and uptake of advanced ICT solutions.

CELTIC Office

c/o Eurescom, Wieblinger Weg 19/4
69123 Heidelberg, Germany
Phone: +49 6221 989 0
E-mail: office@celticnext.eu
www.celticnext.eu

eureka