



Joint Policy Takeaways

“Operational challenges in digital security” Workshop

26 March 2026.

Privanova
Research & Consulting



www.privanova.com



comms@privanova.com



34, avenue des Champs-Élysées, Paris



Funded by
the European Union

The present Joint Conclusions have been developed with contributions from the following experts: Kristina Isakzay ([Privanova](#)); Prof. George Smaragdakis ([TU Delft](#)); Gideon Hazani ([LibereU](#)); Dr. Attila Wootsch ([Privanova](#)); David Arroyo ([CSIC](#)); Genny Dimitrakopoulou ([KEMEA](#)); and André Alegria ([Polícia Judiciária, Portugal](#)). The contributors represent a range of EU-funded security innovation projects operating within the framework of the [LEA Projects Cluster](#), including [IAMI](#), [SafeHorizon](#), [SECUR-EU](#) and [ENACT](#) projects.

Executive Summary

Digital security efforts in the European Union continue to face persistent operational challenges, particularly related to fragmented data environments, limited interoperability, and the slow uptake of research results in practice. Insights from the [LEA Projects Cluster](#), led by [Privanova](#) in cooperation with the [Center for Security Studies \(KEMEA\)](#), indicate that, while technological capabilities are advancing, their consistent use in operational contexts remains uneven. The Joint Takeaways from the event are highlighting that current challenges increasingly relate to how data and tools are integrated, governed, and applied in practice. Addressing these issues requires a stronger focus on interoperability, usable solutions, and more effective collaboration between research and operational actors.

Problem Definition

Key points:

- Digital security efforts remain constrained by fragmented data environments and limited interoperability
- A persistent gap exists between research innovation and operational adoption
- Legal and governance constraints continue to limit effective data sharing
- SMEs remain a structurally vulnerable segment in the cybersecurity landscape

Fragmentation of data, identities and knowledge across systems and actors

Information relevant to investigations is often distributed across multiple systems, organisations, and jurisdictions. This fragmentation makes it difficult to combine data and build a coherent operational picture in a timely manner. In practice, identities linked to the same actor may be spread across communication platforms, financial systems, and online environments, which complicates correlation even when data is available. At the same time, differences in systems and standards limit interoperability across agencies. This creates additional friction in cross-border and cross-agency cooperation.

Limited Ability to Correlate and Interpret Data

Research within the IAMI project demonstrates that combining multiple weak identifiers, such as email addresses, IP data, and device-related attributes, can significantly improve identification when analysed together. However, such approaches require integrated data environments and analytical capabilities that are not yet consistently available across operational contexts.

Gap between research innovation and operational adoption

EU-funded research projects continue to develop advanced tools and analytical capabilities. However, many of these solutions do not yet reach sustained operational use. This reflects challenges such as limited access to real operational data during development, insufficient alignment with existing workflows, and a lack of structured pathways for deployment. At the same time, experience from the SafeHorizon project shows that operational impact is achievable. For example, project activities identified approximately 22,000 compromised servers across multiple countries and supported remediation efforts, including the cleanup of a majority of affected systems in a European data centre.

Constraints related to access to operational data

The discussion also highlighted the constraints related to access to operational data. Researchers often face limitations due to legal, ethical and procedural requirements, which restrict their ability to test and validate solutions in real-world environments. At the same time, law enforcement authorities operate under strict regulatory frameworks that shape how data can be used and shared. These constraints affect collaboration and slow down the transition from research to practice.

Increasing scale and complexity of data environments

Another key challenge is the increasing scale and complexity of data environments. Investigations rely on large volumes of heterogeneous data from multiple sources. This requires advanced capabilities for data integration, entity resolution and analysis. The ability to correlate information across datasets is increasingly critical for effective intelligence and investigation processes.

Cyber threats continue to evolve in scale and sophistication

In parallel, cyber threats continue to evolve in scale and sophistication. Cybercrime is increasingly organised, service-based and, in some cases, supported by state actors. This creates a dynamic and complex threat landscape that cannot be addressed through isolated efforts. It requires coordinated approaches that combine technological, operational and strategic responses.

Significant gaps in the cybersecurity resilience of SMEs

Finally, the discussion identified significant gaps in the cybersecurity resilience of SMEs. These insights were provided from the SECUR-EU project research. Smaller organisations often lack the resources, expertise and awareness needed to implement effective cybersecurity measures. This makes them particularly vulnerable and creates broader systemic risks. The polling results reinforced this point, highlighting SME cybersecurity resilience as a key area of concern.

