FLASH REPORT 12

EUROPOL INDUSTRY & RESEARCH DAYS

Main Authors
André Alegria (PJ)
Filipe Rodrigues (PJ)

February 2026

ENACT.
European Network Against Crime and Terrorism


sername...
assword...
54%

03

About ENACT

ENACT is a knowledge network focused on the fight against crime and terrorism (FCT). The network is funded under the Horizon Europe Framework Programme in Cluster 3 – Civil Security for Society. The project addresses the call topic HORIZON-CL3-2022-SSRI-01-02 'Knowledge Networks for Security Research & Innovation', aiming to collect, aggregate, process, disseminate and make the most of the existing knowledge in the FCT area.

The project aims to satisfy two major ambitions,

- Provide evidence-based support to the decision-makers in the EU research and innovation (R&I) ecosystem in the FCT domain, targeted explicitly at enabling more effective and efficient programming of EU-funded R&I for the fight against crime and terrorism.

- Act as a catalyst for the uptake of innovation by enhancing the visibility and reliability of innovative FCT security solutions.

Report Feedback

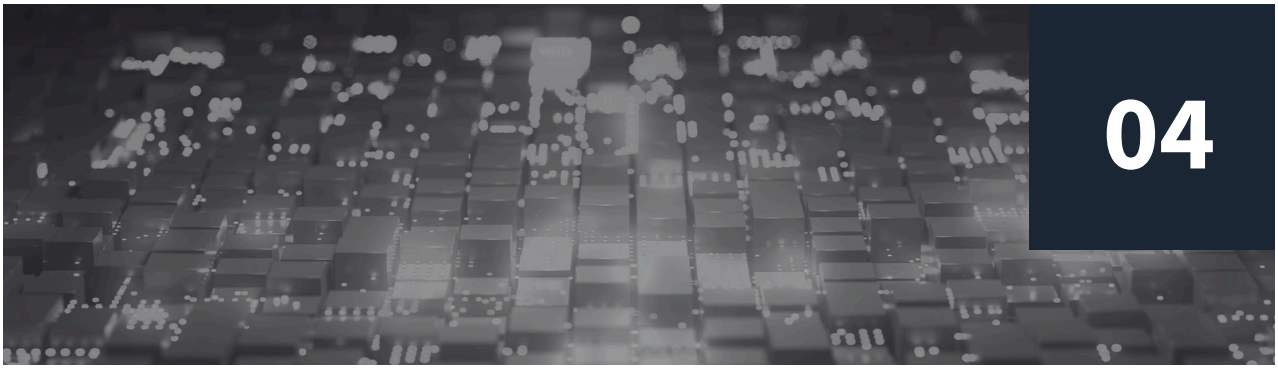
We're collecting feedback on this report through the EU Survey Platform, if you'd like to share your thoughts anonymously please click on the link below.

https://ec.europa.eu/eusurvey/runner/FR-Europol-Industry-Research-Days

Funded by the European Union

Disclaimer

Copyright



04

Europol Industry and Research Days: Overview

Organised by the Europol Innovation Lab, the Europol Industry and Research Days, running annually in The Hague, the Netherlands, is described by Europol as a key platform to foster collaboration, innovation and knowledge exchange among law-enforcement agencies, industry and research.

Europol underlines that law enforcement must keep abreast of new technology not only to work effectively, but also to develop new skills and adapt investigative techniques in response to evolving threats. In this context, the Industry and Research Days are positioned as a bridge between operational needs and technological innovation, offering a secure and controlled environment where practitioners can engage directly with developers and researchers.

