

Methodological Challenges In Investigating the UX of CTI Data Sharing Platforms

Borče Stojkovski

SnT, University of Luxembourg
borce.stojkovski@uni.lu

Vincent Koenig

COSA, University of Luxembourg
vincent.koenig@uni.lu

Gabriele Lenzini



SnT, University of Luxembourg
gabriele.lenzini@uni.lu

Salvador Rivas

COSA, University of Luxembourg
salvador.rivas@uni.lu

Cybersecurity

The ability to protect or defend the use of cyberspace from cyber attacks (NIST)



Definition of Cybersecurity
Gaps and overlaps in standardisation

V1.0
DECEMBER 2015



ENISA overview of cybersecurity and related terminology

VERSION 1
SEPTEMBER 2017

Cybersecurity Domains and Threats



Figure 1: ENISA Threat Landscape 2021 - Prime threats



Communication

Operations

Information

Physical

Public-National

Hacker-for-hire actors

Hacktivists

State-sponsored actors

Cybercrime actors

Cybersecurity Tools

Network Security Monitoring

Encryption

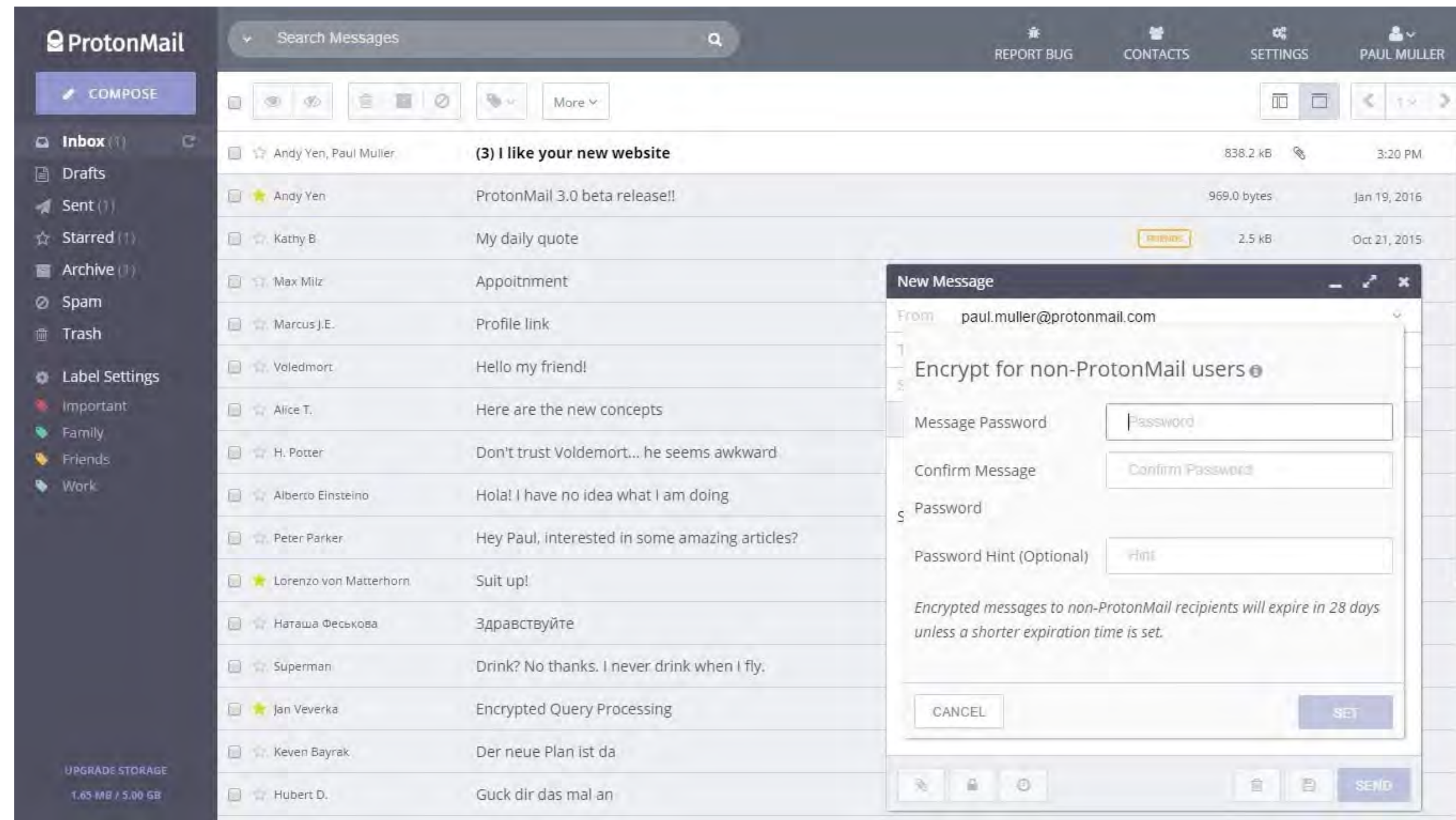
Web Vulnerability Scanning / Intrusion Detection / Sniffers

Penetration Testing

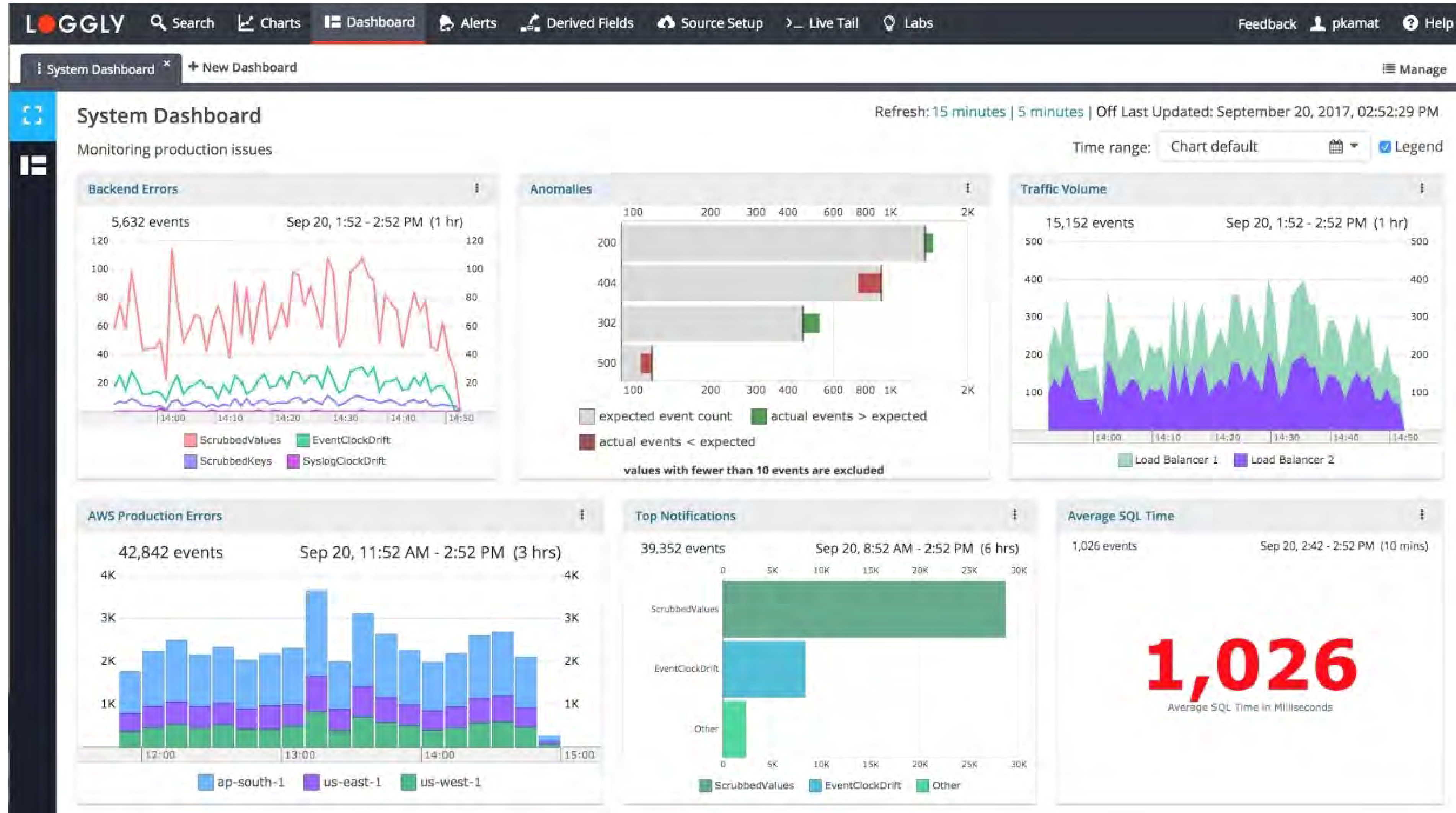
Antivirus

Cyber-Threat Intelligence Platforms

Small Business



Large/Medium Business



Cybersecurity Tools (sociotechnical viewpoint)

Network Security Monitoring

Encryption

Web Vulnerability Scanning / Intrusion Detection / Sniffers

Penetration Testing

Antivirus

Cyber Threat Intelligence

effectiveness?

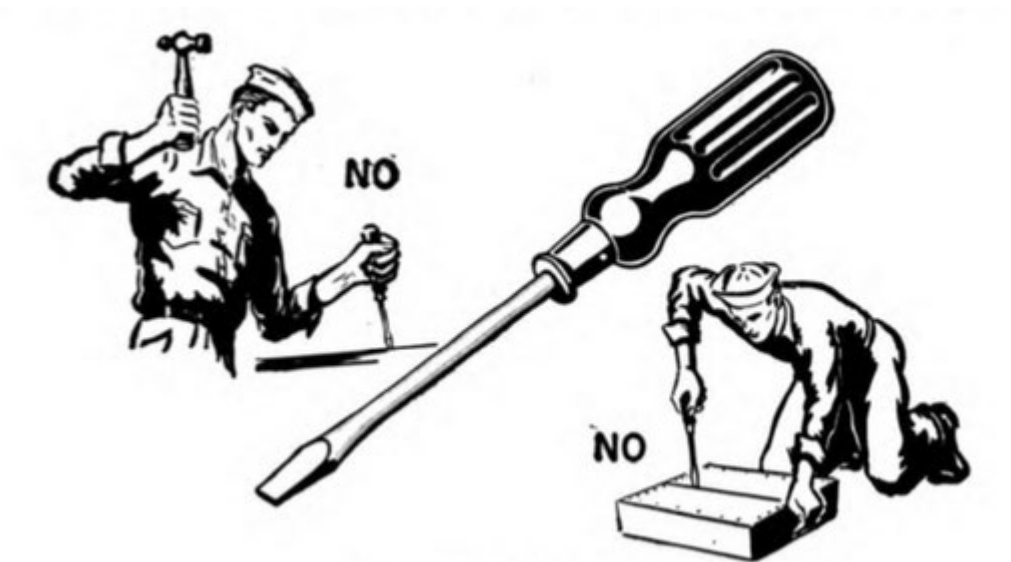
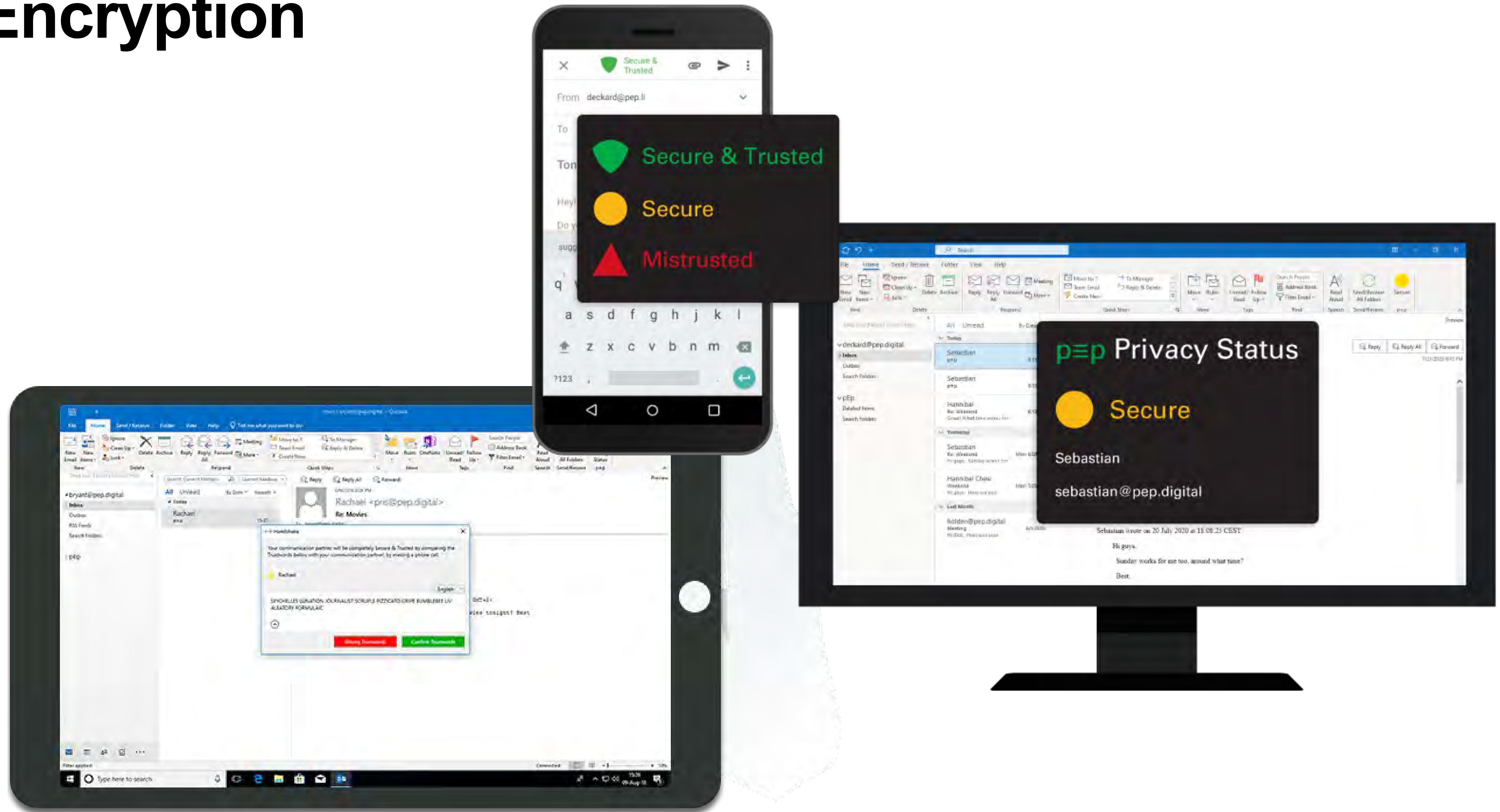


