CAMPUS CYBER

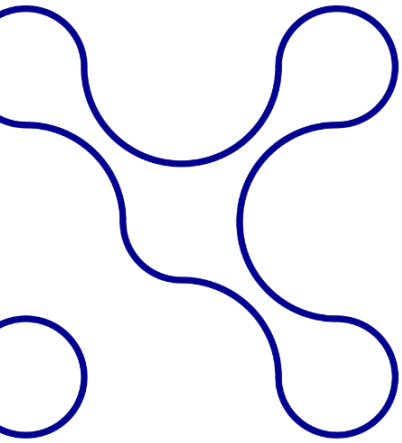
CTI DOCTRINE

Principles, Rules, Methods and Guidelines to create and share Cyber Threat Intelligence

WORKGROUP :

CYBER THREAT INTELLIGENCE

Table of contents



CONTEXT

CAMPUS CYBER RATIONALE

Campus Cyber is a French initiative aiming at federating the cybersecurity industry into a single place and showcase French excellence.

It enables accommodating companies (large groups, SMEs), public services, training organizations, research actors, vendors, contractors and associations on the same site. The Cyber Campus implements actions aimed at uniting the cybersecurity community and developing synergies between these different stakeholders.

CYBER THREAT INTELLIGENCE GOALS

Wise people in Cyber Threat Intelligence often say “sharing is caring” because malicious events encountered by one can become a threat for another one yet anticipated if it is shared.

Malicious events encountered by one can become a threat for another one, yet anticipated if it is shared.

Sharing mechanism requires basic prerequisites:

- Ability to share
- Same language used by senders and recipients
- Format useful to describe threat related topic
- Ability to ingest the shared information

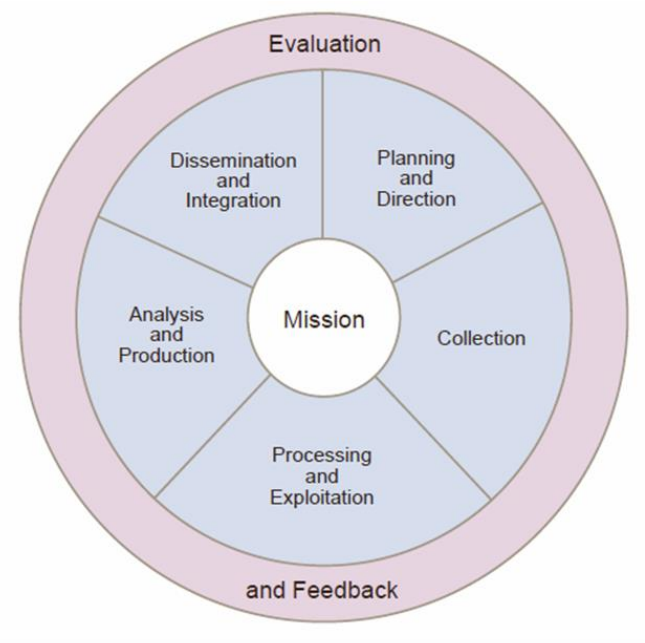
CTI COMMITTEE IN CAMPUS CYBER

Considering the rationale of Campus Cyber, a group of interested people established a CTI committee. This committee implemented CTI goals as previously listed, with very pragmatic considerations:

- Brainstorm and collective feedback
- Best practices in the industry
- Reasonable cost and reasonable time to reach objective

GLOBALS METHODS AND RULES

Cyber Threat Intelligence activities are governed by processes, known under the umbrella-term intelligence cycle, whose main goal is to ensure that a production is trustworthy and is disseminated in an authorized perimeter.



Source: Joint Intelligence / Joint Publication 2-0 (Joint Chiefs of Staff)

To allow dissemination across multiple entities, common rules, mechanisms, and formats must be used to be understood and actionable to anyone. Dissemination of intelligence is the focus of this document, which lays out afferent principles.

"MUST" or "SHOULD" are used to outline either the mandatory dimension of the principle, or its suggested angle.

ABOUT SOURCE

When an information is provided, it is important to keep track of the original source (i.e., producer of this information) to avoid later conflicts.

ID	Description
GLOBAL-SOURCE-1	The original source of CTI object MUST be preserved

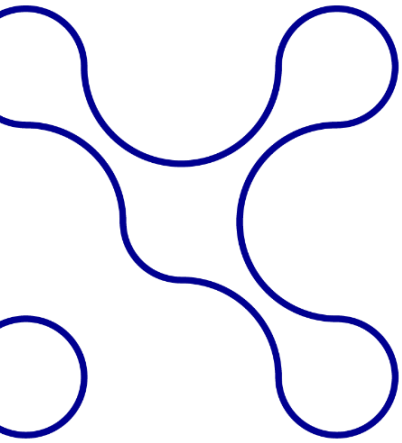
Additionally, the context of the source (the link or the associated report) should be available either directly or through pivoting activities.

ID	Description
GLOBAL-SOURCE-2	The related information (link, report) SHOULD be available to preserve context.

When someone contributed to the modification of an object, changes must be tracked, and their affiliation must be added as an additional source.

