# Questionnaire: Sharing Cyber Threat Intelligence

We are attempting to better understand how (cyber) threat intelligence is shared within the security community. This questionnaire is prepared to give data that may give valuable insight. We will publish all results of our data analysis.

Definition of flat file:

"A file having no internal hierarchy. Typically email content, .txt, .csv, flat json."

"A flat file contains records that have no structured interrelationship. A flat file typically consists of a text file, from which all word processing or other structure characters or markup have been removed."

If you want to share data with no hierarchy or interrelationships, you may use flat files. If you want to share information or knowledge this would arguably require the use of describing relationships between data points, and this would require some other way of communicating. STIX gives the opportunity to do this (but is not the only option).

Part 1: About the respondent

1. What is your role in your organization (examples can be incident responder, threat hunter, security analyst)?
2. Are you in a role where sharing cyber threat intelligence is part of your role/tasks?
3. What is the size of your organization (approx. number of employees)?
4. What sector do you represent?
5. Which country are you from?

Part 2: About sharing CTI

1. Are you or your organization a producer or a consumer of threat intelligence?
2. In what format was the last piece of threat intelligence you SHARED with others?
3. In what format was the last piece of threat intelligence you CONSUMED?
4. Please estimate what percentage(%) of your consumed threat intelligence over the last 6 months was WITHOUT structured interrelationships within the data:
5. Please estimate what percentage(%) of your consumed threat intelligence over the last 6 months was WITH structured interrelationships within the data:
6. Do you STORE the consumed threat intelligence in a structured and easily accessible way?
7. Many use threat intelligence directly for defence purposes, for example, directly in block lists. Further analysis of the threat intelligence may add value. Do you use all your consumed threat intelligence in your organization for analysis?
8. What is the single most common reason, related to personal or professional circumstances, for you NOT to share threat intelligence?

Part 3: About STIX

1. Have you used STIX (any version) in the past 6 months?
2. If you use STIX, which version are you mainly using?
3. Have you manually consumed a STIX file in the past 6 months?
4. Have you automatically consumed a STIX file in the past 6 months?
5. If automatic consumption: do you manage to consume all information enclosed in any STIX file?
6. Have you created a STIX file in the past 6 months?
7. List of all SDOs and Relationships in STIX 2.1. with “used”/”not used” options.

Published with nettskjema.no in june-august 2019.