@CSAUERWEINcom

Cyber Threat Intelligence Sharing Platforms: A Comprehensive Analysis of Software Vendors and Research Perspectives

Clemens Sauerwein

University of Innsbruck, Department of Computer Science (Austria)

Plenary Sessions Day 1

02.11.2022

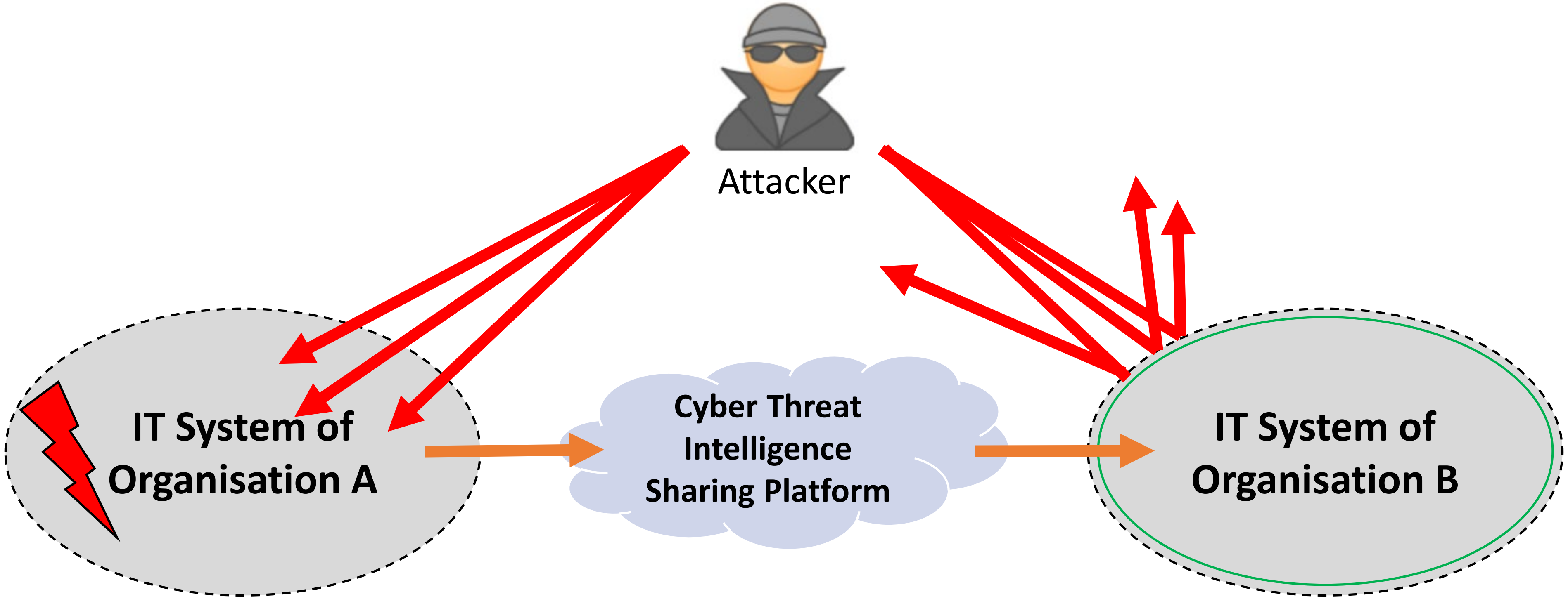
FIRST Cyber Threat Intelligence Symposium 2022, Berlin, Germany

universität innsbruck

Institut für Informatik

2022
**FIRST
Cyber Threat
Intelligence
Symposium**
Berlin, Germany
November 1-3, 2022