Figure 2.—It's the wrong tool!

Encryption



Cyber Threat Intelligence

Malicious activities

Event ID	10878
Uuid	5aec700c-0eb8-468
Org	CIRCL
Owner org	CIRCL
Contributors	
Email	alexandre.dulaunoy
Tags	+
Date	2018-05-04
Threat Level	Low
Analysis	Initial
Distribution	All communities
Info	Malicious activities
Published	No
#Attributes	2
Last change	2018/05/04 02:38:12
Extends	
Extended by	
Sightings	0 (0)
Activity	

10878: Malic...

Distribution graph [atomic event]

■ Your organisation only ■ This community only
■ Connected communities ■ All communities
■ Sharing group

All Attributes Object attributes

Your organisation only Connected communities
This community only All communities
Sharing group Event not distributed to any sharing group

2018-04-20
Your organisation only

Threat Level ?
Analysis ?

Low
Initial

Event Info

Ransomware found on a production server

Extends event

5ad8687b-0e10-4a8b-a157-46a5950d210f

Matched event

Id: 10728

Analysis: Completed

Threat level: Low

Tags:

- circl:osint-feed tlp:white
- malware_classification:malware-category="Ransomware"
- osint:source-type="blog-post"
- misp-galaxy:ransomware="CSGO Ransomware"
- misp-galaxy:ransomware="MC Ransomware"

Info: OSINT - Minecraft & CS:GO Ransomware Strive For Media Attention

50

estimative-language:confidence-in-analytic-judgment="high"

High

Well corroborated information from proven sources. Minimal assumptions. Strong logical inferences and methods. No on

Common Methodological Challenges

- Definition / Metrics (e.g., effectiveness)
- Appropriate Variables (e.g., for usability, UX)
- Methods and instrument of evaluation (e.g., questionnaire)
- **Ecological Validity (e.g., population)**

Cyber Threat Intelligence Platform

- **Collect**
- **Process**
- **Analyse**
- **Deploy**
- **Disseminate**

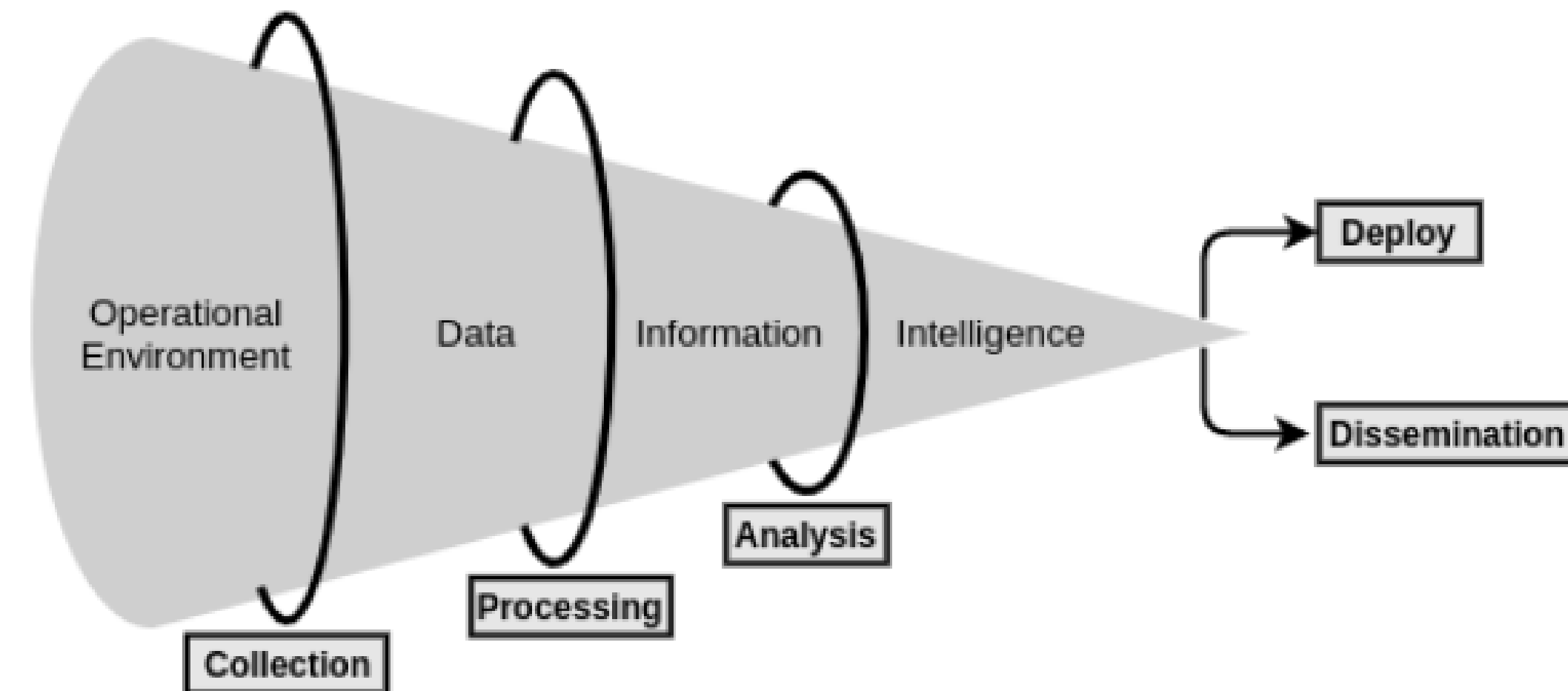


Figure 1. Threat Intelligence Production Process Flow.

From: *A Methodology to Evaluate Standards and Platforms within Cyber Threat Intelligence*. Alessandra de Melo e Silva , João José Costa Gondim Robson de Oliveira Albuquerque, and Luis Javier García Villalba, *Future Internet* 2020, 12, 108

Table 7. Evaluation of TI platforms.

	MISP [59]	OpenCTI [62]	CIF [63,64]	CRITs [60,61]	Anomali STAXX [65]
Holistic Architecture					
Use case applicability	++++	++++	+++		
Adherence 5W3H method	++++	++++	+		
Intelligence Process					
Import formats	OpenIOC, STIX, CybOX, JSON, CSV, XML	STIX, CybOX, JSON, CSV, XML	XML, JSON, Zip	CS	
Automatic gathering	Using MISP feeds	Using connectors with sources or other platforms	Automatic synchronization with different sources	Possib	g
Export format	MISP, OpenIOC, CSV, XML, JSON	CSV, STIX	CSV, JSON, HTML, XLS	CS	
Graphic visualization	General and intuitive dashboard and relationship graphics	Diverse dashboards and STIXv2 based graphics	Command line interface with possible integration with visualization tool	Simp	an ex gener
Correlation	Automatic for every data in platform	Automatic for every data in platform	Not addressed	Neces	
Classification	Based on the type of the indicator	Based on STIXv2 objects	Based on the type of the indicator	Based	
Integration	IDS, SIEMs and other TI platforms	Other TI platforms	IDSs (Snort, Splunk, Bro, Bind)	N	
Sharing method	Reliable group of instances using different models	Particular instance to share between users	Reliable group of instances using a centralized service	Reliabl	
Additional					
Documentation	Extensive and well elaborated	Extensive and well elaborated	Limited detail with succinct descriptions	Satisfa	
License model	Open Source (GNU General Public License)	Open Source (Apache License)	Open Source (GNU General Public License)	Open S	P

Legend: very high (++++) high (+++) medium (++) low (+).

Table 3. Evaluation criteria for CTI platforms.

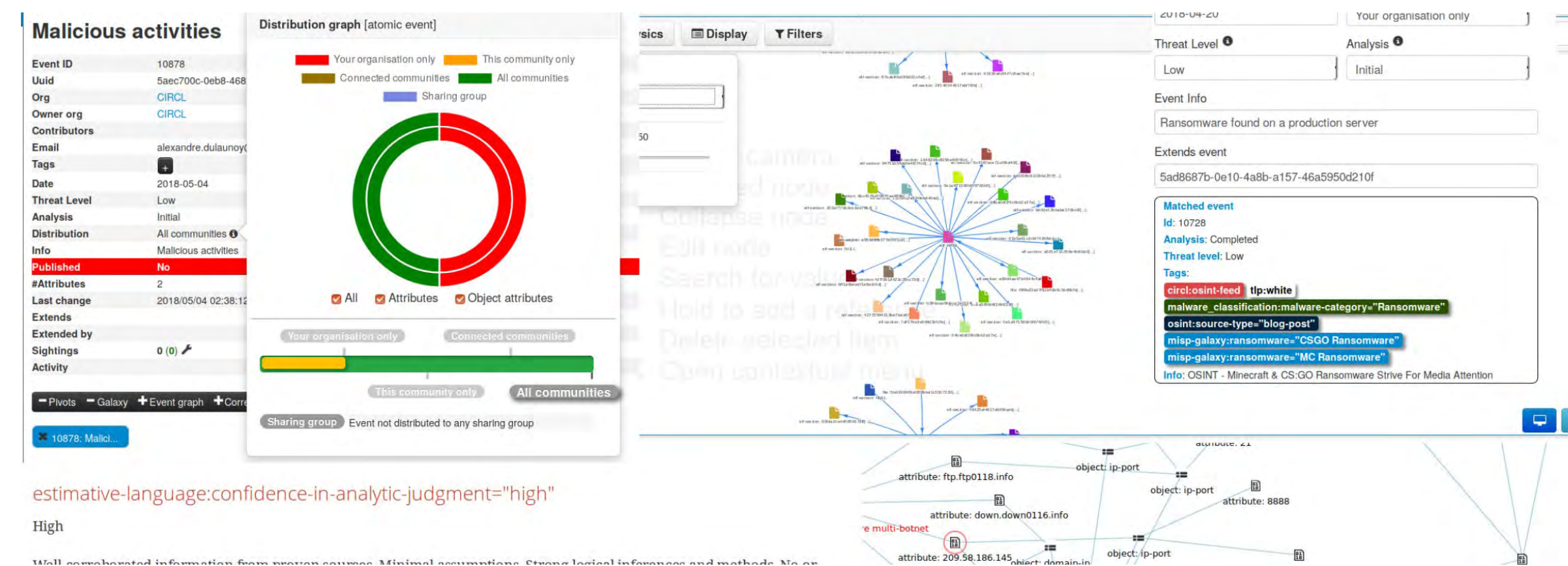
Data Model Architecture	
Holistic Architecture	Use case applicability
5W3H method	Answering capability
Intelligence Process	
Collection	Import formats
	Automatic gathering
Processing	Export format
	Graphic visualization
Analysis	Correlation
	Classification
Deploy	Integration with security systems
Dissemination	Sharing method
Additional	
Usability	Documentation
	License model

