

Rapport fra «Questionnaire: Sharing Cyber Threat Intelligence»

Innhentede svar pr. 1. oktober 2020 13:34

- Leverte svar: **36**
- Påbegynte svar: **0**
- Antall invitasjoner sendt: **0**

Med fritekstsvar

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

What is your role in your organization (examples can be incident responder, threat hunter, security analyst)? *

- Incident responder
- Security Analyst
- Security manager
- Analyst
- Head of IT Security
- Security Engineer
- Researcher
- Cyber security advisor
- Security Analyst/Team leader
- Analyst
- CSIRT member
- Senior Cyber Security Advisor
- Strategic Threat Intelligence
- Incident responder / Security Analyst
- All of them
- threat hunter
- Security analyst
- Architect
- Information Security Engineer
- Analyst
- Security Analyst
- DPO/InfoSec Consultant/Security Analyst
- Teamlead CSIRT Europe
- security analyst
- Intelligence analyst
- security consultant
- Security analyst
- Threat Analyst
- Architect
- Threat Researcher
- Analyst
- Security Analyst
- SOC Operations Manager
- Threat Hunter
- Manager
- Threat intel lead

Are you in a role where sharing cyber threat intelligence is part of your role/tasks? *

Svar	Antall	Prosent	
Yes	30	83,3 %	
No	6	16,7 %	

What is the size of your organization (approx. number of employees)? *

- 60
- 200
- 150
- 500-1000
- 4200
- 400,000
- 1,000+
- 3000

- 8-10000
- 7000
- 16000
- 3500
- 1200
- 10000+
- Thousands
- 100
- 3000
- 25000
- 500
- 200+
- 300
- 50
- 270000
- 10000
- 500
- 5000
- 70000
- 100
- 2000
- 5000
- 20
- 250
- 100000
- 1200
- 3500
- 10000

What sector do you represent? *

- Service producer
- MSSP
- Fintech
- Defense
- Automotive, IoT, IIoT
- Maritime
- Telecom
- Public
- Academic
- Finance
- Banking
- Aviation
- Financial
- Retail
- Telecom
- cyber security
- Telecom
- Telecom
- IT-sector
- IT Sec
- Government
- Public
- Engineering
- Finance
- Government
- tech
- Law enforcement
- IT Security
- Government
- Security Software
- Government
- R&D
- Defense
- Government
- Security
- Finance

Which country are you from? *

- FIN
- Norway
- Norway
- Norway
- Germany
- Norway
- Japan
- Norway
- Norway
- Norway
- Estonia
- Norway
- Norway

- Norway
- United States
- germany
- Japan
- Norway
- Norway
- Norway
- Malaysia
- Danmark
- Germany
- Norway
- Norway
- USA
- Netherlands
- Germany
- Norway
- United States
- Switzerland
- Norway
- United States
- Germany
- Finland
- Norway

Part 2: About sharing and consuming threat intelligence

Are you or your organization a producer or a consumer of threat intelligence? *

Svar	Antall	Prosent	
Producer	0	0 %	
Consumer	11	30,6 % 	
Both	25	69,4 % 	

In what format was the last piece of threat intelligence you SHARED with others? *

- Flat
- plain text
- N/A
- Email
- Portal feed
- PDF
- MISP, CSV, Plain text
- Email
- MISP
- PDF
- MISP JSON
- txt
- PDF
- Shared a link via Social media such as twitter, facebook or linkedin
- Flat file IOCs from OSINT source
- csv
- Email
- Flat file
- written report, pdf document
- PDF
- In MISP and alienvault otx
- Don't know, other did thay
- None
- Blog post
- STIX
- flat
- Stix / taxii
- MISP
- None, our partners may have done it on our behalf.
- Threat Report
- MISP entry (JSON)
- NA
- PDF - EWIN (Early Warning Intelligence)
- SIGMA
- PDF
- Flat

In what format was the last piece of threat intelligence you CONSUMED? *

- Flat
- plain text
- Email
- Article
- PDF Report
- PDF
- MISP, CSV, Plain text

- Email
- Stix, MISP, Csv, raw
- PDF
- JSON via API endpoint
- txt
- PDF
- A shared link from Social media such as twitter, facebook or linkedin
- Same as above
- misp (stix/csv/json?)
- STIX
- Flat file
- video webcast
- PDF
- In MISP and alienvault otx
- PDF
- MISP
- email
- Text
- flat
- Stix / taxii
- MISP
- Encrypted email
- XML
- PDF
- csv
- programmatically via RESTful API
- SIGMA
- PDF
- Flat

Please estimate what percentage(%) of your consumed threat intelligence over the last 6 months was WITHOUT structured interrelationships within the data: *

Definition of f

lat 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."

- 100
- 100%
- 100%
- 80
- 90
- 70%
- 70
- 90%
- 80%
- 50%
- 60%
- 80
- 100
- 10
- 25%
- 50
- 80
- 100
- 0
- More than 50%
- 95
- 0
- 100
- 99
- 80%
- 100%
- 5
- 75%
- 100%
- 80
- 90%
- 100
- 60
- 90
- 95%
- 100%

Please estimate what percentage(%) of your consumed threat intelligence over the last 6 months was WITH structured interrelationships within the data: *

Definition of f

lat 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."

