EUROPEAN CYBER SECURITY ORGANISATION

# POSITION PAPER

## SOCs and CTI

ECSO SOC and CTI Task Force

*June 2022*

www.ecs-org.eu

# POSITION PAPER OF THE ECSO TASK FORCE: EUROPEAN CYBER SECURITY OPERATION CENTRES AND THREAT INTELLIGENCE (ECSOCTI)

## EXECUTIVE SUMMARY

ECSO members consider the upcoming call of the Digital Europe Programme on Security Operation Centre capacity building and Cyber Threat Intelligence as a great opportunity to **strengthen European Digital Sovereignty and Strategic Autonomy** and boost the further development of European competencies in this area. This call also gives a chance to overcome the existing market fragmentation and **accelerate cooperation between European stakeholders** from the private and public sectors to prevent, detect and respond to cyber threats. This paper highlights crucial elements that contribute to the achievement of the above-mentioned goals. Key observations and recommendations:

- **In the current geopolitical situation, SOCs are urgently needed to detect attacks against European networks.**
- **Strong participation of the private sector** and **sectoral-driven cooperation** should be seen as a cornerstone of the robust SOC and CTI ecosystem. New initiatives on SOCs and CTI should **leverage on existing solutions and bridge the information gap between the private and public sector** by federating existing SOCs and CTI platforms.
- When developing SOC capabilities, it is recommended to take a **holistic approach**. Effective SOC solutions should not only help to protect internal organisations' resources but also **ensure resilience of the entire supply chain**. This is why mechanisms for secure information exchange and broader cooperation within the ecosystem must be promoted.
- **SOCs and CTI** serve as equally important elements of strong cybersecurity. While the former concentrates mainly on detection, the latter offers prediction capabilities, and their close alignment is crucial to effectively combat cyber threats. **Significant investments are needed in both domains** as well as the creation of mechanisms to promote cooperation between them.
- **Utilisation of innovative technologies**, including, but not limited to, Artificial Intelligence (AI) or Machine Learning (ML) that **will strengthen SOCs capabilities** and contribute to improved benefits for all stakeholders involved. For instance, AI can be used to analyse data coming from various sources (including from member SOCs), identify the most popular attack tactics and enable the creation of a real-time heat map that serves as an EU-wide Threat Model. Also, data science-based solutions and technologies have a potential to increase the effectiveness of the threat analysis.
- While innovative technologies are important for SOCs, **highly skilled people are still essential**. The **human element** is fundamental to the overall success of both SOCs and CTI and as such should be significantly strengthened. This is especially important as SOC providers face severe shortages in skilled and well-trained manpower responsible for processing intensively growing volumes of security alerts. **Investments in in specialised education and training** are urgently needed to face a rapidly evolving threat landscape.
- The **creation of a trust-based European Cybersecurity Threat Intelligence Alliance** could provide EU-wide information gathering, processing, and sharing. Such an Alliance could benefit from a dedicated European fund to support European CTI service providers and constitute the backbone of CTI sharing in Europe, combining information from public and private actors to better predict upcoming attacks, creating the needed link for best exploitation of data coming from the newly created SOCs network. To better develop the public – private cooperation, the Alliance would coordinate with the Network of National Coordination Centres and the other envisaged or existing European institutional initiatives (e.g. Network of CSIRTs, ENISA, Joint Cyber Unit, etc.). With its years of experience and a proven record of creating cybersecurity communities in Europe, **ECSO would use its network, skills,**

**and know-how to develop a European CTI ecosystem creating and coordinating such an Alliance**, building upon its established suppliers and users communities, reaching in a short term and with limited effort the envisaged objectives.

- The value of the performed CTI analysis is directly linked to the quantity and the quality of the ingested data. **Data and information sharing between members of the Alliance should be incentivised** to unlock the potential of European cooperation. Common data formats should be envisaged to facilitate CTI exchange.
- Trustful cooperation and dissemination of data can be reinforced by:
  - The possible utilisation of **innovative technologies** and Distributed Ledger Technology (DLT) such as blockchain-enabled frameworks (serving among others to securely authenticate and authorise entities that provide raw data)
  - The creation of mechanisms allowing to accept **only vetted members**
  - The implementation of **access controls and innovative solutions** helping to maintain security and privacy but at the same time enabling information sharing.
- The information sharing process will require the development of a **unified approach toward data sharing models: a common framework, interoperability standards, taxonomy, and agreed protocols.** While some good practices exist, an alignment of the joint approach should be achieved.

