SafeHorizon

Preventing Crime-as-a-Service with Cutting-Edge Tools and Intelligence

Project Brochure

Call ID:
HORIZON-CL3-2023-FCT-01

Grant Agreement Number:
101168562

Duration:
01.09.2024 – 31.08.2027

Funded by
the European Union

The vision

Crime-as-a-Service (Caas)

CaaS represents a worrying evolution in the cyber threat landscape, transforming criminal activities into organised and commercialised enterprises. Similar to legitimate Software-as-a-Service (SaaS) platforms, CaaS offers on-demand illicit services such as malware rentals and fraud platforms. This shift lowers barriers to entry for cybercriminals, enabling individuals without technical skills to engage in activities like identity theft and payment card fraud through digital means. The consequence is a significant amplification of criminal operations' scale and impact.

Our Aim

SafeHorizon aims to tackle the emerging threat of Crime-as-a-Service (CaaS) by harnessing intelligence from various sources including the clear web, deep web, dark web, public dumps, and law enforcement datasets. By integrating these data streams with machine learning technologies, the project seeks to extract actionable evidence for legal use.

Use Cases

1

Monitoring transnational crime networks

Monitoring activities of actors in crime networks including ongoing malicious campaigns that may span across different jurisdictions and developing a set of dedicated crawlers which will provide insight and visibility of real-time activity of malicious online activity.

2

Criminal marketplace analysis

In order to assess the efficacy of the crawlers and the correlation engine, this use case is dedicated to the analysis of criminal marketplaces, and includes testing the usefulness of SafeHorizon tools to identify crime networks and investigate their members.

3

Child sexual abuse and trafficking

This use case presents a comprehensive overview of the distribution channels and of the release dates of child sexual abuse material (CSAM).

4

Malware-as-a-Service

Malware-as-a-Service (MaaS) is a business model under which cybercriminals provide access to malicious software and related infrastructure for a fee, and in this use case, we monitor and analyse ongoing malicious campaigns that may target organisations or individuals.

What Do we do

SafeHorizon aims to tackle the emerging threat of Crime-as-a-Service (CaaS) by harnessing intelligence from various sources including the clear web, deep web, dark web, public dumps, and law enforcement datasets. By integrating these data streams with machine learning technologies, the project seeks to extract actionable evidence for legal use.

SafeHorizon will provide LEAs, emergency response teams (CERTs), and computer security incident response teams (CSIRTs) with a comprehensive toolbox of underdevelopment and enhanced open-source solutions that are designed to be user-friendly and easily adaptable.

Project Objectives

1

Monitor CaaS platforms

SafeHorizon will monitor CaaS platforms from various threat actors to understand their modus operandi (arsenal, methods, motivation, strategies, and monetisation mechanisms).

2

Enable seamless collection of digital evidence

SafeHorizon will combine the collected information from the crawlers with malware samples, phishing emails, intelligence feeds, and private and proprietary datasets to extract features that will be used by ML and AI algorithms to generate actionable intelligence.

3

Correlation, attribution, & disruption aligned with EU norms

By monitoring the infrastructure, cryptocurrency transactions, and online presence and using various intelligence feeds beyond attribution, SafeHorizon will provide LEAs with actionable intelligence to facilitate the disruption of malicious campaigns and bring the perpetrators before the court.

4

Real-time threat modelling and exposure assessment

By developing dynamic and stochastic models, SafeHorizon will provide suitable tools for real-time monitoring of threats, better-anticipating changes in risk and optimising risk management policies.

5

EU resilience and cyber sovereignty

By building technology made in the EU, SafeHorizon will reduce European dependency on allies and other third parties while also reducing the time until a vulnerability or an attack on EU infrastructures or critical services is notified to national authorities.

6

Guide responsible and replicable research in FCT

SafeHorizon aims to create a research FCT hub that would allow vetted researchers to access curated datasets and trained models, allowing them to extend and improve results without the need to start from scratch or face legal constraints.

Innovations

The SafeHorizon will collect data from various sources, aggregate them and use machine learning and artificial intelligence to analyse and correlate it, enabling LEAs to gain insights into emerging threats and criminal activities that may not be apparent through traditional investigative methods and their tooling.

Moreover, SafeHorizon will detect threats in real-time or even before they materialise. This early warning system will allow LEAs to take proactive measures to prevent or mitigate potential attacks.

Impact

For LEAs, CSIRTs, CERTs and ISACs

SafeHorizon will develop tools to strengthen the capacity of LEAs, CSIRTs, CERTs and ISACs to tackle local and global criminal activity by identifying transnational criminal networks and marketplaces that enable the operation and monetization of CaaS.