Research Questions

- How do different **security information workers** evaluate the UX of MISIP?
- What **do users value** about MISIP and **what do they think could be improved?**
- Which **user needs are addressed** and accounted for by MISIP?
- Which **are neglected?**

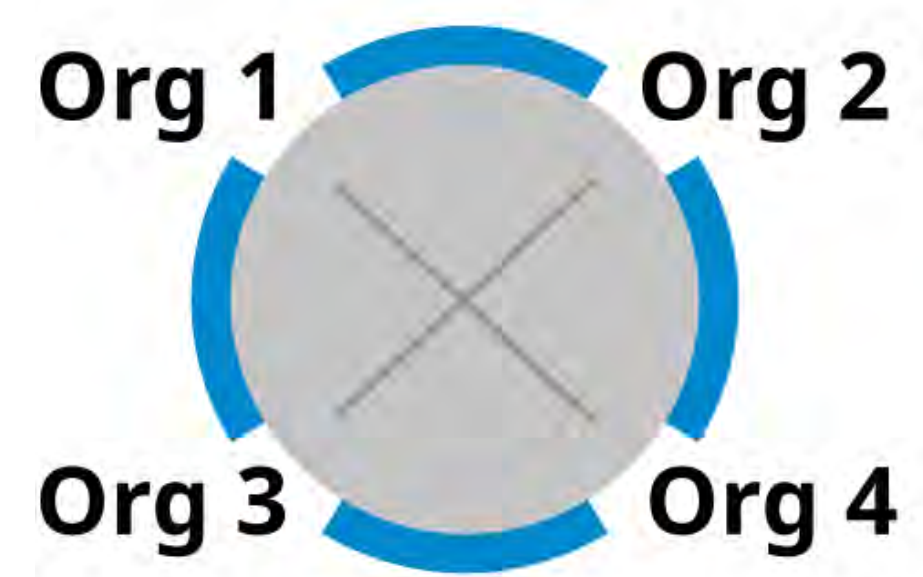
MISP

- A **leading** open-source CTI sharing platform
 - ▶ Inception within military circles 15 years ago
 - ▶ Used by over 6,000 organizations worldwide
 - ▶ UI and API users
 - ▶ Characterized as holistic and applicable in diverse scenarios