## INTRODUCTION

The coming **call of the Digital Europe Programme on Security Operation Centre (SOC) capacity building and Cyber Treat Intelligence (CTI) [1]sharing** has triggered stronger attention on the possible development and coordination between public administrations and, hopefully, also with the private sector in this area. In this context, stronger emphasis should be given to the participation of the private sector and sectoral cooperation to prevent further fragmentation of the European cybersecurity ecosystem.

While **SOCs and CTI are two different markets**, the involved stakeholders are often the same and **interests are linked**. **CTI allows the SOC team to determine correctly to prevent attacks and reduce the time taken to detect**. It can also assist the SOC team in determining the urgency to receive executive support.

**Europe has strong capabilities in SOCs, including certified offers,** both from large and smaller providers, often by Managed Security Service Providers (MssPs) and could, better than in other digital sectors, **satisfy strategic needs when looking from the sovereignty** point of view. These strong European capabilities in SOCs should be enhanced and encouraged to grow. Leveraging on existing capabilities should therefore be a priority to avoid duplication of efforts.

As for CTI, there is currently a large **fragmentation, with different CTI approaches across Europe** on the private sector side. SOC adopters often still lack the information to fully understand how modern SOCs could be used, and how they can contribute to digital sovereignty.

ECSO believes that to strengthen cybersecurity, it is essential to follow all the steps of the "Identity, Protect, Detect, Respond, and Recover" framework. ECSO would therefore advise that the call of the European Commission on SOCs makes sure investments allow **SOCs to be more effective in their contribution to the entire cycle** as shown in Figure 1.

[1] Threat intelligence is evidence-based knowledge, including context, mechanisms, indicators, implications, and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard. *Gartner definition of threat intelligence* https://www.gartner.com/en/documents/2487216


*Figure 1 - NIST Cybersecurity Framework Functions Wheel*

In addition, SOCs capacity building should make sure to allow EU SOC providers to better structure their Threat Intelligence cycle from collection to dissemination so that it can serve a more general purpose of enhanced CTI cooperation at European level (see Figure 2).

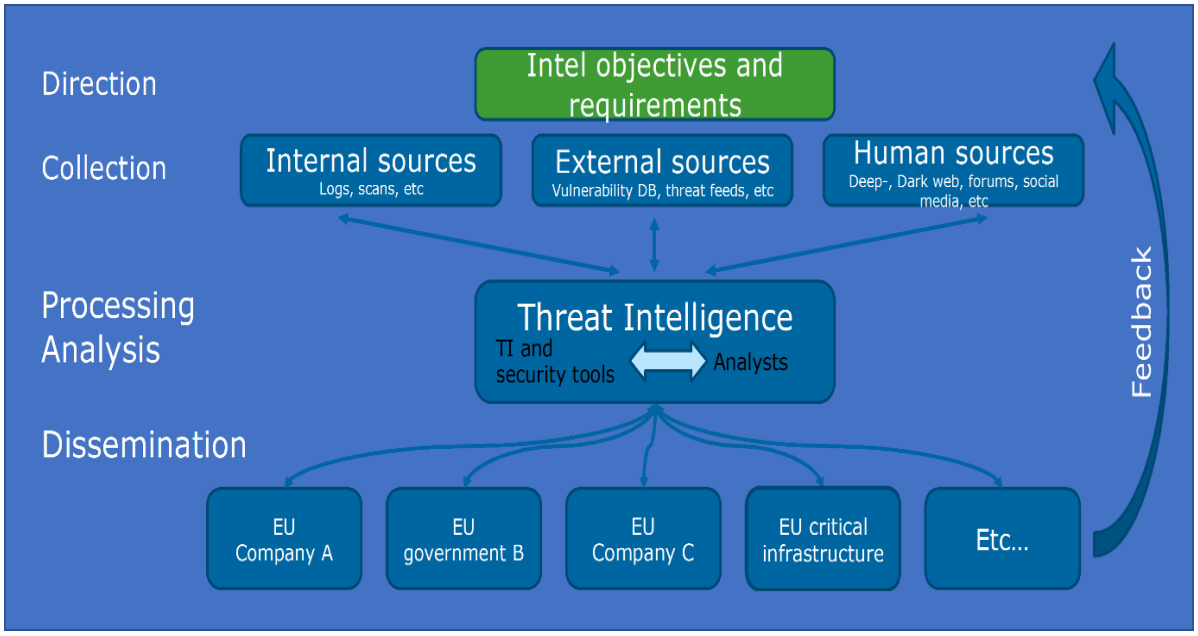



*Figure 2 - Recommended use of CTI in the EU – figure courtesy of ATOS*

**Cyber Threat Intelligence** is a flourishing cybersecurity market, the primary objective of which is to obtain a knowledge advantage over the attacking party. CTI is relevant when it represents actionable information by the end users.

