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*
Cyber Threat Intelligence Sharing Platform

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

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\[4,5\]

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?

Evaluation Framework

Adapted Intelligence Cycle

A. Planning and Direction
B. Collection
C. Pre-Processing
D. Analysis and Production
E. Dissemination and Integration

Evaluation & Feedback

A. Planning and Direction
B. Collection
C. Pre-Processing
D. Analysis
E. Dissemination
F. Evaluation and Feedback

Cross-Process Support
- Security & Privacy
- Data Quality
- Trust
- Collaboration

Example - Platform Functions

<table>
<thead>
<tr>
<th>Intelligence Process</th>
<th>Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Planning &amp; Direction</td>
<td>-</td>
</tr>
<tr>
<td>Pre-Processing</td>
<td>Data Cleaning, Data Normalization, Data Classification, Data Editing,…</td>
</tr>
<tr>
<td>Analysis</td>
<td>Expert Analysis, Collaborative Analysis, Data Investigation &amp; Sandboxing, Search, Statistical Analysis, Correlation, Pattern Recognition, Rating &amp; Prioritization, White- &amp; Blacklisting, Monitoring, Prediction,…</td>
</tr>
<tr>
<td>Dissemination</td>
<td>Feed Export, Alerting &amp; Notifications, Synchronization &amp; Export Connector, Manual Download,…</td>
</tr>
<tr>
<td>Evaluation &amp; Feedback</td>
<td>Dashboard, Standardized Reporting, Individual Reporting, Feedback,…</td>
</tr>
</tbody>
</table>

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.

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

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/