



LEA Projects Cluster meeting

Law Enforcement Innovation & Synergies Workshop

29/01/2026

Privanova
Research & Consulting



comms@Privanova.com



34, avenue des Champs-Élysées, Paris



Funded by
the European Union



Welcome to the fourth LEA Cluster Projects meeting!

Law Enforcement Innovation & Synergies Workshop

Agenda

What to expect from today's event?

Time	Session	Speaker
11:00 - 11:05	Welcome and Introduction	Kristina Isakzay, PN (moderator)
11:05 - 11:10	Opening remarks	Farhan Sahito, PN
11:10 - 11:30	Keynote <i>Investigations in the digital realm: EU Priorities for innovation</i>	Gilles Robine, DG Connect
11:30 - 11:40	Keynote <i>Emerging training priorities for law enforcement agencies</i>	Estonian Police
11:40 - 11:50	Keynote <i>Preparing Law Enforcement Professionals for New Operational and Technological Realities</i>	Serbian Police Academy
11:50 - 12:00	Project IAMI AI-Driven Entity Identification and Intelligence Support for LEAs	Gideon Hazzani, LibereU IAM I Project Technical Manager
12:00 - 12:10	LEAs Feedback Session IAM I project Requirements	Kristina Isakzay, PN (moderator)
12:10 - 12:20	Project SafeHorizon Intelligence and Situational Awareness Against Crime-as-a-Service	Constantinos Patsakis, Athena Research Center, SafeHorizon Coordinator
12:20 - 12:30	LEAs Feedback Session SafeHorizon Awareness & Acceptance	Kristina Isakzay, PN (moderator)
12:30	Closing remarks	Kristina Isakzay, PN (moderator)