For EU cybersecurity and security providers

SafeHorizon enhances the European Union's sovereignty in digital technologies by developing tools and technologies within its jurisdiction, enabling EU security providers to access reusable technology and actionable threat intelligence without reliance on external entities.

For service providers

SafeHorizon will provide an integrated dashboard showing to the service providers the potential risks and offering threat intelligence capabilities stemming from an in-depth view of the modus operandi of threat actors.

For policy makers

SafeHorizon research results will support policy makers, organisations and institutions to design and/or improve policies related to online crime and cybercrime prevention.

For end-users and society

SafeHorizon equips citizens and LEAs to combat online crime and cyber risks, addressing growing family concerns about internet safety for youth. By disrupting malicious campaigns, it reduces cyberattacks on critical infrastructure, safeguarding essential services and boosting trust in cyber-physical systems.

Partners

Athena Research Center (Coordinator)

Athena RC studies a broad spectrum of research issues within these fields, including some raised by other sciences, industrial applications, or societal challenges. Together with research, innovation is also a fundamental pillar of the mission of Athena RC. Research institutes, spin-off companies, and three highly-specialised clusters in knowledge-intensive thematic sectors (nano/microelectronics-based systems and applications, space technologies and applications and gaming and creative technologies and applications) create a fertile technological innovation ecosystem within the Center, with mutually beneficial collaborations between its members and systematic efforts to bring to market any research results with such potential.

Data Centric

Data Centric is a pioneering research and innovation-focused SME, providing data-centric solutions to address complex challenges in the cyber realm. The company specialises in a broad range of areas, including cybercrime prevention, open-source intelligence (OSINT), AI-driven software security, and network science. By leveraging large-scale data collection, machine learning, knowledge graphs, and cutting-edge language models, DC explores the untapped potential of the data landscape.

Vicomtech

Vicomtech is an applied research centre for Interactive Computer Graphics and Multimedia located in San Sebastian (Spain). It is a non-profit foundation, established in 2001 as a joint venture by the Fraunhofer INI-GraphicsNet Foundation and the EiTB Broadcasting Group.The main research group that will be contributing to the execution of the project is the Digital Security department. The department is currently working on the design of subtle and specific attack detection indicators using logs and network captures within several use cases. In addition, this research group is also creating synthetic data and analysing transactions in a blockchain simulator environment. In this context, new tools to analyse network flux and covert channels are being designed.

KEMEA - Center for Security Studies

The Center for Security Studies (KEMEA) is a think tank on homeland security policies and an established research center since 2005 within the Hellenic Ministry of Citizen Protection, aiming to support security policy implementations in Greece at a strategic level. More specifically, the activities KEMEA is involved in include: certification of private-security professional practitioners at the national level, research and development in the context of National and European projects, in close cooperation with LEAs, working under the auspices of the Ministry of Interior and training of practitioners in new systems and technologies.

CSIC / GiCP

The Cybersecurity and Privacy Protection Research Group (GiCP) is part of the Spanish National Research Council (CSIC), which is the largest public research performing organisation (RPO) in Spain and the fourth most relevant public institution in the European Union. GiCP brings together expertise in early detection of cyber attacks and information operations and in the development of cryptographic techniques for anonymisation and secure software execution in order to guarantee the security, authenticity and integrity of information. The aim of CSIC is the promotion, coordination, development and dissemination of multidisciplinary scientific and technological research to contribute to the advancement of knowledge and economic, social, and cultural development, as well as the training of personnel and advice to public and private entities.

Tampere University

The primary objective of the Network and Information Security Group (NISEC) at Tampere University is to bring together expertise in education, research, and practice in the field of information security and privacy. Active since 1996, NISEC has notable achievements nationally, such as pioneering the deployment of native IPv6 in Finnish campus networks, introducing and rolling out Eduroam-based wireless roaming in Finland, forming the TREX regional Internet exchange point, establishing internationally federated research testbeds with PlanetLAB and GENI, as well as creating two successful spinoff companies. The core competencies of NISEC currently traverse four areas: Network Security; IoT Security; Hardware-Assisted Security; Privacy and Usable Security.

Privanova

Privanova is a Paris-based Research & Innovation consultancy specialising in law, ethics, and security. As a leading provider of Privacy Compliance and Risk Management Solutions, Privanova offers comprehensive services to address privacy, data protection, and information security needs. Privanova excels in EU-funded, interdisciplinary research projects. Our expertise spans the entire EU project lifecycle, from consortium building and proposal drafting to communication, dissemination, and exploitation. Privanova's team includes former INTERPOL and UN professionals, as well as experienced Evaluators, Reviewers, and Ethics Experts for the European Commission.