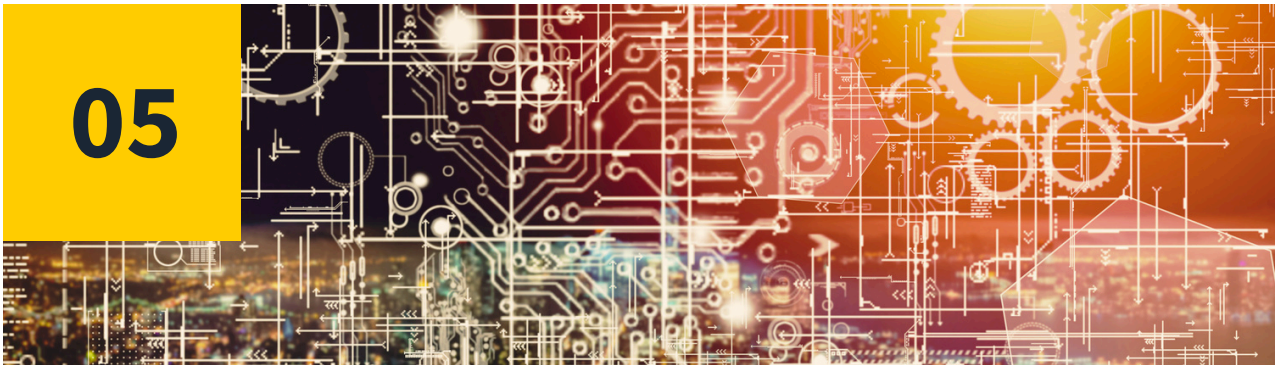
Participation is deliberately targeted. On the user side, the audience consists mainly of Europol staff, national and international law-enforcement practitioners, and relevant EU stakeholders. On the supply side, speakers and demonstrators come from private companies, universities and research and technology institutes selected through calls for expressions of interest.

Europol's communication emphasises that selected solutions respond to needs expressed by the law-enforcement community and are chosen against criteria such as innovative character and operational relevance.

Acknowledgement

ENACT would like to thank the Europol Innovation Lab for their support in the preparation and review of this report. More information on the Industry and Research Days can be found on the Europol website. https://www.europol.europa.eu/how-we-work/innovation-lab/industry-and-research-days

05



Europol Industry and Research Days 2025: A view on the Security Market

From a security and innovation market perspective, the Europol Industry and Research Days 2025 can be characterised as a compact, curated showcase of technologies that are closest to operational deployment in law enforcement, rather than as a broad commercial trade fair. The event concentrated a small number of providers and research projects that presented solutions aligned with specific operational priorities, particularly within the six thematic areas defined for the edition.

Unlike large open fairs such as TECNOSEC, SICUR, EUROSATORY or the UK Security & Policing Event, which bring together extensive catalogues of equipment and services for a very wide security audience, the Industry and Research Days focused on a narrow, high-impact segment of the market. The emphasis was on advanced analytics, software platforms and integrated systems addressing challenges such as target detection and tracking in complex visual environments, the detection and analysis of deepfakes and other synthetic media, the use of advanced biometrics in forensic and investigative contexts, the exploitation of information from private or semi-closed online channels, and the tracing of financial flows involving cryptocurrencies.

In this context, hardware such as robots, drones and other unmanned systems appeared mainly as enablers for software-defined capabilities, particularly in the areas of sensing, data collection and situational awareness. The added value presented at the event was often located in the orchestration, integration and analytical layers: systems that could bring together sensor feeds, biometric data, OSINT and financial information into coherent operational workflows.

The 2025 edition also highlighted that innovation in this segment of the market is increasingly shaped by law-enforcement demand. Technologies were not presented in the abstract, but embedded in specific scenarios, for example the investigation of synthetic media as evidence, the analysis of cryptocurrency transactions in money-laundering schemes, or the monitoring of criminal activity in closed communication environments. This demand-driven approach, combined with the controlled setting of Europol Headquarters, positions the Industry and Research Days as a focused interface between the most advanced part of the security-technology market and the daily realities of policing and criminal investigation.

Looking ahead, the logic and content of the 2025 edition naturally act as a teaser and reference point for the 2026 Industry and Research Days. The areas that dominated the 2025 programme (AI-based analytics, unmanned systems, deepfake detection, advanced biometrics, OSINT in private channels, and cryptocurrencies, financial intelligence and cybersecurity) can be expected to remain central, with further consolidation and maturation of solutions as law-enforcement needs and EU policy frameworks continue to evolve.