Opening remarks

Dr. Farhan Sahito

Partner, Privanova



CC-DRIVER

01 CC-DRIVER

May 2020

LEA Project Cluster initiated

19 Projects

Over the course of 3 years



02 CYBERSPACE

February 2023

CYBERSPACE took over the leadership

36 Projects

17 projects joined the cluster



03 SAFEHORIZON

September 2024

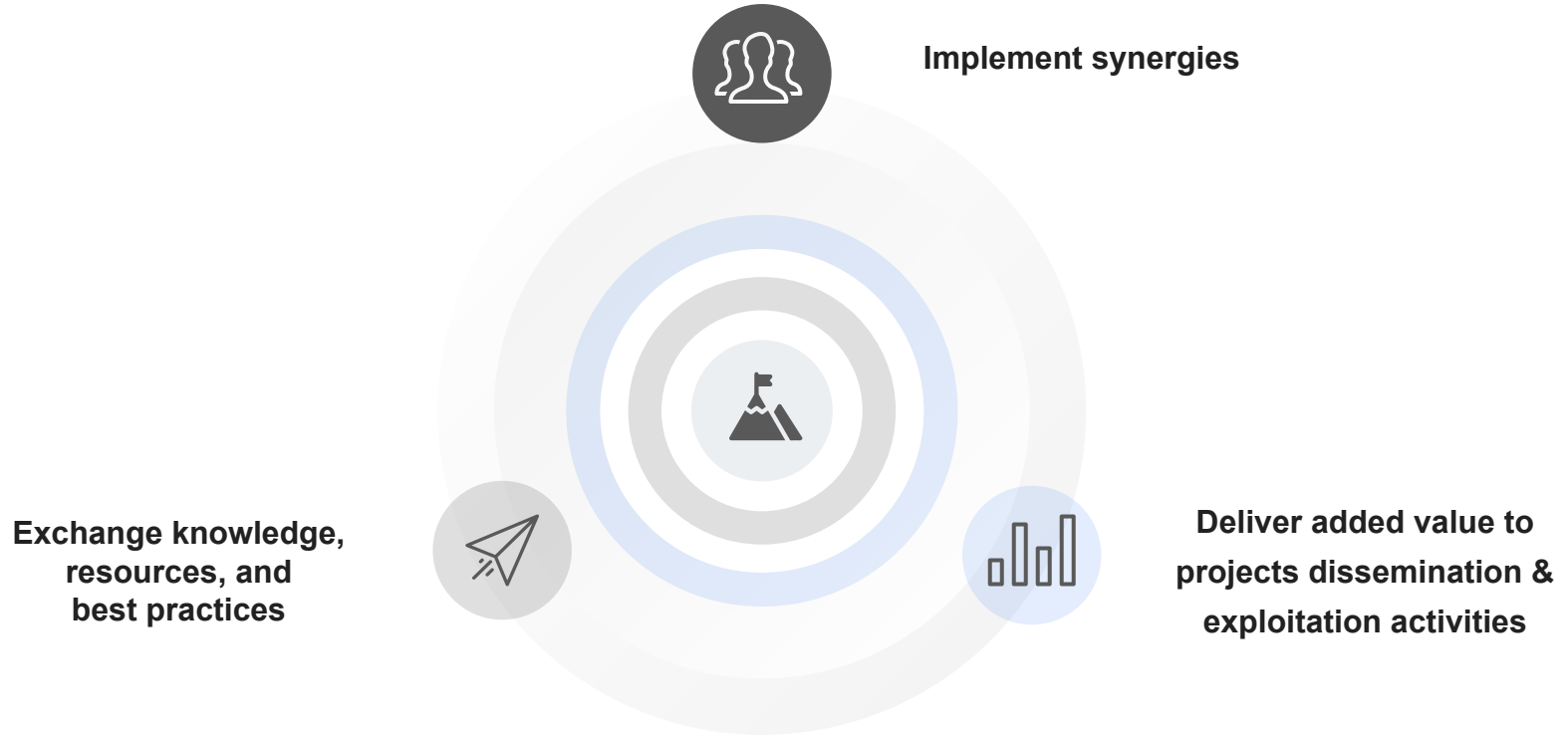
SafeHorizon took over the leadership

48 Projects

12 projects joined the cluster

COLLABORATIVE PLATFORM

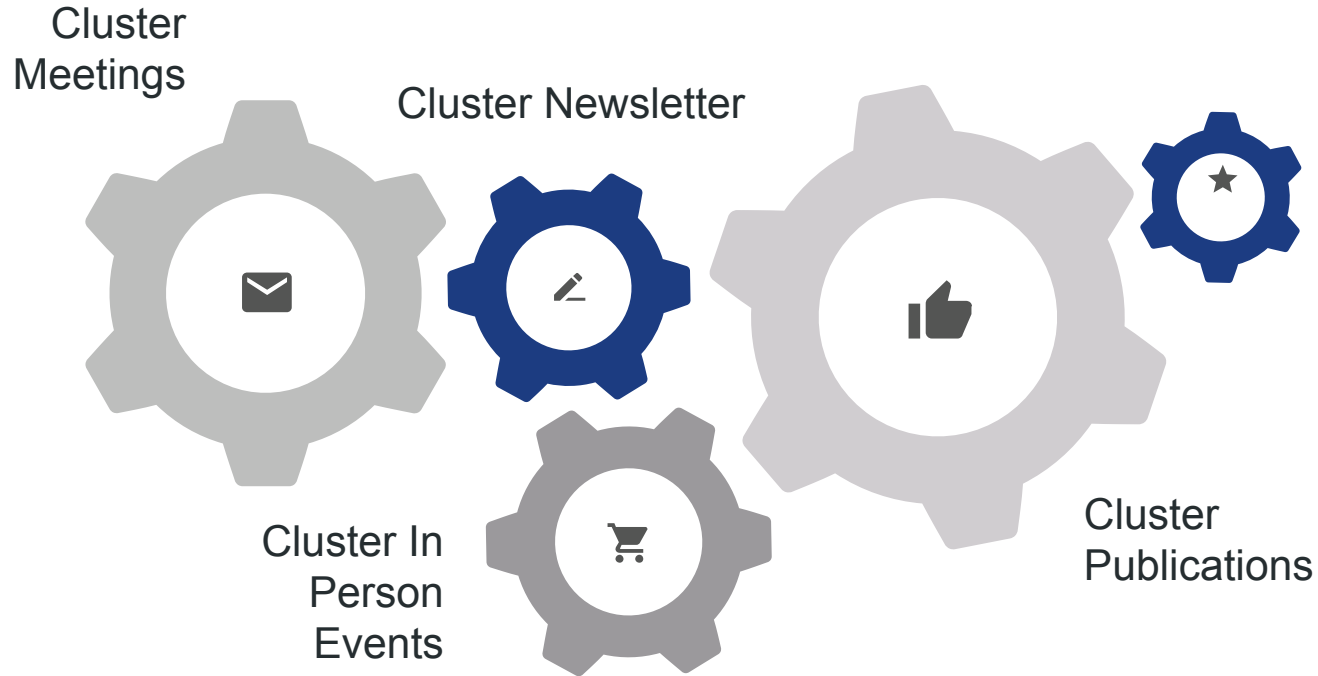
Our shared **purpose**





LEA Projects Cluster is **fast growing** community: **48 projects / 200+ partners**

Engagement, Communication & Visibility



New projects **recently joining** the **LEA Projects Cluster**



VANGUARD aims to strengthen the fight against trafficking in human beings (THB) through the provision of improved intelligence picture, delivery of an advanced and trustworthy suite of tools, and realisation of innovative training activities. Through its interdisciplinary consortium, VANGUARD will foster collaboration, provide policy recommendations, and raise awareness for sustainable impact against the exploitation of human beings.



EINSTEIN aims to enhance physical and digital identity checks, privacy-preserving identity management, and fraud detection for border and police authorities by developing and validating six advanced applications, including mobile and online checks, document authentication, pre-registration, and biometric fast-track solutions.



INCIDENTRON is an EU-funded project focused on improving how organizations report and manage cybersecurity incidents. It develops a modular and scalable architecture, an open-source incident reporting framework, and a platform that supports end-to-end reporting across major EU regulations including NIS2, CER, DORA, GDPR, and the Cyber Resilience Act (CRA).

Keynote

Gilles Robine,
DG Home

Investigations in the digital realm: EU Priorities for innovation

LEA Discussion & Feedback

Keynote

Kaisa Ellandi,
Estonian Police and Border Guard Board

Emerging training priorities for law enforcement agencies



Short introduction

Who am I?

- **Name:** Kaisa Ellandi
- **Organization:** Estonian Police and Border Guard Board
- **Experience:** Development projects and innovation in the field of prevention and offence proceedings
- **Personal interests:** Horseback riding and dog training
- **Get in touch:** Open to cutting-edge project proposals in law enforcement

Questions

What changes are already taking place in Estonia and around the world, or are upcoming, that will significantly affect our work?

What new training needs are emerging as a result of these changes?



Why are we talking about the future?

We are not predicting the future. We are not talking about science fiction. We are talking about changes that **have** already **begun**.

Police work does not change because we want it to - it changes because **society**, **technology**, and **crime** are changing anyway.

Not all trends are good or bad. They represent new **risks** and new **opportunities**, at the same time.



Changes in police work – where are we headed?

Who is the offender?

Increasingly, cases involve a combination of a human + automation + multi-platform tools.

How do we prove who committed the act — was it a human?

How is responsibility divided between the individual and the owner of the platform or tool?

Crime is becoming automated

Semi-automated AI-driven crime-as-a-service markets are emerging - AI handles customer interaction, negotiations, and recruitment.”

Crime types are converging

Organised crime is increasingly intertwined with other phenomena: cyberattacks, fraud, money laundering, and more.

Traditional crime is becoming digitalized

Cyber investigation is becoming commonplace even in cases that are not classical cybercrimes.



What this means for training?

- Digital competence
- Adapting to new crime patterns
- Human skills & communication
- Resilience & stress management
- Ethics & fundamental rights



**Police work does not change
because we want change; it
changes because society,
technology, and crime are
changing anyway.**

We have to act before we are forced to.

LEA Discussion & Feedback

Keynote

Prof. Zvonimir Ivanovic,

University of Criminal Investigation and Police Studies

Bridging Innovation and Operation: Training Experiences in Horizon Europe Security Projects

Empowering law enforcement through Ceasefire, Anita, Salvus, and Sparkup²⁰

Introduction & Philosophy

Core Message: Horizon Europe projects produce cutting-edge technology, but *training* is the bridge that makes these tools usable for Law Enforcement Agencies (LEAs).

Our Role: We translate complex R&I results into operational capability.

Key Themes:

- Operationalizing AI tools.
- Harmonizing legal best practices.
- Cross-sector talent development.



Project Ceasefire (Firearms Trafficking)

Context: Combating illicit firearms trafficking using advanced AI and cross-border data fusion.

Training Focus: "Operationalizing Technology"

What we trained on:

- *Mobile Detection:* Training field officers to use the "On-the-Spot" mobile app for rapid firearm identification at crime scenes.
- *Intelligence Tracking:* Teaching analysts to use the "Firearms Incident Tracking Tool" to link ballistic data across borders.
- *Dark Web Analysis:* How to interpret AI-generated alerts from darknet marketplaces.

Key Result: LEAs moved from manual checks to automated, AI-assisted recognition.



Project Anita (Illegal Trafficking)

Context: Fighting online illegal trafficking (drugs, counterfeit goods) using heterogeneous data (text, video, crypto).

Training Focus: "The Human-in-the-Loop"

What we trained on:

- *Investigative Systems:* Training investigators to interact with the Anita knowledge graph—teaching them not just to "read" data, but to feed their domain expertise back into the system.
- *Crypto-analysis:* Training on tracing cryptocurrency transactions linked to trafficking networks.
- *Curriculum Development:* Creating specific modules for "Online Intelligence Analyst" profiles.

Key Result: Bridging the gap between data scientists and police investigators.



Project Salvus (Child Sexual Abuse - CSA)

Context: Ensuring safer justice outcomes in online and undercover CSA investigations.

Training Focus: "Ethics, Law & Best Practice"

What we trained on:

- *Harmonization:* Training practitioners on the new European Best Practice Guidance for evidence collection (standardizing how evidence is gathered to ensure it stands up in cross-border courts).
- *Child-Centered Approaches:* Specialized training on victim identification that prioritizes the rights and psychological safety of the child.
- *Legal Frameworks:* Navigating the complex differences in admissibility of digital evidence across EU member states.

Key Result: Moving beyond just "technical" training to "procedural and ethical" competence.

Project SparkUp (CBRNE & Innovation)

Context: Strengthening CBRNE (Chemical, Biological, Radiological, Nuclear, Explosives) preparedness and talent development.