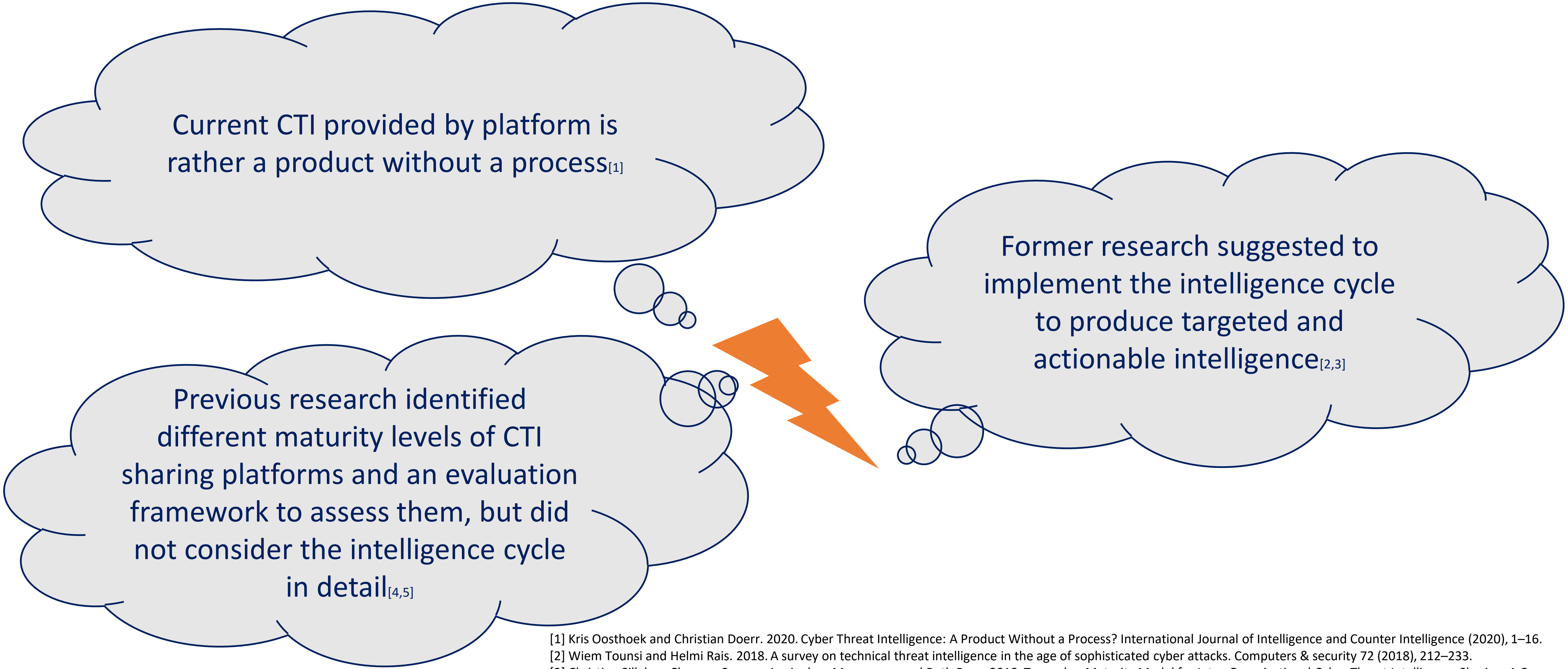
Cyber Threat Intelligence Sharing Platform


Attacker
IT System of Organisation A
Cyber Threat Intelligence Sharing Platform
IT System of Organisation B

…supports organizations in information sharing, enable automation and facilitate the refining and vetting of threat data.[1]

[1] Dandurand, Luc, and Oscar Serrano Serrano. "Towards improved cyber security information sharing." 2013 5th International Conference on Cyber Conflict (CYCON 2013). IEEE, 2013.

Gap



Current CTI provided by platform is rather a product without a process[1]

Former research suggested to implement the intelligence cycle to produce targeted and actionable intelligence[2,3]

Previous research identified different maturity levels of CTI sharing platforms and an evaluation framework to assess them, but did not consider the intelligence cycle in detail[4,5]