Strategic Priorities for Action

Key points:

- Enhancement of interoperability and data integration across systems and actors
- Establishment of structured and trusted data-sharing frameworks addressing legal and organisational constraints
- Support for the operational uptake of EU-funded research solutions through validation and alignment with end-user needs
- Strengthening of SME cybersecurity resilience through accessible tools, awareness and targeted support.

Interoperability enhancement and data integration across systems and actors

Rather than continuing to develop isolated tools and platforms, future efforts should focus on enabling seamless interaction between systems across agencies and Member States. This requires the development of common standards, the adoption of modular and API-based architectures, and stronger coordination at the EU level, particularly involving the European Commission and Europol. Interoperability should not be treated as an additional feature, but as a core design requirement.

Structured and trusted data-sharing frameworks need to be established

Create a structured and trusted data-sharing frameworks that reconcile operational needs with legal and ethical constraints. Current approaches often treat data sharing as a purely technical issue, while in practice it is equally a matter of governance and institutional trust. Establishing common frameworks for data access, use, and accountability would enable more consistent and legally robust collaboration across stakeholders, including law enforcement, research organisations, and the private sector.

Acceleration of the operational uptake of EU-funded research results

This requires a fundamental shift in how projects are designed and evaluated. End users, particularly law enforcement practitioners, must be systematically involved throughout the development process, not only at the validation stage. In parallel, mechanisms for testing and deploying solutions in real operational environments should be strengthened, ensuring that tools are not only innovative but also usable and relevant in practice.

Strengthening Data Integration & Analytical Capabilities

Investigative processes increasingly depend on the ability to analyse large volumes of heterogeneous data and to identify connections across datasets. Strengthening capabilities in data integration, entity resolution, and advanced analytics is therefore essential. This includes investment in shared analytical infrastructures and the integration of AI-supported tools that can enhance, rather than replace, human decision-making.

Strengthening the cybersecurity capacity of SMEs

Finally, the cybersecurity resilience of small and medium-sized enterprises must be addressed as a systemic issue. SMEs often lack the resources and expertise required to implement adequate security measures, which may increase their exposure to cyber threats. Targeted support, accessible tools, and increased awareness are necessary to reduce this vulnerability and strengthen the overall resilience of the EU digital ecosystem.

Enabling Conditions

The effectiveness of these priorities depends on broader enabling conditions.

- Policy and regulatory frameworks must be better aligned with operational realities, ensuring that safeguards do not inadvertently hinder legitimate and necessary data use.
- At the same time, stronger coordination is needed across the EU security ecosystem to avoid duplication of efforts and to maximise the impact of existing initiatives.
- Equally important is the development of trust between stakeholders. This cannot be achieved solely through technical solutions, but requires transparency, clear governance structures, and shared standards. Without trust, even the most advanced systems will remain underutilised.

Conclusions

The European Union has made significant investments in digital security research and innovation. However, the operational use of resulting tools and capabilities remains uneven across contexts. The findings suggest that existing challenges are increasingly linked to the integration and application of available solutions, rather than their development. This points to the need for improved interoperability, more consistent data-sharing practices, and stronger alignment between research outputs and operational requirements. Addressing these issues requires a more systematic approach to involving end users, supporting testing in operational environments, and ensuring that governance frameworks enable, rather than constrain, appropriate data use. Strengthening these aspects would contribute to a more coherent and usable digital security ecosystem in the EU.

About the Cluster

The [LEA Projects Cluster](#), led by [Privanova](#), brings together more than 50 EU-funded security research and innovation projects to strengthen Europe's collective capacity to address emerging security challenges. The LEA Projects Cluster contributes to addressing fragmentation in EU security research by connecting projects, law enforcement authorities, and institutional stakeholders. It contributes to reducing fragmentation in EU security research by connecting projects, law enforcement authorities, and institutional stakeholders. The Cluster enhances the visibility of available capabilities, facilitates knowledge exchange, and supports alignment between research outputs, policy priorities, and operational needs.

Join the LEA Projects Cluster

If your organisation coordinates or participates in an EU-funded security research project and would like to learn more about the [LEA Projects Cluster](#) or explore opportunities for collaboration, please contact Cluster Coordinator **Kristina Isakzay**: kristina.isakzay@privanova.com.