06

Europol Industry and Research Days 2025: Exhibitors products and services

The Europol Industry and Research Days 2025 were structured around six tightly defined themes that together sketch a very clear picture of where innovation for law enforcement is heading. Robots, Drones and other Unmanned Systems captured the drive to extend police reach and situational awareness through remote and automated platforms. Deepfake Detection and Advanced Biometrics for Forensic Analysis addressed the growing challenge of working with complex digital evidence and reliably establishing identity in large and noisy datasets. AI Tools for Target Detection, Identification and Tracking focused on extracting operational value from vast streams of visual, audio and geospatial data. OSINT Analysis of Private Channels highlighted the importance of accessing and interpreting information in semi-closed online environments, while the theme on Cryptocurrencies, Financial Intelligence and Cybersecurity brought to the foreground the financial and digital infrastructures that underpin modern organised crime and terrorism.

Robots, drones and other unmanned systems

In the theme “Robots, drones and other unmanned systems,” the exhibitor set illustrated how law enforcement is beginning to operationalise unmanned platforms as integral parts of its toolkit. **Hi IBERIA** showcased an AI platform for strategic law enforcement response using satellite data, while **AirHub B.V.**, as well as **Supervision B.V.** brought solutions focused on the control, coordination and integration of UAVs and UGVs into wider operational environments. **ANARKY Labs** and **VTT Technical Research** showcased technologies that combine advanced sensing, swarm control, navigation and situational-awareness components, helping to translate unmanned data into actionable views for operators. The **Innovation Lab of the State Criminal Police Office of North Rhine-Westphalia** and **Roboverse Reply** added the perspective of the direct collaboration with law-enforcement innovation units that develops and pilots its own concepts for using unmanned systems in daily policing, highlighting how user-side labs are now part of the exhibitor landscape alongside traditional vendors.

Deepfake detection

The “Deepfake detection” theme brought together exhibitors working at the intersection of media forensics and artificial intelligence. **Magnet Forensics** presented tools designed to assess the authenticity of digital media and support forensic workflows, while **Issured Ltd** focused on secure evidence management and trusted remote interviewing environments where the risk of deepfake interference needs to be managed from the outset. **Future Space** contributed solutions oriented towards AI-based analysis of disinformation campaigns, and **RESARO** demonstrated capabilities for testing and benchmarking deepfake-detection approaches by generating synthetic material and using it to stress-test detection tools. Collectively, these exhibitors covered both the detection of manipulated or synthetic media and the broader challenge of maintaining confidence in digital evidence

Advanced Biometrics for Forensic Analysis

Under the theme “Advanced Biometrics for Forensic Analysis,” exhibitors concentrated on robust identification and verification technologies. **Bee The Data S.L.** presented data-driven biometric and analytical solutions aimed at extracting and correlating identity-related information from large datasets. **Quadible Greece P.C.** focused on behavioural biometrics, offering ways to link devices and digital traces to individuals based on usage patterns and behaviour rather than only on physical traits. **Rank One Computing Corporation** contributed algorithms and systems for face and other biometric recognition optimised for high accuracy and speed in large repositories, with direct relevance for forensic and investigative use. Together, these exhibitors illustrated how the biometric field is expanding beyond single-modality face recognition to encompass behavioural and multimodal approaches.

AI Tools for Target Detection, Identification, and Tracking

The theme “AI Tools for Target Detection, Identification, and Tracking” brought together a set of exhibitors whose solutions often sit at the junction of sensing, analytics and operational deployment. **AXON** presented a C2 ecosystem in which AI-powered detection and tracking of drones and other objects is integrated with evidence platforms and situational-awareness dashboards. **Cellebrite** demonstrated investigative and analytical platforms that can extract, process and correlate data from multiple sources for the purposes of identifying persons, devices and communication patterns. **Phonexia s.r.o.** showcased voice-biometrics and speech technologies that support speaker identification and audio analysis, while **GEOSAT** highlighted the role of satellite imagery and earth observation in detecting and monitoring activities of interest. **Eyedea Recognition Ltd** added capabilities in visual recognition and analysis, and Trilateral Research presented its data-driven tools designed to detect and monitor risk in areas such as child protection and exploitation. Collectively, this group showed how AI can be applied across visual, audio and geospatial domains to support detection and tracking tasks at scale.