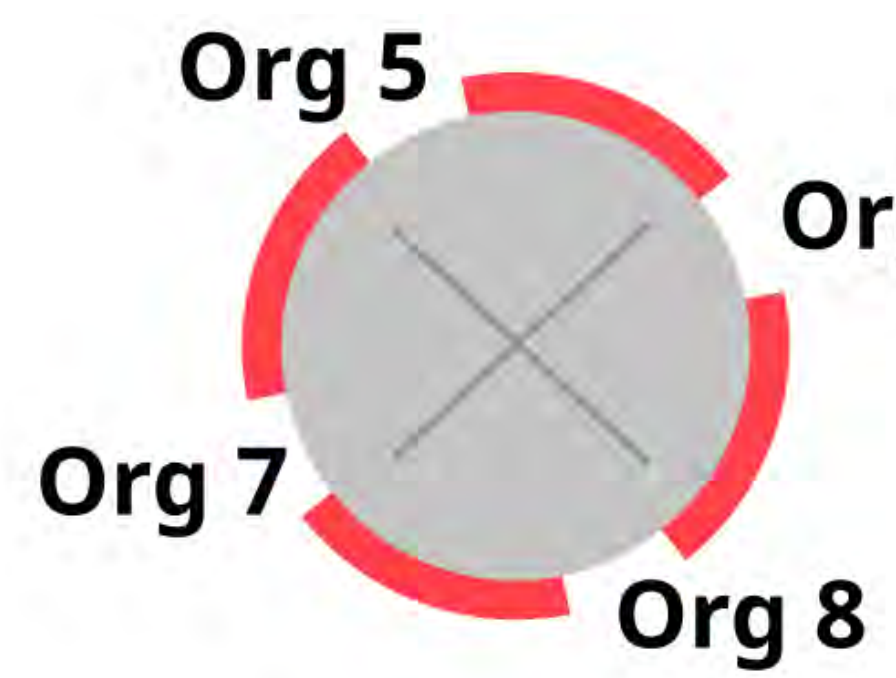


More info: <https://www.misp-project.org>

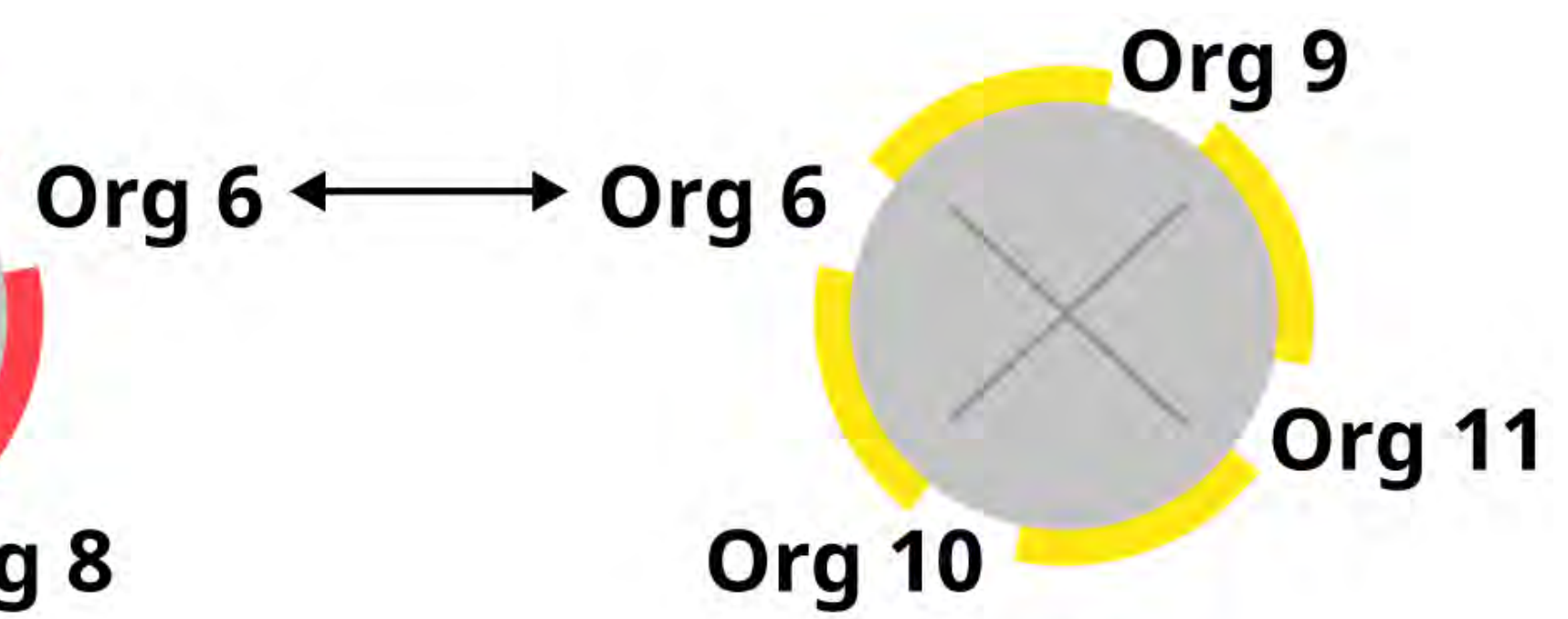
MISP: Sharing and Event Representation



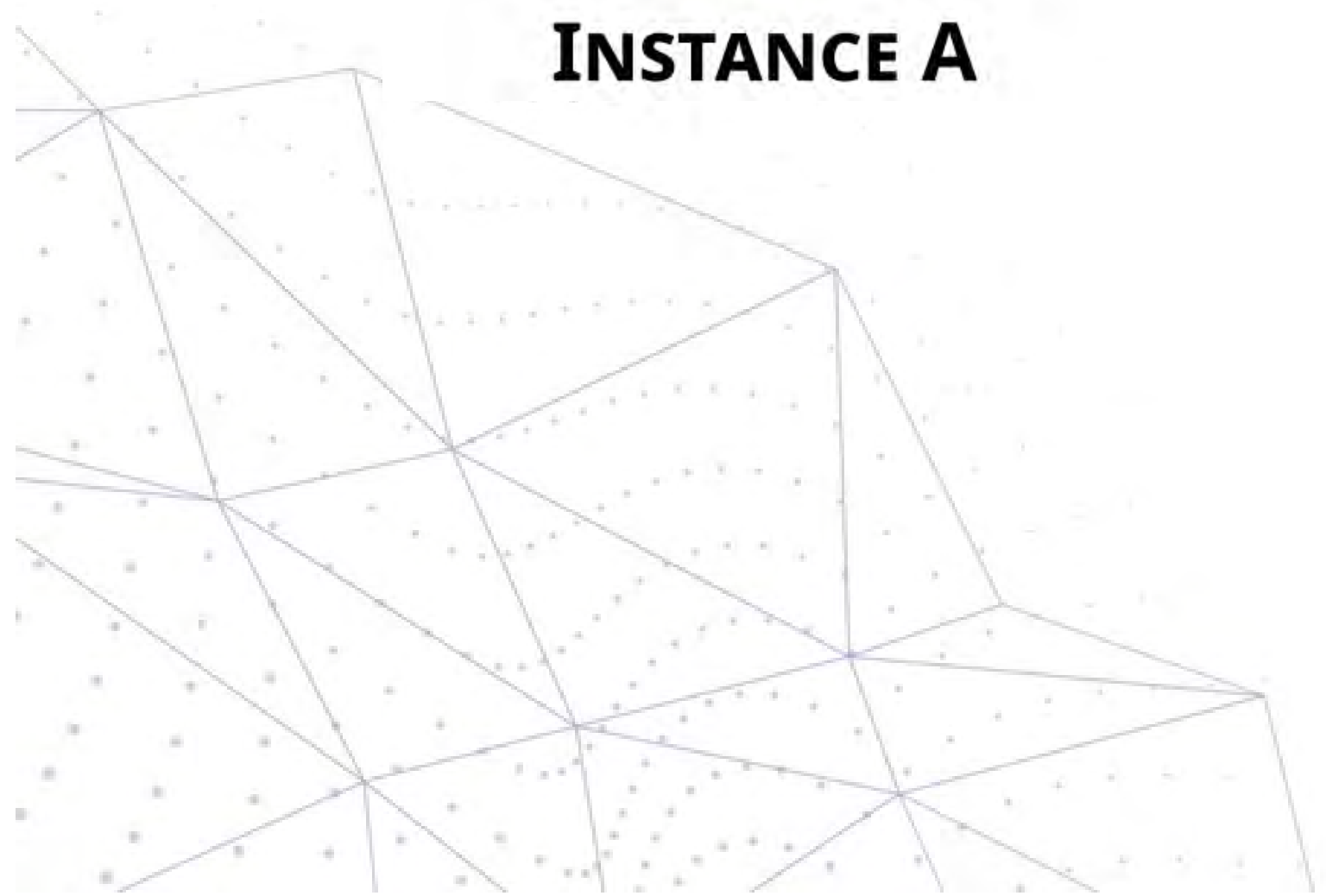
INSTANCE A



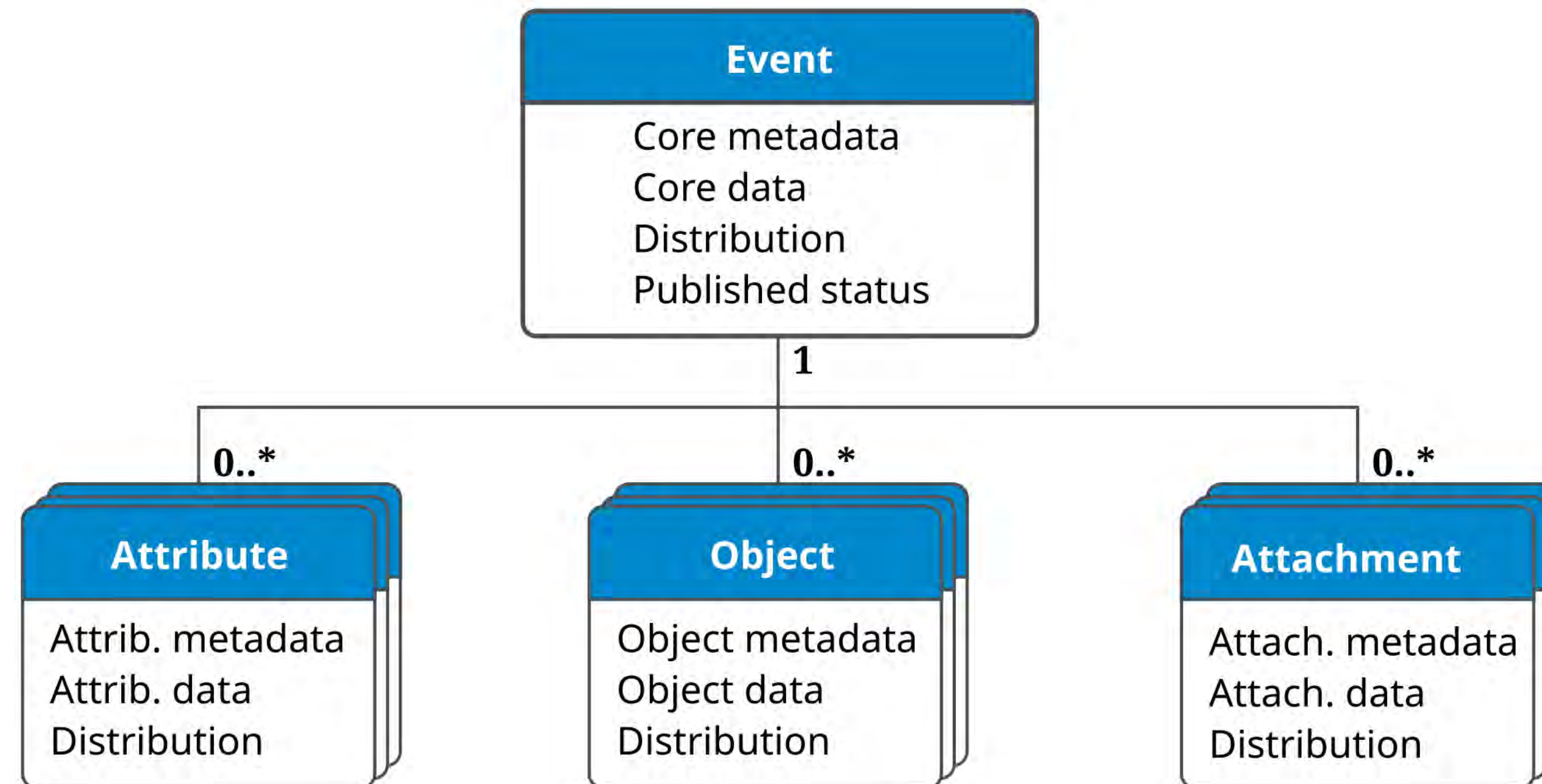
INSTANCE B



INSTANCE C



MISP: Sharing and Event Representation



MISP: Sharing and Event Representation



Methodological Challenges

Reaching out the “right” population

- Professionals (i.e., busy)
- Not always keen to be visible (i.e., sensibility)
- Users are not MISP contributors
- No known list of users

Research Questions

- How do different **security information workers** evaluate the UX of MISP?
- What **do users value** about MISP and **what do they think could be improved?**
- Which **user needs are addressed** and accounted for by MISP?
- Which **are neglected?**

Methodological Questions

How to reach out the “right” population?

- How to recruit?
- Where (e.g., at SPARTA, CyberSecurity4Europe)?
- How to incentivize participation?
- ...

Research Questions

- How do different **security information workers** evaluate the UX of MISP?
- What do **users value** about MISP and **what do they think could be improved**?
- Which **user needs are addressed** and accounted for by MISP?
- Which **are neglected**?

MISP Training Events

MISP Events

Want to join us at an event, discuss opportunities or projects around the MISP project, share your experience about threat intelligence or discuss how MISP could be improved to support security professionals?

MISP hackathon

- [Open Source Security Hackathon](#) - pen Source Security hackathon - Monday 25th October 2021 and Tuesday 26th October 2021

MISP at conferences

- [Virtual MISP Summit 0x06](#) - Thursday 21st October 2021.

Current MISP Training(s)

(some) Past MISP Training(s)

- (FULL) Thursday 25th February 2021 - Online MISP Training - Introduction to CTI (French) - [Registration](#)
- Tuesday 2nd March 2021 - Online MISP Training - MISP - Threat Intelligence Introduction for Analysts - [Registration](#)
- Wednesday 3rd March 2021 - Online MISP Training - MISP - Threat Intelligence for Administrators and Building Information Sharing Communities - [Registration](#)
- [MISP Covid training](#) Remote on how to use MISP in the scope of sharing information about COVID-19 - 27 March 2020 at 14:00 CET (2 hours)
- [MISP Training - Hands-on workshop for analysts and MISP users](#) in Luxembourg, February 19, 2020
- [MISP Training - Threat Intelligence Introduction for Analysts and Administrators](#) in Luxembourg, February 18, 2020
- [MISP Training \(Slovenia\)](#) in Ljubljana 2019 FIRST Technical Colloquium, November 13–14, 2019
- [MISP Training - Threat Intelligence Introduction for Analysts and Administrators](#) in Luxembourg, December 03, 2019
- [MISP Training - Hands-on workshop for analysts and MISP users](#) in Luxembourg, December 04, 2019

Attending MISP Training Events

Initial Install, please configure



Welcome to MISP on ubuntu, change this message in MISP Settings

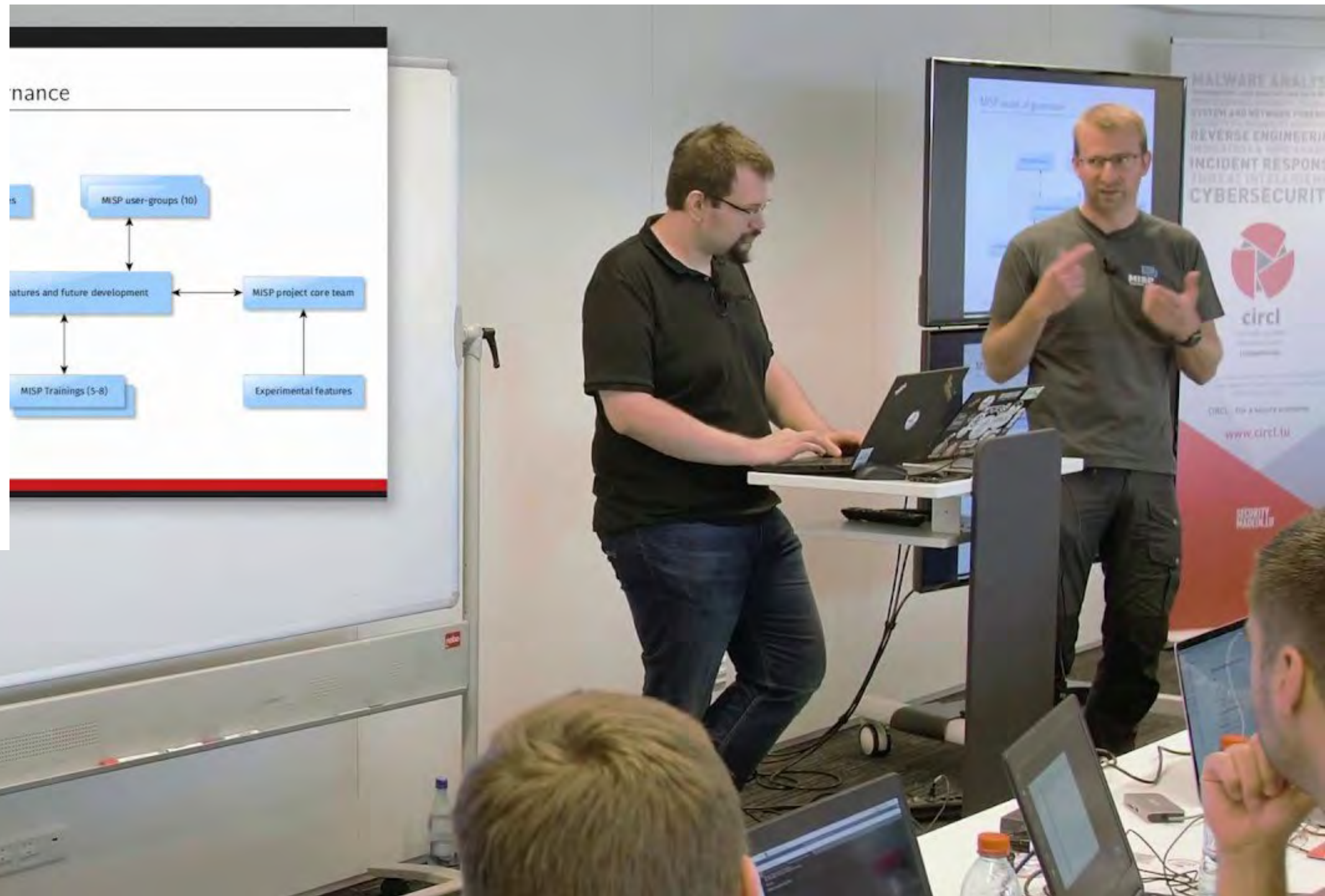
Login

Email

Password

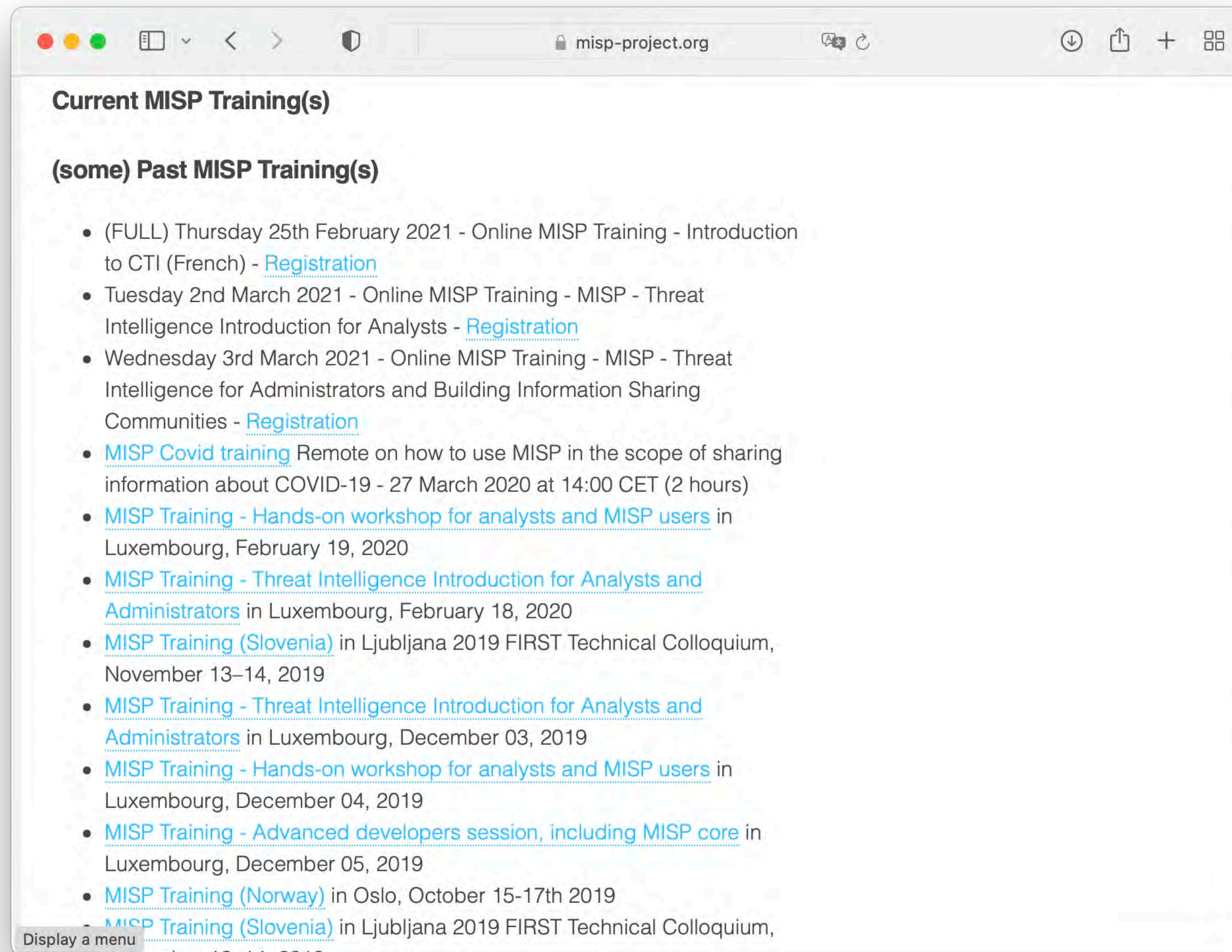
[No account yet? Register now!](#)