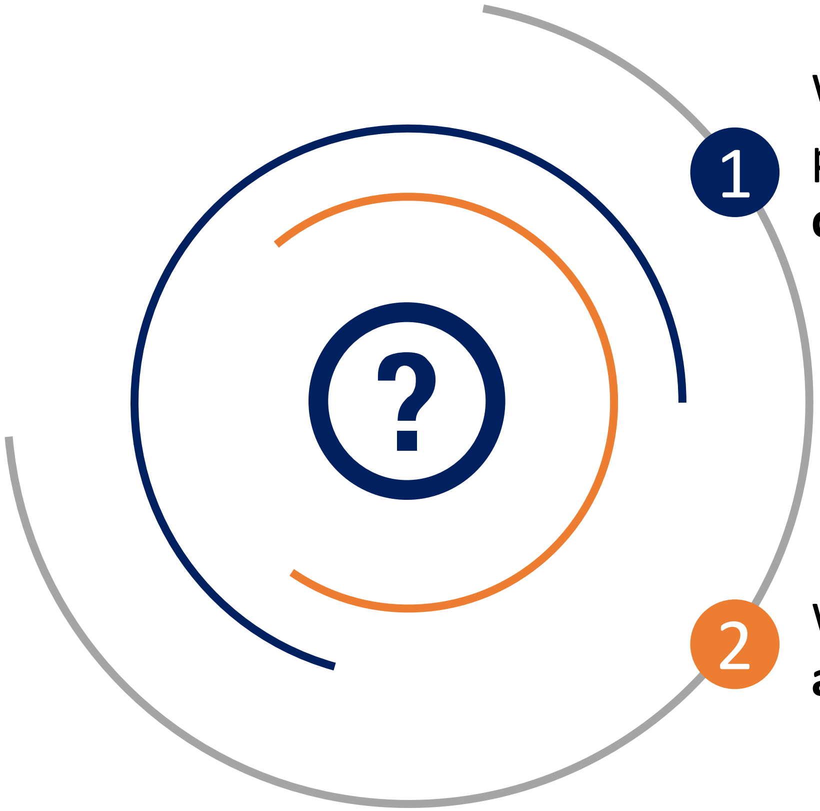
[1] Kris Oosthoek and Christian Doerr. 2020. Cyber Threat Intelligence: A Product Without a Process? International Journal of Intelligence and Counter Intelligence (2020), 1–16.

[2] Wiem Tounsi and Helmi Rais. 2018. A survey on technical threat intelligence in the age of sophisticated cyber attacks. Computers & security 72 (2018), 212–233.

[3] Christian Sillaber, Clemens Sauerwein, Andrea Mussmann, and Ruth Breu. 2018. Towards a Maturity Model for Inter-Organizational Cyber Threat Intelligence Sharing: A Case Study of Stakeholders' Expectations and Willingness to Share. In Proceedings of Multikonferenz Wirtschaftsinformatik. 1409–1420

[4] Sara Bauer, Daniel Fischer, Clemens Sauerwein, Simon Latzel, Dirk Stelzer, and Ruth Breu. 2020. Towards an Evaluation Framework for Threat Intelligence Sharing Platforms. In Proceedings of the 53rd Hawaii International Conference on System Sciences.