OSINT Analysis of Private Channels

The “OSINT Analysis of Private Channels” theme gathered exhibitors whose products are aimed at intelligence and investigations in environments that are not fully open but still accessible under legal conditions. **Maltego Technologies GmbH** and **Paliscope AB** demonstrated platforms for open-source intelligence that allow investigators to correlate entities, events and content across the surface web, social media and semi-open channels. **DarkOwl LLC** provided long-running coverage of hidden and dark-net spaces, while **SOCRadar Cyber Intelligence Inc** focused on cyber-threat intelligence with strong links to monitoring communication and activity in less visible parts of the internet. Bitdefender showcased AI-assisted capabilities that cut across multiple sources and languages from either darknet or clearnet. **Elephantastic Software** and **INNOSYSTEC GmbH** presented solutions for large-scale data integration and analysis, enabling investigators to manage very high volumes of information from diverse feeds. **EACTDA**, with **Byron Labs**, brought a solution for ransomware monitoring and intelligence. Together, these exhibitors illustrated how OSINT is evolving into a sophisticated, multi-layered activity that spans private channels, dark-web content and complex data ecosystems.

Cryptocurrencies, financial intelligence and cybersecurity

Finally, the theme “Cryptocurrencies, financial intelligence and cybersecurity” brought financial and cyber aspects of crime and terrorism to the forefront. **Crypto Asset Technology Labs** showed tools for identifying and recovering cryptocurrency-related artefacts in digital evidence, helping investigators to locate wallets, keys and transactions. **ChainComply BV** presented solutions for combining on-chain blockchain analysis with off-chain data from exchanges and other service providers, making it possible to reconstruct complex transaction paths. Siren contributed search and intelligence capabilities that support link analysis and complex queries across structured and unstructured data in financial and investigative contexts. **Zepo Intelligence** focused on the human and organisational side of cyber risk, using social-intelligence approaches to identify vulnerabilities and reduce the success of social engineering. **Aegis Technologies** presented a solution for collecting and exploiting unstructured or semi-structured data in clear, usable formats without manual intervention. The **Innovation Lab of the State Criminal Police Office of North Rhine-Westphalia** appeared again in this theme, this time with an app to be used by officers on the field for the quick identification of symbols.

09

Europol Industry and Research Days 2025: Policy areas

Mapping the exhibitors to the EU security market taxonomy shows a programme strongly aligned with concrete, operational policy priorities rather than generic capability groupings. Within organised crime, the most consistently addressed areas relate to economic crime, corruption and fraud. This reflects the prominence of solutions designed to strengthen financial disruption, asset tracing and evidence exploitation in complex, cross-border investigations.

Within terrorism and radicalisation, the most visible policy anchor is protection of public spaces. This alignment is reinforced by capabilities linked to situational awareness, detection and tracking, and counter-unmanned-system challenges, alongside investigative platforms that support threat identification, case development and evidential handling. Terrorism financing is also clearly addressed through the subset of exhibitors operating in cryptocurrency and financial intelligence, particularly where tools support tracing transaction flows, identifying services and entities of interest, and enabling disruption or recovery actions.

Within cybercrime, the mapping concentrates around digital forensics, attacks against information systems, online identity theft and dark net ecosystems, including illicit markets and cryptocurrency-enabled crime. The prominence of OSINT analysis in private channels, cyber-intelligence capabilities and crypto-related investigative tooling reflects the reality that many contemporary investigations require structured access to semi-closed environments and the ability to translate complex technical traces into admissible investigative outputs.

Horizontal policy areas are also meaningfully represented, especially disinformation and fake news, driven by the deepfake detection theme and by solutions concerned with authenticity, provenance and evidential integrity in environments where manipulation and synthetic content are increasingly accessible.