ECSO believes it is fundamental for the EU's sovereignty to enhance **public / private cooperation in the CTI domain as well as create the basis for an increased and more efficient exchange of threat information among private stakeholders**.

A true European Cyber Threat Intelligence ecosystem will be reached only by combining quality Threat Intelligence, with a reliable way to **share information with other stakeholders** to better anticipate and counter threats.

## 1. HOW TO STRENGHTEN EUROPEAN SOC CAPABILITIES TO ADDRESS DIGITAL SOVEREIGNTY CONCERNS?

### *1.1 Understanding the needs and bringing more transparency to the market*

Investments in security features to strengthen EU SOC capabilities depend on what one wants to detect. The choice for the most adapted SOC can be based upon "rating systems" leveraging on maturity models and requirements (e.g. a small company needs a different type of SOC than a large mature enterprise).

These rating systems depend on the topology of SOCs. There are roughly 4 types of high-level SOC topologies:

- SIEM (Security Information and Event Management)
- SIEM + SOAR (Security Orchestration, Automation and Response)
- SIEM + SOAR + CTI
- SIEM + SOAR + CTI + AI

Different topologies respond to different needs.

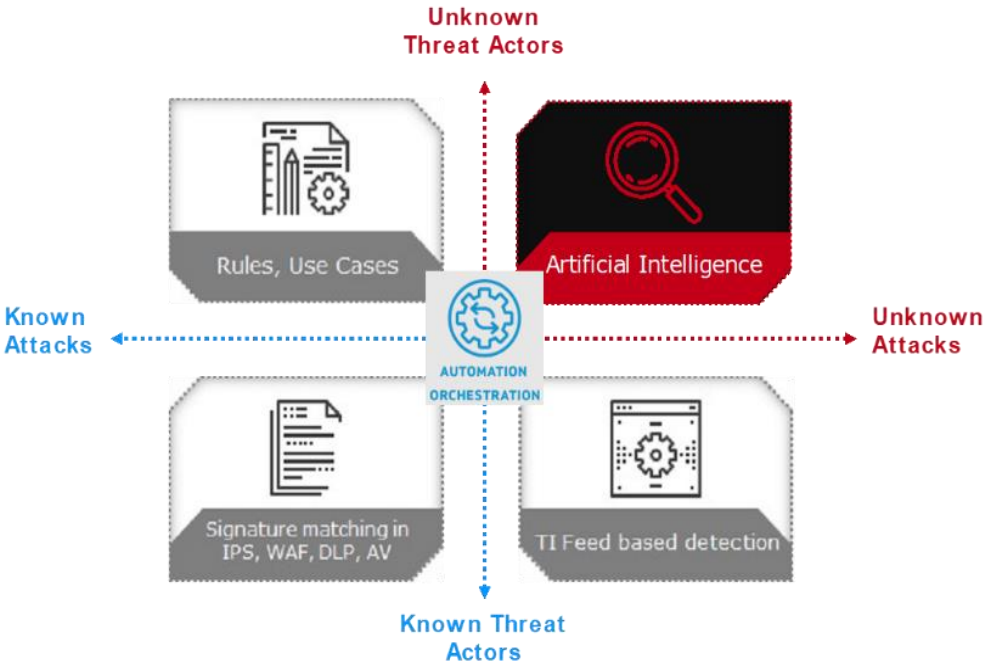



*Figure 3 - courtesy of ATOS*

The rating system should help clarify to customers where they need SOC services using SIEM, SOAR, CTI and AI, depending on their needs. AI can be deployed on more layers than just SIEM. For example, AI can be federated to EDR (Endpoint Detection and Response), NDR (Network Detection and Response), Sentinel, cloud, etc. It must be highlighted however, that even if AI is very promising, the human skills remain an essential part of the whole process and AI works best when paired with human analysis.

The rating system, and hence the choice for an adequate SOC, should also take into consideration the possible use of (EU) sovereign tools and services, with targeted calls for tender open to EU companies only[2], especially if the CTI generated is critical/sensitive for a Member State.