Training Focus: "Capacity Building & Future Skills"

What we trained on:

- *Talent Development:* Upskilling programmes that help academic researchers understand LEA needs, and vice-versa (bridging the "Valley of Death" in innovation).
- *Immersive Learning:* Utilization of VR (Virtual Reality) tools and "Game-based training" for hazardous CBRNE scenarios where real-life training is too dangerous or costly.
- *Center of Excellence:* Establishing long-term training hubs (e.g., at Police Universities) to ensure the project results survive beyond the funding period.

Key Result: Building a sustainable ecosystem of talent rather than just delivering a one-off workshop.

Our Training Methodology

Co-Creation: We don't just "lecture"; we design curricula *with* the LEAs (as seen in Salvus).

Train-the-Trainer: Empowering local officers to continue the training after the project ends (essential in Ceasefire).

Scenario-Based Learning: Using real-world use cases (e.g., a specific trafficking route in Anita) to make training relevant.

Formats:

- Physical Pilot Trainings (Workshops).
- E-Learning Platforms (MOOCs).
- VR/AR Simulations (SparkUp).

Impact & Conclusion

Metrics:

- Number of LEA officers trained.
- Number of jurisdictions reached.
- Adoption rate of tools post-training.

Final Thought: "Tools are only as effective as the people using them. Our experience across Ceasefire, Anita, Salvus, and SparkUp proves that dedicated, domain-specific training is the key to EU security project success."

Methodology & Quality Assurance

Adhering to European Law Enforcement Training Standards (LEEd / CEPOL Framework)

Training Needs Analysis (TNA):

- **Evidence-Based Design:** Curricula are not random; they are built on a rigorous *Gap Analysis* of current LEA capabilities vs. emerging threats (as performed in *Salvus HE* WP2).
- **Multi-Stakeholder Validation:** Content is co-created with field practitioners, legal experts, and ethical boards to ensure operational relevance and legal compliance.

Andragogical Approach: "Blended Learning" Model:

- **Asynchronous:** Self-paced e-learning modules (hosted on platforms compatible with LEEd) for theoretical foundations (Legal frameworks, EU Directives).
- **Synchronous/Immersive:**
 - *Scenario-Based Learning:* Real-world use cases (e.g., *Ceasefire* ballistic tracking) to test decision-making under pressure.
 - *XR/VR Simulations:* Safe-environment training for high-risk CBRNE scenarios (standardized in *SparkUp HE*).

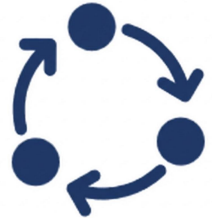
Methodology & Quality Assurance

The "Cascade" Multiplier Effect:

- **Train-the-Trainer (ToT):** We do not just train officers; we train *instructors*. This ensures the knowledge remains within the agency after the project ends.
- **Standardized Toolkits:** Delivery of "Training Packs" (Instructor Manuals, Student Handbooks, Evaluation Grids) to facilitate local replication.

Assessment & Certification:

- **Kirkpatrick Model Implementation:**
 - *Level 1 (Reaction):* Immediate feedback from participants.
 - *Level 2 (Learning):* Pre- and post-testing of skills.
 - *Level 3 (Behavior):* Long-term follow-up on tool adoption in actual investigations (6-12 months post-project).



Methodology & Quality Assurance

Cross-Border Interoperability:

- **Harmonized Lexicon:** Ensuring that a "High Priority Alert" in an *Anita* dashboard means the same to an officer in Spain as it does to one in Poland.
- **Joint Exercises:** Multi-agency pilot trainings to foster trust and test data exchange protocols.

Training Impact Matrix

Project Name	Primary Target Audience	Training Format & Tools	Key Outcome / Capability Gap Filled
CEASEFIRE 	Field Officers, Ballistics Experts, Border Guards	Mobile App Workshops & Hands-on: "On-the-Spot" detection training; automated ballistics comparisons.	Operational Speed: Reduced time for firearm identification from days (lab) to minutes (field).
ANITA 	Criminal Intelligence Analysts, Cyber-Investigators	Simulation & Platform Training: Knowledge Graph interaction; Dark Web monitoring; Crypto-tracing exercises.	Cognitive Augmentation: Enabled analysts to uncover hidden trafficking networks that manual analysis missed.
SALVUS 	Special Victims Units, Prosecutors, Judges	Procedural & Ethical Seminars: Child-centered interviewing techniques; Legal harmonization workshops.	Legal Robustness: Standardized evidence collection to prevent case dismissal in cross-border CSA trials.
SPARKUP 	First Responders, Innovation Managers in LEAs	Immersive Tech (VR/XR): Virtual Reality scenarios for hazardous CBRNE environments; Innovation management bootcamps.	Safety & Future-Readiness: allowed high-risk training without physical danger; bridged the gap between R&D and Police.

Thank you

Zvonimir Ivanovic, UCIPS, Serbia

CERIS DG – Home,

Chevening fellow

Leading team manager, ANITA,

CEASEFIRE, Salvus,

Team member SPARKUP



LEA Discussion & Feedback

Keynote

Gideon Hazzani,

LibereU, IAMI technical coordinator

AI-Driven Entity Identification and Intelligence Support for LEAs

IAMI overview and status

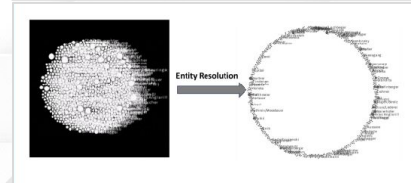
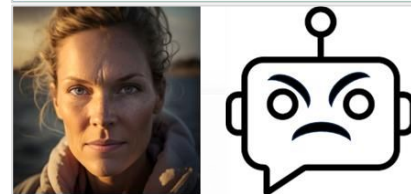
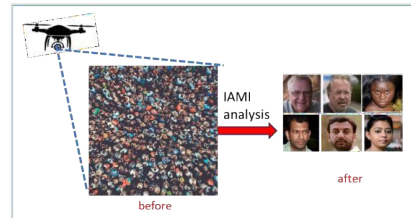
Entity Identification (EI) and Entity Resolution (ER) in counter terrorism contexts

- **Entity Identification (EI)**- Verifying, uniquely and undoubtedly recognizing an individual/organization based on different types of collected probe attributes.
- **Entity Resolution (ER)**- Resolving entities' identity discrepancies and duplicities (such as variations in names and nicknames, different name spellings or aliases).
 - Associating/merging related data or records (from different sources) that refer to the same entity (whether individual or organization).
 - Deduplicating (grouping) entities which mistakenly are considered as multiple entities, but essentially are the same entity.

The Challenge:

Addressing critical gaps in EI/ER

- IAMI targets the urgent need for advanced **Entity Identification (EI)** and **Entity Resolution (ER)** in counter-terrorism contexts, addressing limitations in existing identification and analysis systems.
- The project overcomes the following limitations:
 - EI/ER in noisy, poor-footage, dynamic, disguised, fake-ID, remote distance, crowded or biometric-deficient scenarios.
 - EI/ER in high data volumes environments.
 - Identifying/resolving **flux** of entities swiftly and accurately in order to allow LEAs cope well with real-time/unfolding threat scenarios (high throughput).
 - Resolving identity discrepancies/variations/aliases/unknown-duplicities to streamline investigation and intelligence efforts.
 - Support broad range of identity attributes types (not limited to biometric).
 - Support multi-entity types (individuals, organizations, bots/avatars).