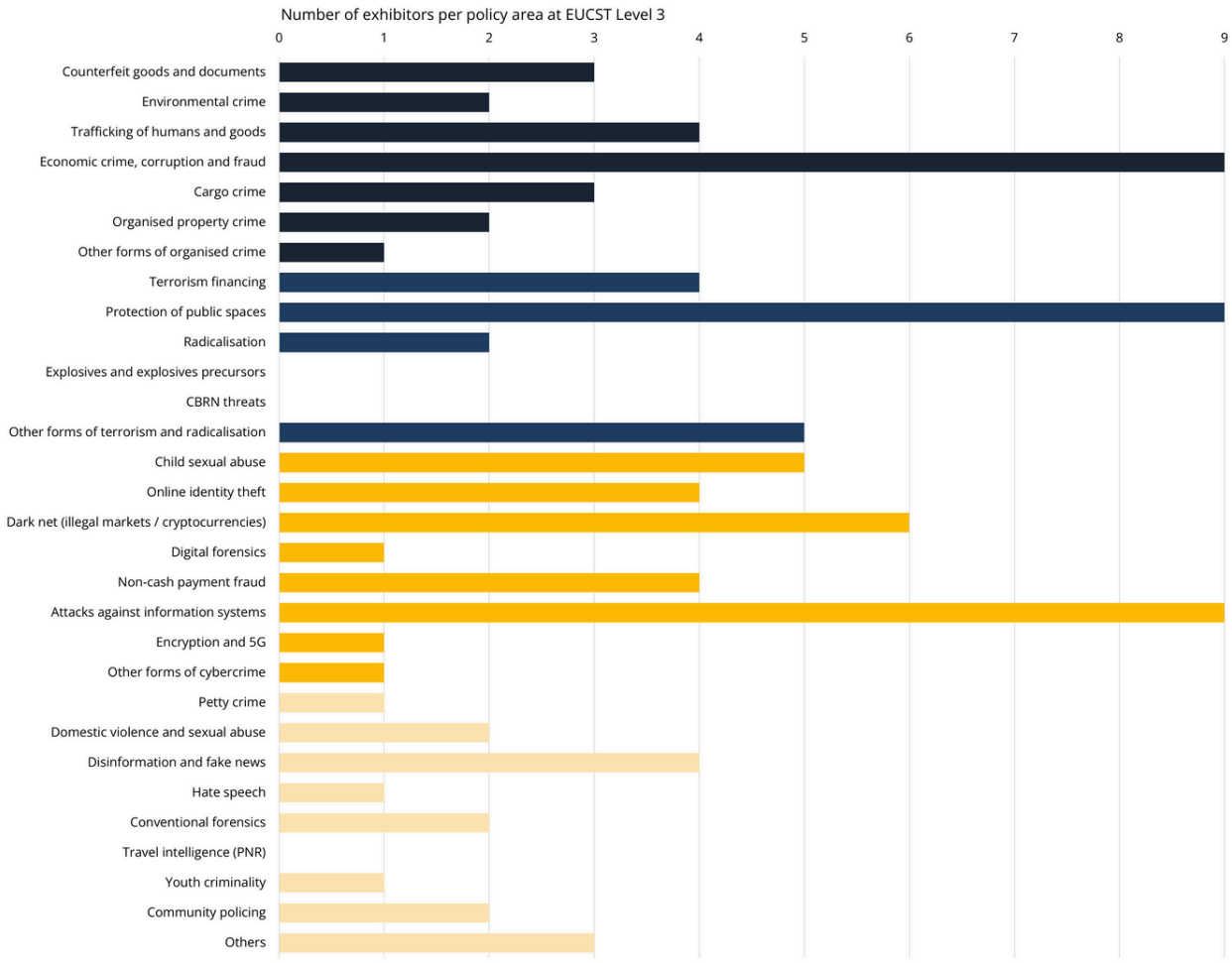


Figure 1: Number of exhibitors at the Europol Industry and Research Days classified per policy area of the EU Civil Security Taxonomy

Europol Industry and Research Days 2025: Function areas

Mapping the exhibitors against the taxonomy's function areas shows a clear dominance of data-centric capability provision. "Data, information and intelligence gathering, management and exploitation" is the most consistently represented function across the exhibitor set mapped for this report. This confirms that, across all six themes, the operational value proposition is frequently anchored in accelerating the conversion of fragmented inputs into defensible investigative insight, whether the starting point is OSINT, biometrics, satellite or drone-derived sensing, deepfake analysis, or cryptocurrency and financial data.

A second strong functional cluster relates to "Investigation and forensics." This includes both traditional investigative workflow support and more specialised forensic capability, particularly in digital investigations, media authenticity, device and platform exploitation, and the handling of complex evidence streams. The emphasis on defensibility and workflow integration is notable in this function area, as many exhibitors position their tools not as isolated analytics engines but as components embedded into acquisition, preservation, analysis and reporting chains.

