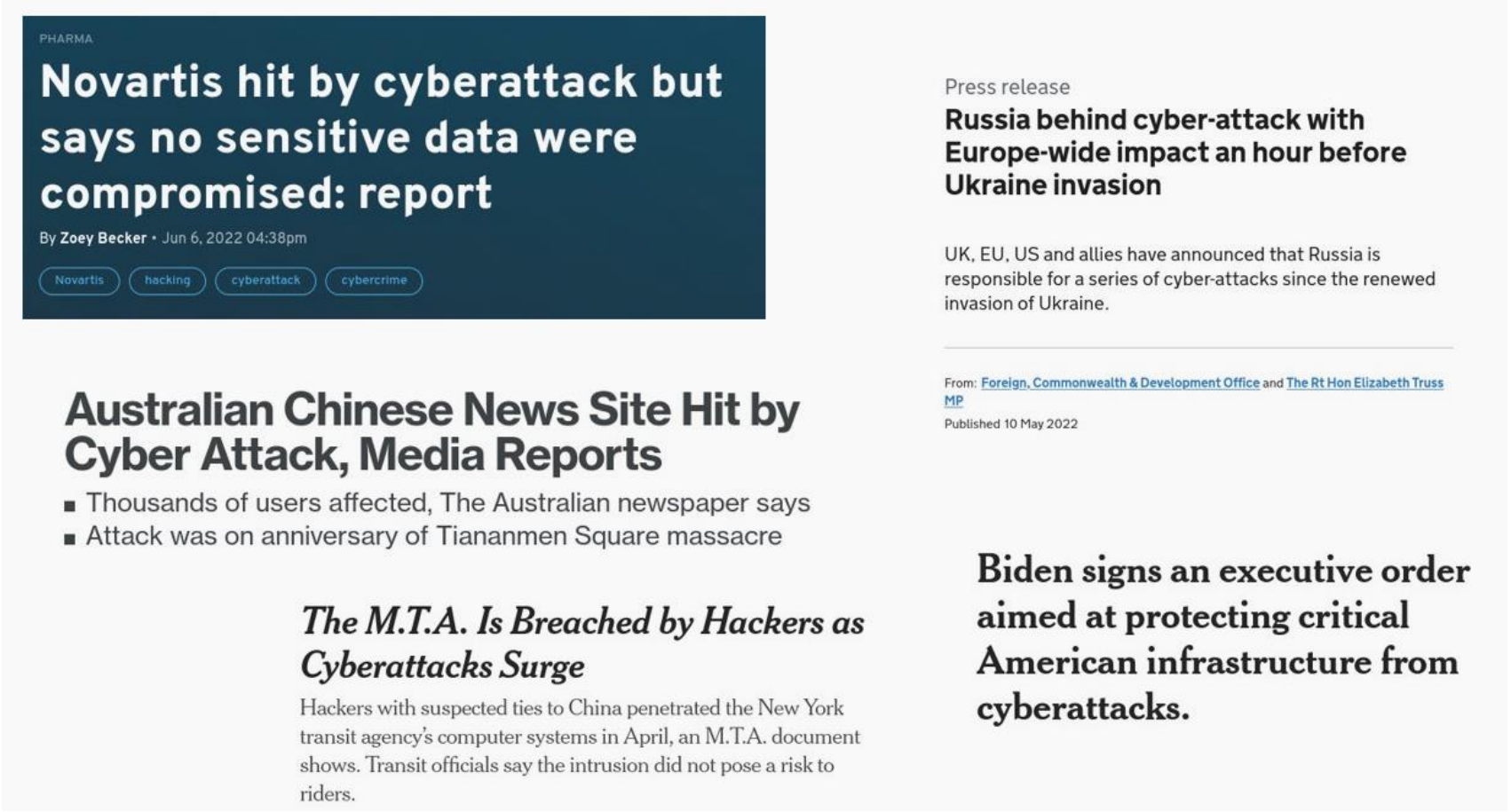
Measuring Data Quality in STIX-based SOAR Platforms

Hagenberg, 21.09.2022

Konstantin Papesh

The Motivation



PHARMA

Novartis hit by cyberattack but says no sensitive data were compromised: report

By **Zoey Becker** • Jun 6, 2022 04:38pm

Novartis | hacking | cyberattack | cybercrime

Australian Chinese News Site Hit by Cyber Attack, Media Reports

- Thousands of users affected, The Australian newspaper says
- Attack was on anniversary of Tiananmen Square massacre

The M.T.A. Is Breached by Hackers as Cyberattacks Surge

Hackers with suspected ties to China penetrated the New York transit agency's computer systems in April, an M.T.A. document shows. Transit officials say the intrusion did not pose a risk to riders.

Press release

Russia behind cyber-attack with Europe-wide impact an hour before Ukraine invasion