ID	Description
GLOBAL-SOURCE-3	An entity MUST be mentioned when it modifies or enriches a CTI object.

Using audit trail mechanism adds an extra layer of traceability that can be required on specific situations



ABOUT TRUST

By default, a source should not be considered as reliable, unless it is assessed and reported by analysts to be a trustworthy information producer.

Their reliability is assessed and rated through the NATO Admiralty Code[1], defined as follows:

Rating	Description
A Reliable	No doubt about the source's authenticity, trustworthiness, or competency. History of complete reliability.
B Usually reliable	Minor doubts. History of mostly valid information.
C Fairly reliable	Doubts. Provided valid information in the past.
D Not usually reliable	Significant doubts. Provided valid information in the past.
E Unreliable	Lacks authenticity, trustworthiness, and competency. History of invalid information.
F Cannot be judged	Insufficient information to evaluate reliability. May or may not be reliable.

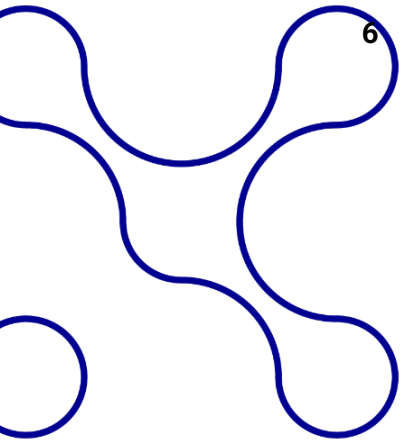
[1] https://en.wikipedia.org/wiki/Admiralty_code

ID	Description
GLOBAL-TRUST-1	A reliability score MUST be associated with sources

Confidence comes from density of evidence confirming a hypothesis. Cyber Threat Intelligence objects and associated relationships must be given a confidence score to optimize later operational actions.

Confidence in reported information can be evaluated based on the NATO Admiralty Code, where:

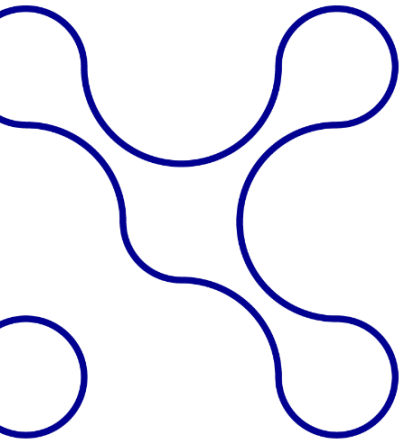
	Rating	Description
1	Confirmed	Logical, consistent with other relevant information, confirmed by independent sources.
2	Probably true	Logical, consistent with other relevant information, not confirmed.
3	Possibly true	Reasonably logical, agrees with some relevant information, not confirmed.
4	Doubtfully true	Not logical but possible, no other information on the subject, not confirmed.
5	Improbable	Not logical, contradicted by other relevant information.
6	Cannot be judged	The validity of the information cannot be determined.



ID	Description
GLOBAL-TRUST-2	A confidence score MUST be associated with objects

ID	Description
GLOBAL-TRUST-3	A confidence score MUST be associated with relationships

Note: To help analyst define the correct reliability score and confidence level, a procedure will later illustrate these requirement



ABOUT TIMELINE

Things are continuously changing, everywhere, every time. To bring more value to an information, specifically indicators, it must be timestamped, as soon as relevant and possible, including:

- When the information was considered to be valid
- When the information was created
- When the information is considered to be irrelevant

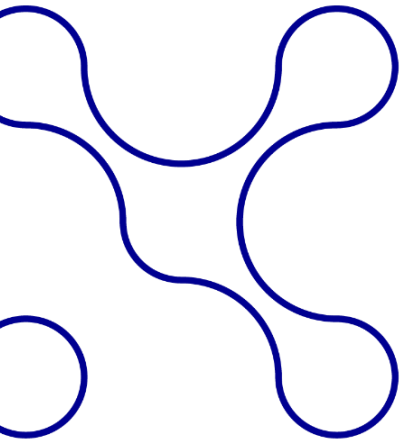
ID	Description
GLOBAL-TIME-1	A “Valid from” timestamp SHOULD be present

ID	Description
GLOBAL-TIME-2	A “Creation date” timestamp MUST be present

ID	Description
GLOBAL-TIME-3	A “Valid until” timestamp SHOULD be present

If a change occurs on a CTI artefact, the modification date must be clearly visible, preserving the other timestamps

ID	Description
GLOBAL-TIME-4	A “Modification date” timestamp MUST be present



ABOUT SENSITIVITY

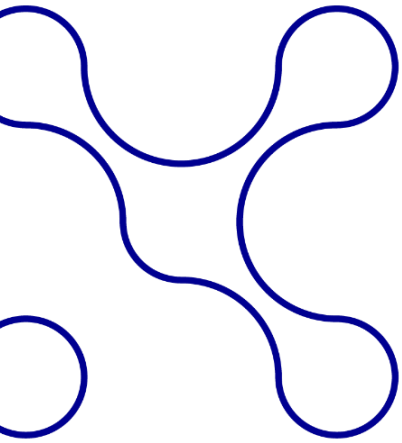
Some information can be considered as more sensitive than others within a community. To take this into account, the application of several principles should be enforced when sharing information.