[2] "EU companies" are defined as companies with Head Quarters in an EU Member State and operating mailing in the EU internal market

### *1.2 Protecting critical infrastructures and their ecosystems*

**SOCs should not only protect single organisations, but whole critical ecosystems, including suppliers down the supply chain.** Since each organisation's critical set of services is unique, each SOC should adapt to the requirements of each client and support them as they evolve. To enhance collective security, the clients of a SOC have an incentive to share information with the SOC**. Mechanisms for exchanging confidential information with the SOC are needed, especially to design multiple lines of and defence in depth.**

### *1.3 AI-powered SOCs*

An AI-powered SOC, fed by the data from all member SOCs, could identify the current most popular attack tactics as defined by the MITRE framework and create a real-time heat map that serves as an EU-wide Threat Model. Filters such as industry-specific or country-specific could be applied depending on the available data.

The conversion of Tactics Techniques and Procedures (TTPs) and Indicators of Compromise (IOCs) into research models is a very important aspect for the efficiency of a SOC. Responding promptly and effectively is the most important parameter and indicator of SOCs. To this end, AI is established as a resource to improve and automate incident response preparedness (SOAR). AI can assist (and eventually empower) a SOC analyst in converting an event or incident into an investigation with aggregated and resolution-oriented data by a forensic analyst.

Deploying and implementing AI-powered tools for the SOCs is not simple and, if not done correctly, it could result in additional burden for the human analysts. There is already a community working on Trusted AI / Hybrid AI that can be enriched with experts that can architect best practices for choosing, testing, deploying, and automating such analytics systems efficiently.

Investing in AI uptake in EU SOCs is key as well as clarifying to end-users, through the proposed rating system above, what it really means for a SOC to rely on AI.

### *1.4 The human factor and the needed skills: education investments for accessible and specialised training*

SOCs are not only about technology. Specific skills are needed when working in SOCs, especially AI-powered SOCs and thus, specific training should be envisaged.

**Investments in accessible and specialised education are urgently needed to face an** increasing threat landscape that leads to growing security alert volumes, increasing number or legislations to obey, lack of investments in security, overworked SOC analysts, and staff shortages.

Relevant education programmes are currently rather costly, with only a few exceptions that are mostly known in the corporate environment. There is therefore an opportunity for educational programmes in cybersecurity to target specialised certifications like ISO.

Today it is difficult to find and retain cybersecurity professionals in this area. Closer cooperation with schools and universities should be investigated to:

- Recruit students.
- Tailor studies so graduates get ready to use skills in cybersecurity (including data scientists, AI specialists, etc.).
- Set up training programmes to train non-cybersecurity candidates from the labour market.
- Create learning streams for data scientists applied to cybersecurity (e.g. threat hunting, as successful threat hunts can provide valuable information for other companies in the same field or sector. Developing a way to collaborate on patterns discovered in a threat hunting exercise can provide a way for peers to do the same and improve vulnerability footprint, data interpretation and retention, while leveraging open-source solutions where feasible).

### *1.5 Other needs for data sharing, from SOCs to CTI*

- **TRUST:** Once data is available, it should be shared in an EU-wide CTI sharing mechanism. This is more easily achievable when trust is built between EU-based stakeholders that know each other. For this reason, **ECSO is already developing a European Community of Chief Information Security Officers** (CISOs) – currently counting more than 170 CISOs from 26 different European countries – from all those private companies and stakeholders that have an interest in CTI and sovereign and trusted offers for SOCs. To guarantee trust on a wider scale however, innovative technologies like blockchain could be used as a possible tool to promote trust between people that do not know each other.
- **Interoperability STANDARDS, a common TAXONOMY and agreed PROTOCOLS** will be needed for an effective sharing platform.
- **INCENTIVES**: Organisations are reluctant to exchange CTI due to fear of exposure, reputational damage, and lack of incentives. Existing CTI-sharing platforms rely on centralised trusted architectures that could suffer from a single point of failure and risk companies' privacy as the central node maintains CTI details.
- **Definition of DATA OWNERSHIP, ACCESS CONTROL (including of enabling data owners to control the use of their data), CONFIDENTIALITY**

## 2. TOWARDS A EUROPEAN CYBER THREAT INTELLIGENCE

There are three overarching, but not categorical - classes of cyber threat intelligence (CTI)[3]:

- **Tactical**: technical intelligence (including Indicators of Compromise such as IP addresses, file names, or hashes) which can be used to assist in the identification of threat actors.
- **Operational**: details of the motivation or capabilities of threat actors, including their tools, techniques, and procedures.
- **Strategic**: intelligence about the overarching risks associated with cyber threats which can be used to drive high-level organisational strategy.