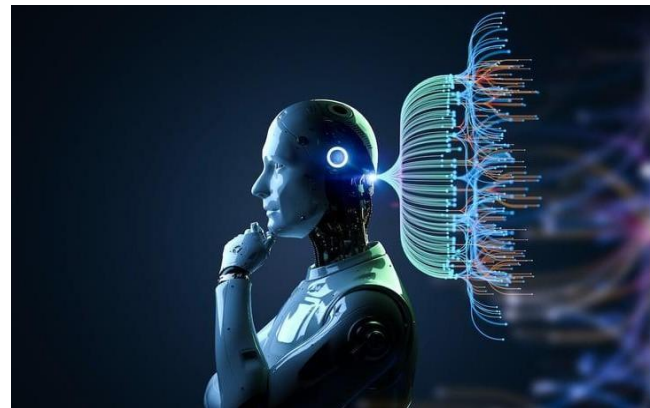


Main Outcomes and System Capabilities

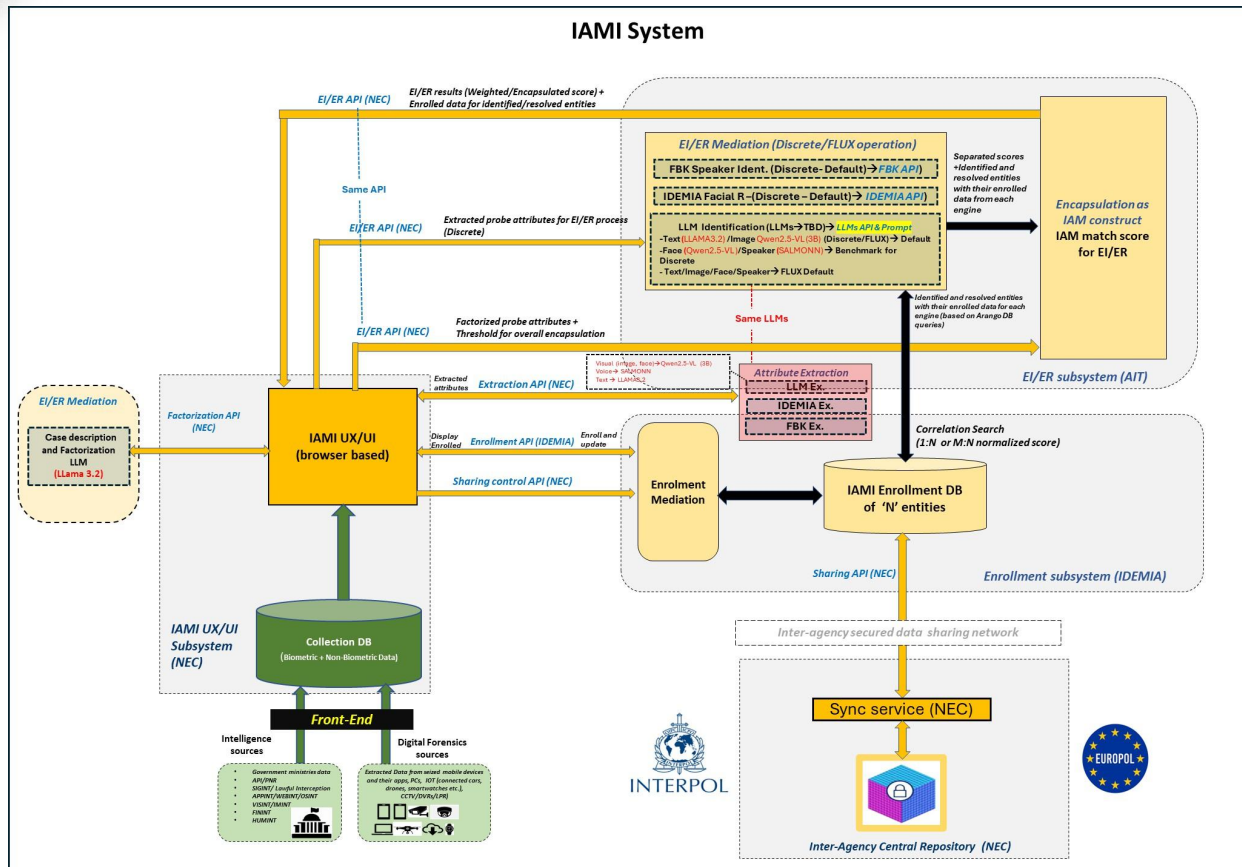
- Cutting-edge AI-powered EI/ER system enabling high-confidence, multi-entity identification and resolution.
- Fusion-based approach where combinations of weak, non-biometric attributes form strong identifiers.
- Multi-modal processing across text, audio, image, and video.
Multi-source intelligence ingestion including Digital Forensics, CCTV, LPR, API and PNR data, SIGINT, LI, WEBINT and OSINT, and structured information systems.
- Significant use of LLMs alongside traditional AI, including benchmarking of multi-modal LLMs against classical AI methods.
- High-capacity processing in challenging, noisy, and dynamic operational environments.
- Reduced false positives, faster processing, and scalable enrollment databases to enhance operational efficiency.

Main Outcomes and System Capabilities (cont.)

- Two EI/ER operational modes:
 - ✓ **Discrete mode**: fully manual, human-controlled, high-capacity processing
 - ✓ **Flux mode**: semi-automatic, human-supervised processing for very large data volumes
- Controlled and verified high-capacity enrollment, always manual to ensure trust and data quality
- Enhanced detection of fake identities, synthetic personas, and bots
- Human-controlled and calibrated AI processes ensuring accountability and explainability
- Cross-border and cross-agency attribute sharing framework supporting EU-wide collaboration
- Full compliance with EU AI Act 2024/1689 and GDPR
- Validation via joint Europol and CENTRIC tools under CC4AI



IAMI integration architecture



Strategic impact on EU Security

- Strengthens counter-terrorism capabilities
- Improves public space protection
- Supports rapid response to emerging/unfolding threats
- Enhances cross-border cooperation



System development status (IAMI V1.0)

- ✓ APIs
 - ✓ Subsystems functionalities
 - ✓ UX/UI (almost)
 - ✓ Selection of M.M. LLMs
 - ✓ Data for training AI/LLM models
-
- **Soon:** Establishing Development and Testing environment on-perm HW purchase and installation at **IGP, in Chisinau (pending GA amendment execution)**
 - Security and remote access
 - Start development and integration

Pilots and workshops

- **Pilot 1: EI and ER**
 - **Scenario-A:** Real-time identification and threat prevention in crowded public events (EI scenario)
 - **Scenario-B:** Using IAMI to detect company ban evasion (ER scenario)
- **Pilot 2: EI, ER and cross-border collaboration**
 - **Scenario A:** Mass transit security through collaborative IAMI data sharing (EI and data sharing scenario)
 - **Scenario B:** Identification and resolution of extremists' avatars/bots (EI and ER scenario)
- **Five workshops for EU LEAs** , Europol , Interpol and other stakeholders during the lifecycle of the project (M6, M13, M19, M26, M36)



Connect with IAMI



Funded by
the European Union

Funded by the European Union under Grant Agreement No 101168272. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency (REA). Neither the European Union nor the granting authority can be held responsible for them.