ID	Description
GLOBAL-SENSITIVITY-1	Within a sensitive community, clearance SHOULD be given, coming from affiliation or individual trust

Some indicators can be considered highly sensitive, as follow-up measures and actions could lead to critical consequences.

PAP (Permissible Actions Protocol) was created to describe how sensitive the information is and what follow-up actions can be performed.

	Description
PAP:RED	Handling limited over internal and dedicated infrastructures that are unexposed to public networks
PAP:AMBER	Handling limited to actions that are not directly visible to malicious sources
PAP:GREEN	Controlled handling that may allow for non-intrusive interactions with malicious sources
PAP:WHITE	Free handling (respecting licences and law)



ID	Description
GLOBAL-SENSITIVITY-2	The use of PAP MUST be enforced

If not explicitly mentioned in the document, applicable PAP by default will be of similar TLP color-codes.

Campus Cyber stakeholders do not aim to share classified information and will need to be cautious about it.

ID	Description
GLOBAL-SENSITIVITY-3	CTI MUST be unclassified to enable dissemination to reach foreign entities.

ABOUT CONTENT

In the past years, different approaches to produce threat intelligence have raised, emerged, and sometimes died.

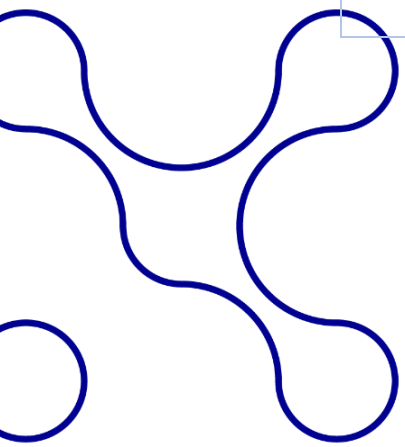
Today, it is accepted that intelligence is as much about relationships as about content. This leads to represent threat intelligence as a graph made of nodes (CTI objects) linked together through relationships.

STIX (Structured Threat Intelligence Information eXpression) is a standard format to build and manage a Threat Intelligence database based on this vision.

ID	Description
GLOBAL-CONTENT-1	Threat Intelligence MUST be normalized under the STIX standard.

The goal of a graph-based Threat Intelligence is enabling pivoting from one object to related objects. This allows for continuous contextualisation of threat intelligence artefacts.

ID	Description
GLOBAL-CONTENT-2	Objects SHOULD always be related to other objects. Independent objects should be banished.



Threat Intelligence is supposed to be shared, from a domestic to a worldwide audience. Therefore, a unified language shall be used to facilitate the associated uses and workflows

ID	Description
GLOBAL-CONTENT-3	Content produced from Threat Intelligence activities MUST be written in English language. If original content is not written in English, the original data do not have to be translated.

ABOUT QUALIFICATION

To ensure reliability and confidence in the threat intelligence production output, a qualification mechanism is necessary to avoid false positive at a later stage.

ID	Description
GLOBAL-QUALIFICATION-1	A basic qualification mechanism MUST be enforced. This can be enforced by integrated check algorithms, warning messages, AI assistance etc. Some examples could be: ○ An IP address is identified as RFC1918 or other non-relevant pool (i.e., CDN or cloud providers IP ranges which may host legitimate hosts) ○ A domain name is risky because it's very common based on public or private Domain top lists ○ A new object has no context or no relation ○ A new object strictly matches an existing object with no additional context

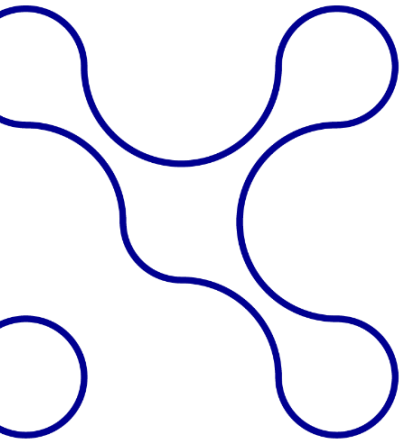
ID	Description
GLOBAL-QUALIFICATION-2	An advanced qualification mechanism SHOULD be enforced. This can be enforced by manual or automated testing of information in detection systems (real-time or in the past) aiming at removing « noisy ». Some examples could be: ○ Activating the real-time network detection on indicators for 24 hours ○ Looking for occurrences of new indicators in logs within the past month

ID	Description
GLOBAL-QUALIFICATION-3	Qualification mechanisms MUST respect applicable PAP

ABOUT VALIDATION

To ensure reliability and confidence in the threat intelligence production process, a validation mechanism is a good practice.

ID	Description
GLOBAL-VALIDATION-1	A validation mechanism SHOULD be enforced. This can be achieved through authoritative review or peer review.



ABOUT SHARING

In addition to sensitivity protection measures, intelligence dissemination across a community of interest also matters. If and when intelligence is shared beyond a first circle of recipients, rules apply to avoid sensitive information being available where it should not.

If information is available within a specific community, considered as a first circle, other communities can gain access to this intelligence on specific conditions.

