

***Euro Cyber Resilience Board for pan-European Financial Infrastructures (ECRB) - Cyber Information & Intelligence Sharing Initiative: Community Rulebook***

***August 2020***

**CHANGE LOG**

<b>Version</b>	<b>Date</b>	<b>Comments</b>
1.0	03 August 2020	N/A

## Background

Cyber threats pose a serious risk to the stability of the European and global financial system. Cyber threats are borderless and the capabilities of the attackers are constantly evolving, threatening to disrupt the interconnected global financial systems. To successfully combat cyber risk, financial infrastructures need to actively participate in information and intelligence sharing arrangements and collaborate with trusted stakeholders within the industry as a whole.

The core objectives of the Cyber Information and Intelligence Sharing Initiative (CIISI-EU) are to protect the financial system by preventing, detecting and responding to cyberattacks; to facilitate the sharing of information, intelligence and good practices between financial infrastructures; and to raise awareness of cybersecurity threats. The CIISI-EU community is comprised of pan-European financial infrastructures, central banks (in their operational capacity), critical service providers, ENISA and EUROPOL, as represented in the Euro Cyber Resilience Board for pan-European Financial Infrastructures (ECRB). The members of the CIISI-EU community and initiative will share vital strategic, operational and tactical information among themselves using an automated platform; and create a trusted community where they will meet to discuss cybersecurity threats and share related information and intelligence and best practices.

By exchanging cyber information and intelligence within the CIISI-EU community, members can leverage the collective knowledge, experience, and capabilities of the sharing community to gain a more complete understanding of the threats they may face. Using this knowledge, members of the community can make threat-based decisions regarding defensive capabilities, threat detection techniques and mitigation strategies.

At the 4th meeting of the ECRB on 27 February 2020, the above mentioned entities agreed to establish and join CIISI-EU<sup>1</sup>. The high level framework for establishing and participating in CIISI-EU; the core objectives for information sharing; and the terms to enable the safe and effective information and intelligence sharing within the CIISI-EU Community were set out and agreed in the **Cyber Information & Intelligence Sharing Initiative: Terms of Reference** (Annex A). This document, the '*CIISI-EU ECRB Community Rulebook*' (CIISI-EU Rulebook), builds on the Terms of Reference<sup>2</sup> and sets out more details on:

- The governance of CIISI-EU;
- The building blocks of CIISI-EU;
- The principles for information and intelligence that will be applied by the members; and
- The taxonomies, frameworks, terminology and conventions to be used for the sharing of information and intelligence (i.e. the sharing schema).

---

<sup>1</sup> [https://www.ecb.europa.eu/press/pr/date/2020/html/ecb.pr200227\\_1~062992656b.en.html](https://www.ecb.europa.eu/press/pr/date/2020/html/ecb.pr200227_1~062992656b.en.html)

<sup>2</sup> Text taken from the Terms of Reference is indicated in this document in grey call-out boxes

## Section 1. Governance of CIISI-EU

The CIISI-EU Rulebook is not legally binding and does not constitute terms capable of becoming a contract by acceptance. The CIISI-EU Rulebook sets out a detailed approach and rules that members agree to follow in order to effectively operationalize CIISI-EU. The CIISI-EU Rulebook does not, and shall not, be construed in any way to create any binding or legally enforceable obligations on part of the members, including without limitation, the obligation to continue negotiations and/or discussions under these rules, nor is any member obliged to conduct negotiations and/or discussions in a pre-defined manner or to compensate any costs incurred by the CIISI-EU Community or any of the other members in connection with such negotiations and/or discussions.

The CIISI-EU Community is comprised of members listed in the Terms of Reference and decisions are made on a consensual basis by the Community as a whole. The key stakeholders in the overall implementation of CIISI-EU are: **the CIISI-EU Community Members; the CIISI-EU Secretariat; the third-party cyber threat intelligence provider<sup>3</sup> and the third-party platform provider (hereafter CIRCL (MISP))<sup>4</sup>.**

The current third-party cyber threat intelligence provider for CIISI-EU is Security Alliance B.V. The terms and conditions for the implementation and subsequent operation of CIISI-EU are set out in the Terms of Reference, the CIISI-EU Rulebook, the CIISI-EU Services Agreement (between the members and the third-party cyber threat intelligence provider) and the general agreement between the members and CIRCL (MISP).

The section below builds on the Terms of Reference and sets out further procedures and processes for the overall governance of CIISI-EU.

### 1. CIISI-EU Community Members

"The 'CIISI-EU Community' is open to members of the ECRB, i.e. pan-European financial infrastructures, central banks (in their operational capacity), critical service providers, ENISA and EUROPOL. The third-party cyber threat intelligence provider is not a CIISI-EU Community member<sup>5</sup> itself but provides services to the CIISI-EU Community members, and therefore participates in the information and intelligence exchange. Thus, the third-party cyber threat intelligence provider is a participant in CIISI-EU but not a member.

Authorities in their capacity as regulators, overseers and/or supervisors are not part of the CIISI-EU Community and regulatory reporting on cyber incidents and data breaches are

---

<sup>3</sup> Security Alliance B.V. has been selected as the third-party cyber threat intelligence provider for the CIISI-EU, including the use of their ThreatMatch portal.

<sup>4</sup> MISP (formerly known as Malware Information Sharing Platform) is an open source threat intelligence and sharing platform. It is a platform for sharing, storing and correlating Indicators of Compromises of targeted attacks but also threat intelligence such as threat actor information, financial fraud information and many more. A MISP instance is a mini-platform, set up at each member's institution, that will be connected to a centralised MISP platform accessible to all CIISI-EU members. This central MISP will be provided by the Computer Incident Response Centre in Luxembourg (CIRCL).

<sup>5</sup> CIRCL (MISP), the third-party platform provider, is also not a CIISI-EU Community Member.

outside the scope of the intelligence sharing within the CIISI-EU Community. Central banks that are part of the CIISI-EU Community must ensure that an internal “Chinese Wall” separates their respective Security Operating Centres and its system operator functions from the regulatory, oversight and supervisory functions it may have to the extent permitted by law. The list of the CIISI-EU Community member institutions is shown in Appendix B.”

*[CIISI-EU Terms of Reference – Section 5]*

The CIISI-EU Member’s Commitments are set out in Section 8 of the Terms of Reference, and Members should ensure that they abide by these commitments for the effective implementation of CIISI-EU.

In general, decisions of the CIISI-EU Community are agreed by consensus, i.e. there is no sustained opposition to substantial issues. When this is not possible, decisions will be ratified by a simple majority of the members.

## **2. Role of CIISI-EU Secretariat**

“The CIISI-EU Community will be served by a CIISI-EU Secretariat. The CIISI-EU Secretariat will act as a liaison towards the CIISI-EU Community members and the third-party cyber threat intelligence provider and CIRCL (MISP). In agreement with the CIISI-EU Community members, the CIISI-EU Secretariat can delegate administrative tasks to the respective third-party providers. The CIISI-EU Secretariat will rotate among the CIISI-EU Community members at agreed upon intervals.”

*[CIISI-EU Terms of Reference – Section 6]*

The CIISI-EU Secretariat will be provided for by one elected member of the CIISI-EU Community and will rotate every 18 months. The member providing for the CIISI-EU Secretariat will make available the appropriate resources during its term and will not be remunerated. The CIISI-EU Secretariat can be nominated for by any member and their appointment will be ratified by the Community as a whole via written consultation. A member can volunteer for more than one term.

During its tenure, the CIISI-EU Secretariat will have the following roles and responsibilities:

- i. The CIISI-EU Secretariat will be the central contact point for the CIISI-EU Community Members; the third-party cyber threat intelligence provider and CIRCL (MISP), and facilitate any decision making required for the ongoing implementation of CIISI-EU;
- ii. The CIISI-EU Secretariat will facilitate the 24 month review process of the Terms of Reference and the CIISI-EU Rulebook, and the annual stock take of the initiative to make improvements (as deemed necessary);
- iii. The CIISI-EU Secretariat will co-ordinate the monthly Trusted Group call and bi-annual in-person meetings, in close collaboration with the third-party cyber threat

intelligence provider. This will include setting the agenda for the calls and meetings; arranging the dates and times of the calls and meetings; chairing the calls and meetings; drafting (in conjunction with the third-party cyber threat intelligence provider) the summaries; and disseminating the agenda and summaries to the CIISI-EU Community in a timely fashion;

- iv. The CIISI-EU Secretariat will be the central contact point for any complaints by the CIISI-EU Community Members, and will facilitate any improvements to the initiative, if raised by the Community Members;
- v. The CIISI-EU Secretariat will liaise closely with the ECRB Secretariat, to raise any issues that require discussion at the ECRB;
- vi. The CIISI-EU Secretariat will liaise with the other stakeholders during any potential on/off boarding of the CIISI-EU Community Membership; and
- vii. The CIISI-EU Secretariat will liaise with potential information and intelligence sharing communities that could forge a strategic relationship with the CIISI-EU Community;<sup>6</sup> and
- viii. The CIISI-EU Secretariat will monitor the overall amount billed by the third-party cyber threat intelligence provider and CIRCL (MISP) to the CIISI-EU members for the provision of the CIISI-EU services. (see Section 5: Financial obligations).

Three months prior to the end of the tenure of the CIISI-EU Secretariat, the CIISI-EU Community Members will be requested to nominate a Community Member to take over the role and responsibilities of the CIISI-EU Secretariat, and this will be subject to a written procedure for agreement. The proposed Member with the majority will be appointed as the next CIISI-EU Secretariat.

In case there are no nominations, the current CIISI-EU Secretariat will nominate up to three appropriate CIISI-EU Community Members, in order of preference, and liaise with them directly to discuss and agree a handover. It is essential that the CIISI-EU Secretariat function continues and members should bear responsibility for its maintenance to ensure the long term success of the overall initiative.

### **3. Composition of the CIISI-EU Community – on/off boarding**

“Members are committed to participate in the CIISI-EU Community for an initial period of three years. Thereafter, CIISI-EU membership will automatically be re-affirmed on an annual basis unless a member wishes to withdraw its membership, which must be undertaken by written confirmation to the CIISI-EU Secretariat with a minimum of three months’ notice before the prescribed membership is due to be prolonged. In rare cases, the exclusion of an existing CIISI-EU member must be subject to a majority agreement by the other CIISI-EU members.

Requests for new membership, outside the existing CIISI-EU Community, needs to be sent to the CIISI-EU Secretariat and will be subject to an evaluation and voting process by the

---

<sup>6</sup> See Section 4 (Strategic Partnerships) of this Rulebook.

members. If there are no objections, the requesting party will enter a staging process for a period of one year, as a prospective member. During that period, the prospective member's participation, collaboration and overall activity will be evaluated by the collective CIISI-EU Community. At the end of that period, the prospective member has the option to decide whether or not to confirm its request for membership, and, provided the input is deemed satisfactory by the current full members of the CIISI-EU Community, there will be a proposal for full membership submitted to the CIISI-EU Community. If no objection from any CIISI-EU Community member is received, full membership will be granted."

*[CIISI-EU Terms of Reference – section 7]*

In terms of on-boarding new members, the following process will be applied:

- In cases of a change to the composition of the ECRB, the new member(s) will be offered the opportunity to join the CIISI-EU Community. In such cases, the new ECRB member will be required to sign the Terms of Reference; agree to observe the CIISI-EU Rulebook; sign the contractual terms with the third-party cyber threat intelligence provider and CIRCL (MISP); and contribute<sup>7</sup> to the initiative on the same terms as the other CIISI-EU Community Members. In order to facilitate this process, the prospective new member should liaise closely with the ECRB Secretariat and CIISI-EU Secretariat, and with the third-party providers for the operationalisation of the technical platforms.
- In cases where non-ECRB members would seek to join the CIISI-EU Community, the prospective member should send a proposal to the CIISI-EU Secretariat. The prospective member must ideally be a pan-European financial infrastructure, central bank (in an operational capacity) or critical service provider. In all cases a prospective member should provide an explanation and justification for their participation in the CIISI-EU Community, their value-add and how their participation will be in the public interest, supporting the safe and sound operation of the financial system in the European Union.

Upon receipt of the proposal for membership, the CIISI-EU Community will conduct an evaluation and vote for the on-boarding of the prospective member on a majority basis. The CIISI-EU Secretariat will be responsible for facilitating this end-to-end process.

In all cases, the on-boarding of a new member to the CIISI-EU Community must be subject to a non-objection by the ECRB.

The process for off-boarding are set out in the Terms of Reference. In rare cases that off-boarding may be a result of complaints or the CIISI-EU Member not observing the rules, there are further details set out in the Complaint Process below.

---

<sup>7</sup> In this context, "contribute" refers to active sharing of information and intelligence and participation on calls and in meetings.

#### 4. Complaint Process

“Each member shall abide by the membership rules, and undertakes to respect the confidentiality and integrity of the CIISI-EU Community, and of information and intelligence shared within the CIISI-EU Community.

If a member does not observe these rules, the other CIISI-EU Community members reserve the right to terminate its membership.

Termination will be effected by a motion from one member, supported by a simple majority vote of all members.”

*[CIISI-EU Terms of Reference – section 10]*

As a general principle, off-boarding/termination of a CIISI-EU Community Member as a result of a complaint is expected to be rare and such a decision will be taken in extreme circumstances and will be a measure of last resort. The process will take a three step approach, as below:

- i. Where a CIISI-EU Community Member does not observe the rules, or brings the overall initiative into disrepute by compromising the confidentiality or integrity of the other members, a member can confidentially raise a complaint to the CIISI-EU Secretariat in writing. The CIISI-EU Secretariat will liaise with the complainant and defendant, to conduct a fact-finding. Following the fact-finding, the CIISI-EU Secretariat will speak to the member in question, provide an initial warning – if appropriate - and ask the member to improve its participation, based on the facts.
- ii. In cases where the complaints persist and there have been no signs of remediation, the CIISI-EU Secretariat will set out the facts and raise the issues within the CIISI-EU Community, allowing all parties to provide their perspectives. In these circumstances, the CIISI-EU Community will look to resolve the issues in a pragmatic manner, to ensure the continuity of the entire membership.
- iii. Following the above two steps and in rare cases where the issue cannot be resolved, termination of the member will be supported by a simple majority vote of all members. The CIISI-EU Secretariat will inform the ECRB Secretariat accordingly.

In such circumstances, the terminated member must delete all data that it obtained during its participation in CIISI-EU; the member will be disconnected from the technical platforms; and they will not be refunded for the costs they incurred to the third-party cyber threat intelligence provider and CIRCL (MISP) for that calendar year. However, the member will not be liable to pay any further costs the following calendar year.

Under all circumstances, if the complainant requests it, their identify shall be kept confidential and will not be divulged to the CIISI-EU community.

## 5. Financial obligations

“Costs incurred for the provision of services from CIRCL (MISP) and the third-party cyber threat intelligence provider will be borne by members of the CIISI-EU Community on an equal basis and as set out in the contractual terms by the providers. Exceptions can be agreed by the ECRB. Costs related to participation at the in-person meetings will be borne by each member itself.

The *CIISI-EU ECRB Community Rulebook* sets out in more detail the financial implications (including the policies and procedures) related to changes in the number of participants of the CIISI-EU Community.”

*[CIISI-EU Terms of Reference – section 14]*

CIISI-EU follows the principle that each CIISI-EU member bears its own costs for participating in and contributing to CIISI-EU and its community. The costs for the provision of services by the third-party providers will be borne by members on an equal basis, as set out in the contractual terms by these respective third-party providers. It is the responsibility of each member to ensure that their liabilities are paid in a timely manner and in accordance with the contractual terms. The third-party cyber threat intelligence provider and CIRCL (MISP) will provide a financial statement to the CIISI-EU Secretariat which consolidates the fees charged to each member and the associated payment status.

In cases where a member has been involuntarily off-boarded/terminated and removed from the membership, the costs for the remaining - contractually agreed upon - full calendar years will be spread equally amongst the remaining members of the community. The costs for the calendar year in which a member was off-boarded will be paid by the off-boarded member.

In cases where a new member has joined the Community, the new member will be liable to pay the same amount as the other members and in line with the contractual terms agreed with the third-party providers (i.e. the third-party cyber threat intelligence provider and CIRCL (MISP)).

In cases where payments have not been made to the third-party cyber threat intelligence provider and CIRCL (MISP), the aforementioned providers may escalate the issue to the CIISI-EU Secretariat.

If a member leaves voluntarily, they will have to fulfil their full financial obligations, in accordance with the respective contracts.

## 6. Review process

Every 24 months, the aforementioned stakeholders will review the Terms of Reference and CIISI-EU Rulebook and update them accordingly. The review will be led by the CIISI-EU Secretariat; members will be given the opportunity to review the documents and provide any updates via written procedure; and the decision for the updated documents will be ratified

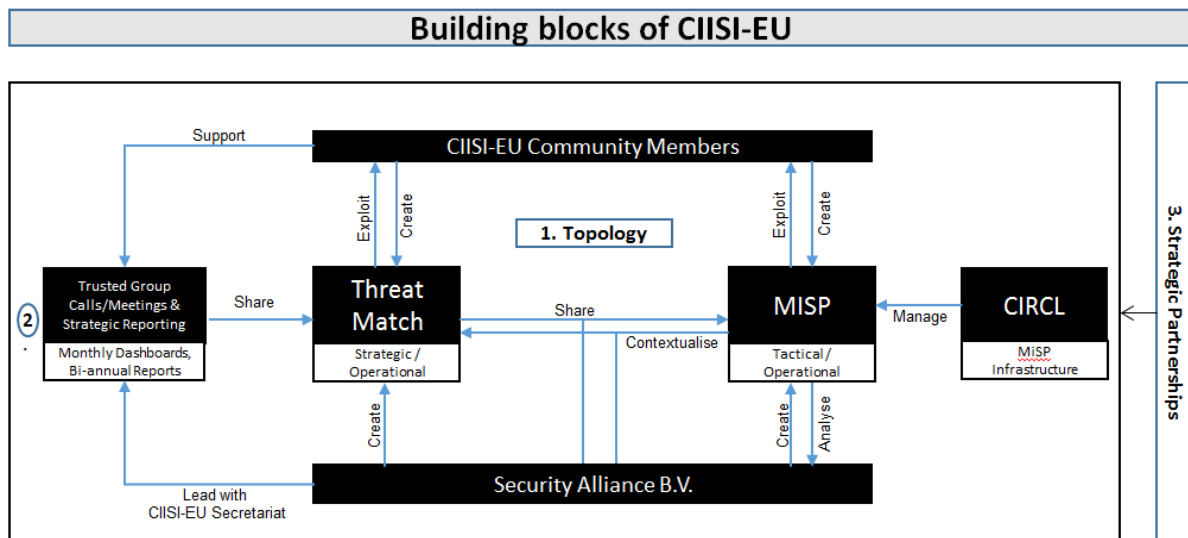


by the CIISI-EU Community Members. The CIISI-EU Secretariat will inform the ECRB Secretariat on the outcome of the review process.

A core principle of CIISI-EU is learning and evolving, and as the initiative develops over time, it is important that the CIISI-EU Community assesses the implementation of the initiative and continuously looks to improve it. Although this is an evolving process and changes to operations can be made at any point, the CIISI-EU Secretariat should facilitate at least an annual discussion with the stakeholders, to take stock and to consider how improvements can be made.

## Section 2. Building blocks of CIISI-EU

Sharing across the CIISI-EU Community is based on a number of building blocks:



### 1. Topology

#### a. Threat Intelligence Feeds:

CIISI-EU community members are expected to keep their existing commercial / open source threat intelligence feeds. If information from these sources are relevant for the CIISI-EU Community, members can share them voluntarily and on a best efforts basis to the extent legally and contractually possible. The process for evaluating such information and intelligence and the modalities of sharing them are set out in the next sections of this Rulebook (Sections 3 and 4).

#### b. MISP:

The CIISI-EU Community Members commit to using MISP as the central platform for information sharing. CIRCL will be responsible for hosting the CIISI-EU MISP platform; each member will connect to the CIRCL's hosted central MISP platform, in one of three ways: 1) a CIISI-EU Member will host its own MISP instance at its premises, which will connect to the central MISP platform; 2) a CIISI-EU Member may connect directly to the central MISP platform using web browser; or 3) a CIISI-EU member will interface its existing, in-house technical platform to the central MISP platform. In all cases, the network of MISP connections will synchronise with each other and the collective will operate as a closed and trusted group.

The terms and conditions for the use of the MISP platform are set out in the general agreement between the CIISI-EU Community Members and CIRCL, the third-party platform provider.

It is the responsibility of each CIISI-EU Community Member to ensure the confidentiality, integrity and availability of its own MISP Instance or equivalent connection (including the information held therein); to maintain an up-to-date list of users at their organisation; and to ensure that access rights are granted, amended and/or removed to new joiners, leavers and movers as required by the organisation.

In cases where CIISI-EU Community Members require training for the use of MISP, the CIISI-EU Secretariat should liaise with CIRCL to arrange such collective sessions. In case a member requires specific bilateral training, it should interact with CIRCL directly to arrange this, at its own costs.

The principles, rules and conventions for sharing information and intelligence on MISP are set out in Sections 3 and 4, and the Sharing Schema in Annex C.

**c. Security Alliance B.V. ThreatMatch Portal:**

In addition to having access to the MISP platform, the CIISI-EU Community Members will have access to the third-party cyber threat intelligence provider's (Security Alliance B.V.) own threat intelligence portal and interactive collaborative space – ThreatMatch. The principles, rules and conventions for sharing information and intelligence on the ThreatMatch Portal are set out in Sections 3 and 4 of this Rulebook, and the annexed Sharing Schema (Annex C).

Each CIISI-EU Community Member is allocated up to ten users that can access the ThreatMatch Portal. Each individual CIISI-EU Community Member can order additional user licences in case of need; the costs related to the additional user licences have to be covered by the respective CIISI-EU Member. It is the responsibility of each CIISI-EU Community Member to inform the third-party cyber threat intelligence provider of the users that will require access to the portal; to maintain an up-to-date list of users at their organisation; and to ensure that access rights are granted, amended and/or removed to new joiners, leavers and movers as required by the organisation.

In cases where CIISI-EU Community Members require training for the use of ThreatMatch Portal, the CIISI-EU Secretariat should liaise with the third-party cyber threat intelligence provider to arrange such collective sessions. In case a member requires specific bilateral training, it should interact with the third-party cyber threat intelligence provider directly to arrange this, at its own cost.

**d. Information and Intelligence Sharing:**

In general, the CIISI-EU Community Members will use the MISP platform and ThreatMatch Portal to share information and intelligence with each other. Each CIISI-EU Community Member will elect what information or intelligence is important enough to warrant disseminating onto the shared platform and portal.

The third-party cyber threat intelligence provider will have access to the centralised MISP platform and ThreatMatch Portal and will add value through the synthesis of strategic analysis based on the collective tactical and operational intelligence on the shared MISP platform and the ThreatMatch Portal, and based on their own knowledge of the cybersecurity threat landscape.

The principles, rules and conventions for sharing information and intelligence on the MISP platform and ThreatMatch Portal are set out in Sections 3 and 4 of this Rulebook, and the annexed Sharing Schema (Annex C).

## **2. Trusted Group calls and in-person meetings & Strategic Reporting**

Core foundations of CIISI-EU are the Trusted Group calls and in-person meetings. These calls and meetings will be held on a regular basis, with the CIISI-EU Community Members and the third-party cyber threat intelligence provider in attendance, to establish and foster trust within the CIISI-EU Community.

At least one staff member from each CIISI-EU Community Member is expected to attend the calls and meetings. The staff member should ideally be from the Security Operating Centre, cybersecurity function, threat intelligence function or operational function. Each CIISI-EU Community must nominate at least one staff member to attend these calls and meetings, and may nominate up to three individuals, who can act as an alternate.

### **a. Trusted Group calls and Trusted Group meetings**

The Trusted Group calls will be held once per month, typically on the last Friday of each month.

The Trusted Group in-person meetings will be held twice per year. The in-person meetings should be hosted by a CIISI-EU Community Member, and should alternate each meeting. CIISI-EU Community Members can convene an ad-hoc in-person meeting at any time, if there is general agreement to do so.

In case of any specific items for discussion for the Trusted Group call, any CIISI-EU Community Member should send any specific questions or discussions points to the CIISI-EU Secretariat and the third-party cyber threat intelligence provider at least three working days before the call and at least five working days before the meeting. Although in some cases, these timelines can be shortened, given the dynamic nature of the threats; however, consideration should be given to the third-party cyber threat intelligence provider's ability to deliver robust responses in case of shortened timelines for information and analysis.

The CIISI-EU Secretariat will liaise with the third-party cyber threat intelligence provider to finalise the agenda for each call and meeting, taking into account any questions or discussion points raised by CIISI-EU Community Members, and send this out to the CIISI-EU Community no later than two working days before the call and no later than seven working days before the meeting.

In general, the agendas of the call and meeting could include:

- Welcome and opening remarks by the CIISI-EU Secretariat;
- Overview of the cyber threat landscape by the third-party cyber threat intelligence provider;
- Sharing of best practices by a CIISI-EU Community Member;

- Information and intelligence exchange – discussion by all; and
- Closing

The discussions during the Trusted Group call and meeting are confidential and should not be disclosed outside of the Trusted Group, or beyond the organisations that constitute the CIISI-EU Community, unless explicitly and unanimously agreed upon by the participants in the Trusted Group call and/or meeting.

No minutes will be drafted for the Trusted Group calls and meetings. The CIISI-EU Secretariat, in close collaboration with the third-party cyber threat intelligence provider, will make available a summary of the analysis as presented by the third-party cyber threat intelligence provider to the CIISI-EU Community shortly after the call and/or meeting.

CIISI-EU Community Members should openly share information and intelligence with each other during the calls and meetings, as well as best practices of their internal cybersecurity measures and innovations, to foster trust and collaboration amongst the Community.

Depending on the circumstances, and in case of urgent need (e.g. large cyber incident), the CIISI-EU Community Members can invoke an ad-hoc Trusted Group call and/or in-person meeting. In such cases, the respective member should liaise with the CIISI-EU Secretariat.

#### **b. Strategic Reporting**

The third-party cyber threat intelligence provider will produce strategic intelligence and bi-annual reports, focussed at Board level and written in business language, as well as monthly threat dashboards and bespoke reports (when necessary). The third-party cyber threat intelligence provider will present its bi-annual reports at the bi-annual in-person ECRB meetings.

The bi-annual reports and monthly dashboards will be made available on the ThreatMatch Portal.

The CIISI-EU Secretariat and the third-party cyber threat intelligence provider will liaise with the ECRB Secretariat to ensure that the bi-annual reports are prepared and made available to the ECRB members for their bi-annual meetings<sup>8</sup>.

In general, the bi-annual reports and monthly dashboards should cover the following topics,

- Monthly threat (or six monthly) threat assessment, with evidence and analysis;
- Strategic intelligence update by threat actor category (i.e. nation state activity, organised crime group activity, hacker and researcher activity, hacktivist activity, insider activity);
- Significant global cyber events of relevance to the financial system; and

---

<sup>8</sup> In case an ECRB meeting does not take place – irrespective of the reason – a bi-annual report will be drafted and distributed among the ECRB members.

- Quarterly horizon scanning, outlining the global political, economic, social, technological, legal, environmental and military developments, and the underlying analysis of their potential impact on the financial system.

The strategic reporting is a key cornerstone of CIISI-EU, and will be an iterative process. CIISI-EU Community Members should continuously review the outputs and liaise with the CIISI-EU Secretariat and the third-party cyber threat intelligence provider to suggest improvements, so the reporting can add the most value for each organisation and their cyber resilience capabilities.

### **3. Strategic Partnerships**

"The CIISI-EU Community will build strategic relationships with other information sharing communities to enrich the information and intelligence and to bridge communities. All strategic relationships must be agreed upon by all members of the CIISI-EU Community on a unanimous basis."

*[CIISI-EU Terms of Reference – section 3]*

The CIISI-EU Community will have the possibility to build strategic relationships with other information sharing communities to enrich the information and intelligence and to bridge communities.

Strategic partnerships should be carefully considered and should add value to both communities. The CIISI-EU Secretariat will be the central liaison for discussions with potential strategic partners, and will present the proposal to the CIISI-EU Community. All strategic relationships must be agreed upon by all members of the CIISI-EU Community on a unanimous basis. The CIISI-EU Secretariat will inform the ECRB Secretariat accordingly.

Once strategic partnerships have been established, the CIISI-EU Community will determine, through close discussions with the partner, how the partnership will be operationalised and how both communities will interact with each other. For example, on an ad-hoc basis, members from the strategic partner may be invited to the Trusted Group call or in-person meeting to share information and intelligence, best practices, etc.

### **Section 3. Principles of information and intelligence sharing**

#### **a. Levels of information and intelligence - Strategic, Operational and Tactical**

As set out in the Terms of Reference, the CIISI-EU Community will share Strategic, Operational and Tactical information and intelligence.

Building on this, the CIISI-EU Community has adopted the NATO standard definitions<sup>9</sup> for these levels of information and intelligence. The CIISI-EU Community Members will share information and intelligence at all levels in order to support decision makers in all roles. Inherently information and intelligence sharing initiatives have focused on the operational and tactical intelligence needs. One of CIISI-EU's core objectives is "to synthesize and actively propagate the sharing of strategic intelligence in addition to operational TTPs and tactical IOCs indicators".

##### **i. Strategic Information and Intelligence**

The sharing of strategic information and intelligence drives decision makers and planning in the mid to long term, typically at senior level. In this instance, strategic information and Intelligence supports the CIISI-EU Community on setting strategy and objectives based on the changing landscape and future considerations.

*NATO definition: 'The level at which a nation or group of nations determines national or multinational security objectives and deploys national, including military, resources to achieve them'.*

##### **ii. Operational Information and Intelligence**

Sharing of operational information and intelligence drives intelligence and security operations in order to support, 'Business as usual' security objectives and decision making.

*NATO definition: 'Intelligence required for the planning and conduct of 'campaigns' at the operational level'.*

##### **iii. Tactical Information and Intelligence**

Tactical intelligence is usually data and sometimes information. Inherently this is data or sets of data that are related to adversary actions or planned actions. It is usually but not always 'Indicators of compromise' (IOCs) and primarily supports 'detection operations'.

*NATO definition: 'Intelligence required for the planning and execution of operations at the tactical level'.*

---

<sup>9</sup> <https://nso.nato.int/natoterm/Web.mvc>

As set out in the Terms of Reference, the scope of sharing strategic, operational and tactical information and intelligence encompasses the following:

1. Indicators of Compromise (IOCs)
2. Tactics, Techniques, and Procedures (TTPs)
3. Security Alerts
4. Threat Intelligence Reports
5. Tool Configurations
6. Motives and goals of threat actors

The sharing of any of the above must be in line with a number of principles, which govern the overall implementation of CIISI-EU and its members. These are set out below.

#### **b. Overarching Principle**

The overarching principle for the sharing of information and intelligence within the CIISI-EU Community is to deliver information to the community as quickly and accurately as possible in a format that is accessible by all in order to allow members to better protect themselves, and in so doing, achieve 'herd immunity' against current and likely future threats.

Each member of the CIISI-EU Community is responsible for contributing the information and intelligence and insights they gain within their own organisation to the CIISI-EU community. Every member is expected to be an active participant, i.e. not only benefiting by consuming but also by actively contributing.

#### **c. General principles for sharing information and intelligence**

In order to achieve the overall objectives set out within the Terms of Reference, the CIISI-EU Community will apply the following information and intelligence sharing principles:

- i. **Actionable and Relevant.** The information and intelligence needs to be actionable and relevant to the end-user.
- ii. **Common taxonomy.** The nature of information and intelligence being shared must be commonly agreed by the CIISI-EU Community, following the 'CIISI-EU Sharing Schema' (see Annex C). This will avoid unnecessary duplication of effort and ensure efficient and economical use of resources.
- iii. **Centralised Control.** The CIISI-EU Secretariat will operate as the central function providing direction to the third-party providers and support in ensuring the centralized and easy flow of information
- iv. **Responsiveness.** The CIISI-EU Community Members must be responsive to the needs of other members to support their needs in a timely manner.
- v. **Objectivity.** When creating and sharing intelligence and assessments, effort must be made to remove any potential bias and to present objectively.



- vi. **Systematic Exploitation.** CIISI-EU Community Members and the third-party cyber threat intelligence provider must actively and continuously exploit the information and intelligence shared in the platforms in order to provide additional insights.
- vii. **Source Protection.** The Traffic Light Protocol (TLP) – see Annex B - must always be used and followed.
- viii. **Continuous Review.** CIISI-EU Community Members, the CIISI-EU Secretariat and the third-party providers will continually review both the intelligence they share and the processes by which they share it, in order to continuously enhance their value to the community
- ix. **Format and accessibility.** CIISI-EU Community Members must use the prescribed formats, protocols and taxonomies prescribed in this document to allow the information and intelligence to be fully utilised, exploited and easily consumed.
- x. **Timeliness.** Timeliness is a crucial feature of information and intelligence sharing for it to be effective at mitigating potential cyber-threats and as an input into response and recovery. Information and intelligence must be disseminated to the CIISI-EU Community in an accurate and timely manner.
- xi. **Compliant.** The information and intelligence shared must comply with applicable Laws and Regulations (e.g. GDPR, copyright, other legal/contractual obligations, etc).

#### **d. Principle to determine what to share**

CIISI-EU Community Members should endeavour to share as much information and intelligence that they assess to be accurate, of relevance and that meets the objectives of CIISI-EU.

The CIISI-EU Community has adopted the “MoSCoW” principle to help organisations understand what they should share - **MoSCoW: Must, Should, Could, Wont.**

All sharing must be in line with Section 13 (Data Privacy) of the Terms of Reference.

##### **i. Must Share**

As a guiding principle, each member should share all the information and intelligence where they are the originator (author) or where they have been given permission to share with other parties. If the member answers, ‘yes’ to the following: ‘would a fellow CIISI-EU member benefit from having of knowing X’, then the intelligence **must** be shared.

Though, ‘need-to-know’ is a well-known intelligence concept, ‘need-to-share’, is less known, but is fundamentally more important to success. Effectively the wider and faster the sharing, the less likely there will be an ‘intelligence failure’.

Examples include - (please see the Sharing Schema in Annex C for full details):

- **Cyber Security Incidents** (and the associated metadata) related to the operation of financial infrastructures and involving an adversary either against your organisation, another participant, another financial organisation or an organisation within the supply chain; and
- **Knowledge of an adversary** including details of their infrastructure, TTPs, Modus Operandi, Malware, Operations, campaigns, intent, or any information and intelligence that will better allow its profiling, thus supporting prediction, detection, response and remediation efforts.

## ii. **Should Share**

CIISI-EU has a wider remit than the sharing of technical information and intelligence that supports Security Operations. Members **should** share information and intelligence or aspects that support the wider cyber resilience mission. For instance, participants should share knowledge of how they are detecting and responding to particular techniques or malware families.

Members should not just reply to automated feeds but share **insights and context** on wider issues affecting the threat landscape, such as political or geopolitical events, technological advances or legal and compliance changes.

Examples include: (please see the Sharing Schema for full details)

- Enhancement of or explanation in the context of a specific tool, a MITRE ATT&CK Technique Detection method;
- YARA rules for the detection of Malware; and
- Insights into compliance changes in non-EU nations that will effect data privacy or information security.

## iii. **Could Share**

Business as usual, standard operating procedures and best practices are as valuable as intelligence insights if it supports the operational effectiveness of a Security Operations team. Where possible, members **could** look to share the methodologies that they believe would be of value to the community.

This is particularly true should the methodology or practice be new or innovative.

Examples include - (please see the Sharing Schema in Annex B for full details):

- Internal intelligence reporting, intelligence dashboarding or security reports
- Success Metrics
- Target Operating Models
- Policy, Procedure, Process or Methodology documents or flowcharts

#### **iv. Won't Share**

Members should always be aware of the legal and commercial environment in which they exist. Whilst the Terms of Reference describes the relevant legal restrictions, in practice intelligence practitioners should be aware that they cannot share, for example:

- Personal data that is contrary to data privacy legislation in their own countries;
- Details that could be seen as 'targeting of an individual';
- Derogatory or inflammatory material of any kind;
- Any information or intelligence where the quality of the original source cannot be measured or that could support any false information campaigns; and
- Any information or intelligence that does not support the overall mission of CIISI-EU.

In all cases, when sharing information or intelligence that has originated from an outside organisation, the participant should ensure there is no legal or commercial restrictions on the sharing of that material.

## Section 4. Taxonomies, frameworks, terminology and conventions for sharing

Once CIISI-EU Community Members have determined whether they will share a form of strategic, operational and/or tactical information and intelligence, based on the principles set out in Section 3, they should do so in line with the taxonomies, frameworks, terminology and conventions set out below. This will ensure a common understanding and approach to sharing, and ensure that the initiative operates effectively.

The taxonomies, frameworks, terminology and conventions for sharing are based on well known, well used and open source protocols. They have also been chosen as they are all either mapped to MISP taxonomies or exist as tags within MISP. These taxonomies, frameworks and terminologies also integrate with ThreatMatch.

In summary, the CIISI-EU Community will share information and intelligence using the **MITRE ATT&CK and STIX 2.1 Frameworks**. Taxonomies for integration between these elements exist within the MISP Taxonomies guidelines (<https://www.misp-project.org/taxonomies.html>). When integrating with MISP, the MISP Framework is preferred over the STIX to MISP converter. When integrating with ThreatMatch, either MISP or STIX is suitable.

### a. Taxonomies

Taxonomies currently in use for CIISI-EU are noted below. This may change or be updated as CIISI-EU matures and MISP develops. The below is for the sharing of Threat Alerts, Incidents, Malware Analysis and Adversary Operations. The sharing of Actor, Malware and Country Profiles will be done using **MISP Clusters**. The below are open source, freely available taxonomies available within MISP.

- Admiralty-scale
- Estimative-language
- TLP
- TM\_Incident
- MISP:alert\_type
- ThreatMatch:Sector
- ThreatMatch:Malware\_type

### b. Frameworks

**MITRE ATT&CK** was created by and maintained by the MITRE Corporation.<sup>10</sup> ATT&CK will be used by the CIISI-EU members when describing the Tactics, Techniques and Procedures of an

---

<sup>10</sup> <https://www.mitre.org/>

adversary. CIISI-EU will be adopting the latest version of ATT&CK which includes the adoption of Sub-Techniques<sup>11</sup>. New MISP taxonomies will be built for this integration.

**STIX™** (Structured Threat Information Expression) is a language for expressing cyber threat and observable information. It was created by and is maintained by Oasis Open.<sup>12</sup>

The documentation for the latest version of STIX is available here: <https://docs.oasis-open.org/cti/stix/v2.1/stix-v2.1.html>.

Where integration directly into MISP is not possible using the MISP format, STIX 2.1 should be used.

### **c. Terminology**

Critical to the successful dissemination of an information and intelligence assessment is consistency of language and terminology and its use. As identified above in the MISP taxonomies, CIISI-EU will be communicating via the use of '**Estimative-Language**'.

This framework is widely used in NATO and Allied Nations. Estimative-Language has also been used as a historical precedent in MISP and will allow for great international adoption and recognition.

Further details on the Estimative-Language are set out in Annex A.

### **d. Conventions for sharing**

The Traffic Light Protocol (TLP) used within the CIISI-EU Community has been adapted from the IS TLP version 1.1 as published by Trusted introducer at <https://www.trusted-introducer.org/ISTLPv11.pdf> and will be used to facilitate the information and intelligence exchange within the CIISI-EU Community. Information and intelligence will be shared orally in the Trusted Group calls/in-person meetings and through the use of the shared MISP platform. Each member may classify (or designate) each piece of information and intelligence they provide with one of four information sharing levels, in accordance with their wishes for the handling of their information by other members.

It is the responsibility of the member offering the information and intelligence to specify its sharing level and for all to respect the designated sharing levels of all information and intelligence offered. If the member offering the information and intelligence does not designate a sharing level, the information and intelligence will be assumed to be TLP:AMBER, and the source (identity of the providing organization) be assumed to be TLP:RED. If any member has any doubt whether information and intelligence is TLP:RED, they must contact the person who offered it before taking any action on it.

---

<sup>11</sup><https://medium.com/mitre-attack/attack-with-sub-techniques-is-now-just-attack-8fc20997d8de>

<sup>12</sup>[https://www.oasis-open.org/committees/tc\\_home.php?wg\\_abbrev=cti](https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cti)

The Traffic Light Protocol (TLP) conventions for sharing are set out in Annex B.

**e. Sharing schema**

The overall sharing of information and intelligence, at the three levels (strategic, tactical and operational) will be done in line with the aforementioned principles, taxonomies, frameworks, terminology and conventions. This overall approach, when consolidated, represents the Sharing Schema as set out in Annex C.

# ***Annexes***

## **Annex A: Estimative-Language**

The below is extracted from the MISP taxonomy which in turn has come from Community Directive 203 (ICD 203) and JP 2-0, Joint Intelligence.

**Likelihood-probability** properly expresses and explains uncertainties associated with major analytical judgments - Analytical products should indicate and explain the basis for the uncertainties associated with major analytical judgments, specifically the likelihood of occurrence of an event or development, and the analyst's confidence in the basis for this judgment. Degrees of likelihood encompass a full spectrum from remote to nearly certain.

Analysts' confidence in an assessment or judgment may be based on the logic and evidentiary base that underpin it, including the quantity and quality of source material, and their understanding of the topic.

Analytical products should note causes of uncertainty (e.g., type, currency, and amount of information, knowledge gaps, and the nature of the issue) and explain how uncertainties affect analysis (e.g., to what degree and how a judgment depends on assumptions). As appropriate, products should identify indicators that would alter the levels of uncertainty for major analytical judgments.

Consistency in the terms used and the supporting information and logic advanced is critical to success in expressing uncertainty, regardless of whether likelihood or confidence expressions are used.

- estimative-language:likelihood-probability="almost-no-chance"
  - Almost no chance - remote - 01-05%
- estimative-language:likelihood-probability="very-unlikely"
  - Very unlikely - highly improbable - 05-20%
- estimative-language:likelihood-probability="unlikely"
  - Unlikely - improbable (improbably) - 20-45%
- estimative-language:likelihood-probability="roughly-even-chance"
  - Roughly even change - roughly even odds - 45-55%
- estimative-language:likelihood-probability="likely"
  - Likely - probable (probably) - 55-80%
- estimative-language:likelihood-probability="very-likely"
  - Very likely - highly probable - 80-95%
- estimative-language:likelihood-probability="almost-certain"
  - Almost certain(ly) - nearly certain - 95-99%

**Confidence-in-analytic-judgment** is based on three factors: number of key assumptions required; the credibility and diversity of sourcing in the knowledge base; and the strength of argumentation.



Each factor should be assessed independently and then in concert with the other factors to determine the confidence level. Multiple judgments in a product may contain varying levels of confidence. Confidence levels are stated as Low, Moderate, and High.

- estimative-language:confidence-in-analytic-judgment="low"
  - Uncorroborated information from good or marginal sources. Many assumptions. Mostly weak logical inferences, minimal methods application. Glaring intelligence gaps exist. Terms or expressions used: 'Possible', 'Could, may, might', 'Cannot judge, unclear.'
- estimative-language:confidence-in-analytic-judgment="moderate"
  - Partially corroborated information from good sources. Several assumptions. Mix of strong and weak inferences and methods. Minimum intelligence gaps exist. Terms or expressions used: 'Likely, unlikely', 'Probable, improbable' 'Anticipate, appear'.
- estimative-language:confidence-in-analytic-judgment="high"
  - Well-corroborated information from proven sources. Minimal assumptions. Strong logical inferences and methods. No or minor intelligence gaps exist. Terms or expressions used: 'Will, will not', 'Almost certainly, remote', 'Highly likely, highly unlikely', 'Expect, assert, affirm'.

## Annex B: Conventions for sharing – TLP Protocol

### **RED:**

Non-disclosable information and restricted to members present at the telco or meeting only. If a document is received, then the document is solely for that individual and no other parties. Members must not disseminate the information outside of that exchange. TLP:RED information may be discussed during the telco/in-person meeting, where all members present have signed up to these rules. The meeting minutes will only mention the topic but no details will be shared in the minutes (they can be obtained on a bi-lateral basis).

The use of TLP:RED should be limited as much as possible as it considerably restricts the possibility of acting upon the shared information. Indicators exchanged in a TLP:RED message will be considered TLP:AMBER unless they can be specifically attributed to a CIISI-EU Community member. In that case, they will be kept TLP:RED and the receiving party cannot share them within their organization. This will allow the receiving party to use the indicators that were shared to protect or defend itself. The rest of the message will remain TLP:RED.

### **AMBER:**

Limited disclosure and restricted to members of the CIISI-EU Community and those within their organizations (whether direct or affiliate's employees, consultants, contractors or outsource-staff working in the organization and affiliates, that do not have a conflict of interest with any CIISI-EU member or provider) who have an unequitable need to know in order to take action and may be used by the receiving party only to protect or defend itself or its affiliates.

### **GREEN:**

Information can be shared with other organizations, information exchanges or individuals in the network security community at large, but not published or posted on the web. Information cannot be shared with vendors without prior approval by the source of the information.

### **WHITE:**

Information that is for public, unrestricted dissemination, publication, web-posting or broadcast. Any member may publish the information, subject to copyright.

## Annex C: Sharing Schema

The '**Sharing Schemas**' have been designed to help CIISI-EU members understand what information or intelligence they should be **sharing**. It is a guide that helps the members know what the minimum requirements are for each type of information and intelligence they are sharing and what the preferred dissemination platform should be.

*For example: CIISI-EU Member X has received a highly **targeted spear-phishing email***

*Instruction:* Refer to the tables below and establish that this is a **Tactical piece of information**, of which fellow CIISI-EU members would benefit from having or knowing it. As such, CIISI-EU Member should share this via the **MISP platform**. When sharing, include **details, the type of incident (Spear-phishing), a brief description, who this information should be shared with and a TLP level**. Also, include all **relevant Tags (IOCs), dates, target geographies or sectors and any other associated events**. If known, one could also **associate an actor**.

*Further developments:* Following an investigation, the CIISI-EU Member X realises that this was part of a bigger campaign against the organisation. As such the CIISI-EU Member X should continue to upload the tactical level data, linking them together. However, after the incident is closed, the **CIISI-EU Member X should share its incident report that contains more verbose commentary with important actions, recommendations and assessments**. As such, the CIISI-EU Member X could decide to **upload this report to the ThreatMatch Portal** using the 'Reporting' module, disseminating it to a peer organisation. The CIISI-EU Member X can also then redact some more sensitive elements and disseminate it the whole CIISI-EU Community.

## Annex C: Sharing Schema – Strategic Intelligence Sharing

Level	Strategic Reporting					
<b>Description</b>	This is inherently information and intelligence that drives decision makers and planning in the mid to long term, typically at senior level. In this instance, Strategic Intelligence supports the ECRB on setting strategy and objectives based on the changing landscape and future considerations. NATO - The level at which a nation or group of nations determines national or multinational security objectives and deploys national, including military, resources to achieve them.					
<b>Potential Sources</b>	Governments, Regulators, International Institutions, Universities, Political & Strategic Studies Orgs, Geo-political analysts, Financial Market Analysts, News and Media, Human Intelligence, Trend analysis of Tact & Op data					
<b>Preferred Dissemination Medium</b>				<b>PRIMARY</b>	<b>SECONDARY</b>	
<b>Intelligence Type</b>	<b>What to Share</b>	<b>Required Content</b>	<b>MSC<sup>13</sup></b>	<b>ThreatMatch Taxonomy</b>	<b>MISP Taxonomy</b>	<b>Note(s)</b>
<b>Incidents</b>	Incidents of a <b>strategic nature</b> not previously covered in 'Threat Incidents Tactical' or 'Threat Incidents Operational'	Originator Type of Incident Title Description Start DTG End DTG Target Target Sector Target Geo Ass. Actors Ass. Events Dissemination TLP Levels	M M M M S S M S S S C M M	<i>TM -&gt; Incident</i> Show Org Name Incident Tag Title Overview Date Date Targets Sector Relevance Target Geography Associated Profiles Associated Profiles Distribution TLP	<i>MISP -&gt; Event</i> orgc_id TM:Incident MISP Taxonomy info attribute > external analysis > text first_seen (external analysis attribute) last seen (external analysis attribute) Text Tag TM:Sector MISP Taxonomy MISP Galaxy Geography see SecAlliance actor profile galaxy Event ID Sharing Group TLP Tag - MISP Taxonomy	

<sup>13</sup> MoSCoW Principal – Must Have, Should have, Could have, Wont have

		Other Tags	S	Overview Tags	Tags	
<b>Threat Alerts</b>	Alerts of a <b>strategic nature</b> not previously covered in 'Threat Alerts Tactical' or 'Threat Alerts Operational'	Originator Type of Threat Title Description Assessment Recommendation When Discovered When Occurred Threat Severity App. Sectors Ass. Events Ass. Actors Dissemination TLP Level Other Tags	M M M M S S M S M S C S M M S	<i>TM -&gt; Alert</i> Show Org Name Alert Type Title Overview Assessment Recommendation Discovery Date Event Date Severity Sectors Associated Profiles Associated Profiles Distribution TLP Tags	<i>MISP -&gt; Event</i> Org_id TM:Alert_Type MISP Taxonomy info attribute > external analysis > text attribute > external analysis > text attribute > external analysis > text publish_timestamp timestamp Threat_level_id TM:sector Event ID see SecAlliance actor profile galaxy Sharing Group TLP Tag MISP Taxonomy Tags	
<b>Threat Reporting</b>	Actor mid to long term intent and motivations Regulatory or Legal Threats Economic/Market influences Technology Developments Social changes Environmental / non-traditional threats Adversary Nation	Title Date Exec Summary Content Assessment Sectors Assoc. Actors Assoc. Events Assoc. Ops Assoc. Incidents Dissemination	M M S M M S S S S S M	<i>ThreatMatch -&gt; Report</i> Title Date Exec Summary Intelligence Report Assessment Sector Relevance Associated Profiles Associated Profiles Associated Profiles Associated Profiles Distribution	<i>MISP -&gt; Event</i> info date attribute > external analysis > text attribute > external analysis > text TM Sector MISP Taxonomy TM Actor Galaxy Event ID Operation Events Incident Events Sharing groups	

	developments National, regional, and international political impacts Regional/geographic security impacts Sector Reporting Regional Reporting	TLP Tags	M S	TLP Tags	TLP tags Tags	
<b>Nation State Profiling</b>	Profiling of Nation States with an offensive cyber capability	Author Name Demographics Introduction Capabilities Agencies and Actors Hosted Actros Ass. Incidents Ass. Operations Pol. Landscape Geopolitics Actor Profiles Dissemination TLP	M M M M S S S S S S M M	<i>ThreatMatch</i> -> <i>Country Profile</i> Show Org name Title Key facts Summary Capability Nation State Actors and Agencies Home Grown Actors Incidents Operations Domestic Politics Geopolitics Actor Profiles Dissemination TLP	NA	Security Alliance Nation State profiles are currently only available in ThreatMatch

### Annex C: Sharing Schema – Operational Intelligence Sharing

Level	Operational Intelligence					
<b>Description</b>	This can be data, information or Intelligence that drives intelligence and security operations in order to support, 'Business as usual' security objectives and decision making. NATO - Intelligence required for the planning and conduct of 'campaigns' at the operational level.					
<b>Potential Sources</b>	Incident reports, Malware analysis, Threat Hunting, Intrusion Detection, Incident Response reports, Vendor reporting, Security Operations, Security tools and network infrastructure / logging, Vendor Reporting, Dark Web, Deep Web, Breach Sites, Social Media, Technical Forums, Vendor sites, Suppler Sites, 3rd party infrastructure, Paste and Dump sites, Forums and Repositories, Human Intelligence (HUMINT), Vulnerability databases, Exploit databases, Threat Hunting, Gov. and Agency Sources					
<b>Preferred Dissemination Medium</b>				<b>PRIMARY</b>	<b>SECONDARY</b>	
<b>Intelligence Type</b>	<b>What to share</b>	<b>Required Content</b>	<b>MSC</b>	<b>MISP Taxonomy</b>	<b>ThreatMatch Taxonomy</b>	<b>Note(s)</b>
<b>Incidents</b>	Any <b>analysis, reporting and or assessment</b> from the following types of incidents:  ATM Attacks Botnet Activity Business Email Compromise Exec Targeting Crypto Mining Data breach/compromise Data Dump Data Leakage	Originator Type of Incident Title Description Start DTG End DTG Target Target Sector Target Geo Ass. Actors Ass. Events Dissemination TLP Levels Other Tags	M M M M S S M S S S C M M S	<i>MISP -&gt; Event</i> orgc_id TM:Incident MISP Taxonomy info attribute > external analysis > text first_seen (external analysis attribute) last seen (external analysis attribute) Text Tag TM:Sector MISP Taxonomy MISP Galaxy Geography see SecAlliance actor profile galaxy Event ID Sharing Group Tlp Tag - MISP Taxonomy Tags	<i>TM -&gt; Incident</i> Show Org Name Incident Tag Title Overview Date Date Targets Sector Relevance Target Geography Associated Profiles Associated Profiles Distribution TLP Overview Tags	

	Defacement activity DDoS Disruption Activity Espionage Activity Exposure of data Extortion Activity Fraud Activity Hacktivist Activity Malicious insider Malware infection Man in the Middle Attacks Mobile malware Phishing Activity Ransomware Activity Social engineering Activity Social media compromise Spear-phishing Activity Spyware SQL injection Activity Supply chain compromise Trojanised software MFA attack Unknown Vishing Website attack (other) Attempted Exploitation					
--	--	--	--	--	--	--



<b>Threat Alerts</b>	Any <b>analysis, reporting and or assessment</b> from the following:  Credential Breaches Phishing Attempts Pastebin dumps Sensitive information disclosures Information leakages High Impact Vulnerabilities Nefarious Forum mention Actor Campaigns Malware Analysis DDoS Alert of Incidents Nefarious Domains Supply chain Event Technical exposure PII exposure Exploit Alert Trigger events Threat Actor Updates Social Media Alerts General Notifications	Originator Type of Threat Title Description Assessment Recommendation When Discovered When Occurred Threat Severity App. Sectors Ass. Events Ass. Actors Dissemination TLP Level Other Tags	M M M M S S M S M S C S M M S	<i>MISP -&gt; Event</i> Org_id TM:Alert_Type MISP Taxonomy info attribute > external analysis > text attribute > external analysis > text attribute > external analysis > text publish_timestamp timestamp Threat_level_id TM:sector Event ID see SecAlliance actor profile galaxy Sharing Group TLP Tag MISP Taxonomy Tags	<i>TM -&gt; Alert</i> Show Org Name Alert Type Title Overview Assessment Recommendation Discovery Date Event Date Severity Sectors Associated Profiles Associated Profiles Distribution TLP Tags	
<b>Actor Operations</b>	Any <b>analysis, reporting and or assessment</b> from adversary operations, such as:	Originator Title Description	M M M	<i>MISP -&gt; Event</i> orgc_id Info attribute > external analysis > text	<i>TM -&gt; Operation</i> Show Org Name Title Overview	

	Actor Tactics Actor Techniques Actor Procedures Attack preparation Negative Sentiment Regional/geographic security impacts	Date from Date to Tactics Techniques Procedures Assoc. Incidents Targets Target Sector Target Geo. Ass. Profiles Ass. Events Dissemination TLP	S S S S S S S S S S S M M	first_seen last seen attribute > external text > text (ATT&CK) attribute > external text > text (ATT&CK) attribute > external text > text (ATT&CK) attribute > external text > text (ATT&CK) attribute > external text > text TM:Sector MISP Taxonomy MISP Galaxy Geography see SecAlliance actor profile galaxy Event ID Sharing Group Tlp Tag - MISP Taxonomy	Date Date ATT&CK Tag ATT&CK Tag ATT&CK Tag Incidents Text Target Text Target Geography Target Sector Associated Profiles Associated Profiles Distribution TLP	
<b>Threat Reporting</b>	Actor            Operation Mapping Actor            Campaign Mapping RFI Responses Intelligence Summary Intelligence Reports	Title Date Exec Summary Content Assessment Sectors Assoc. Actors Assoc. Events Assoc. Ops Assoc. Incidents Dissemination TLP Tags	M M S M M S S S S S M M S	<i>ThreatMatch -&gt; Report</i> Title Date Exec Summary Intelligence Report Assessment Sector Relevance Associated Profiles Associated Profiles Associated Profiles Associated Profiles Distribution TLP Tags	<i>MISP -&gt; Event</i> info date attribute    >    external analysis > text attribute    >    external analysis > text attribute    >    external analysis > text TM Sector MISP Taxonomy TM Actor Galaxy Event ID Operation Events Incident Events Sharing groups TLP tags Tags	

<b>Malware Profiling</b>	Full and historical profiling of a piece of Malware or Malware family	Originator Names & Aliases Overview Malware Family Malware Type Time Active Availability Targets Target Sectors Target Geo Protective Mechanisms Persistent Techniques Network Behavior Other Attributes Associated Actors Associated Incidents Associated Operations Associated Malware Dissemination TLP	M M M S S C C S S S S S S S C S S C C M M	<i>ThreatMatch -&gt; Malware Profile</i> Show Org Name Title Overview Malware Family Malware Type Known Period of Activity Availability Targets Target Sectors Target geography Protective Mechanisms Persistent Techniques Network Behavior Additional technical Detail Associated Profiles Associated Profiles Associated Profiles Associated Profiles Dissemination TLP	<i>Galaxy title:</i> <i>GalaxyCluster.Galaxy.name</i> = "TM Malware Profiles" GalaxyCluster.value description "Malware Family" key/value "Malware Type" key/value "Known Period of Activity" key/value "Availability" key/value "Targets" key/value "Target Sectors" key/value "Target Geography" key/value key/value key/value key/value GalaxyClusterRelation Automatically added when galaxy is present in event Automatically added when galaxy is present in event GalaxyClusterRelation	Security Alliance Malware profiles are currently only available in Threat-Match
--------------------------	---	---	---	--	--	--

<b>Actor Profiling</b>	Full and historical profiling of a Threat Actor	Author Actor Category Names Alias Overview Active Since National Origin Target Geographies Languages Sector relevance Operations Incidents Motivation Intended Effects Resources Malware and Tools TTPs  Associations Capability Score Dissemination TLP	M M M S M S C S C C S C C C S S S S S S S S M	ThreatMatch -> Actor Profile Show Org Name Category Tag Title Known as Overview Active Since Country of Origin Target Geography  Languages Sector relevance Operations Incidents Motivation Intended Effects Resources Malware and Tools  Reconnaissance Weaponization Delivery Exploitation Installation Command & Control Actions On Associated Profiles Capability Score Distribution groups TLP	GalaxyCluster.Galaxy.name = "TM Threat Actor Profiles" authors  GalaxyCluster.value "Known as" key/value description "Active Since" key/value "Country of Origin" key/value "Target Geography" key/value  "Languages" key/value "Sector Relevance" key/value Automatically added when galaxy is present in event "Motivation" key/value "Intended Effects" key/value "Resources" key/value "Malware and Tools" GalaxyClusterRelation key/value key/value key/value key/value	
------------------------	---	--	---	--	---	--

			M		key/value key/value GalaxyClusterRelation "Capability Score" key/value distribution/sharing_group _id	
--	--	--	---	--	---	--

## Annex C: Sharing Schema – Tactical Intelligence Sharing

Level	Tactical Intelligence					
Description	This is data or sets of data that are related to adversary actions. All data types that could be shared are references in the MISP taxonomy documentation. Tactical Intelligence is usually data and sometimes information. It is usually but not always 'Indicators of compromise' (IOCs) and primarily supports 'detection operations'. NATO - Intelligence required for the planning and execution of operations at the tactical level					
Potential Sources	Incident report, Malware analysis, Threat Hunting, Intrusion Detection, Incident Response reports, Vendor reporting, Security Operations, Security tools and network infrastructure/ logging					
Preferred Dissemination Medium			PRIMARY		SECONDARY	
Intelligence Type	What to Share	Required Content	MSC	MISP Taxonomy	ThreatMatch Taxonomy	Note(s)
<b>Incidents</b>	<p><b>Any Technical indicators that are derived from any of the following types of incidents:</b></p> <p>ATM Attacks            Botnet Activity            Business Email            Compromise            Exec Targeting            Crypto Mining            Data breach/compromise            Data Dump            Data Leakage</p>	<p>Originator            Type of Incident            Title            Description            Start DTG            End DTG            Target            Target Sector            Target Geo            Ass. Actors            Ass. Events            Dissemination            TLP Levels            Other Tags</p>	<p>M            M            M            M            S            S            M            S            S            S            C            M            S            S</p>	<p><i>MISP -&gt; Event</i>            orgc_id            TM:Incident MISP Taxonomy            info            attribute &gt; external analysis &gt; text            first_seen (external analysis attribute)            last seen (external analysis attribute)            Text Tag            TM:Sector MISP Taxonomy            text tag MISP Taxonomy            see SecAlliance actor profile galaxy            Event ID            Sharing Group            Tlp Tag - MISP Taxonomy            Tags</p>	<p><i>TM -&gt; Incident</i>            Show Org Name            Incident Tag            Title            Overview            Date            Date            Targets            Sector Relevance            Target Geography            Associated Profiles            Associated Profiles            Distribution            TLP            Overview Tags</p>	

	Defacement activity DDoS Disruption Activity Espionage Activity Exposure of data Extortion Activity Fraud Activity Hacktivist Activity Malicious insider Malware infection Man in the Middle Attacks Mobile malware Phishing Activity Ransomware Activity Social engineering Activity Social media compromise Spear-phishing Activity Spyware SQL injection Activity Supply chain compromise Trojanised software MFA attack Unknown Vishing Website attack (other) Attempted Exploitation					
--	--	--	--	--	--	--

<b>Threat Alerts</b>	<b>Any Technical indicators that are derived from any of the following:</b>  Credential Breaches Phishing Attempts Pastebin dumps Sensitive information disclosures Information leakages High Impact Vulnerabilities Nefarious Forum mention Actor Campaigns Malware Analysis DDoS Nefarious Domains Supply chain Event Technical exposure PII exposure Exploit Alert Trigger events Threat Actor Updates Social Media Alerts General Notification	Originator Type of Threat Title Description Assessment Recommendation When Discovered When Occurred Threat Severity Ass. Sectors Ass. Events Ass. Actors Dissemination TLP Level Other Tags	M M M M S S M S M S C S M M S	<i>MISP -&gt; Event</i> Org_id TM:Alert_Type MISP Taxonomy info attribute > external analysis > text attribute > external analysis > text attribute > external analysis > text publish_timestamp timestamp Threat_level_id TM:sector Event ID see SecAlliance actor profile galaxy Sharing Group TLP Tag MISP Taxonomy Tags	<i>TM -&gt; Alert</i> Show Org Name Alert Type Title Overview Assessment Recommendation Discovery Date Event Date Severity Sectors Associated Profiles Associated Profiles Distribution TLP Tags	
----------------------	---	---	---	--	---	--