- 0
- 0%
- 0%
- 20
- 10
- 30%
- 30
- 10%
- 20%
- 50%
- 40%
- 20
- 0
- 90
- 25%
- 50
- 20
- 0%
- 80%
- 100
- More thqn 50%
- 5
- 100
- 0
- 1
- 0
- 95
- 25%
- 0
- 20
- 10%
- 0
- 40
- 10
- 5%
- 0%

Do you STORE the consumed threat intelligence in a structured and easily accessible way? *

Svar	Antall	Prosent	
Yes	11	30,6 % 	
No	7	19,4 % 	
Partially	18	50 % 	

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? *

Svar	Antall	Prosent	
Yes	12	33,3 % 	
No	24	66,7 % 	

What is the single most common reason, related to personal or professional circumstances, for you NOT to share threat intelligence ? *

- Lack of further analysis of the situation
- lack of trust
- Where and how to share it?
- Classification and source protection
- Time and proper channels to do so
- Content may contain critical information. Revealing parts of our Enterprise IT infrastructure. If PII is inside a CTI event it may not be GDPR conform. Trust levels with other stakeholders may be too low. No IEP in place.
- TLP:RED
- Not obliged to share, depends on the information
- Likely Highly damaging to individuals (privacy)
- Confidentiality
- Adding context to atomic indicators can be time consuming
- TLP limitation and no structured way
- Internal information classification or the sensitivity of the information can have severe consequences for the company.
- Not all TI is relevant to share, some does not apply
- Information on internal network threats
- legal issues/questions
- Personal information

- Trust
- not enough time
- TLP
- to ensure customer data privacy
- Source data already classified as TLP:Red.
- Sharing everything can obscure the important stuff
- Missing maturity, confidence and processes
- Time
- Sensitivity
- Not allowed to share by law, due to classification
- sensitivity (e.g. internal hostnames in malware config, campaign codes hinting at victim)
- We have outsourced threat intelligence.
- Much of it is client data and cannot be shared
- TLP:RED or Secret information
- Customers sensitivity
- TLP
- Confidentiality
- We sell intelligence so giving it away for free would undermine the business model
- capacity

Part 3: About STIX

Have you used STIX (any version) in the past 6 months? *

Svar	Antall	Prosent	
Yes	11	30,6 % 	
No	25	69,4 % 	

If you use STIX, which version are you mainly using? *

Svar	Antall	Prosent	
1.2 (XML)	2	18,2 % 	
2.0 (JSON)	9	81,8 % 	
Other	0	0 %	

Have you manually consumed a STIX file in the past 6 months? *

Svar	Antall	Prosent	
Yes	6	54,5 % 	
No	5	45,5 % 	




Have you automatically consumed a STIX file in the past 6 months?

Svar	Antall	Prosent	
Yes	11	100 % 	
No	0	0 %	

If automatic consumption: do you manage to consume all information enclosed in any STIX file?

Svar	Antall	Prosent	
Yes	3	27,3 % 	
No	8	72,7 % 	

Have you created a STIX file in the past 6 months?

Svar	Antall	Prosent	
Yes, STIX v1.2	3	27,3 % 	
Yes, STIX v2.0	3	27,3 % 	
Yes, other STIX version	0	0 %	
No	5	45,5 % 	

Which of the following STIX v2.0 Domain Objects have you used when creating STIX files?

Svar fordelt på antall

	Used	Not Used
Attack Pattern *	4	2
Campaign *	3	3
Course of Action *	3	3
Identity *	5	1

Indicator *	5	1
Intrusion Set *	4	2
Malware *	5	1
Observed Data *	4	2
Report *	3	3
Threat Actor *	5	1
Tool *	3	3
Vulnerability *	4	2

Svar fordelt på prosent

	Used	Not Used
Attack Pattern *	66,7 %	33,3 %
Campaign *	50 %	50 %
Course of Action *	50 %	50 %
Identity *	83,3 %	16,7 %
Indicator *	83,3 %	16,7 %
Intrusion Set *	66,7 %	33,3 %
Malware *	83,3 %	16,7 %
Observed Data *	66,7 %	33,3 %
Report *	50 %	50 %
Threat Actor *	83,3 %	16,7 %
Tool *	50 %	50 %
Vulnerability *	66,7 %	33,3 %

Which of the following STIX v2.0 relationships have you used when creating STIX files?

Svar fordelt på antall

	Used	Not used
Relationship *	4	2
Sighting *	3	3

Svar fordelt på prosent

	Used	Not used
Relationship *	66,7 %	33,3 %
Sighting *	50 %	50 %

This questionnaire is produced and distributed as part of the TOCSA project at the University of Oslo, in collaboration with mnemonic:

<https://www.mn.uio.no/ifi/english/research/projects/tocsa/>

Results will be published.

Se nylige endringer i Nettskjema (v1039_0rc165)