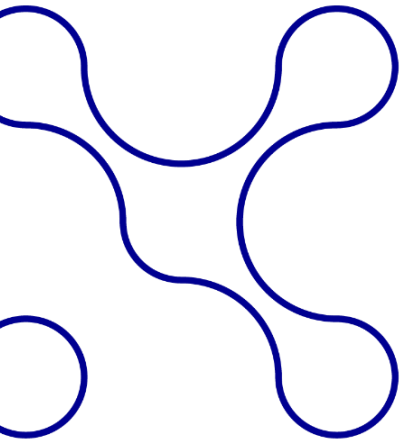
ID	Description
GLOBAL-SHARING-1	Sharing rules MUST exist to define the requirements that a connected community must fulfil to receive entire or part of intelligence produced in the previous circle.

ID	Description
GLOBAL-SHARING-2	It SHOULD be possible to define filters to allow the sharing between communities based on specific conditions such as: ○ Specific type of objects ○ Defined scope of industrial sectors ○ Selected group of sources …

TLP (Traffic Light Protocol) is an international standard to define how information or intelligence can be shared. TLP (version 2[2]) is structured this way:

[2] https://www.first.org/tlp/

	Description
TLP:RED	For the eyes and ears of individual recipients only, no further disclosure. Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. Recipients may therefore not share TLP:RED information with anyone else. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting.
TLP:AMBER	Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. Note that TLP:AMBER+STRICT restricts sharing to the organization only. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note: if the source wants to restrict sharing to the organization only, they must specify TLP:AMBER+STRICT.
TLP:GREEN	Limited disclosure, recipients can spread this within their community. Sources may use TLP:GREEN when information is useful to increase awareness within their wider community. Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP:GREEN information may not be shared outside of the community. Note: when “community” is not defined, assume the cybersecurity/defense community.
TLP:CLEAR	Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.



ID	Description
GLOBAL-SHARING-3	The use of TLP MUST be enforced

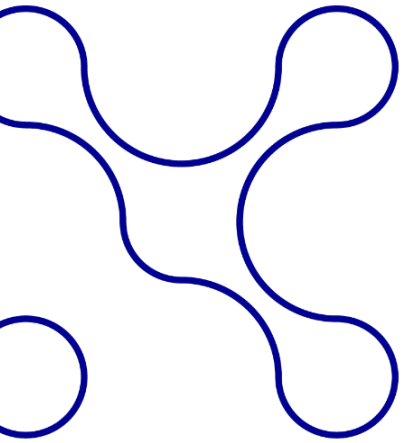
In some circumstances, an entity is willing to share but is not willing to disclose its identity. This scenario can occur when the principle of “sharing is caring” is agreed upon at the originator level, but the impact of sharing can be damaging for the sender itself. In this case, the sender expects the possibility to share anonymously or at least to have its name redacted.

In some circumstances, an entity is willing to share but is not willing to disclose its identity.

ID	Description
GLOBAL-SHARING-4	The possibility to share without disclosing the name of the originator SHOULD be possible.

For some sensitive production, the author might want to apply a policy rule that would supersede the TLP or other marking definition. This policy rule is supposed to remain through every step of the dissemination process, so to preserve the protection requirements initially requested by the author.

ID	Description
GLOBAL-SHARING-5	Policy rules SHOULD be made possible and assigned with a set of objects for sensitive goals. This can involve: ○ Define a minimal TLP level ○ Define if a connected peer requires an authentication key ○ Define how many hops the intelligence can jump into ○ Define friendly or internal organization identities and flatten the hops for them

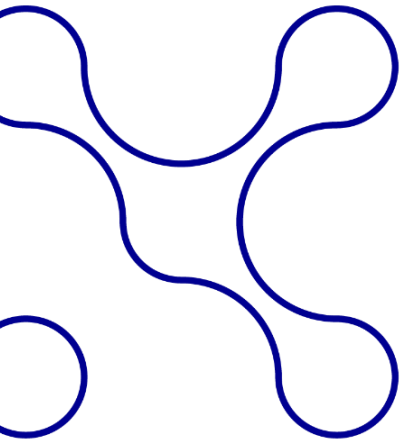


Received intelligence shared from others can use different formats. Widely used formats must be supported for threat intelligence import.

ID	Description
GLOBAL-SHARING-6	Import must be possible using STIX format, MISP format, CSV file, PDF file and plain text.

Produced intelligence also need to be delivered in widely used format to be shared with others.

ID	Description
GLOBAL-SHARING-7	Export must be possible using STIX format, MISP format, CSV file and text file.



CYBER THREAT INTELLIGENCE DELIVERABLE

THREAT INTELLIGENCE REPORT

Campus Cyber aims at being able to produce its own Cyber Threat Intelligence reports. These reports will be based on a template that will allow CTI users to contribute individually in a way it can eventually be integrated easily into a joint document.