LEA Discussion & Feedback

Keynote

Prof. Constantinos Patsakis,
Athena Research Center, SafeHorizon Coordinator

Intelligence and Situational Awareness Against Crime-as-a-Service

Introducing SafeHorizon

Project



Call ID	HORIZON-CL3-2023-FCT-01-05 RIA
Duration	1.9.2024-31.8.2027
Coordination	Athena Research Center



Scope

Crime-as-a-Service (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.

Use case scenarios

SafeHorizon tools and technologies will be tested and validated by LEAs through 4 use-case scenarios:

- Monitoring transnational crime networks,
- Criminal marketplace analysis
- Child sexual abuse and trafficking, and
- Malware-as-a-Service

Contact us if you want to participate in the T&V phase.

Tools/Training

ClickFix

Dashboard

Statistics

Users

IOC Channels

IOCs

Login Logs

Theme

Signed in as
admin
[Logout](#)

ClickFix Atlas
Campaign Intelligence Dashboard

[Search](#)

8,390
Total Reports

1,556
Unique Domains

18-01-2025
First Report

05-01-2026
Last Report

Recent Reports

All Reports

Telegram Channels

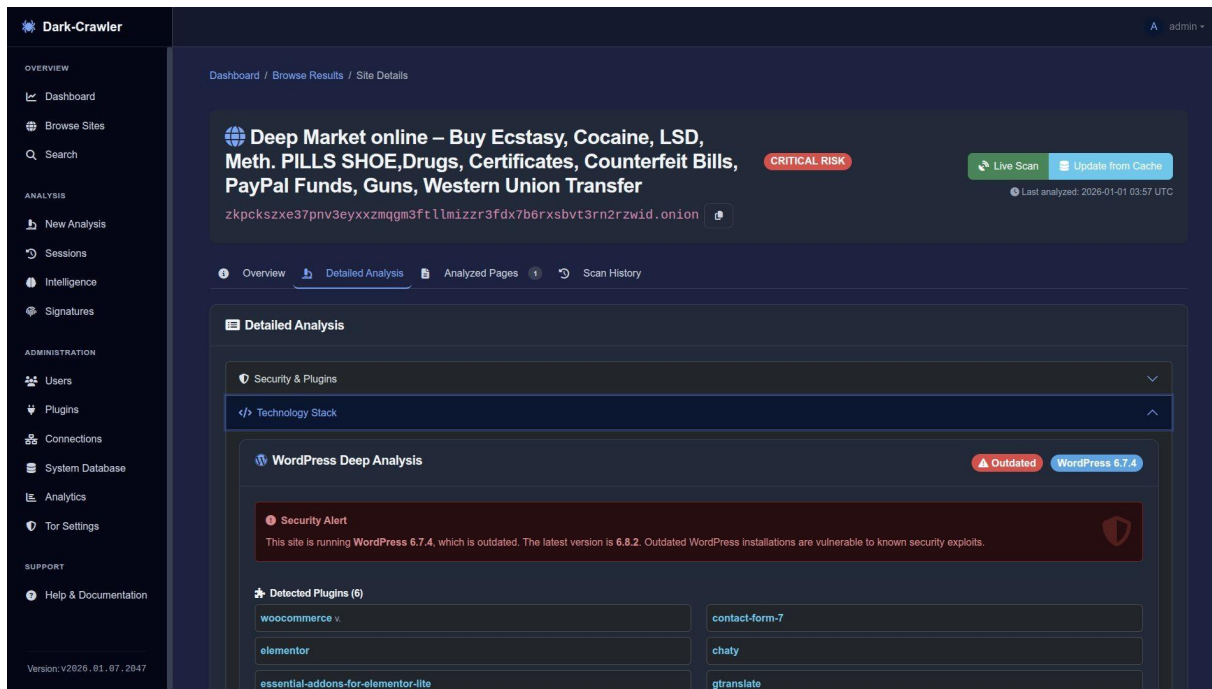
TIMESTAMP	DOMAIN	URL	COUNTRY	OBFUSCATED	ACTIONS
05-01-2026 10:55:20	34.102.116.83	http://34.102.116.83/	United States	No	View
05-01-2026 10:55:18	3.150.227.197	http://3.150.227.197/	United States	No	View
05-01-2026 05:13:04	stlt.com.tn	https://stlt.com.tn/	France	No	View
05-01-2026 02:55:39	zvezda-44.ru	https://zvezda-44.ru/	Russian Federation	No	View
05-01-2026 02:55:19	3.128.241.168	https://3.128.241.168/	United States	No	View
04-01-2026 20:15:57	sqlcapture.com	http://sqlcapture.com/	United States	No	View
04-01-2026 14:55:42	zvezda-44.ru	https://zvezda-44.ru/	Russian Federation	No	View
04-01-2026 14:55:24	89.108.127.231	https://89.108.127.231/	Russian Federation	No	View
04-01-2026 10:55:45	zvezda-44.ru	https://zvezda-44.ru/	Russian Federation	No	View
04-01-2026 06:55:15	18.220.10.43	https://18.220.10.43/	United States	No	View



**Stay tuned.
More to come!**

Designed to be integrated
in AI pipelines

Tools/Training



The screenshot displays the Dark-Crawler web application interface. The left sidebar contains navigation menus for OVERVIEW, ANALYSIS, and ADMINISTRATION. The main content area shows the 'Detailed Analysis' of a website. The target site is identified as 'Deep Market online' with a 'CRITICAL RISK' status. The analysis includes a 'WordPress Deep Analysis' section, which highlights a 'Security Alert' stating that the site is running an outdated version of WordPress (6.7.4) and is vulnerable to known security exploits. Below this, a table lists the detected plugins: woocommerce v., contact-form-7, elementor, chaty, essential-addons-for-elementor-lite, and gtranslate.

Dark-Crawler

Dashboard / Browse Results / Site Details

Deep Market online – Buy Ecstasy, Cocaine, LSD, Meth. PILLS SHOE, Drugs, Certificates, Counterfeit Bills, PayPal Funds, Guns, Western Union Transfer **CRITICAL RISK** [Live Scan](#) [Update from Cache](#)

zkpckszxe37pnv3eyxxmqgm3ftllmizzr3fdx7b6rxsbvt3rn2rzwid.onion

Overview Detailed Analysis Analyzed Pages 1 Scan History

Detailed Analysis

Security & Plugins

Technology Stack

WordPress Deep Analysis **Outdated** **WordPress 6.7.4**

Security Alert

This site is running WordPress 6.7.4, which is outdated. The latest version is 6.8.2. Outdated WordPress installations are vulnerable to known security exploits.