### *2.1 Key gaps and opportunities in CTI*

Although the overarching goal of CTI is to bring unity to the process of cybersecurity management via enhanced decision-making, **the existing CTI landscape is somewhat fragmented** with only a few common denominators in terms of approaches organisations are taking. This leads to a general lack of an accurate methodology for the analysis, interpretation, and correlation of the CTI data. There are several models and frameworks where all the information is funnelled into, but the actual interpretation of CTI is still a purely subjective matter and not an actual science. Overall, we are missing consensus in many areas of the CTI landscape.

The quality of the performed CTI analysis is directly linked with the quantity and the quality of the ingested data. There are parameters such as false positive ratio, completeness, and timeliness, which are used to evaluate the quality of a CTI source over another, but this is not sufficient for vetting conclusions about the actual information. The origin and the technique used to collect the actual information is rarely disclosed, leaving a lot to be desired in terms of traceability, stripping the analysts of the ability to create custom confidence and scoring metrics. Furthermore, organisations operating in critical sectors are most often reluctant to share even basic internal information inducing a lack of available real-world data in the academia and research community, hence prohibiting the growth of collaborative security.

The use of the Dark Web and especially Darknet Markets (DNMs) can provide proactive CTI value through automated analysis of new trends and exploits. The Dark Web remains a vastly unexplored source of automatic CTI collection, since most information in DNMs is noisy, unlabelled, and hidden behind many layers

[3] https://www.enisa.europa.eu/events/2018-cti-eu-event/cti-eu-2018-presentations/cyber-threat-intelligence-standardization.pdf

of protection. This inherent difficulty in accessing DNMs is what makes them popular among cyber criminals but also an excellent source for effective, timely and relevant intelligence. Even though some prototype tools attempt to gather intelligence from the Dark Web, a more holistic solution could be the catalyst in the transition from a traditional CTI approach to a more proactive posture.

There are many information sharing networks currently operating in the EU, each one having its own circle of members and trust. Unfortunately, most of these networks either work in complete isolation, or their membership eligibility criteria are limited to specific vertical markets (e.g. energy sector). However, to cope with and predict advanced threats and contemporary attack vectors and patterns, large amounts of diverse data are required for in-depth analysis, thus there is a need to collect information from various sectors and their respective security systems. This creates a need to incentivise closed communities into **sharing information outside their circle and provide a platform that guarantees that the data will not be misused, ensure that proper data sanitisation techniques are used, while maintaining a balance between security and usefulness of shared data.**

### *2.2 Tackling sensitive CTI exchange issues*

For legal reasons, it might be difficult to share data and many  are looking into **federated models to share data** without having legal issues due to privacy or data ownership / competition issues.

Threat Intelligence Platforms (TIPs) enable organisations to exchange critical threat information to prevent further similar attacks to those that have already occurred. However, the sensitive nature of data managed in certain environments may cause entities to refuse to share certain information.

Under these circumstances, **a privacy-preserving and trust-minimised network could enable organisations to share only the critical information related to specific attacks or further threat events they may encounter**, providing strong mechanisms to ensure, at least:

- **Access control** to the exchanged information, empowering organisations to keep control of what they want to share and with whom.
- **Privacy** of certain data being shared, enabling the obfuscation of sensitive attributes related both to stakeholders and organisations in the sharing network.
- **Auditing** resources, allowing involved actors to assess the provenance, integrity, and immutability of shared information during its whole lifecycle.

On this aspect, a system that ensures the previous points and covers the shortcomings of most state-of-the-art proposals should include the basis of an **open-source TIP (Malware Information Sharing Platform - MISP)**, enhanced with the following modules:

- **Access control mechanisms based on attribute-based encryption.**
- A **permissioned platform** for auditing purposes, powered by innovative technologies like blockchain.
- **Privacy-Enhancing Technologies (PETs)**, based on the use of well-known anonymisation algorithms such as K-anonymity, L-diversity, or T-closeness, to protect sensitive data that needs to be shared.
- A **Federated Learning (FL)** to enhance accuracy in local intrusion detection mechanisms, making possible the use of private data of external parties to train a global threat-detection Machine Learning model without sharing any data, thus ensuring its privacy.

### *2.3 CTI – info sharing models*

Threat intelligence sharing provides access to threat information that would otherwise be unavailable to an organisation. By utilising shared resources, organisations can improve their security posture by proactively leveraging the knowledge, experience, and capabilities of their partners. Enabling “one organisation’s detection to become another's prevention” is a powerful paradigm that can advance the overall security of organisations that actively share threat intelligence.