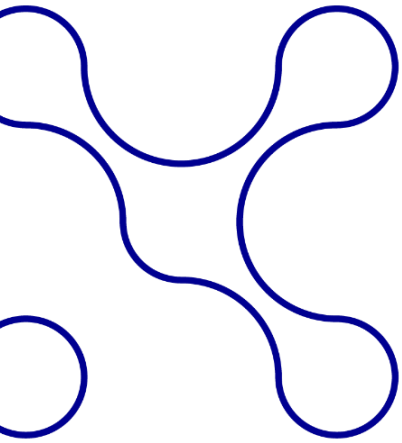
These reports will both display the Campus Cyber brand and individual contributors' brand.

ID	Description
REPORT-TEMPLATE-1	A template mechanism MUST be available

ID	Description
REPORT-TEMPLATE-2	Final document MUST feature the brand of all contributors except for those who are not willing to.

Considering the rationale of Campus Cyber of showcasing French excellence in the cybersecurity field, these reports must be considered as relevant enough either because they present an innovative angle or focusses on new topics.

ID	Description
REPORT-CONTENT-1	Content MUST be relevant enough: ○ Something presenting a fresh point of view or analysis even based on already published information ○ Something new ○ Something sharing good practices



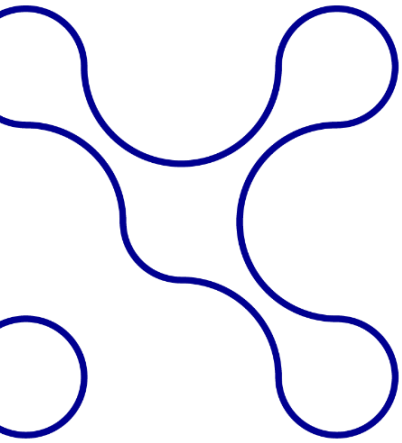
Publishing a report is not an innocuous action, it represents a commitment from the participating members at the time of publication and in the long term.

That's why a validation process is necessary to authorize the report to be shared across the community or wider.

ID	Description
REPORT-VALIDATION-1	A validation process MUST exist and apply to each report publication

ID	Description
REPORT-VALIDATION-2	A designated person or a committee SHOULD be designated to ensure the final validation stage.

ID	Description
REPORT-SHARING-1	The contributing sources of the report SHOULD be mentioned



OSINT SELECTION AND CURATION

As Campus Cyber aims to federate the Cyber security industry into a single place, cyber threat intelligence savvy people ought to consume CTI in a federated way into a single place.

Numerous relevant information is regularly published as OSINT (Open-Source Intelligence) on the Internet. Consuming and leveraging it can be a strong base for Cyber Threat Intelligence purpose.

The ability to ingest OSINT information, curate and transform it into useful threat intelligence is a very smart way to get the community to work together on a common dataset and collective purpose.

Some rules must be considered to reach this objective.

Numerous relevant information is regularly published as OSINT (Open-Source Intelligence) on the Internet.

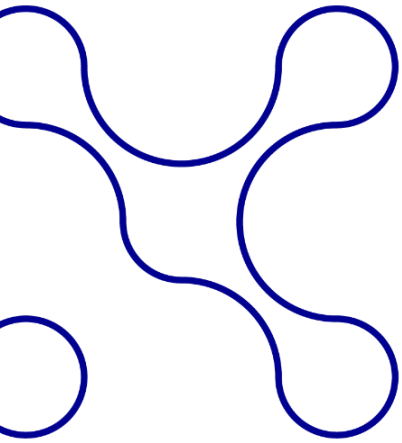
ID	Description
OSINT-SOURCE-1	Information MUST come from an OSINT source or at least from a source accommodating of broad data sharing (TLP:CLEAR, TLP:GREEN) and will be marked accordingly

ID	Description
OSINT-CONTENT-1	OSINT data MUST bring something new before being transformed as intelligence.

ID	Description
OSINT-CONTENT-2	Duplication of existing validated intelligence SHOULD not be done except to fix/improve an original incorrect artefact.

ID	Description
OSINT-CONTENT-3	OSINT content SHOULD always be contextualized.

ID	Description
OSINT-CONTENT-4	OSINT content MUST be enriched (relationships between objects or metadata).



THREAT MODELLING

Threat modelling is a core activity in the Cyber Threat Intelligence process. Campus Cyber stakeholders want to have access to a threat modelling capability. Intelligence produced as a deliverable stemming from this threat modelling could be used exclusively for internal purposes or could be shared to connected communities in accordance with sharing possibilities (TLP).

Threat modelling activity will respect the rules defined in the GLOBAL section and will also require specific controls.

Threat modelling is a core activity in the Cyber Threat Intelligence process.

ID	Description
MODELLING-SOURCE-1	If multiple sources contribute to threat modelling, all of them SHOULD be listed as external references on the central object of the modelling

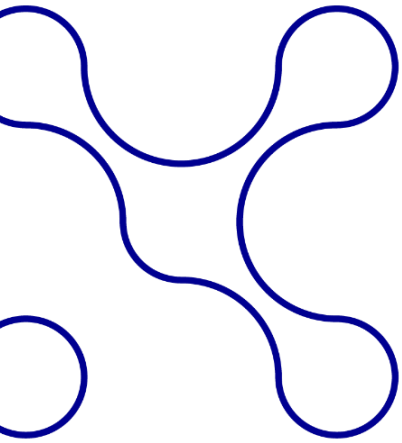
ID	Description
MODELLING-CONTENT-1	STIX best practices (Operation Guidelines) MUST be followed to create a new threat modelling

ID	Description
MODELLING-CONTENT-2	Kill-chain stage MUST be positioned for every object that can be translated as an attacker progress when observed: indicator, attack pattern (TTPs), malware or tool MITRE ATT&CK matrix SHOULD be preferred to represent this kill-chain

ID	Description
MODELLING-TIME-1	In addition to GLOBAL-TIME-X measures, a specific attention SHOULD be drawn to define the validity period of an indicator depending on its type. This is a precious property for later detection or retro hunting purposes.