Login





Attending MISP Training Events



The screenshot shows a web browser window with the URL misp-project.org. The page content is as follows:

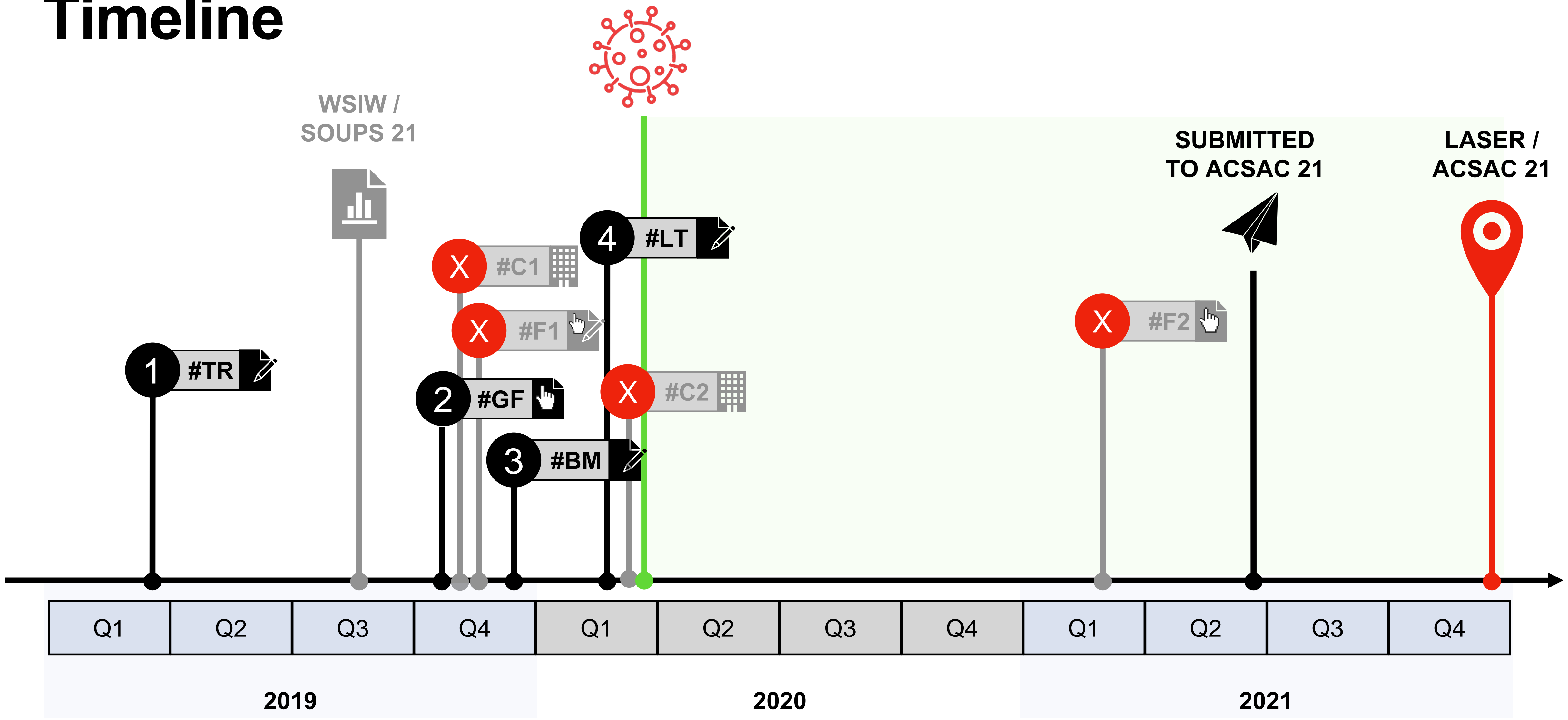
Current MISP Training(s)

(some) Past MISP Training(s)

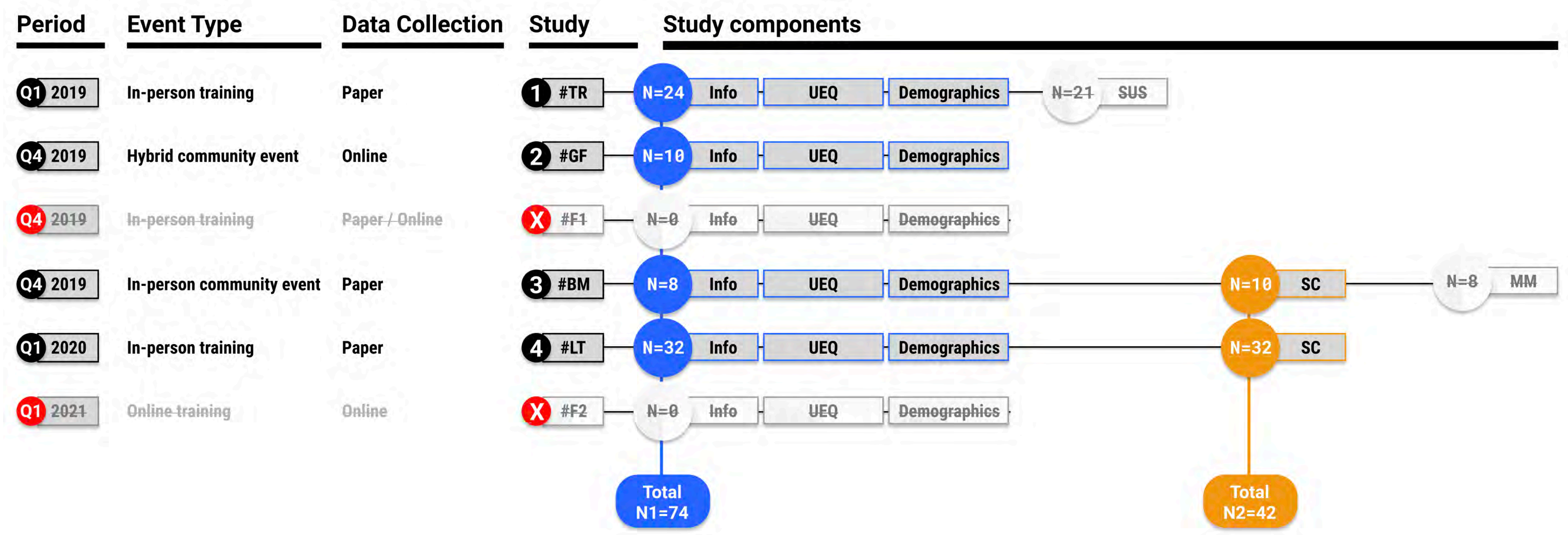
- (FULL) Thursday 25th February 2021 - Online MISP Training - Introduction to CTI (French) - [Registration](#)
- Tuesday 2nd March 2021 - Online MISP Training - MISP - Threat Intelligence Introduction for Analysts - [Registration](#)
- Wednesday 3rd March 2021 - Online MISP Training - MISP - Threat Intelligence for Administrators and Building Information Sharing Communities - [Registration](#)
- [MISP Covid training](#) Remote on how to use MISP in the scope of sharing information about COVID-19 - 27 March 2020 at 14:00 CET (2 hours)
- [MISP Training - Hands-on workshop for analysts and MISP users](#) in Luxembourg, February 19, 2020
- [MISP Training - Threat Intelligence Introduction for Analysts and Administrators](#) in Luxembourg, February 18, 2020
- [MISP Training \(Slovenia\)](#) in Ljubljana 2019 FIRST Technical Colloquium, November 13–14, 2019
- [MISP Training - Threat Intelligence Introduction for Analysts and Administrators](#) in Luxembourg, December 03, 2019
- [MISP Training - Hands-on workshop for analysts and MISP users](#) in Luxembourg, December 04, 2019
- [MISP Training - Advanced developers session, including MISP core](#) in Luxembourg, December 05, 2019
- [MISP Training \(Norway\)](#) in Oslo, October 15-17th 2019
- [MISP Training \(Slovenia\)](#) in Ljubljana 2019 FIRST Technical Colloquium, November 13–14, 2019

Display a menu

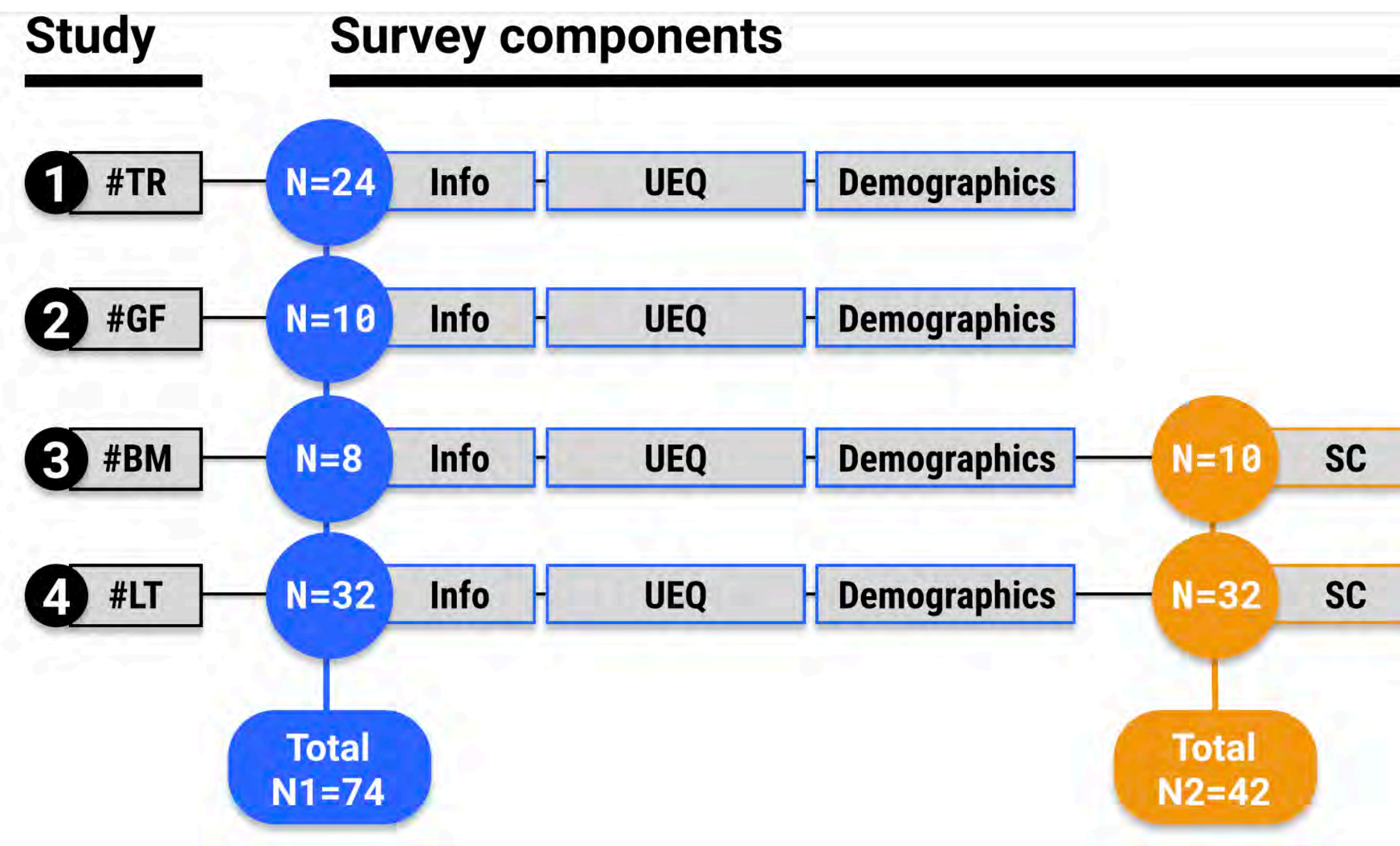
Timeline



Methodology



Methodology



Methodology (ACSAC paper materials)

MISP Threat Sharing **User Experience Questionnaire**

For the assessment of the MISP platform, please fill out the following questionnaire, which consists of pairs of contrasting attributes that may apply to the platform. You can express your agreement with the attributes by ticking the circle that most closely reflects your impression.

Example:
attractive unattractive

This response would mean that you rate the application as more attractive than unattractive.

Please decide spontaneously. Don't think too long about your decision to make sure that you convey your original impression. Sometimes you may not be completely sure about your agreement with a particular attribute or you may find that the attribute does not apply completely to the platform. Nevertheless, please tick a circle in every line, it is your personal opinion that counts. Please remember: there is no wrong or right answer!

	1	2	3	4	5	6	7	
annoying	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	enjoyable
not understandable	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	understandable
creative	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	dull
easy to learn	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	difficult to learn
valuable	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	inferior
boring	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	exciting
not interesting	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	interesting
unpredictable	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	predictable
fast	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	slow
inventive	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	conventional
obstructive	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	supportive
good	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	bad
complicated	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	easy
unlikable	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	pleasing
usual	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	leading edge
unpleasant	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	pleasant
secure	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	not secure
motivating	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	demotivating
meets expectations	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	does not meet expectations
inefficient	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	efficient
clear	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	confusing
impractical	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	practical
organized	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	cluttered
attractive	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	unattractive
friendly	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	unfriendly
conservative	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	innovative

MISP Threat Sharing **MISP Users - Questionnaire**

The purpose of this questionnaire is to better understand the types of users and their respective needs on the MISP platform. Participation is voluntary.

1. Which of the following roles best describes how you (intend to) use MISP?

- Malware reverser: e.g. willing to share indicators of analysis with respective colleagues
- Security analyst: e.g. searching, validating and using indicators in operational security
- Intelligence analyst: e.g. gathering information about specific adversary groups
- Fraud analyst: e.g. willing to share financial indicators to detect financial frauds
- Risk analyst: e.g. willing to know about the how threats, likelihood and occurrences
- Law enforcer: e.g. relying on indicators to support or bootstrap DFIR cases
- Academic researcher
- Other: _____

2. Which of the following categories best describes the organization you work in?

- National or Governmental CSIRT
- Military
- Energy
- Law enforcement agency
- Banking and Finance
- Insurance
- Computer hardware manufacturer
- Software company
- ICT Consulting / Advisory
- Public Health
- Telecommunications
- Transportation
- Academic institution
- Other: _____

3. How long have you been using MISP?

- I have never used MISP before
- < 1 month
- 1 - 6 months
- 6 - 12 months
- 1 - 2 years
- > 2 years

4. If applicable, how often do you use MISP?

- Less than once a week
- Between once and three times a week
- Between three times a week & every day
- Every day

5. Have you attended a training session on MISP before?

- No
- Yes

6. Have you used the MISP training materials before?

- No
- Yes

7. Have you used the MISP virtual machine before?

- No
- Yes

8. Have you used PyMISP - the Python library to access MISP via the API before?

- No
- Yes

MISP Threat Sharing **Sentence Completion**

Please complete the sentences below. There are no wrong replies, respond rather quickly without thinking too long. You can leave a sentence without an answer if you feel that it is not suitable for your situation.

When I use MISP, I feel ...

MISP is best for ...

MISP is not suitable for ...

I think the appearance of MISP is ...

I am happy with MISP because ...

The problem with MISP is ...

People who use MISP are typically ...

Compared to other threat information sharing platforms, MISP is ...

Methodology (All materials)

MISP Threat Sharing **User Experience Questionnaire**

For the assessment of the MISP platform, please fill out the following questionnaire, which consists of pairs of contrasting attributes that may apply to the platform. You can express your agreement with the attributes by ticking the circle that most closely reflects your impression.

Example:
attractive unattractive

This response would mean that you rate the application as more attractive than unattractive.

Please decide spontaneously. Don't think too long about your decision to make sure that you convey your original impression. Sometimes you may not be completely sure about your agreement with a particular attribute or you may find that the attribute does not apply completely to the platform. Nevertheless, please tick a circle in every line. It is your personal opinion that counts. Please remember: there is no wrong or right answer!

1	annoying	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	enjoyable	1
2	not understandable	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	understandable	2
3	creative	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	dull	3
4	easy to learn	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	difficult to learn	4
5	valuable	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	inferior	5
6	boring	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	exciting	6
7	not interesting	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	interesting	7
8	unpredictable	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	predictable	8
9	fast	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	slow	9
10	inventive	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	conventional	10
11	obstructive	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	supportive	11
12	good	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	bad	12
13	complicated	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	easy	13
14	unlikable	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	pleasing	14
15	usual	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	leading edge	15
16	unpleasant	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	pleasant	16
17	secure	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	not secure	17
18	motivating	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	demotivating	18
19	meets expectations	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	does not meet expectations	19
20	inefficient	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	efficient	20
21	clear	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	confusing	21
22	impractical	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	practical	22
23	organized	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	cluttered	23
24	attractive	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	unattractive	24
25	friendly	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	unfriendly	25
26	conservative	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	innovative	26

MISP Threat Sharing **MISP Users - Questionnaire**

The purpose of this questionnaire is to better understand the types of users and their respective needs on the MISP platform. Participation is voluntary.

1. Which of the following roles best describes how you (intend to) use MISP?

- Malware reverser: e.g. willing to share indicators of analysis with respective colleagues
- Security analyst: e.g. searching, validating and using indicators in operational security
- Intelligence analyst: e.g. gathering information about specific adversary groups
- Fraud analyst: e.g. willing to share financial indicators to detect financial frauds
- Risk analyst: e.g. willing to know about the new threats, likelihood and occurrences
- Law enforcer: e.g. relying on indicators to support or bootstrap DFIR cases
- Academic researcher
- Other: _____

2. Which of the following categories best describes the organization you work in?

- National or Governmental CSIRT
- Military
- Energy
- Law enforcement agency
- Banking and Finance
- Insurance
- Computer hardware manufacturer
- Software company
- ICT Consulting / Advisory
- Public Health
- Telecommunications
- Transportation
- Academic institution
- Other: _____

3. How long have you been using MISP?

- I have never used MISP before
- < 1 month
- 1 - 6 months
- 6 - 12 months
- 1 - 2 years
- > 2 years

4. If applicable, how often do you use MISP?

- Less than once a week
- Between once and three times a week
- Between three times a week & every day
- Every day

5. Have you attended a training session on MISP before?

No Yes

6. Have you used the MISP training materials before?

No Yes

7. Have you used the MISP virtual machine before?

No Yes

8. Have you used PyMISP - the Python library to access MISP via the API before?

No Yes

MISP Threat Sharing **Instructions**

Please check the box that reflects your immediate response to each statement. Don't think too long about each statement. Make sure you respond to every statement. If you don't know how to respond, simply check box 3.

Questionnaire

Strongly Disagree Strongly Agree

1. I think that I would like to use this system frequently. 1 2 3 4 5

2. I found the system unnecessarily complex. 1 2 3 4 5

I thought the system was easy to use. 1 2 3 4 5

I think that I would need the support of a technical person to be able to use this system. 1 2 3 4 5

I found the various functions in this system were well integrated. 1 2 3 4 5

I thought there was too much inconsistency in this system. 1 2 3 4 5

I would imagine that most people would learn to use this system very quickly. 1 2 3 4 5

I found the system very cumbersome to use. 1 2 3 4 5

I felt very confident using the system. 1 2 3 4 5

I needed to learn a lot of things before I could get going with this system. 1 2 3 4 5

MISP Threat Sharing **Group Work**

Please work in pairs or a small group. Read the following scenario and provide your input on a separate sheet. With this task we would like to understand better how different users perceive the deletion functionality within MISP.

IDs: _____

Your organization has been using MISP for a few years now and is part of a number of sharing communities. Over the years you have seen data being leaked or unintentionally shared beyond the intended recipients.

A new junior member, Jerry, is joining your team and your task is to explain to Jerry how deletion of events in MISP works.

You can freely choose how you would like to describe the deletion process, for example by drawing a diagram, sketch etc, or writing it down in words.

MISP Threat Sharing **Sentence Completion**

Please complete the sentences below. There are no wrong replies, respond rather quickly without thinking too long. You can leave a sentence without an answer if you feel that it is not suitable for your situation.

When I use MISP, I feel ...

MISP is best for ...

MISP is not suitable for ...

I think the appearance of MISP is ...

I am happy with MISP because ...

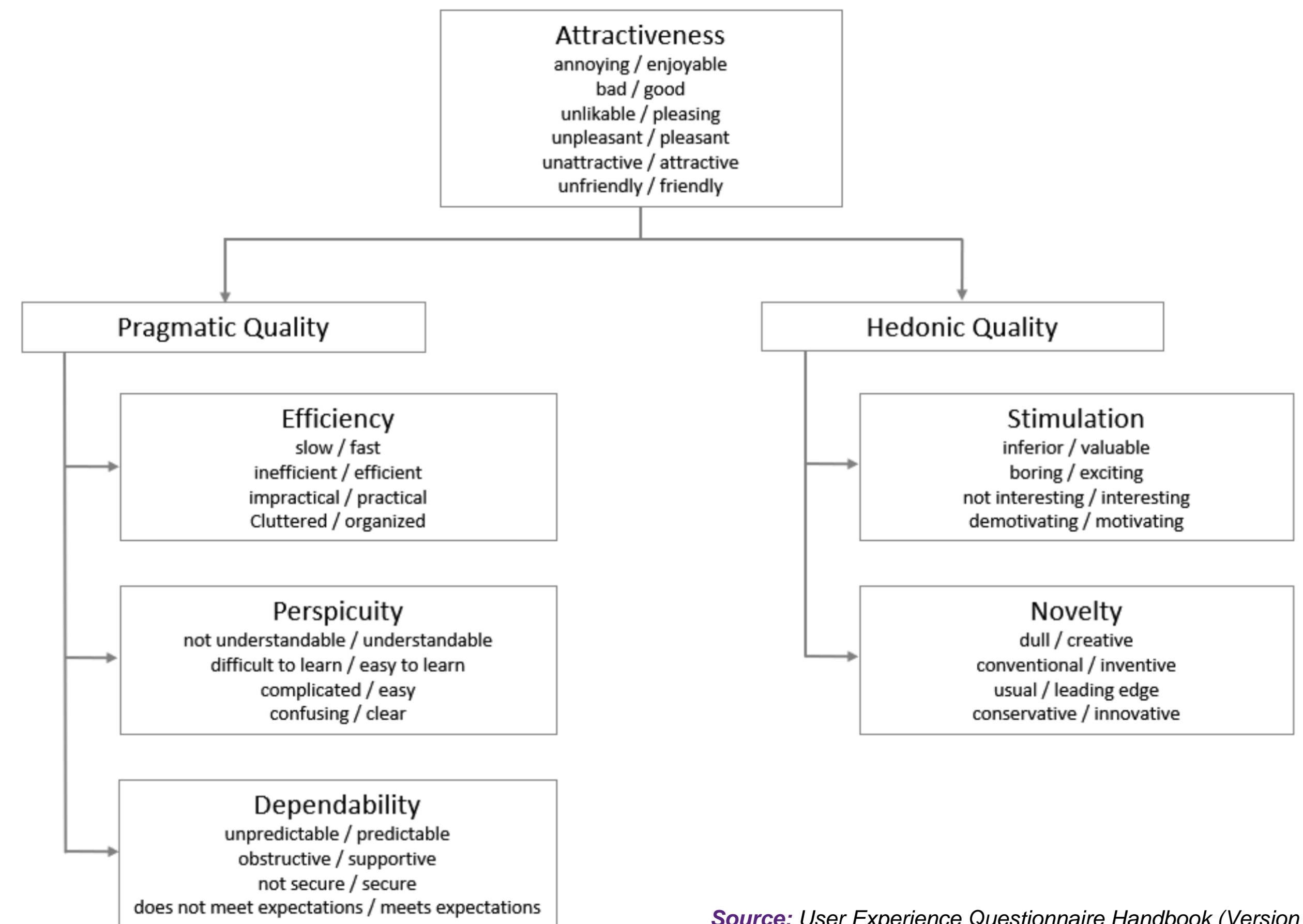
The problem with MISP is ...

People who use MISP are typically ...

Compared to other threat information sharing platforms, MISP is ...

Methodology - User Experience Questionnaire

	1	2	3	4	5	6	7		
annoying	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	enjoyable	1
not understandable	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	understandable	2
creative	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	dull	3
easy to learn	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	difficult to learn	4
valuable	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	inferior	5
boring	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	exciting	6
not interesting	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	interesting	7
unpredictable	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	predictable	8
fast	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	slow	9
inventive	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	conventional	10
obstructive	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	supportive	11
good	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	bad	12
complicated	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	easy	13
unlikable	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	pleasing	14
usual	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	leading edge	15
unpleasant	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	pleasant	16
secure	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	not secure	17
motivating	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	demotivating	18
meets expectations	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	does not meet expectations	19
inefficient	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	efficient	20
clear	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	confusing	21
impractical	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	practical	22
organized	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	cluttered	23
attractive	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	unattractive	24
friendly	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	unfriendly	25
conservative	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	innovative	26



Source: User Experience Questionnaire Handbook (Version 8)

Methodology - MISP Users - Questionnaire

1. Which of the following roles best describes how you (intend to) use MISP?

- Malware reverser: e.g. willing to share indicators of analysis with respective colleagues
- Security analyst: e.g. searching, validating and using indicators in operational security
- Intelligence analyst: e.g. gathering information about specific adversary groups
- Fraud analyst: e.g. willing to share financial indicators to detect financial frauds
- Risk analyst: e.g. willing to know about the new threats, likelihood and occurrences
- Law enforcer: e.g. relying on indicators to support or bootstrap DFIR cases
- Academic researcher
- Other: _____

2. Which of the following categories best describes the organization you work in?

- | | |
|--|---|
| <input type="radio"/> National or Governmental CSIRT | <input type="radio"/> Software company |
| <input type="radio"/> Military | <input type="radio"/> ICT Consulting / Advisory |
| <input type="radio"/> Energy | <input type="radio"/> Public Health |
| <input type="radio"/> Law enforcement agency | <input type="radio"/> Telecommunications |
| <input type="radio"/> Banking and Finance | <input type="radio"/> Transportation |
| <input type="radio"/> Insurance | <input type="radio"/> Academic institution |
| <input type="radio"/> Computer hardware manufacturer | <input type="radio"/> Other: _____ |

3. How long have you been using MISP?

- | | |
|---|-------------------------------------|
| <input type="radio"/> I have never used MISP before | <input type="radio"/> 6 - 12 months |
| <input type="radio"/> < 1 month | <input type="radio"/> 1 - 2 years |
| <input type="radio"/> 1 - 6 months | <input type="radio"/> > 2 years |

4. If applicable, how often do you use MISP?

- | | |
|---|--|
| <input type="radio"/> Less than once a week | <input type="radio"/> Between three times a week & every day |
| <input type="radio"/> Between once and three times a week | <input type="radio"/> Every day |

5. Have you attended a training session on MISP before?

- No Yes

6. Have you used the MISP training materials before?

- No Yes

7. Have you used the MISP virtual machine before?

- No Yes

8. Have you used PyMISP - the Python library to access MISP via the API before?

- No Yes

Methodology - Sentence Completion

When I use MISP, I feel ...

MISP is best for ...

MISP is not suitable for ...

I think the appearance of MISP is ...

I am happy with MISP because ...


The problem with MISP is ...

People who use MISP are typically ...

Compared to other threat information sharing platforms, MISP is ...

Adapted from: Kujala et al. (2014)

Methodology - MM - Group Activity



IDs:


Group Work

Please work in pairs or a small group. Read the following scenario and provide your input on a separate sheet. With this task we would like to understand better how different users perceive the deletion functionality within MISP.

Your organization has been using MISP for a few years now and is part of a number of sharing communities. Over the years you have seen data being leaked or unintentionally shared beyond the intended recipients.

A new junior member, Jerry, is joining your team and your task is to explain to Jerry how deletion of events in MISP works.

You can freely choose how you would like to describe the deletion process, for example by drawing a diagram, sketch etc, or writing it down in words.



IDs:

Group Work

Please work in pairs or a small group. Read the following scenario and provide your input on a separate sheet. With this task we would like to understand better how different users perceive the deletion functionality within MISP.

Your organization has been using MISP for a few years now and is part of a number of sharing communities.

Over the years you have occasionally seen data being leaked or unintentionally shared beyond the intended recipients, and unfortunately, Jerry, a new junior member to your team has just informed you that he might have shared something he was not supposed to.

He would like to rectify it, and has asked you to explain to him how deletion of events in MISP works.

You can freely choose how you would like to describe the deletion process, for example by drawing a diagram, sketch etc, or writing down in words.

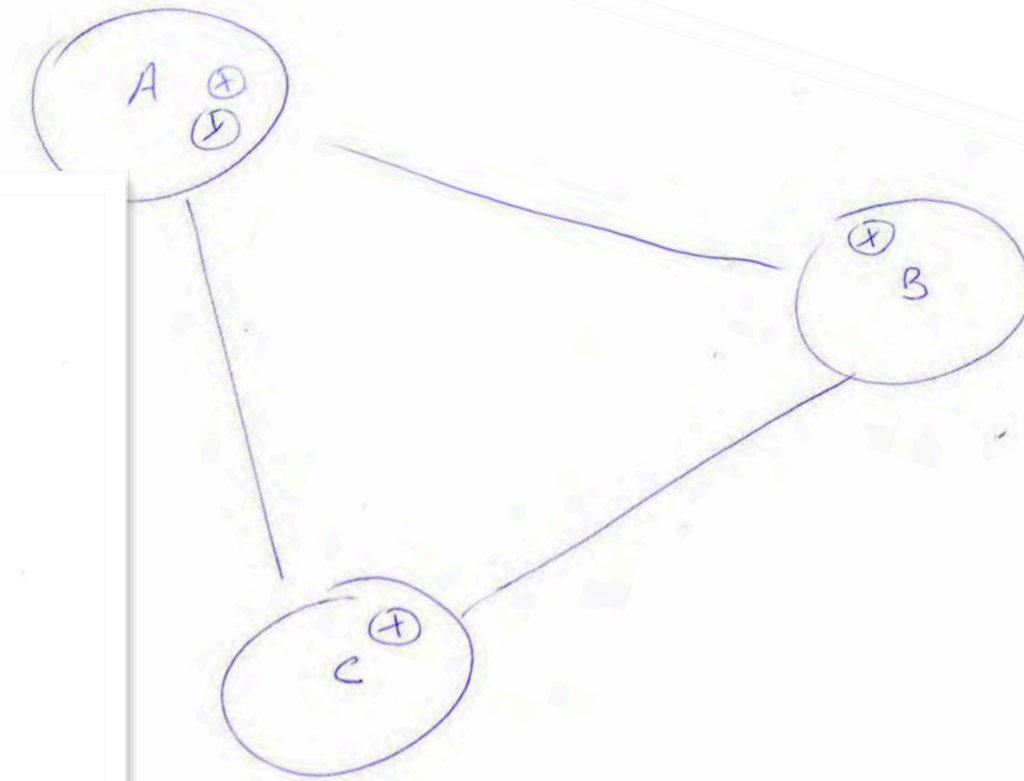
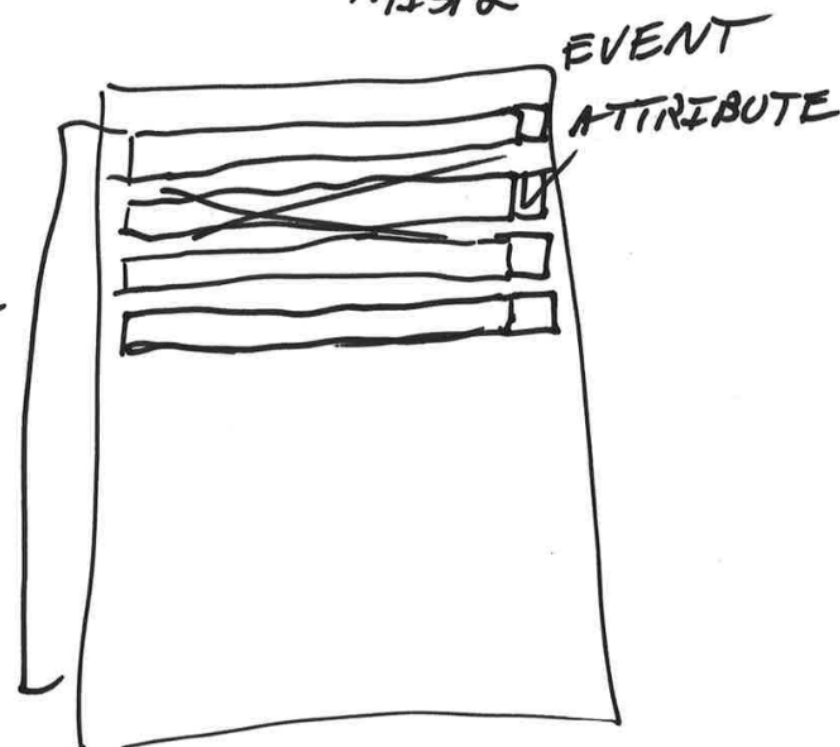
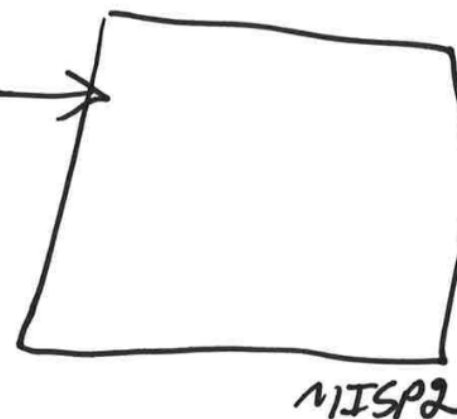
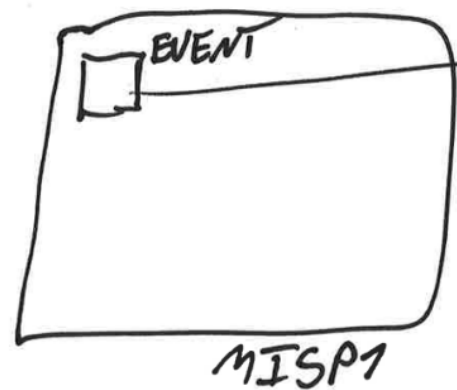
Methodology - MM - Group Activity

Once an event has
out side of our
requests are
with our
Not (and s
Jerry,
don't
to

been published
deletion
basis

Event?
Delete Event on Left

JERRY



like it with no problem → Hard way

deleted, it will be shared with instances (B, C)
placed on the blacklist. events. → Soft way.

3 Discussion Points



Artifacts

Did you use **experimentation artifacts** borrowed from the community?

- **NO**

- ▶ First study of its kind
- ▶ No baseline to qualify the observed measurements within the CTI context

- **YES**

- ▶ Measured values set in relation to benchmark datasets provided with the UEQ
- ▶ General benchmark (452 product evaluations) & Web sites and Web services (85 product evaluations)

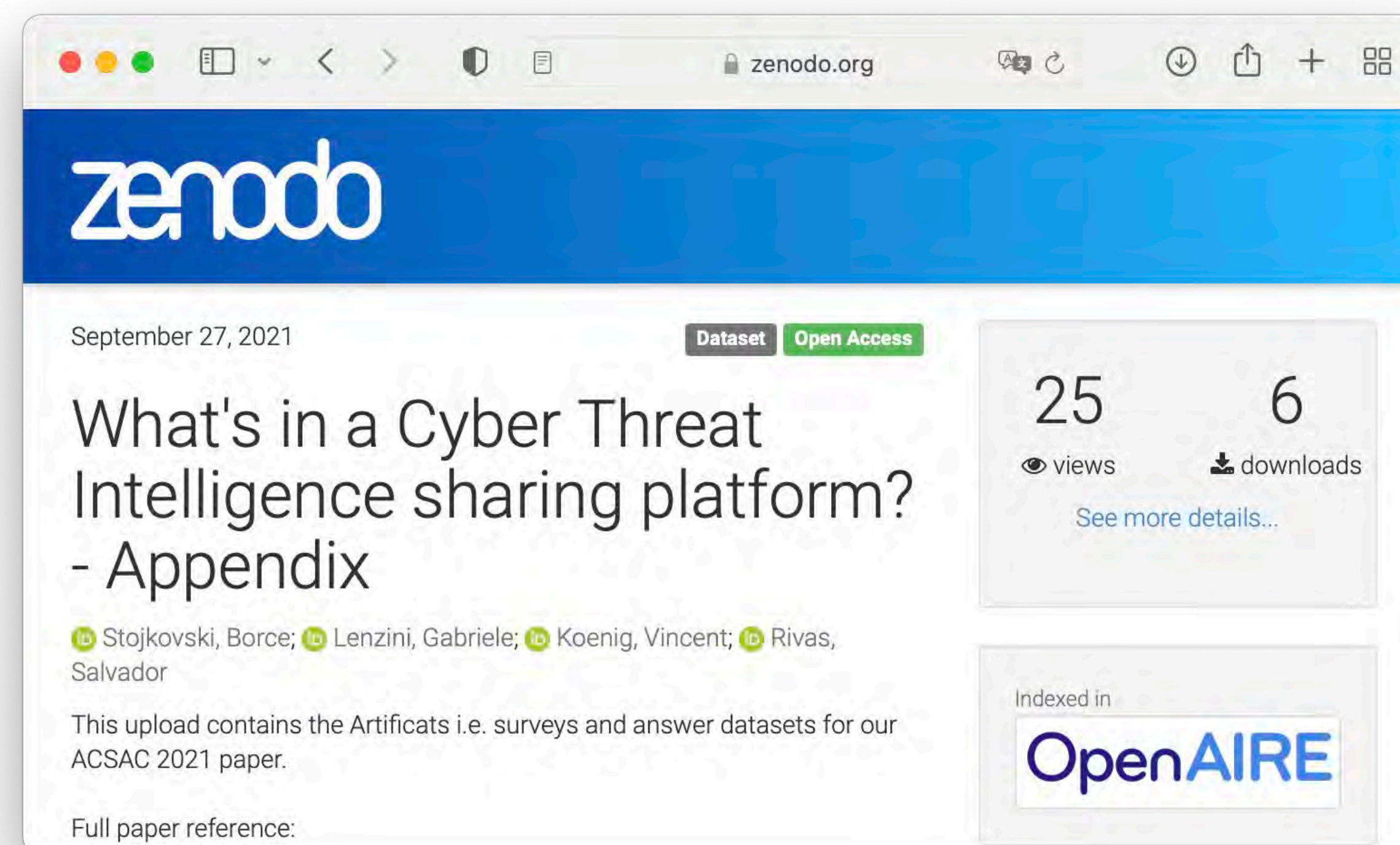
Artifacts

Did you share **experimentation artifacts** with the community?

- **We have released our dataset (surveys and anonymized responses)**

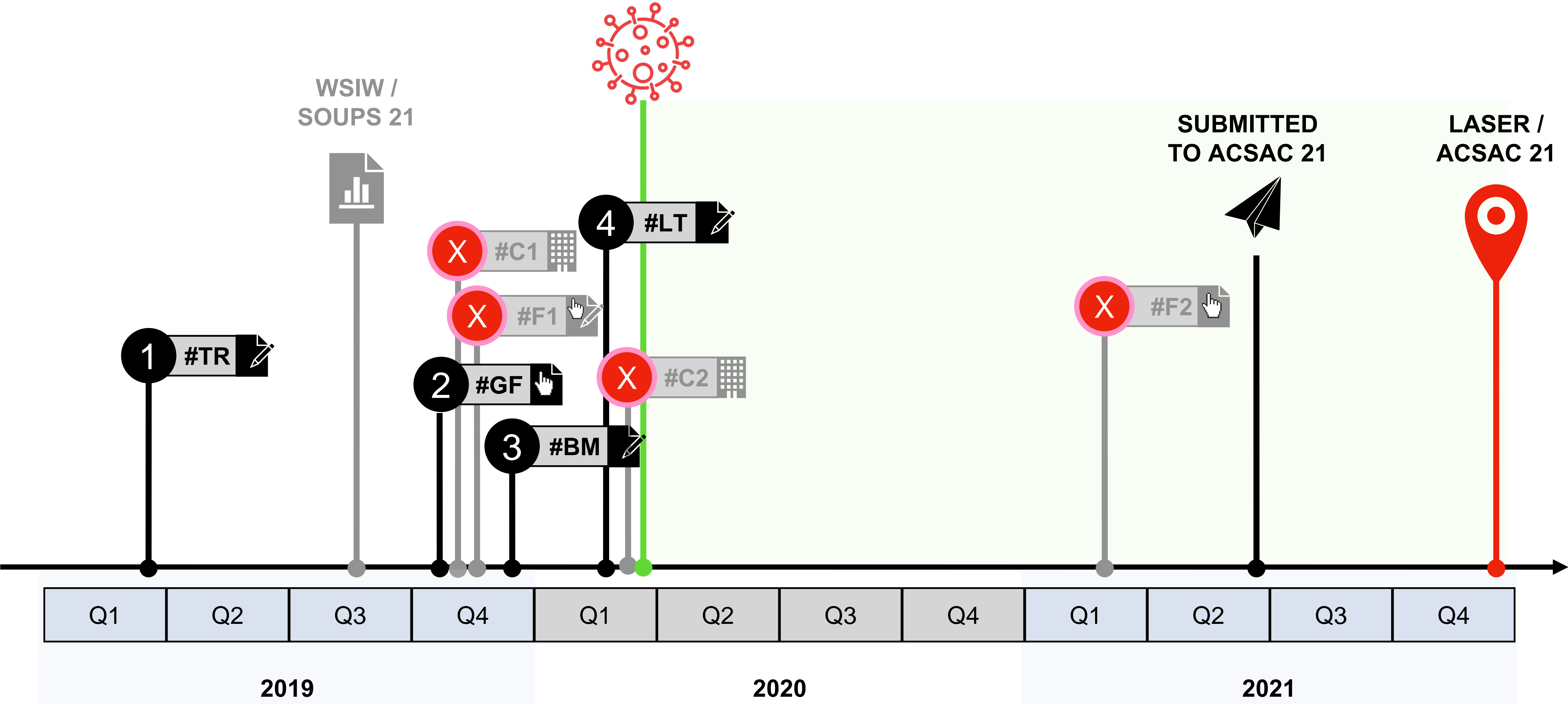
- ▶ Stojkovski, Borce, Lenzini, Gabriele, Koenig, Vincent, & Rivas, Salvador. (2021). What's in a Cyber Threat Intelligence sharing platform? - Appendix [Data set]. Zenodo.

<https://doi.org/10.5281/zenodo.5531990>



Failures

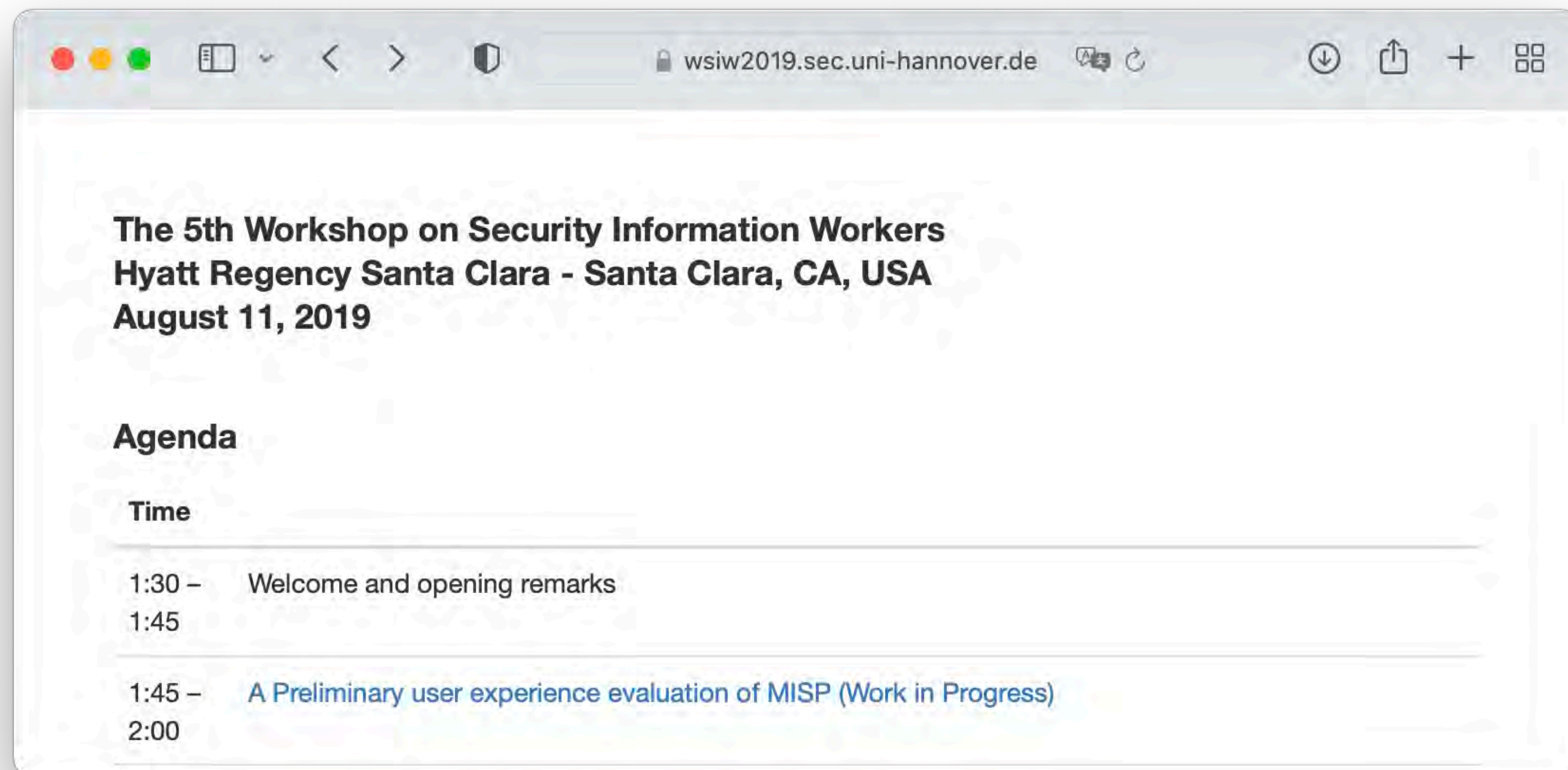
What did you try that **did not succeed** before getting to the results you presented?



Failures

What did you try that **did not succeed** before getting to the results you presented?

- **Discussing early-stage research / work in progress at WSIW / SOUPS 2019**



Failures

What did you try that **did not succeed** before getting to the results you presented?

- **Collecting new inputs during two additional training sessions (#F1 & #F2)**
 - ▶ In-person training, #F1 in Q4-2019, survey distribution on paper and online
 - ▶ Online training, #F2 in Q1-2021, survey distribution online

Failures

What did you try that **did not succeed** before getting to the results you presented?

- **Onboarding two private organizations (#C1 & #C2) to participate in our study**
 - ▶ Contact established following training sessions in Q4-2019 and Q1-2020
 - ▶ Invitation to take part in an online survey
 - ▶ Confirmation of interest, but no follow up

Failures

What did you try that **did not succeed** before getting to the results you presented?

- **Collecting a large number of user inputs via the online survey**
 - ▶ Survey launched in Q4-2019
 - ▶ Total number of responses: 12
 - ▶ 9 in Q4-2019
 - ▶ 1 in Q2-2020, 1 in Q3-2020, 1 in Q4-2020

Lessons learned (discussion)

What can be learned from your methodology & your experience?

- **Point**

- ▶ Subpoint

- ▶ Subpoint

- **Point**

- ▶ Subpoint

- ▶ Subpoint

3 Discussion and Future Work



Github Usability and UX related issues

Overview of MISP GitHub issues identified in trainings per year

URL: <https://github.com/MISP/MISP>

Search query: label:from:training created:YYYY-MM-DD..YYYY-MM-DD label:"feature request"

	2020	2019	2018	2017	Total
Open	5	103	17	1	126
Feature Requests	4	20	6		30
Usability		4	2		6
Closed	1	22	2	0	25
Feature Requests		2	1		3
Usability		1			1
Total	6	125	19	1	151

	2020	2019	2018	2017	Total
Open	4	17	20	18	59
Feature Requests	3	5	2	1	11
Closed	2	11	11	6	30
Feature Requests	2	0	1	0	3
Total	6	28	31	24	89



Thank you for your attention! Any questions?

Our original ACSAC 2021 paper:

[What's in a Cyber Threat Intelligence sharing platform? A mixed-methods user experience investigation of MISP](#)

Borce Stojkovski; Gabriele LENZINI; Vincent KOENIG; Salvador RIVAS

Gabriele Lenzini

Gabriele.lenzini@uni.lu

Borče Stojkovski

SnT, University of Luxembourg

borce.stojkovski@uni.lu

94D2 ED64 1642 66E2



IRiSC

Interdisciplinary Research in
Sociotechnical Cybersecurity

uni.lu | **SnT**