**The objective should be the generation of dedicated information sharing models for all actors in the supply** chain: end-users, enabling actors such as First.org or CSIRTs, and private industry intelligence providers

supported by a platform that allows for an early warning and specialised observatory for different industry verticals. This information sharing model should discern by industry (utilities, energy, automotive, manufacturing) and provide authenticated and authorised communications channels dedicated to each industry's supply chain.

Encouraging formal, specialised communication between different teams (public SOC, private SOC, cross industry / specialised SOC, CERT/CSIRT/ CIRTS, etc.) could break the communication siloes that currently exist and support the creation of data exchange models and common knowledge repositories (e.g. MISP Repository). This would allow the identification and creation of a network of specialised SOCs (Operational Technology (OT) SOC, Vehicle SOC, etc.), while assessing the industry dimension and the minimum scope required for a SOC creation, and the establishment of best practices for PPPs (public-private partnerships) around SOCs.

The overall goal is to **strengthen the cooperation and information sharing between public and private SOCs** but also between Member States' response and prevention teams altogether. This can be done by establishing for example reliable data sharing models (e.g., ensure data anonymisation …). Such collaboration models can help optimise the pattern recognition of incidents and attacks, tune alerts, help with the interoperability of solutions, but also improve the deployment models for SOCs and foster the creation of solid PPPs.

Cooperation in the SOC and CTI domains in the EU should strengthen its sovereignty in cybersecurity.

**A model describing the actual cooperation is key to its success**.

Part of the model could be described by the following items:

- **Who:**
  - Procurement for the SOCs network should be limited to EU legal entities (main establishment in the EU and not controlled by a third country). Participation in CTI sharing should be open to all entities agreed by national administrations. Such entities could include, but should not be limited to, public companies, private companies, (local) governments, government organisations, etc.
- **What:**
  - Identification of the sources
  - Agreement on what will be shared
  - Kind of information (qualitative/quantitative)
  - Kind of Operating System, Software, Hardware…
  - Open-Source Intelligence
  - Use of paid feeds
  - TI must be of high quality: relevant, timely, actionable, and accurate
- **How**:
  - Strengthened cooperation should be based on building up central mechanisms to support the intelligence cycle?
  - EU CTI processes and tools should be implemented so that the EU CTI team can aggregate, normalise, correlate, and analyse threat data from multiple sources in real time:
    - Curated, relevant, and widely sourced threat intelligence
    - TI should be usable for security planning, monitoring and detection, incident response, threat hunting, threat assessment and sharing threat information
    - The EU CTI team should be able to drive smart practices back into SIEMs, intrusion detection, and other security tools
  - There should be agreements on how and when to share CTI.
  - Incentives can motivate companies to share and should be part of the cooperation model.
  - Adequate training on how to contribute to/use the EU CTI.
  - Training on how to leverage CTI to improve European detection capabilities.

### *2.4 Public investments on CTI*

While private companies are already heavily investing in CTI, public investments should be targeted at **consolidating and supporting the cyber intelligence cycle,** both centrally for EU SOC and sharing with EU SOC suppliers/users.