ID	Description
MODELLING-ENRICH-1	Enrichment actions SHOULD be applied by analyst to get a better and in-depth view of the threat in a global context. The obvious purpose of doing so is to get multiple properties of one single artefact to represent this artefact with different vantage points

ID	Description
MODELLING-ANALYSIS-1	Multiple hypothesis of investigation SHOULD be applied by analysts and best one should be kept.



FOCUSED THREAT INTELLIGENCE

Having the capability to place a specific focus on a threat over time is precious for people working in Cyber Threat Intelligence industry. This capability can allow stakeholders to both participate and ingest intelligence in almost real time on subject matters related to a pressing topic.

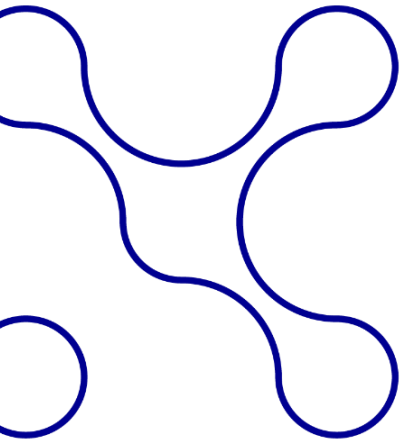
Considering a focused threat intelligence is part and included with other threat intelligence activities, it should be seen as an option that can be both showcased as a hot topic to raise concerns and flagged easily for those willing to contribute to the orientation or just willing to consume the results easily.

ID	Description
FOCUS-CONTENT-1	A focused threat intelligence production MUST be associated with a tag related to the subject matter at hand.

ID	Description
FOCUS-SHARE-1	Tagged threat intelligence SHOULD be shared with either the global community or specific groups accordingly to GLOBAL-SHARING-2

ID	Description
FOCUS-SHARE-2	Each Tag SHOULD be associated with a policy rule (by default applicable TLP and PAP) that would be transmitted accordingly to GLOBAL-SHARING-5.

ID	Description
FOCUS-SHARE-3	It SHOULD be possible to ingest the focused threat intelligence based on a tag selection to create a specific feed



CYBER-ATTACK INCIDENT REPORT

The highest value of threat intelligence comes from the willingness to share details on cyber-attacks or incidents our peers previously dealt with.

This means targeted or impacted entities endorse the “sharing is caring” approach and accept to disclose part of their investigation results or observations to help other organizations to adapt their cyber defence posture.

ID	Description
INCIDENT-CONTENT-1	Incident modelling MUST be evidence-based. Assumptions are authorized but the confidence SHOULD be rated accordingly.

The highest value of threat intelligence comes from the willingness to share details on cyber-attacks or incidents our peers previously dealt with.

ID	Description
INCIDENT-CONTENT-2	Incident modelling SHOULD allow to describe several objects related to the incident. The more precise the incident timeline is, the better the protection will be for others. STIX incident extension would be the most suitable format

ID	Description
INCIDENT-TIME-1	Each artefact associated with the incident MUST be timestamped precisely to establish an attack timeline

ID	Description
INCIDENT-SHARING-1	The author of the incident report and other related threat intelligence might not feel comfortable to have his name or the organization disclosed. Accordingly with GLOBAL-SHARING-4, an anonymization option SHOULD be offered

SIGHTING AND OBSERVATIONS WITHIN A COMMUNITY

Within a community, some stakeholders have the capability to observe technical activities, either on IT systems or on the network.

Using this capability with threat intelligence can provide statistics on observed indicators. These observations are useful to gain insight into attack trends:

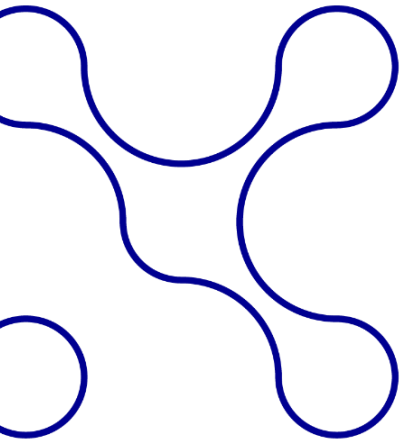
- Is there any observation of an attack within a community?
- Is there a peak of malicious activity at a precise time?
- When did it start?
- When did it stop?

To make it real and efficient, some rules have to be considered.

ID	Description
SIGHTING-LOCATION-1	The location of the sighting SHOULD be detailed to have a clear understanding on where it was observed. It could be into the author perimeter or into another environment.

