Threat Intelligence Sharing Agreement

version 1.2

Introduction

This document sets out the rules of engagement for using the CERN MISP instance at *https://misp.cern.ch*. It covers the use of the threat intelligence shared using this service.

Community-based incident response

CERN strongly believes that sharing sensitive information among the community is the best way to fight sophisticated adversaries at acceptable costs, and it fundamentally relies and contributes to a community-based incident response model to respond to global threats.

The effectiveness of this model solely relies on all trusted parties and both their commitment and ability to share back positive or negative sightings, false positives as well as any specific indicator or contextual information they are allowed to share with the community.

Information usage policy

The information shared via the CERN threat intelligence sharing platform may be used exclusively for the benefit of the trusted parties, solely for the purpose of detecting, containing, mitigating and resolving security attacks.

Whenever TLP guidelines are insufficient and not specific enough to take appropriate action, please contact cert-sec@cern.ch for clarifications. Generally, CERN commits to, and encourages its trusted partners to:

- For non-public information, work on a “need-to-know” basis
- For personal information, conduct a privacy impact assessment to understand risk–benefit ratio
- Adopt a risk-based strategy, commensurate to the scale of the issue at hand

All information not specifically tagged with a TLP flag must be considered TLP:AMBER.

SCI

CERN fully supports the adoption of the SCI trust framework version 2 as defined in:
https://wise-community.org/wp-content/uploads/2017/05/WISE-SCI-V2.0.pdf

In particular, CERN implements, and also expect its trusted partners to support, the [IR] assertions below:

[IR1] A process to maintain security contact information for all service providers and communities.

[IR2] A documented Incident Response procedure. This must address: roles and responsibilities of individuals and teams, identification and assessment of incidents, minimisation of damage to the infrastructure, response and recovery strategies to restore services, communication and tracking tools and procedures, and a post-mortem review to capture lessons learned.

[IR3] The capability to collaborate in the handling of security incidents with affected service providers, communities, and infrastructures, together with processes to ensure the regular testing of this capability.

[IR4] Policies and procedures to ensure compliance with information sharing restrictions on incident data exchanged during collaborative investigations. If no information sharing guidelines are specified, incident data will only be shared with other security teams on a need to know basis, and will not be redistributed further without prior approval.

Commitments

As a trusted party using the CERN threat intelligence sharing platform, you confirm you commit to:

- Follow and obey the TLP guidelines and sharing restrictions
- Follow and obey the SCIv2 trust framework assertions above
- Follow and obey the information usage policy
- Share back information whenever you believe it may be beneficial to a trusted party and are in a position to do so

CERN highly values the confidence and the trust placed on it by its partners and fully commits to all the points above.

Violations and sanctions

Trust violations are particularly detrimental to a community-based response to security threats. Information sharing violations are taken extremely seriously and your access to the CERN threat intelligence sharing platform may be revoked at any time temporarily or permanently without notice.

Appendix: traffic Light Protocol

CERN and its threat intelligence sharing platform extensively rely on the Traffic Light Protocol (TLP) as defined at https://www.first.org/tlp/, in particular:

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:WHITE = 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.

If a recipient needs to share the information more widely than indicated by the original TLP designation, they must obtain explicit permission from the original source.

Dr. Moisés Torres Martínez
Director General de CUDI

Document versioning		
12th Jun 2020	Romain Wartel	Initial draft
18th Jun 2020 - v1.1	Romain Wartel	Modifications from David Crooks, Dave Kelsey, Ian Neilson, Liviu Vâlsan
12th Jul 2023 - v1.2	Romain Wartel	Updated the TLP version