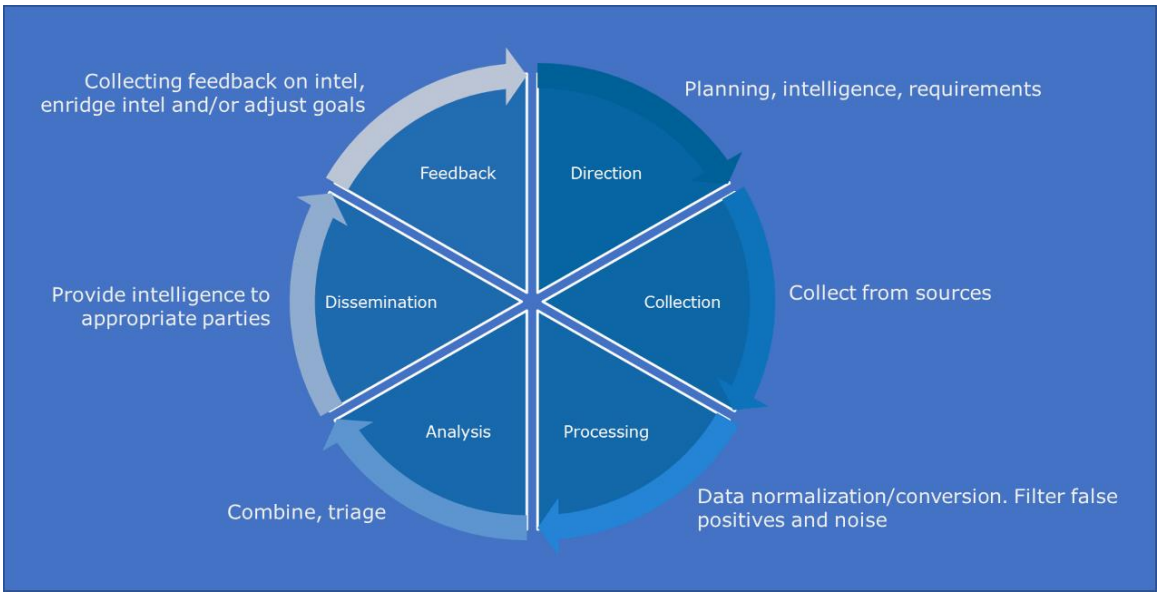



*Figure 4 - CTI cycle – figure courtesy of ATOS*

Investments are also needed to develop **centralised threat hunting capabilities** based on utilising (central) AI, CTI and data telemetry of members of an EU SOC platform (combination of data telemetry available from the public and private sector could allow the discovery of attack patterns and identify future advanced threats in different sectors.

Efforts should be directed towards federating existing SOCs and CTI platforms to bridge the information gap between public and private sector. Added value could also be achieved in the establishment of common data formats to facilitate CTI sharing at EU level.

### *2.5 Governance: European Cybersecurity Threat Intelligence Alliance*

ECSO is looking towards an increased **public / private cooperation in the CTI domain as well as to create the basis for an increased and more efficient exchange of threat information among private stakeholders**.

ECSO has studied different CTI models existing at national level in Europe (in France and Germany) and in the United States[4]. They are usually driven by some major companies, but it is unclear how much they are "independent" and avoid conflict of interest when sharing information.

The **creation of a European Cybersecurity Threat Intelligence Alliance** within ECSO should guarantee a level of independence and to gather and organise cooperation and interoperable solutions according to European rules, as well as to increase European's sovereignty. Such an Alliance could benefit from a dedicated European fund to support European CTI service providers. The Alliance would **coordinate with National Administrations** (and possibly with **European Institutions**) and could be a model that works and provides the **right kind of incentives and value added proposition to share information**.

This alliance would trigger new specific **concrete initiatives in the CTI domain** to support the business development and market growth of its members and the competitiveness of the European economy.

[4] https://www.mdpi.com/2079-9292/11/9/1401

This alliance, starting from cybersecurity providers, could also interact with users / operators in the different vertical sectors to strengthen needs and focus activity on actual strategic cyber issues.

It would also support moving from a traditional CTI approach based upon response to a **more proactive (threat anticipation) posture.**

**A major objective of such an alliance would be to reduce fragmentation in Europe** and the creation of an effective **European Cybersecurity Intelligence** upon which the public and the private sector could trustfully build their digital transformation and foster trusted information exchange.

## *3.* OTHER INITIATIVES NEEDED TO REMOVE MARKET BARRIERS OR INCREASE CLARITY FOR CUSTOMERS

One of the objectives of the European Commission's call is to *"Identify potential critical dependencies on foreign suppliers and solutions in the area of threat intelligence and develop an EU supply chain on threat intelligence".*

The objective, as it is stated, does not explicitly provide an incentive for developing sovereign solutions that would reduce this dependency.

EU's dependency on foreign technology for Endpoint Detection and Response (EDR), Network Detection and Response (NDR), and Security Orchestration, Automation and Response (SOAR) is already quite established.

More stringent specifications from the EC in these areas would be needed with explicit support for trusted EU technology development, noting that previous investments have failed to land in the market and that cybersecurity very much needs agile investment to adapt to the short innovation cycles. Other use cases can be enriched with technologies like Cloud/Edge monitoring (public, hybrid).

## ABOUT ECSO

The European Cyber Security Organisation (ECSO) is a non-for-profit organisation, established in 2016 to support the Public – Private Partnership on cybersecurity with the European Commission. ECSO unites more than 270 European cybersecurity stakeholders, including large companies, SMEs and start-ups, research centres, universities, end-users, operators, associations, and national administrations. ECSO works with its Members and Partners to develop a competitive European cybersecurity ecosystem providing trusted cybersecurity solutions and advancing Europe's cybersecurity posture and its technological independence.

More information: www.ecs-org.eu .

## CONTACT PERSONS

For any questions or comments, feel free to contact Joanna Świątkowska (COO) or Francesco Bordone (Junior Manager).

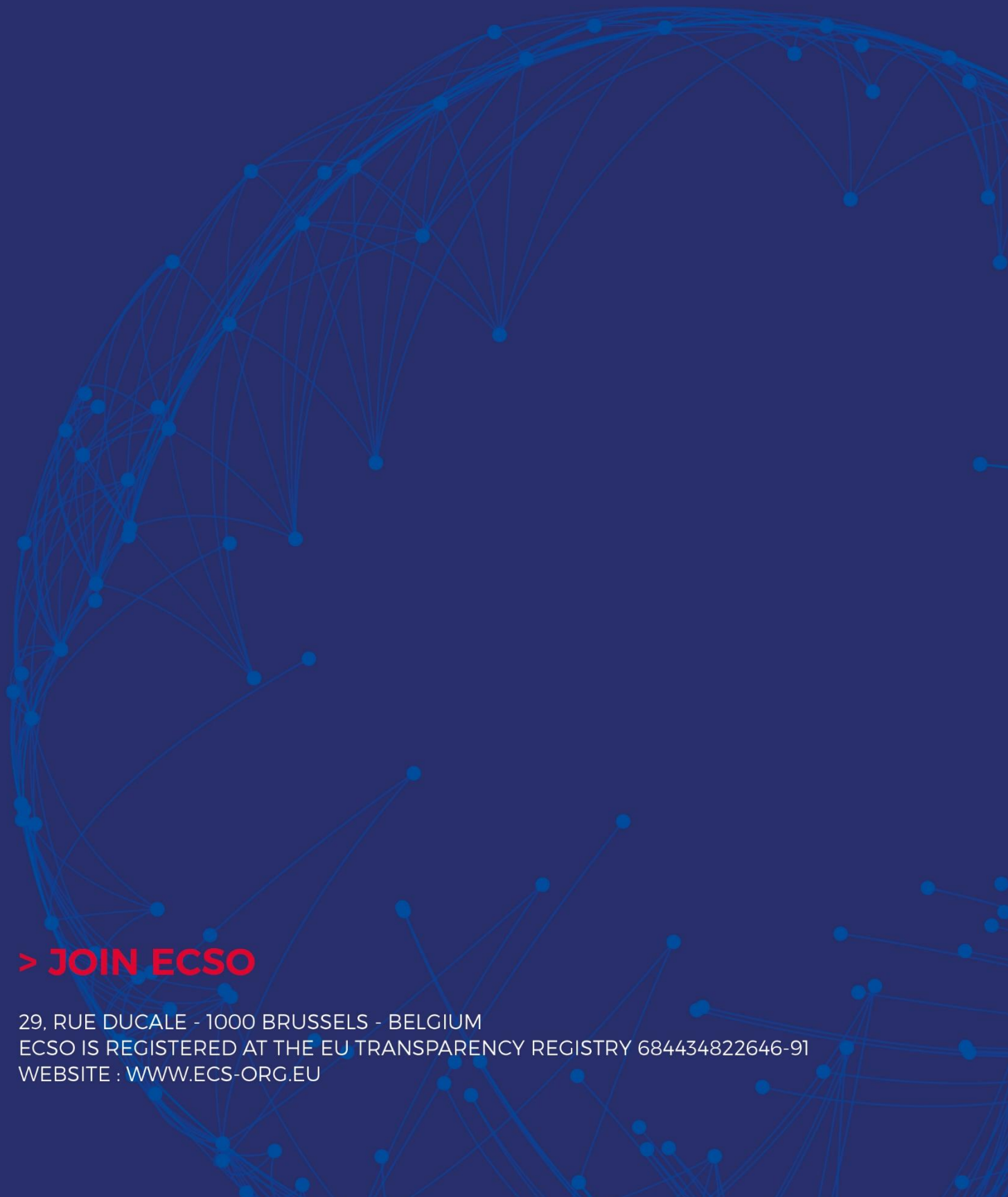
joanna.swiatkowska@ecs-org.eu

francesco.bordone@ecs-org.eu

European Cyber Security Organisation (ECSO)

ECSO is registered at the EU Transparency registry: 684434822646-91

ECS
EUROPEAN CYBER SECURITY ORGANISATION



## > JOIN ECSO

29, RUE DUCALE - 1000 BRUSSELS - BELGIUM
ECSO IS REGISTERED AT THE EU TRANSPARENCY REGISTRY 684434822646-91
WEBSITE : WWW.ECS-ORG.EU