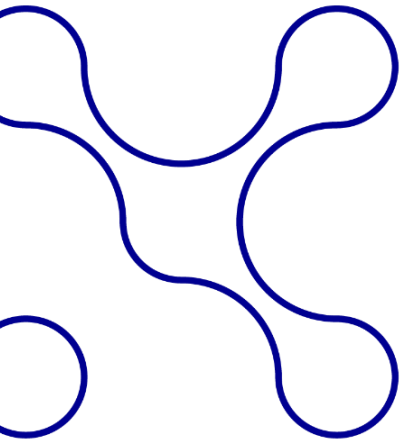
ID	Description
SIGHTING-TIME-1	The sighting MUST have a timestamp ○ First seen timestamp ○ A last seen timestamp

ID	Description
SIGHTING-CONTENT-1	The sighting MUST provide a “count” number to clarify the number of observed occurrences.



ID	Description
SIGHTING-CONTENT-2	The sighting MUST refer to an indicator or more precisely to an observable related to an indicator

ID	Description
SIGHTING-HISTORY-1	Sighting changes SHOULD be kept. A simple illustration would be: update with count+1 & last_seen=current_time. A history of these updates would allow to build a timeline of sighting evolution



OPERATIONAL GUIDELINES

HOW TO USE STIX OBJECTS

CAMPAIGN

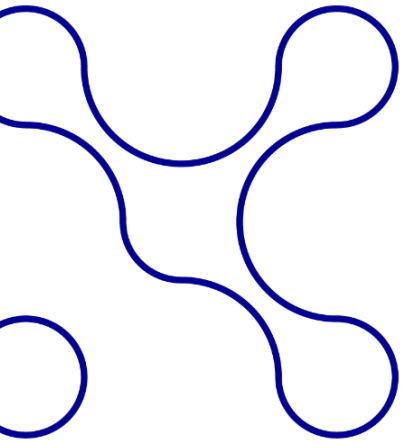
This object is the central one to describe a threat and its impact.

Make sure that:

- The campaign is properly dated. If not available in the report, please use the first seen of available IOC as a starting date of the documented campaign.
- Campaign description is a summary of the reported cyber malicious activity, if available, make sure to include – origin, date, and duration of the campaign, observed victimology.
- The campaign is properly and transparently named. If available, campaign name includes (in this order) – name of the Intrusion Set, reported victimology (i.e., country, geographical area, verticals) and used tool/malware/TTP. When given, campaign code name, e.g., “BlueBanana Operation”, is included as an alias name of the object. For instance – APTXX targets finance related organizations in Europe with InfoData Backdoor.
- The campaign is properly sourced (source name and reference).
- Relationships are properly made.

The campaign is properly and transparently named.

! *All IOCs and TTPs should be linked to a campaign by default.*



INTRUSION SET (IS)

Based on OASIS description, an Intrusion Set is a grouped set of adversarial behaviours and resources with common properties that is believed to be orchestrated by a single organization. An Intrusion Set may capture multiple Campaigns or other activities that are all tied together by shared attributes indicating a commonly known or unknown Threat Actor. New activity can be attributed to an Intrusion Set even if the Threat Actors behind the attack are not known. Threat Actors can move from supporting one Intrusion Set to supporting another, or they may support multiple Intrusion Sets.

Make sure that IS:

- Includes at least one relationship with a campaign, a malware, and / or a Location, a Sector, TTPs.
- Is properly described. Intrusion Set description exclusively includes first observed activity, past targeted countries, and sectors, as well as a description of their toolbox.
- Is properly named with all aliases. Main IS name is chosen by the analyst, based on the most well-known alias in the CTI community. (i.e., APT28 is wider known than Fancy Bear or STRONTIUM)
- Public attribution can be included, notably with hyperlink either directing to open-source reports or threat actors' entries.
- Displays a goal (limited to the following - Espionage, Lucrative, Influence, Sabotage, Disruption)
- Resource level and motivations fields are optional.
- Includes at least one source (source name + URL in external references).
- Includes a "last update" mention at the end of the description for update purposes.

! *In the case of private companies or individuals developing malware used by unrelated Intrusion Sets (such as NSO Group, or Malware-as-a-service or MaaS)*

those are not represented as Intrusion Sets. In the context of Ransomware-as-a-Service (RaaS), there is a relationship (attributed to) between the ransomware operators (Intrusion Set) and the coordinator of the affiliate program (Threat actor).

THREAT ACTOR (TA)

As per OASIS definition, Threat actor (TA) Threat Actors are actual individuals, groups, or organizations believed to be operating with malicious intent. A Threat Actor is not an Intrusion Set but may support or be affiliated with various Intrusion Sets, groups, or organizations over time. Threat Actors leverage their resources, and possibly the resources of an Intrusion Set, to conduct malicious cyber campaigns against targets. Threat Actors can be characterized by their motives, capabilities, goals, sophistication level, past activities, resources they have access to, and their role in the organization.

When available, a TA can be associated to a Location object (originates from).

A Threat Actor is not an Intrusion Set but may support or be affiliated with various Intrusion Sets, groups, or organizations over time.