Two additional function areas appear with comparable frequency in the mapping: "Monitoring and surveillance of environments and activities" and "Security of information systems, networks and hardware." The first is primarily associated with unmanned systems, counter-UAS capabilities and broader monitoring platforms. The second reflects the presence of cybersecurity and resilience-oriented offerings, particularly where investigative environments themselves are targets for compromise or manipulation, and where the integrity of systems is inseparable from the integrity of investigative outcomes.

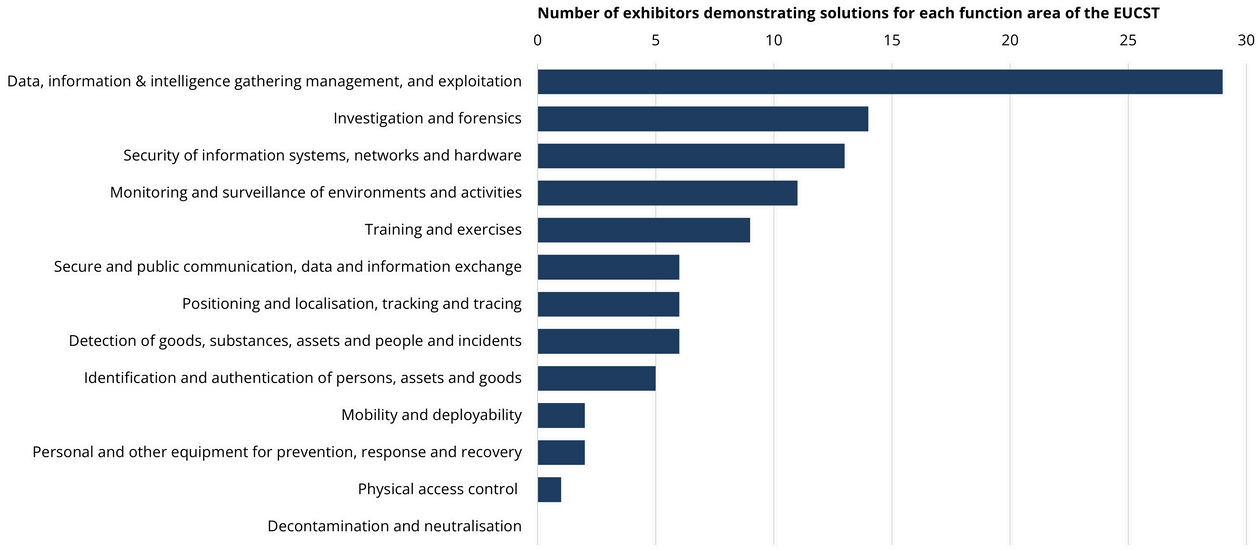


Figure 2: Number of exhibitors at the Europol Industry and Research Days classified per functions area of the EU Civil Security Taxonomy

Europol Industry and Research Days 2025: Technology areas

The technology mapping produces a coherent picture of a platform-heavy, analytics-led exhibitor landscape. “Data analytics” is, by a wide margin, the most represented technology area in the mapping conducted for this report, followed by “Data storage and exchange” and “Specialised management and control systems.” Taken together, these three categories reflect an internal security technology market where investigative advantage is built through the ability to process large volumes of heterogeneous information, preserve and manage it correctly, and deploy it through operationally usable workflows that support auditability and defensibility.

A second tier of technology areas includes “Facilitation systems and secure databases,” “Monitoring tools and services,” and “Digital security products and services.” This grouping aligns with the event’s focus on operational deployment readiness: systems are expected to run in sensitive environments, to integrate with existing infrastructures, to manage access and governance constraints, and to operate robustly against adversarial behaviour. The presence of facilitation systems and secure databases is particularly relevant for solutions that depend on cross-dataset correlation, persistent repositories, and controlled sharing.

“Surveillance systems” and “Tracking, navigation and guiding systems” appear with meaningful frequency, reflecting the unmanned systems theme, counter-UAS capability and wider situational awareness tooling. “Internet-based investigation” also appears as a consistently represented technology area, reinforcing the importance of OSINT and private-channel intelligence exploitation as mainstream elements of contemporary investigations.

