

NEWSLETTER

Empowering SOC's Through Innovation



The Missing Link in Critical Infrastructure Cybersecurity: Threat Intelligence Sharing

Critical infrastructure is undergoing rapid digital transformation, bringing both new opportunities and heightened exposure to cyber threats. As organisations continue to digitalise their operations and integrate IT and operational technology (OT), cyberattacks are becoming more sophisticated, targeted and difficult to detect. At the same time, the consequences of a successful attack continue to grow, particularly in sectors such as energy, where disruptions can affect businesses, public services and millions of citizens.

To address these risks, organisations have invested heavily in cybersecurity technologies. Security Operations Centres (SOCs), Security Information and Event Management (SIEM) platforms, artificial intelligence (AI), machine learning (ML), and automated response tools have become essential components of modern cyber defence strategies.

However, technology alone is no longer enough.

Modern Cybersecurity Requires More Than Internal Visibility

Many organisations still approach cybersecurity from an internal perspective. Their SOC continuously monitors their own networks, analyses security events and responds to incidents occurring within their own environment.

While this approach remains essential, it also has a significant limitation - organisations often lack visibility into threats that have already been identified elsewhere.

Cybercriminals rarely target a single organisation. The same attack techniques, malicious infrastructure or compromised indicators are often reused across multiple organisations, sectors and even countries. If every SOC works independently, each organisation is forced to discover these threats on its own, losing valuable time during the early stages of an attack.

This is why threat intelligence has become one of the most valuable assets in modern cybersecurity.

The Growing Importance of Threat Intelligence Sharing

Threat intelligence provides actionable information about cyber threats, including indicators of compromise (IOCs), attacker tactics, techniques and procedures (TTPs), emerging vulnerabilities and malicious infrastructure.

When this intelligence is shared between trusted organisations, every participant gains a broader understanding of the evolving threat landscape. Instead of reacting only after detecting suspicious activity internally, organisations can proactively strengthen their defences based on attacks already observed elsewhere.

For operators of critical infrastructure, this collaborative approach is particularly important. Cyber threats targeting the energy sector, public administration or other essential services often affect multiple organisations simultaneously. Sharing threat intelligence enables faster detection, more informed decision-making and significantly shorter response times.

In other words, cybersecurity is evolving from an organisation-centric model towards a collective defence approach.

Building Collaborative Cyber Resilience

Effective threat intelligence sharing is not simply about exchanging data. Information must be accurate, timely, relevant and trustworthy. At the same time, organisations must ensure that sensitive operational information remains protected and that all exchanges comply with privacy and regulatory requirements.

This requires secure platforms capable of collecting, enriching and distributing threat intelligence in a standardised and privacy-compliant manner. Modern technologies such as AI and ML can further improve this process by automatically enriching threat data, identifying relationships between incidents and helping security analysts prioritise the most significant risks.

As cybersecurity threats continue to evolve, collaboration is becoming just as important as technology itself.

How INTERCEPT Addresses This Challenge

The INTERCEPT project was created to strengthen this collaborative approach to cybersecurity.

As an EU-funded initiative, INTERCEPT is developing a secure cross-border Threat Sharing Platform (TSP) that enables Security Operations Centres and other trusted cybersecurity stakeholders in Slovenia and Croatia to exchange actionable threat intelligence quickly, securely and in compliance with privacy requirements.

Rather than relying solely on internal observations or generic commercial threat feeds, participating organisations will be able to access regionally relevant intelligence enriched with local context. This provides greater visibility into threats affecting critical infrastructure and enables organisations to detect and respond to attacks much earlier.

The platform combines data from multiple trusted sources, including SOCs, national CERTs and public threat intelligence repositories. By integrating AI-driven analytics, machine learning and automated anonymisation, INTERCEPT enhances the quality of shared intelligence while ensuring that sensitive information remains protected.

The project also supports the adoption of collaborative cybersecurity practices through workshops, training activities and knowledge exchange between public institutions, critical infrastructure operators, SMEs and managed security service providers (MSSPs). By strengthening both technology and cooperation, INTERCEPT contributes to a more resilient regional cybersecurity ecosystem.

Towards a More Connected Cybersecurity Future

Cybersecurity is no longer defined solely by the technologies an organisation deploys within its own network. Success increasingly depends on the ability to anticipate threats before they arrive,

learn from the experiences of others and collaborate across organisational and national boundaries.

Threat intelligence sharing is rapidly becoming a strategic capability for protecting critical infrastructure and strengthening Europe's cyber resilience.

Projects such as INTERCEPT demonstrate how secure collaboration, advanced technologies and trusted partnerships can transform isolated cyber defence into a collective approach that benefits organisations, critical infrastructure and society as a whole.

Follow INTERCEPT journey on Digital media platforms

- [WEBSITE](#)
- [LINKEDIN](#)
- [YOUTUBE](#)
- [X](#)

Follow INTERCEPT



www.interceptcybersecurity.eu



Co-funded by
the European Union



ECCC
EUROPEAN CYBERSECURITY
COMPETENCE CENTRE

The project funded under Grant Agreement No. 101190460 is supported by the European Cybersecurity Competence Centre.

Disclaimer: Funded by the European Union. Views and opinions expressed at the website and in the documents are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the European Cybersecurity Competence Centre can be held responsible for them.