VULNERABILITY

Make sure that Vulnerability:

- Name's contains the name of the vulnerable solution / equipment / software etc and its provider.
- Contains a short yet relevant description of the vulnerability (impacted versions, date of patch)
- Is properly sourced (name + URL as external reference).

MALWARE

Make sure that Malware:

- Is properly described, using multiple sources if needed (intrusion vector, installation including registry keys for instance, C2 communication process, encryption etc.).
- Includes at least one relationship with a campaign, an indicator, and / or an Intrusion Set, a Location, a Sector.
- Is properly associated (authored by / used/ targets)
- Displays a KillChain phase.

- Displays a MITRE ATT&CK TTP.
- Includes all sources (source names + URLs as external references)
- Is properly dated (first seen

TOOL

Make sure that Tool:

- Is properly described, using multiple sources if needed.
- Includes at least one relationship with a campaign, and / or an indicator, an Intrusion Set, and Is properly associated with another malware (variant-of, drops, uses, controls, downloads)
- Displays a KillChain phase.
- Displays a MITRE ATT&CK TTP.
- Includes all sources (source names + URLs as external references)

! *As tools mentioned in CTI activities are leveraged with malicious intent, it can sometimes be complex to differentiate between tool and malware.*

Rule of thumb is that malware are used for intrusion and data theft by-design, while tool can also be used for legitimate purposes. For instance :

TOOL	MALWARE
WinRAR	Cobalt Strike
Filezilla	Pupy RAT
ConnectWise	
Mimikatz	

When multiple tools are “packaged” (i.e., Mex), and as it is not possible to create relationships between tools, it is allowed to create a malware object, whose description must include all observed tools.

INDICATOR

While Indicators can be automatically created as final objects, most of them should be related to observables.

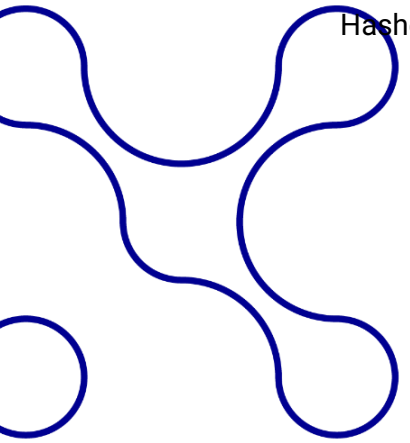
Make sure that indicator:

- Includes at least one relationship with a campaign, a malware, and / or an Intrusion Set.
- Is properly dated (upon verification on VT, RiskIQ etc. or based on internal mechanisms).
- Displays a KillChain phase aligning on the object it indicates.
- Displays a MITRE ATT&CK TTP, aligning on the object it indicates.
- Displays a Sigma pattern (if not automated through the indicator module).
- Includes at least one source (source name).

When creating a relationship between an Indicator and another object, it is possible to assess the credibility of said relationship. By default, confidence rating is 1.

Observables often related to indicators include:

Autonomous System	Organization	Individual
Filename	IPv6	Email Address
MAC Address	IPv4	Phone Number
Mutex	User Account	Domain Name
URL	Windows Registry Key	Text
X509 Certificate	File	Directory
Hashes	Address	



LOCATION

This object is added to indicate the origin or the target of the documented malicious cyber activity.

Make sure that Location:

- Includes at least one relationship with a campaign, and / or an indicator, an Intrusion Set, a Threat Actor
- Displays a proper relationship (targets / originates from)

IDENTITY

This object is added to indicate the origin or the target of the documented malicious cyber activity

This object is used for:

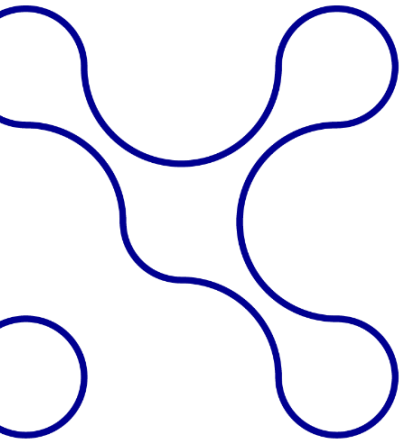
- A new source (“is a source” option)
- Individuals
- Targeted organisations

For the two latter, make sure that context and relevant information are provided, and that it is properly sourced (name + URL as external reference).

! *When a source, Identity will never show any relationship with other objects. In a context of doxing or public indictment of individuals involved in malicious cyber campaigns (developers, operators), while it would be tempting to create an entity for said individuals, those are considered as Threat Actors.*

ATTACK PATTERN (AP)

This object represents Tactics, Techniques and Procedures (TTPs) observed in the campaign. It should be based on the MITRE ATT&CK framework and is complementary to the TTPs provided in the Malware object. It should automatically feed the Course Of Action (CoA) objects.



COURSE OF ACTIONS (COA)

This object defines solutions that can be enforced to protect against something (mostly Attack pattern). COA should be automatically added when the Attack Pattern is properly informed.

OFFICIAL STIX BEST PRACTICES

Official guide is available at:
https://docs.google.com/document/d/1Az8_zLgYMTcLOeKBqIpheBH1YwXX-Zt6/edit