Overall, the technology profile indicates that the market segment represented at the event privileges integrated ecosystems and end-to-end workflow support over discrete single-function tools, even when the entry point is a highly specialised capability such as biometrics, media authenticity or blockchain analysis.

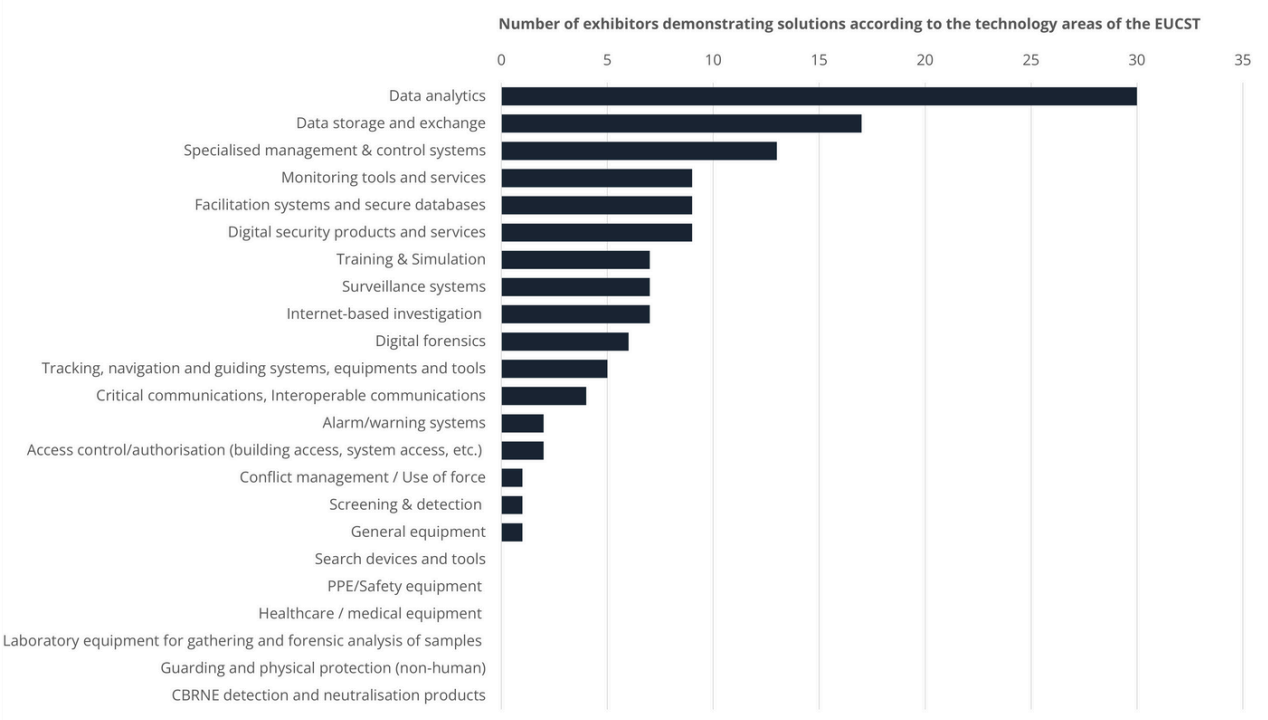
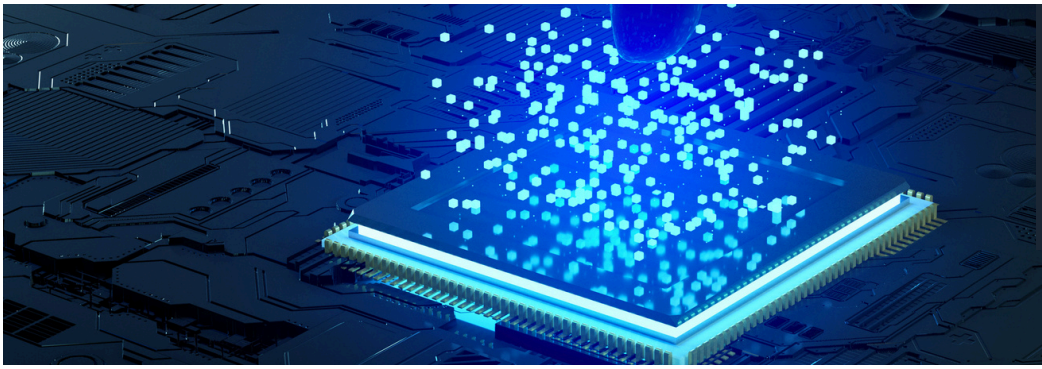