Questions

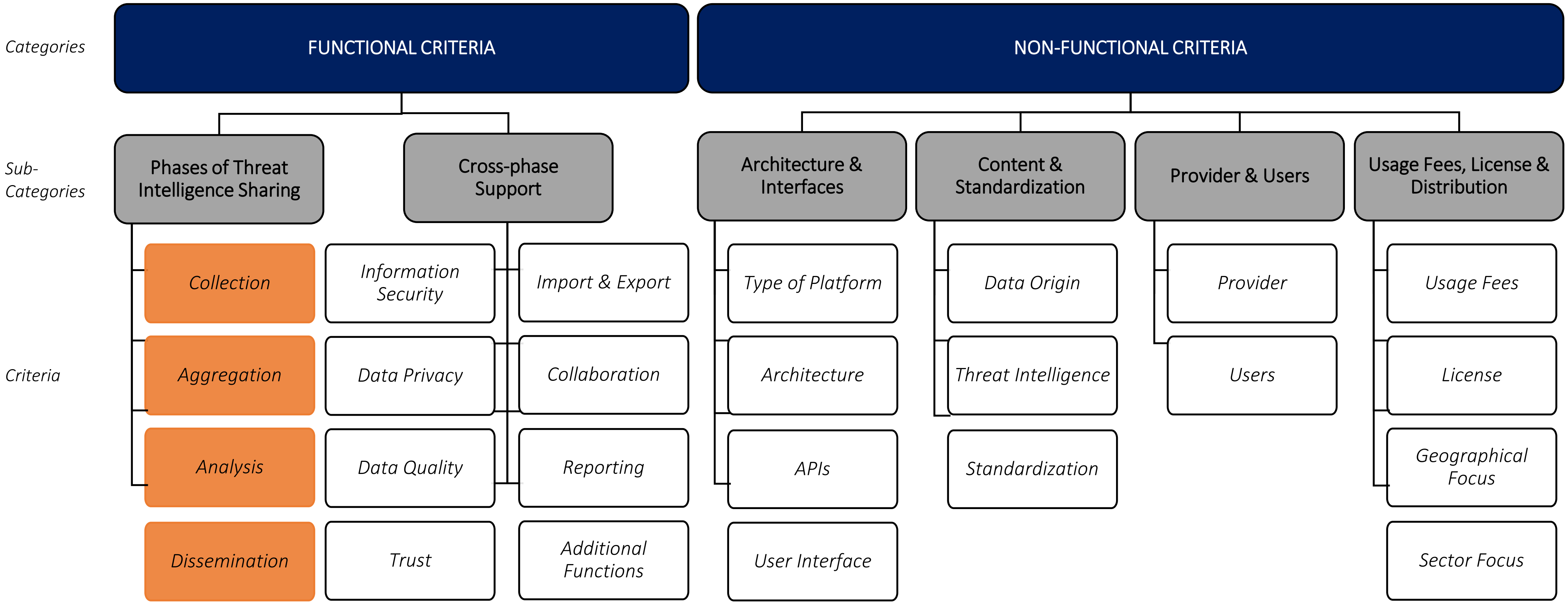


1. Which **software functions are required** by CTI sharing platforms **to support the processes of the intelligence cycle** to generate actionable threat intelligence?

2. Which **intelligence cycle processes** and **functionalities are implemented** by CTI sharing platforms?

Sauerwein, Clemens, Daniel Fischer, Milena Rubsamen, Guido Rosenberger, Dirk Stelzer, and Ruth Breu. "From Threat Data to Actionable Intelligence: An Exploratory Analysis of the Intelligence Cycle Implementation in Cyber Threat Intelligence Sharing Platforms." In *The 16th International Conference on Availability, Reliability and Security*, pp. 1-9. 2021.

Evaluation Framework



Categories

Sub-Categories

Criteria

FUNCTIONAL CRITERIA

Phases of Threat Intelligence Sharing
- *Collection*
- *Aggregation*
- *Analysis*
- *Dissemination*

Cross-phase Support
- *Information Security*
- *Data Privacy*
- *Data Quality*
- *Trust*
- *Import & Export*
- *Collaboration*
- *Reporting*
- *Additional Functions*

NON-FUNCTIONAL CRITERIA

Architecture & Interfaces
- *Type of Platform*
- *Architecture*
- *APIs*
- *User Interface*

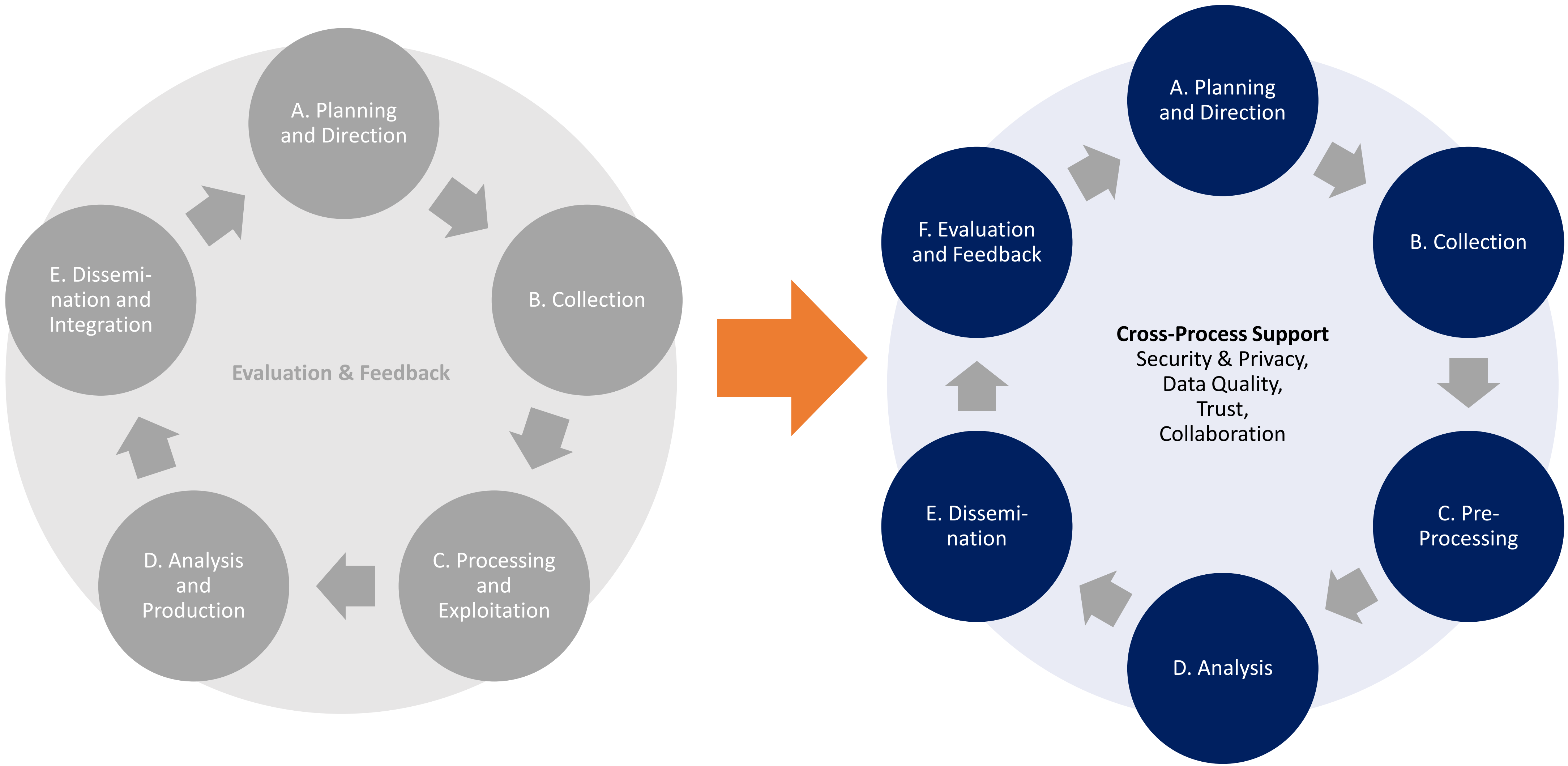
Content & Standardization
- *Data Origin*
- *Threat Intelligence*
- *Standardization*

Provider & Users
- *Provider*
- *Users*

Usage Fees, License & Distribution
- *Usage Fees*
- *License*
- *Geographical Focus*
- *Sector Focus*

Sara Bauer, Daniel Fischer, Clemens Sauerwein, Simon Latzel, Dirk Stelzer, and Ruth Breu. 2020. Towards an Evaluation Framework for Threat Intelligence Sharing Platforms. In Proceedings of the 53rd Hawaii International Conference on System Sciences.

Adapted Intelligence Cycle


A. Planning and Direction
B. Collection
C. Processing and Exploitation
D. Analysis and Production
E. Dissemi-nation and Integration
Evaluation & Feedback
A. Planning and Direction
B. Collection
C. Pre-Processing
D. Analysis
E. Dissemi-nation
F. Evaluation and Feedback
Cross-Process Support
Security & Privacy,
Data Quality,
Trust,
Collaboration

Sauerwein, Clemens, Daniel Fischer, Milena Rubsamen, Guido Rosenberger, Dirk Stelzer, and Ruth Breu. "From Threat Data to Actionable Intelligence: An Exploratory Analysis of the Intelligence Cycle Implementation in Cyber Threat Intelligence Sharing Platforms." In *The 16th International Conference on Availability, Reliability and Security*, pp. 1-9. 2021.

Example - Platform Functions

Intelligence Process	Functions
Planning & Direction	-
Collection	*Manual Data Creation, Manual File Upload, Feed Import, Import Connector, Import Agent, Web Collector,…*
Pre-Processing	*Data Cleaning, Data Normalization, Data Classification, Data Editing,…*
Analysis	*Expert Analysis, Collaborative Analysis, Data Investigation & Sandboxing, Search, Statistical Analysis, Correlation, Pattern Recognition, Rating & Prioritization, White- & Blacklisting, Monitoring, Prediction,…*
Dissemination	*Feed Export, Alerting & Notifications, Synchronization & Export Connector, Manual Download,…*
Evaluation & Feedback	*Dashboard, Standardized Reporting, Individual Reporting, Feedback,…*
Cross-Process Support	*Data Security, Communication Security, Platform Security, Access Control, Data Privacy, Group and Community Management, Communication & Messaging, Teamworking, Data Verification, Data Validation, Rating, Reputation, Traceability,…*

Sauerwein, Clemens, Daniel Fischer, Milena Rubsamen, Guido Rosenberger, Dirk Stelzer, and Ruth Breu. "From Threat Data to Actionable Intelligence: An Exploratory Analysis of the Intelligence Cycle Implementation in Cyber Threat Intelligence Sharing Platforms." In *The 16th International Conference on Availability, Reliability and Security*, pp. 1-9. 2021.

Key Findings- Intelligence Cycle Support

1. A CTI Sharing Platform **requires functions** for ***Planning & Direction***, ***Collection***, ***Pre-Processing***, ***Analysis***, ***Dissemination***, ***Evaluation*** and ***Cross-Process-Support***.
2. **A** common **understanding** on ***Planning & Direction*** is needed
3. **Most functions** have been identified for ***Analysis.***
4. It is **difficult to draw the line** between ***Pre-Processing*** and ***Analysis.***
5. The **functional scope** and **support** in relation to the intelligence cycle **depends on the platform‘s focus.**
6. **Low-functional, medium-functional** and **high-functional** platforms have been identified.

Sauerwein, Clemens, Daniel Fischer, Milena Rubsamen, Guido Rosenberger, Dirk Stelzer, and Ruth Breu. "From Threat Data to Actionable Intelligence: An Exploratory Analysis of the Intelligence Cycle Implementation in Cyber Threat Intelligence Sharing Platforms." In *The 16th International Conference on Availability, Reliability and Security*, pp. 1-9. 2021.

Conclusion and Outlook

- Exploratory analysis of software functions required by a CTI sharing platform to support the intelligence cycle
- Systematic literature review combined with 13 case studies
- Extends the cyber threat intelligence sharing evaluation framework[4] & substantiates the seminal definition[1] of CTI sharing platforms
- Identified a profound lack of research on the process of Planning & Direction

- Future Work
  - Exploring organizational processes on how to plan and direct a CTI initiative
  - Comprehensive evaluation of the use of CTI Platforms

[1] Dandurand, Luc, and Oscar Serrano Serrano. "Towards improved cyber security information sharing." 2013 5th International Conference on Cyber Conflict (CYCON 2013). IEEE, 2013.

[4] Sara Bauer, Daniel Fischer, Clemens Sauerwein, Simon Latzel, Dirk Stelzer, and Ruth Breu. 2020. Towards an Evaluation Framework for Threat Intelligence Sharing Platforms. In Proceedings of the 53rd Hawaii International Conference on System Sciences.

Contact

Ass.-Prof. Clemens Sauerwein, PhD

University of Innsbruck
Technikerstraße 21a
6020-Innsbruck
Austria

Email: Clemens.Sauerwein@uibk.ac.at
Webpage: https://www.csauerwein.com/

@CSAUERWEINcom