General Police Inspectorate of the Republic of Moldova

The General Police Inspectorate of the Republic of Moldova is the main law enforcement authority, responsible for maintaining public order and combating crime in the country. The General Police Inspectorate (GPI) of the Republic of Moldova plays a pivotal role in the SafeHorizon project, contributing expertise in the field of law enforcement and contributing to the development and technical aspects of the artificial intelligence tool.

Delft University of Technology

The Delft University of Technology is the oldest and largest public technical university in the Netherlands. It specializes in engineering, technology, computing, design, and natural sciences. The TU Delft Cybersecurity group at the faculty of Electrical Engineering, Mathematics, and Computer Science will participate in the project.

Cyprus Police

Cyprus Police is the south-eastern Mediterranean safe keeper of the European Union, with the duty to block criminals and any other illegal activity to enter and travel in EU soil. By combating criminality, battling cross-border crime and combating fraud in CY prevents illegal activities from spreading to the EU. Cyprus Police comprises several departments which are dealing with preventing and combating crime in all forms and are working to fulfill the goals set by the European Commission and Council conclusions.

Cyber Intelligence House

Cyber Intelligence House is a leading cyber intelligence company specialised in helping cyber security professionals and law enforcement to assess and monitor cyber exposure from the dark web, deepweb, data breaches and online-assets. It is the trusted provider to government and law enforcement agencies globally, including Interpol and UNODC. Cyber Intelligence House's Cyber Exposure Platform (CEP) provides the world's most comprehensive Cyber Threat database with over 10 years of data. 24/7 collection and storing of new data at a rate of ~600 pages per second. CEP delivers unrivaled search and alerting performance with Deep scanning of over 250 metadata factors and machine learning enabled categorization of threats to provide deep insights into potential cyber threats.

Scorechain

Scorechain Blockchain Analytics is a comprehensive solution designed to track cryptocurrency activities from a risk-AML-CTF perspective. We offer in-depth risk-scoring analysis on transactions, addresses, and entities by identifying counterparts and transaction patterns. We support various blockchains and use internal techniques, which can require manual or algorithmic de-anonymization, to name them. Scorechain Blockchain Analytics offers a comprehensive set of tools and techniques that help our customers and users mitigate the risks associated with cryptocurrency transactions while ensuring compliance with regulatory requirements.

Polish Police

The Provincial Police Headquarters in Kielce is an organizational unit of the Police, constituting an auxiliary apparatus with the help of which the Provincial Police Commander in Kielce, acting on behalf of the Świętokrzyskie Voivode or himself, performs the tasks of the Police, specified in the acts and executive regulations issued on their basis, in the field of protection of human safety and maintaining public safety and order in the area of the Świętokrzyskie Voivodeship.

LEA Projects Cluster Member

LEA projects cluster

SafeHorizon is a member of the The Law Enforcement Agencies (LEA) Project Cluster, led by Privanova.

LEA Project Cluster is a collaborative platform that unites EU-funded projects focusing on cybersecurity, law enforcement, anti-money laundering, and counter-terrorism. This initiative aims to foster synergy among various projects by sharing knowledge, resources, and best practices, thereby enhancing the collective capability to address the complexities of cybercrime and cybersecurity challenges.

Members

TRACY
ODYSSEUS
CYBERSPACE
CounteR
PRECINCT
popAI
UNCOVER
POLIICE
ALIGNER
EU-HYBNET
Resilmesh
securing cyber infrastructures
SafeHorizon
KINAITICS
DYNAMO
AI4CYBER
CEASEFIRE
emeritus
FREE TOOL
PRO TAX
INSPECTr
CC-DRIVER
ROXANNE
LAW-GAME
RAYUELA
a fun way to fight cybercrime
LOCARD
DARLENE
TRACE
GRACE
COPKIT
STARLIGHT
NOTIONES
HEROES
CUT THE CRD
Tools4LEAs
CYCLOPES
PREVISION

SafeHorizon

Project Coordination:

Athena Research Center
Aigialias & Chalepa
15125, Marousi, Greece

Constantinos Patsakis
Email: kpatsak@athenarc.gr

Project Communication:

Privanova SAS
34, avenue des Champs-Elysées
75008 Paris, France

Ivana Hadži Pajić
Email: ivana@privanova.com

GET IN TOUCH: