CERT-EU Cyber Threat Intelligence Framework

TLP:AMBER+STRICT

2025-09-29 - Version: 1

Table of Contents

Introduction

This framework defines the analytical and operational standards used to classify, assess, and prioritise malicious cyber activities relevant to Union entities and their ecosystem. It provides a shared reference model for CERT-EU and Union entities to support consistent reporting, alerting and awareness raising on cyber threat intelligence.

This framework introduces core concepts such as malicious activities of interest, ecosystem, threat categories, domains, and threat (actor) levels. It also outlines scoring mechanisms for adversaries and mitigation. These elements are designed to facilitate handling of cyber threats at various levels in Union entities, including for primary operational contacts (POCs) and local cybersecurity officers (LCOs).

All components of this framework are aligned with recognised intelligence and cybersecurity standards and internal best practices of CERT-EU. Where applicable, terminology and methods follow practices from EU cybersecurity regulations, FIRST,

NATO and threat intelligence industry best practices. The framework may evolve in response to regulatory changes or stakeholder feedback.

Malicious activities of interest (MAI)

A malicious activity of interest (MAI) is defined as any adversarial cyber activity with a potential impact to Union entities or their ecosystem. This includes confirmed compromise, suspicious attempts, adversarial resource development, or reconnaissance activities. We are tracking MAIs to support alerting and awareness raising, as well as response and mitigation of threats by Union entities.

Ecosystem

The Union entities' ecosystem consists of countries of operation, sectors of activity, geopolitical events of interest, partners, providers, systems, and software, as defined in the table below:

ECOSYSTEM COMPONENT	DEFINITION AND EXAMPLES
Countries	Countries in which Union entities operate. This includes all EU Member States as well as non-EU countries where Union entities have a physical presence. Each Union entity is located in one or more country(ies).
Sectors	Sectors in which Union entities are working. They are listed in Chapter Sectors of interest. A Union entity may belong to one or more sectors.
Events	Events of geopolitical nature in which our Union entities are involved and which may trigger or be targeted by malicious cyber activity. Examples of events include conferences, summits, disputes, international negotiation, conflicts, or elections. The nature and the level of involvement of a Union entity might vary (i.e. organisation of or participation to a conference / summit, supporting or sanctioning a party in a conflict, etc.) and therefore malicious cyber activity related to these events might affect Union entities in various ways.
Partners	Organisations with which Union entities are cooperating or exchanging information. Each Union entity can have several partners, in EU countries or outside. These partners can be permanent stakeholders of Union entities or may cooperate on ad hoc initiatives / projects. Examples of partners include other Union entities, ministries or agencies in EU countries, international organisations (i.e. NATO, ICC, ...), or non-profit organisations.

ECOSYSTEM COMPONENT	DEFINITION AND EXAMPLES
Providers	Information technology (IT) companies providing services to Union entities. These include cloud service providers (CSPs), managed service providers (MSPs), internet service providers (ISPs).
Software	Software products used by Union entities. These include operating systems, browsers, edge devices, software security devices, business software, AI software, etc. Software products may be exposed to the internet or not.
Systems	Information systems are made of technologies / software assembled by a specific organisation or group of organisations for collaborative or shared purposes and for their exclusive usage. These include public websites of Union entities, special purpose systems like EU Login, EU Survey, etc.

The classification of an event as a MAI is based on a combination of these factors. Single criteria may be sufficient if the impact is direct and significant; in other cases, multiple weaker indicators may collectively justify attention.

Threat categories

This section defines the core threat categories used to classify MAIs based on the intent of the threat actor or the nature of the action. Note that certain activities as well threat actors may overlap across multiple categories, in some cases to hinder attribution.

CATEGORY	DEFINITION
Policy & law enforcement	undertakings that aim to address malicious cyber activity. These include policy, regulations, cooperation, arrest, seizure, takedown, bans etc.
Cyberespionage & prepositioning	Threat actors steal sensitive information for intelligence purposes or covertly compromise an information system for future exploitation.
Cybercrime	Threat actors compromise systems for financial benefits. This includes ransomware breaches, compromising an IT system to sell access, deploying malware to steal credentials and resell them.
Hacktivism	Threat actors target systems to promote an ideological or political agenda. This includes some website DDoS / defacement attacks, or some hack-and-leak operations.

CATEGORY	DEFINITION
Opportunistic	Non-targeted malicious activity aiming at identifying and exploiting vulnerable systems in the wild. This includes spreading a worm through unpatched routers worldwide, or scanning and attempting automated exploitation of vulnerabilities in publicly exposed assets.
Information operation	The goal of the threat actor is to influence public opinion or sow discord with unauthorised cyber means. This includes fake accounts spreading disinformation during an election, leaking selectively altered documents to mislead the public, or bots amplifying polarising content on social media.
Disruption & destruction	The goal of the threat actor is to disrupt the operations of a victim's information system, destroy the system or destroy data. This includes wiper malware attacks, or DDoS on critical infrastructure.
Data exposure and leaks	The activity leads to information exposure or leaks, thereby causing damage to reputation, or facilitating further cyberattacks. This includes hack-and-leak operations by threat actor, or purposeful exposure or leaks from insider threats. Data exposure and leaks can also happen accidentally.
Unknown	The purpose of the activity is unknown.

Threat domains

This section defines a hierarchical model for classifying the geographical or institutional scope affected by malicious cyber activity. Domains are ranked from the innermost institutional core to the broadest global context. When multiple domains apply, the highest-ranking domain takes precedence.

DOMAIN	DEFINITION
Union entities	The activity targeted one or more organisations as identified in the Cybersecurity Regulation 2023/2841.
EU	The activity targeted entities in one or more EU Member States, including national governments, infrastructure, or private entities.
Europe	The activity targeted entities in one or more European countries outside the EU. This includes some NATO countries, EFTA members, EU candidate and potential candidate countries.
EU Civilian Mission Area	The activity targeted one or more countries outside of Europe hosting an EU civilian mission.

DOMAIN	DEFINITION
World	The activity targeted any country not falling under the above domains.

Threat levels

This section defines the threat level scale used to assess the criticality and proximity of malicious cyber activity in relation to Union entities. These levels reflect analytical judgement based on threat actor intent, technical impact, and known targeting of Union entities. Threat levels are used particularly in Threat Alerts. This scale guides the urgency and prioritisation of mitigation and response.

THREAT LEVEL	DEFINITION
High	An immediate threat to Union entities. Verification and action are required without delay. Examples: • A Significant Incident (SI) affecting one or more Union entities. • Exploitation in the wild of a zero-day in an internet-facing system deployed by multiple Union entities. • State sponsored spearphishing campaign detected in at least one Union entity or in close partners.
Medium	A close threat to Union entities. Close monitoring and checking are strongly recommended. Examples: • Focused cyberespionage campaign against sectors of interest (c.f.: Chapter - Sectors of interest) in the EU. • Opportunistic exploitation of a known vulnerability in software used by Union entities. • Threat actor activity targeting critical infrastructure within the EU.

THREAT LEVEL	DEFINITION
Low	A distant or indirect threat with no immediately identified link to Union entities. Monitoring is advised, and action is recommended depending on available resources and priorities. Examples: • Opportunistic scanning or enumeration activity. • Global cyberespionage campaign targeting multiple continents with no apparent EU focus. • Indicators related to a non-EU incident reused in opportunistic malware campaigns.

Threat actor levels

This section defines the threat actor levels used to assess and prioritise adversaries based on their recent impact on Union entities and their ecosystem. The classification considers both the **period of interest** (e.g. last 3 months, last 12 months, or a defined timeframe such as 2025-Q1) and the **scope** (e.g. a specific constituent or the broader EU constituency).

THREAT ACTOR LEVEL	DEFINITION
Critical	The threat actor caused at least one **Significant Incident** affecting one or more Union entities during the period of interest.
High	The threat actor is responsible for at least one **malicious activity of interest (MAI)**, not qualified as a Significant Incident, affecting one or more Union entities during the period of interest.
Medium	The threat actor is responsible for at least one MAI affecting **two or more elements of the ecosystem** during the period of interest.
Low	The threat actor is responsible for at least one MAI affecting **exactly one element of the ecosystem** during the period of interest.

Tactics, Techniques and Procedures (TTPs)

We use the MITRE ATT&CK framework to map techniques to the malicious activities of interest. This framework provides a shared, behaviour-based taxonomy that links observable actions to known adversary methods — making detection, threat-hunting

and prioritised mitigation far more systematic and repeatable for CERT-EU and Union entities.

Sectors of interest

This section defines the sectors to which Union entities belong. Note that sectors are sorted in alphabetical order and not by importance. These sectors consist of the same sectors defined in the directive NIS2, plus other sectors relevant to Union entities not covered by this directive.

This mapping of Union entities is based on our understanding of your missions and activity. If you would like us to make any changes in these assignments, please feel free to reach out.

SECTOR	ASSOCIATED EU ENTITIES AND BODIES
Agriculture	CPVO, CBE
Chemicals	ECHA
Cybersecurity	CERT-EU, ENISA, EC3, ECCC
Defence	EDA, EUISS, EEAS, SATCEN
Diplomacy	EEAS, EUISS
Education	EACEA, EUSA, EUI, ETF, CEDEFOP
Energy	ACER, F4E, CINEA, CLEAN Hydrogen JU, ESA (EURATOM)
Environment	EEA, CINEA, CBE
Finance	AMLA, EIOPA, ESM, ESRB, ESMA, EIF, EIB, ECB, EBA, SRB
Fisheries	EFCA
Food	EFSA
Fundamental Rights	EUAA, FRA, EDPB, EDPS, EIGE
Health	EU-OSHA, EMA, EFSA, ECDC, EUDA, IHI, Global Health EDCTP3
Intellectual Property	EUIPO, EPO

SECTOR	ASSOCIATED EU ENTITIES AND BODIES
Justice	AMLA, EUROJUST, EPPO, ECA, CJEU (CURIA), FRA, EO
Labour	ELA, EESC / CES, EUROFOUND, EU-OSHA
Law enforcement	AMLA, EUROPOL, FRONTEX, CEPOL, EC3
Local public administration	CoR
Parliamentary administration	European Parliament (EP)
Pharmaceuticals	EMA
Public administration	European Commission (EC), European Parliament (EP), Council of the EU (GSC), all central bodies
Research	REA, JRC, EIT, EuroHPC, KDT, CLEAN Hydrogen JU, IHI, CAJU, ERCEA, EUROFOUND, EUISS, EUROSTAT, OP, Global Health EDCTP3, ECCC, EUIPO, EPO, EISMEA
Space	EUSPA, SATCEN
Technology	EIT, EuroHPC, KDT, CBE
Telecommunications	BEREC, SNS JU
Transport	CINEA
Maritime transport	EMSA
Civil aviation	SESAR, EUROCONTROL, EASA, CAJU
Rail transport	ERA, EU-Rail
Internal administrative services	EPSO, CDT

The sector list supports structured analysis and classification of malicious activity. New sectors may be added as EU operational, regulatory, or policy priorities evolve.

Confidence and Uncertainties

Adhering to common norms for expressing confidence and uncertainties in CTI reporting ensures consistent interpretation, reduces miscommunication, and enhances the credibility and usability of our CTI products for Union entities. This section explains how we assess and express confidence in the information we use in our reporting and how we express uncertainties.

Confidence in information

We use the Admiralty Code, a NATO-standard system that rates the reliability of the source and the credibility of the information independently. The final confidence level is expressed as a combination of both dimensions (e.g. A1, B2).

The Admiralty Code is based on two dimensions:

- **Source reliability**: An assessment of the trustworthiness of the source providing the information, based on their track record, access, and consistency. It is rated from A (completely reliable) to F (unreliable or untested).
- **Information credibility**: An assessment of the plausibility and confirmability of the information itself, regardless of the source. It is rated from 1 (confirmed by multiple sources) to 6 (cannot be judged).

We will use information in our threat intelligence products only if they match one of the **authorised combinations** shown in green in the table below.

CREDIBILITY OF INFORMATION	A (COMPLETELY RELIABLE)	B (USUALLY RELIABLE)	C (FAIRLY RELIABLE)	D (NOT USUALLY RELIABLE)	E (UNRELIAB
1 Confirmed by other sources	Yes	Yes	No	No	No
2 Probably true	Yes	Yes	No	No	No
3 Possibly true	No	No	No	No	No
4 Doubtful	No	No	No	No	No
5 Improbable	No	No	No	No	No
6 Cannot be judged	No	No	No	No	No

For more details on the Admiralty Code, refer to the official NATO documentation: NATO APP-01: Intelligence Reporting.

Communicating on Uncertainties

We implement FIRST guidelines in our CTI reporting to address imperfect information and uncertainty by using standardised language — Levels of Confidence in Assessment (LCA) and Words of Estimative Probability (WEP). This ensures clarity, consistency, and usability for Union entities using our CTI products.

Attribution

This section outlines the principles guiding our approach to attributing MAIs to threat actors. Attribution is the analytical process of linking observed activity to a threat actor, an intrusion set, a state, or an organisation. It is essential to clarify that we engage **only in technical attribution**, on an ad hoc basis only, and under strict conditions. We do **not engage in political attribution**.

- **Political attribution** refers to assigning accountability to a state or an organisation for malicious cyber operations — this falls outside our remit and is the responsibility of national or institutional decision-makers.
- **Technical attribution** involves linking malicious activity to known threat actors based on behavioural patterns, infrastructure reuse, malware indicators, and targeting profiles.

Technical attribution principles

- **Strictly technical:** We do not attribute activity to states or organisations. Our focus is on identifying threat actors based on technical indicators and behavioural consistency.
- **Where required:** We pursue technical attribution only where required to strengthen our Full-Spectrum Adversary Approach.
- **Evidence-based:** Attribution is grounded in observable characteristics, such as TTPs (tactics, techniques, procedures), infrastructure overlaps, malware artefacts, and targeting.
- **Confidence-driven:** We only attribute activity when supported by sufficient evidence and express a level of confidence. We reference open-source or partner analysis when deemed credible.
- **Contextual:** Attribution is valid for a defined period and scope, and may be updated as new information emerges.

Unattributed threat actors

When it’s impossible to attribute a MAI to a known threat actor, particularly if it's qualified as Significant Incident, we link the MAI to an Unattributed Threat Actor (UTA)

to which we append a numeric suffix (example: UTA-53). Depending on further analysis and information received, we might later merge this UTA with a known threat actor.

Scoring

This chapter explains how we calculate and apply scores to prioritise adversaries and defensive measures in the *My Threats* product. These scores help determine which threats and mitigations are most relevant to your operational environment.

Threat scoring

Each threat actor, attacking country, or threat category is assigned a **relevance score** based on how severely and directly it has affected your organisation and its ecosystem. The score reflects both **proximity** (direct impact vs ecosystem impact) and **severity** (high vs low impact).

As of September 2025, we assign the following weights.

Note: the weights may evolve in the future, depending on the respective importance that we want to give to the components of the ecosystem, from a threat perspective.

AFFECTED COMPONENT	WEIGHT
Your organisation (Significant Incident)	100
Your organisation (non Significant Incident)	5
Your host country(ies)	1
Your sectors	1
Your partners	1
Your events	1
Your providers	1
Your software	1
Your systems	1

We use the following function:

```
def compute_score(stats):
   return (
```

```
        stats["org_significant"] * 100 +
        stats["org_normal"] * 5 +
        stats.get("sector", 0) +
        stats.get("country", 0) +
        stats.get("system", 0) +
        stats.get("software", 0) +
        stats.get("provider", 0) +
        stats.get("partner", 0) +
        stats.get("event", 0)
    ) / 12.0
```

> **Example:**
> 1 significant MAI (100) + 5 normal MAIs (25) + 10 ecosystem MAIs (10) = 135
> Final score = 135 / 12 = **11.25**

Higher scores indicate adversaries with greater threat potential to your organisation. These are prioritised in the `adversaries` chapter.

Mitigation scoring

Mitigations are also scored to support prioritised defence planning. The score measures how well a mitigation addresses adversary techniques, protects initial access vectors, and aligns with recognised baseline practices.

We use this formula:

$$\text{Mitigation Score} = K_1 \times \text{MMW} + K_2 \times \text{MIA} + K_3 \times \text{ME8}$$

- `MMW` (Mitigation Weight): Total impact across observed adversary techniques and incidents.
- `MIA` (Mitigation Initial Access): Number of initial access techniques addressed.
- `ME8` (Mitigation Essential Eight): Number of linked Essential Eight controls.

These scores help determine which mitigations offer the greatest security value given observed threat activity. The `mitigations` file ranks defensive measures accordingly.

TLP definition

TLP	DISCLOSURE	MESSAGE
RED	Not for disclosure, restricted to participants only.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed.
AMBER+STRICT	Limited disclosure, restricted to participants' organisations.	Recipients may share TLP:AMBER+STRICT information only with members of their own organisation.
AMBER	Limited disclosure, restricted to participants' organisations and their clients.	Recipients may share TLP:AMBER information only with members of their own organisation and its clients.
GREEN	Limited disclosure, restricted to the community.	Subject to standard copyright rules, TLP:GREEN information may be distributed with peers and partner organisations within their sector or community, but not via publicly accessible channels.
CLEAR	Disclosure is not limited.	TLP:CLEAR information may be distributed freely.