Detected Plugins (6)

woocommerce v.	contact-form-7
elementor	chaty
essential-addons-for-elementor-lite	gtranslate

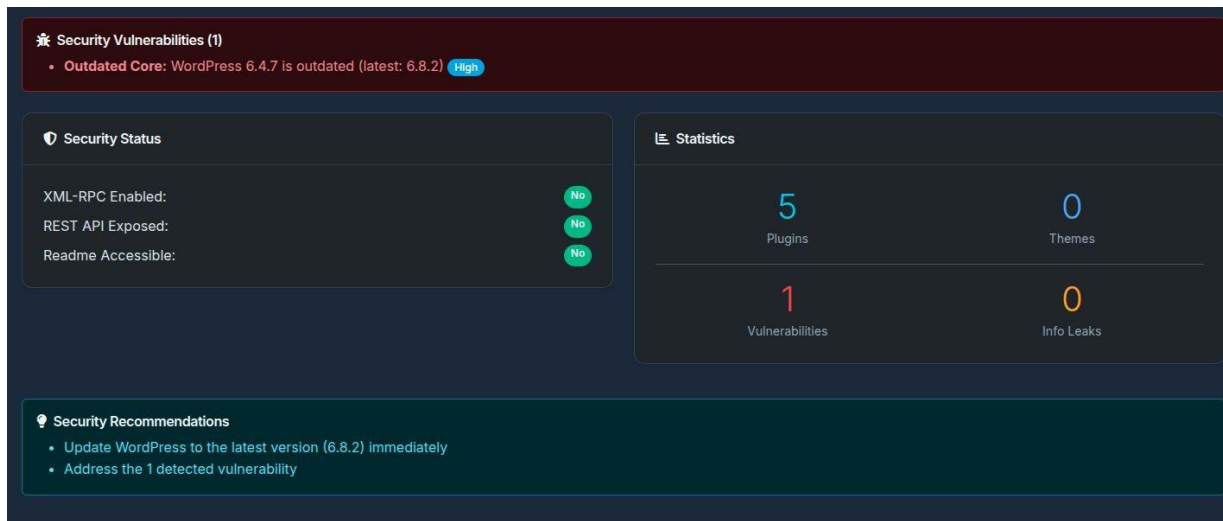
Version: v2026.01.07.2947



**Stay tuned.
More to come!**

Designed to be integrated
in **AI** pipelines

Tools/Training



**Stay tuned.
More to come!**

Designed to be integrated
in **AI** pipelines

Tools/Training

INFOSTEALER INTELLIGENCE INVESTIGATION (III) Search / Reset Worst Offenders CSAM on Tor CSAM Clearweb Tampere University

Select Infostealer Malware Records

Country CSAM - Clearweb CSAM - Darkweb

darkweb_csam 658 users — 0.040% clearweb_csam 26,054 users — 1.603% VPN 166,724 users — 10.255% adult_content 249,103 users — 15.322% chats_for_children 384 users — 0.024%

child_interest_communities 1,108 users — 0.068% dating 15,071 users — 0.927% discord 650,490 users — 40.010% encrypted_email 6,539 users — 0.402% far_right 110 users — 0.007%

file_sharing_sites 306,568 users — 18.856% gambling 114,934 users — 7.069% gore 5,228 users — 0.322% hacking 10,012 users — 0.616% software_developer 263,310 users — 16.195%

tor_explorer 2,122 users — 0.131% zoophilia 535 users — 0.033%

Search by Domain Search domain (e.g. mega.nz) Search

Results

658 matching users found (0.040 % of 1,625,826 indexed)

Country	City	Birth year	Websites authenticated into	Details
BR	Manaus	—	CSAM_ONION_kidflix darkweb_csam discord software_developer tor_explorer	open
IN	Vadodara	—	CSAM_ONION_Rape_and_murder_Shock_photo_and_video_Killing_people adult_content darkweb_csam discord gambling tor_explorer	open
CA	Sherwood Park	1979, 1981, 1995	CSAM_CLEARWEB_fwagsys CSAM_ONION_NAUGHTY_KIDS adult_content clearweb_csam darkweb_csam dating gambling tor_explorer	open
KR	Cheongju-si	—	CSAM_CLEARWEB_maindaydog.ru CSAM_ONION_xPlay_2025_Porn_Video_Streaming_xxx adult_content clearweb_csam darkweb_csam discord file_sharing_sites gambling software_developer tor_explorer	open
US	Philadelphia	—	CSAM_ONION_9Yo_Jenny_Full_Dog_Sucking_Only_kids CSAM_ONION_CP_Tube_streaming_and_video_sharing_JailBait CSAM_ONION_ChildHub_Legit_CP_Teen_free_CP_no_account_required CSAM_ONION_EX_PORN CSAM_ONION_Explore_the_content_Only_Kids adult_content darkweb_csam discord tor_explorer	open
CR	Heredia	—	CSAM_ONION_NAUGHTY_KIDS adult_content darkweb_csam file_sharing_sites tor_explorer zoophilia	open



Stay tuned.
More to come!

Designed to be integrated
in AI pipelines

Tools/Training

Onion OSINT Matcher Dashboard

Dashboard / patrickmm44tngdyxczq4gvccy2kjiygnpfwjx6ryovvf6svopezeyd.onion

patrickmm44tngdyxczq4gvccy2kjiygnpfwjx6ryovvf6svopezeyd.onion:80 Export JSON Export PDF < Previous 192 / 210 Next >

**HTTP Only**
TLS Version

**1**
Total Shodan Matches

**66.1 KB**
Favicon Size

**2.27s**
Response Time

**0**
Total Censys Matches

**0**
Total ZoomEye Matches

**0**
Total FOFA Matches

**0**
Total LeakIX Matches

Fingerprints

Favicon Hash: 1069753405

HTTP Body Hash: 8fb7790d0e078a7d688c0823e3de32b2f6d8718a830e20872c04e70823d549e

Headers Hash: 36e21c352c18674008f59d6e50e5903a62b90a9535b27c0b55968888902d3ee

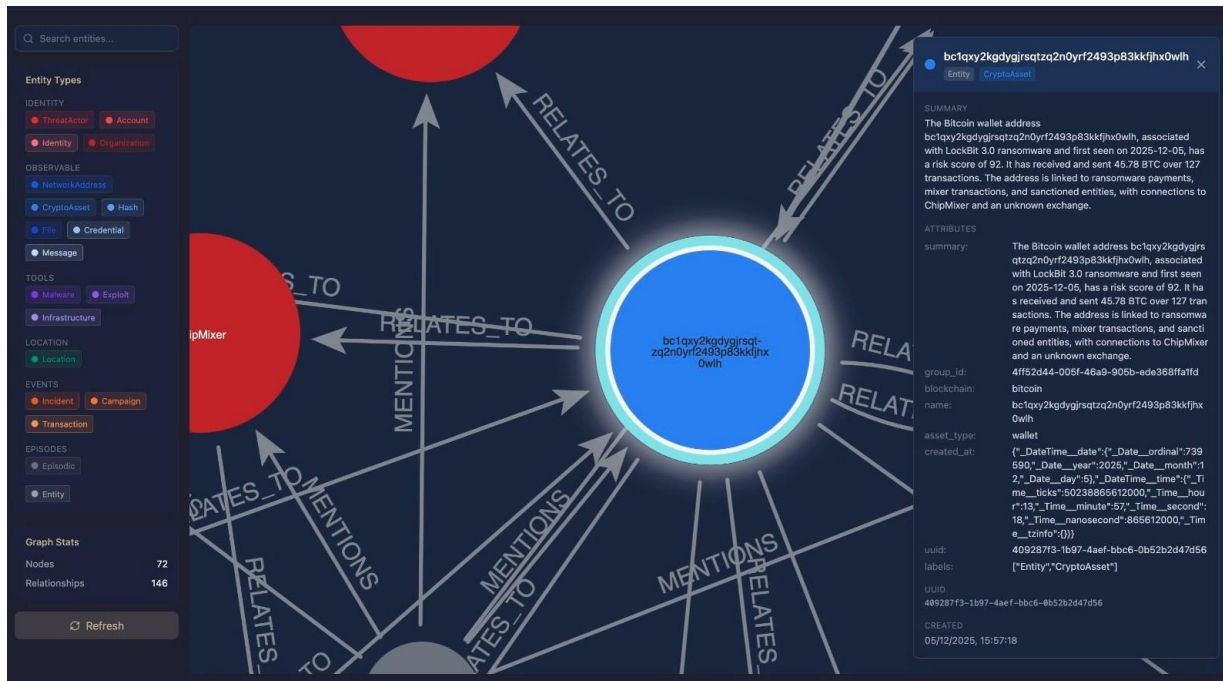
HTTP Response Detected Technologies



**Stay tuned.
More to come!**

Designed to be integrated
in **AI** pipelines

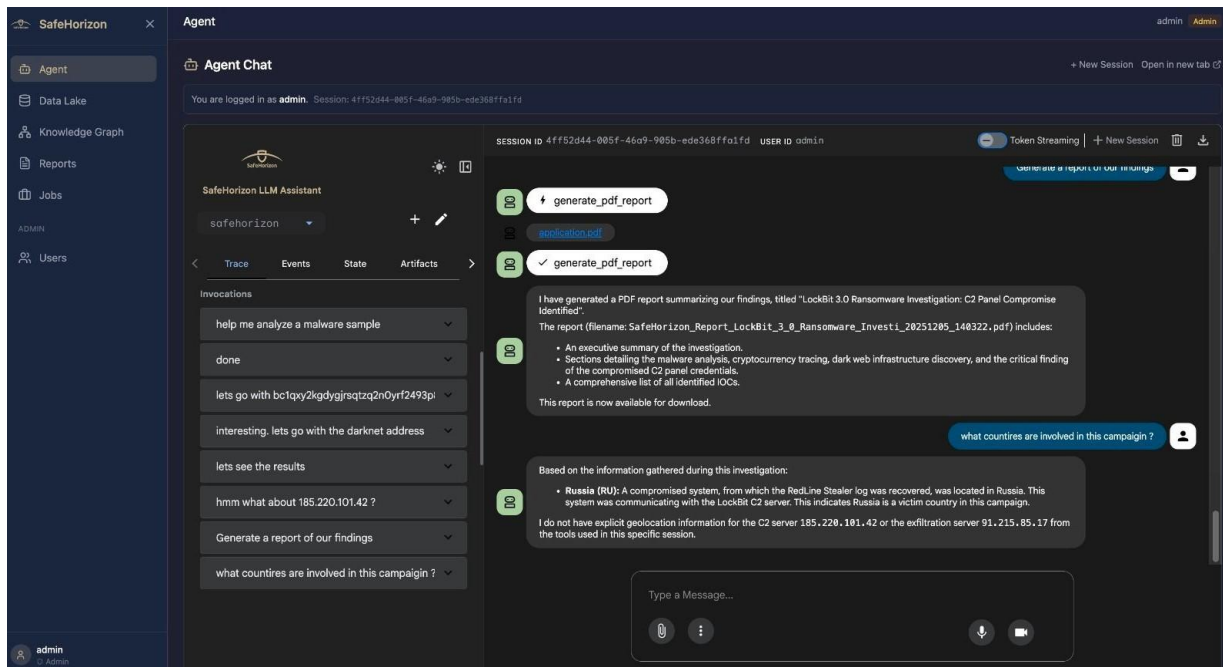
Tools/Training



**Stay tuned.
More to come!**

Designed to be integrated
in **AI** pipelines

Tools/Training



The screenshot displays the SafeHorizon Agent Chat interface. On the left is a sidebar with navigation options: Agent, Data Lake, Knowledge Graph, Reports, Jobs, ADMIN, and Users. The main area is titled 'Agent Chat' and shows a session with 'admin'. The chat history includes several messages from the user and responses from the 'SafeHorizon LLM Assistant'. The assistant has generated a PDF report titled 'LockBit 3.0 Ransomware Investigation: C2 Panel Compromise Identified' and provided a summary of findings, including an executive summary, malware analysis, and a list of identified IOCs. The user has asked for more information, and the assistant has provided a detailed response based on the gathered information.

SafeHorizon LLM Assistant

safehorizon

Trace Events State Artifacts

Invocations

- help me analyze a malware sample
- done
- lets go with bc1qy2kgdyjnsqtzq2n0yrf2493pi
- interesting. lets go with the darknet address
- lets see the results
- hmm what about 185.220.101.42 ?
- Generate a report of our findings
- what countries are involved in this campaign ?

SESSION ID 4ff52d44-005f-46a9-985b-edc368ffa1fd USER ID admin

Token Streaming + New Session

generate_pdf_report

application.pdf

generate_pdf_report

I have generated a PDF report summarizing our findings, titled "LockBit 3.0 Ransomware Investigation: C2 Panel Compromise Identified".

The report (Filename: SafeHorizon_Report_LockBit_3_0_Ransomware_Investi_20251205_140322.pdf) includes:

- An executive summary of the investigation.
- Sections detailing the malware analysis, cryptocurrency tracing, dark web infrastructure discovery, and the critical finding of the compromised C2 panel credentials.
- A comprehensive list of all identified IOCs.

This report is now available for download.

what countries are involved in this campaign ?

Based on the information gathered during this investigation:

- Russia (RU):** A compromised system, from which the RedLine Stealer log was recovered, was located in Russia. This system was communicating with the LockBit C2 server. This indicates Russia is a victim country in this campaign.

I do not have explicit geolocation information for the C2 server 185.220.101.42 or the exfiltration server 91.215.85.17 from the tools used in this specific session.

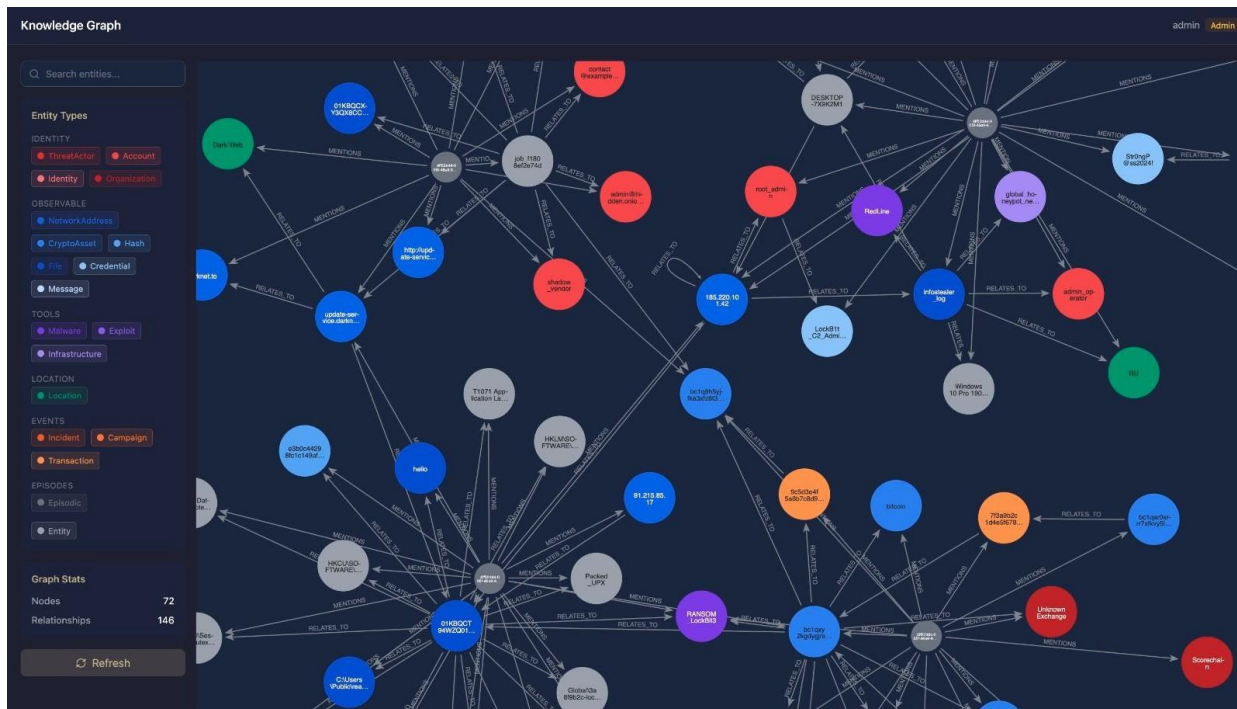
Type a Message...



**Stay tuned.
More to come!**

Designed to be integrated
in **AI** pipelines

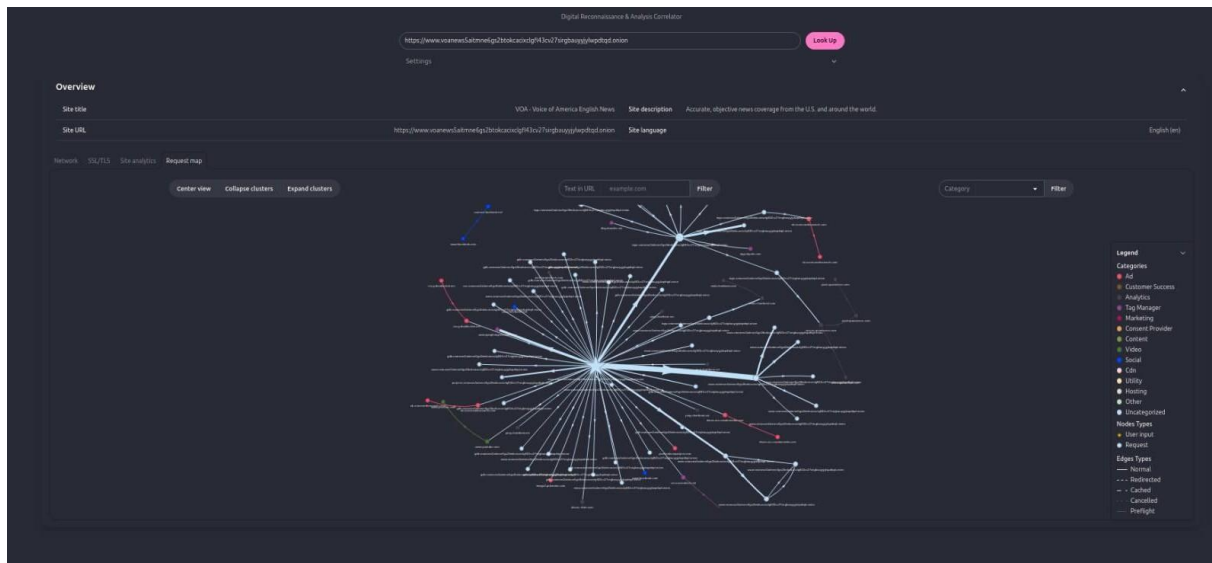
Tools/Training



**Stay tuned.
More to come!**

Designed to be integrated
in AI pipelines

Tools/Training



**Stay tuned.
More to come!**

Designed to be integrated
in **AI** pipelines

Thanks for your attention



LEA Discussion & Feedback

Kristina Isakzay

Project Manager and Legal & Ethics Expert, LEA Projects Cluster Coordinator

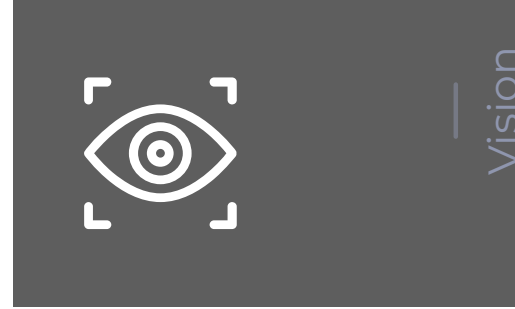
LEA Projects Cluster Strategic Mission and Vision

Q4 2025 - Q2 2027

Strategic Vision Q4 2025 – Q2 2027



Connecting
Projects, Shaping
Policy



Evolving into a
Recognised Cooperation
Hub

Working Groups **Framework**



1

WG1 - Cyber and Digital Crime

2

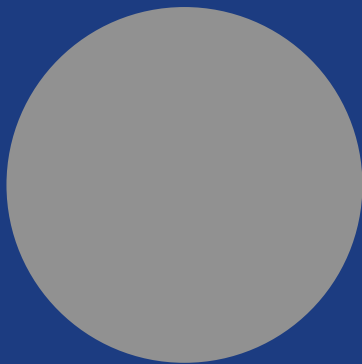
WG2 - Criminal Networks & Financial Crime

3

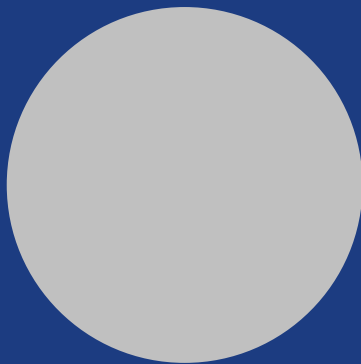
WG3 - Human Security & Environmental Crime

There's still time to join the Cluster Working Groups. Follow the registration link in the chat to express your interest.

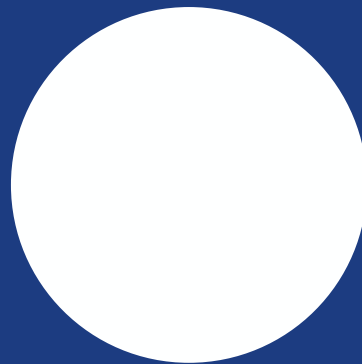
Beyond **Q2 2027**



Unite



Advance



Transform

Our **LEA Projects Cluster team**



Farhan SAHITO

Editor-in-Chief,
Partner

Privanova

farhan@privanova.com



Kristina Isakzay

Cluster Coordinator,
Project Manager &
Legal and Ethics Expert

Privanova

kristina.isakzay@privanova.com



Tamara Krstic

Cluster Communications,
Communications &
Marketing Manager

Privanova

tamara@privanova.com



Privanova
Research & Consulting



comms@Privanova.com

34, avenue des Champs-Élysées, Paris



Funded by
the European Union