Figure 3: Number of exhibitors at the Europol Industry and Research Days classified per technology areas of the EU Civil Security Taxonomy



Europol Industry and Research Days 2026: What to expect

The 2026 edition is positioned to extend the 2025 format rather than simply repeat it, with Europol framing it as a three-day sequence at Europol Headquarters in The Hague, scheduled for 24–26 February 2026. A key structural development is the introduction of a dedicated research showcase on the first day, designed to bring mature outputs from Horizon Europe and Internal Security Fund projects into an operational demonstration setting, explicitly targeting emerging threats through Advanced Digital Evidence Processing and Analysis, Counter-Crime and Counter-Terrorism Technologies and Financial Crime Investigation and Anti-Corruption.

The core “Industry and Research Days” sessions will also be extended to cover almost double the number of areas of expertise, focusing on mature, market-ready solutions including Situational Awareness, Lawful Data Access Solutions, Intelligence Analysis and Multi-Modal Data Processing, Sovereign Cloud Solutions and Quantum Resistant Technologies, Uncrewed Systems for Law Enforcement Operations, Next-Generation Biometric Analysis Solutions and Synthetic Content Detection and Authentication.

Operationally, the 2026 edition is framed as a bridge between innovation and use in the field, while remaining explicit that participation does not imply procurement or endorsement and that the event’s purpose is knowledge exchange, usability assessment and partnership-building rather than acquisition. Taken together, the planned structure and the introduction of a research-to-operations showcase make the 2026 edition a logical continuation of the 2025 priorities, while raising expectations around maturity, evidential defensibility, compliance readiness and practical integration into law-enforcement workflows.

Annex: List of Companies Exhibiting in 2025

AirHub B.V.	https://www.airhub.app/
Roboverse Reply	https://www.reply.com/roboverse-reply/en
VTT Technical Research	https://www.vttresearch.com/en
Supervision B.V.	https://super-vision.nl/
State Criminal Police Office North Rhine Westphalia	https://lka.polizei.nrw/artikel/welcome-to-the-lka-nrw
Magnet Forensic	https://www.magnetforensics.com/
Issured Ltd	https://www.issured.com/
Future Space	https://www.futurespace.es/
RESARO	https://resaro.ai/
Bee The Data S.L.	https://www.beethedata.com/es/home
Quadible Greece P.C.	https://www.quadible.co.uk/
Rank One Computing Corporation	https://roc.ai/
Cellebrite	https://cellebrite.com/
Phonexia s.r.o.	https://www.phonexia.com/
GEOSAT	https://geosat.space/
Eyedea Recognition Ltd	https://www.eyedea.ai/
Maltego Technologies GmbH	https://www.maltego.com/
Paliscope AB	https://www.paliscope.com/
DarkOwl LLC	https://www.darkowl.com/
SOCRadar Cyber Intelligence Inc	https://socradar.io/

Bitdefender	https://www.bitdefender.com/
Elephantastic Software	https://www.elephantastic.io/
INNOSYSTEC GmbH	https://www.innosystec.de/
Byron Labs	https://byronlabs.io/
Crypto Asset Technology Labs	https://www.catlabs.io/
ChainComply BV	https://www.chaincomply.io/
Siren	https://siren.io/
Zepo Intelligence	https://zepo.ai/
Aegis Technologies	https://www.linkedin.com/company/aegis-sovereign-tech
HI Iberia Ingeniería y Proyectos	https://www.hi-iberia.es/

ENACT.

European Network Against
Crime and Terrorism

@enact-network

enact-eu.net

Scan the QR code to visit ENACT online
and read this report in digital format.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.