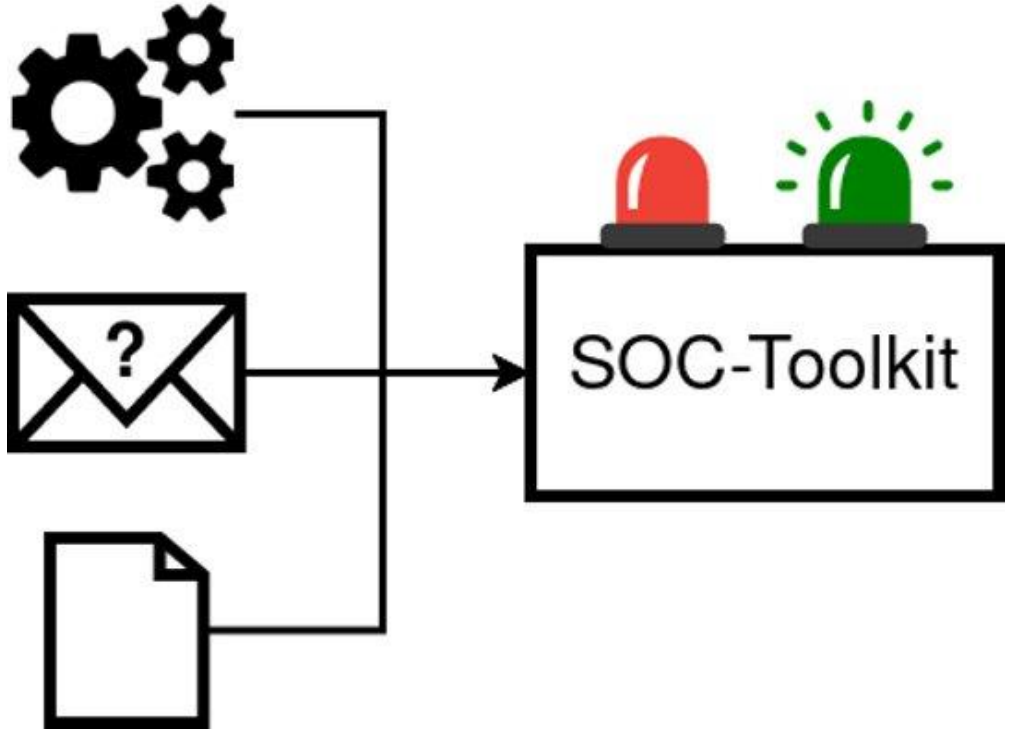
UK, EU, US and allies have announced that Russia is responsible for a series of cyber-attacks since the renewed invasion of Ukraine.

From: Foreign, Commonwealth & Development Office and The Rt Hon Elizabeth Truss MP

Published 10 May 2022

Biden signs an executive order aimed at protecting critical American infrastructure from cyberattacks.

Nextpart SOC-Toolkit



The Background

Measuring Data Quality in **STIX**-based **SOAR** Platforms

- Structured Threat Information Expression (STIX)
- Security Orchestration, Automation, and Response (SOAR)
- Cyber Threat Intelligence (CTI)

STIX Graph

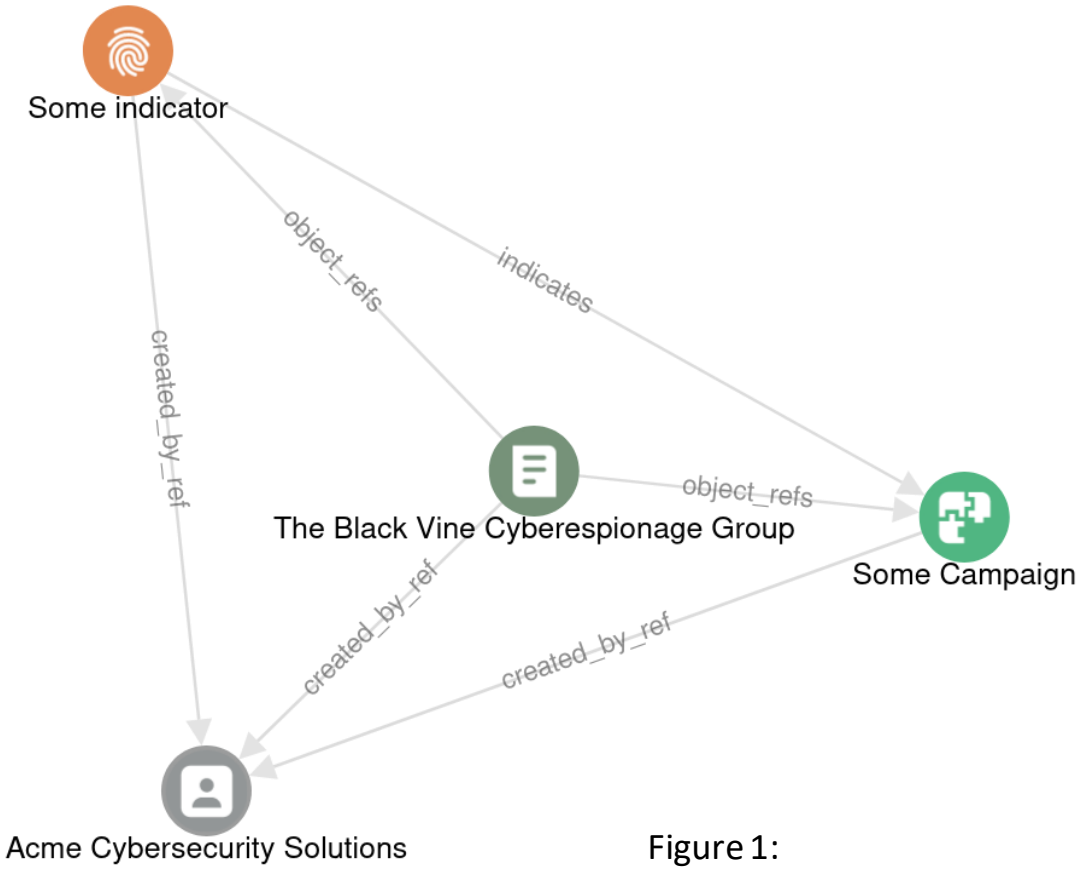


Figure 1:
STIX graph example.
Taken from [1], visualised with [2].

STIX Graph (revised)

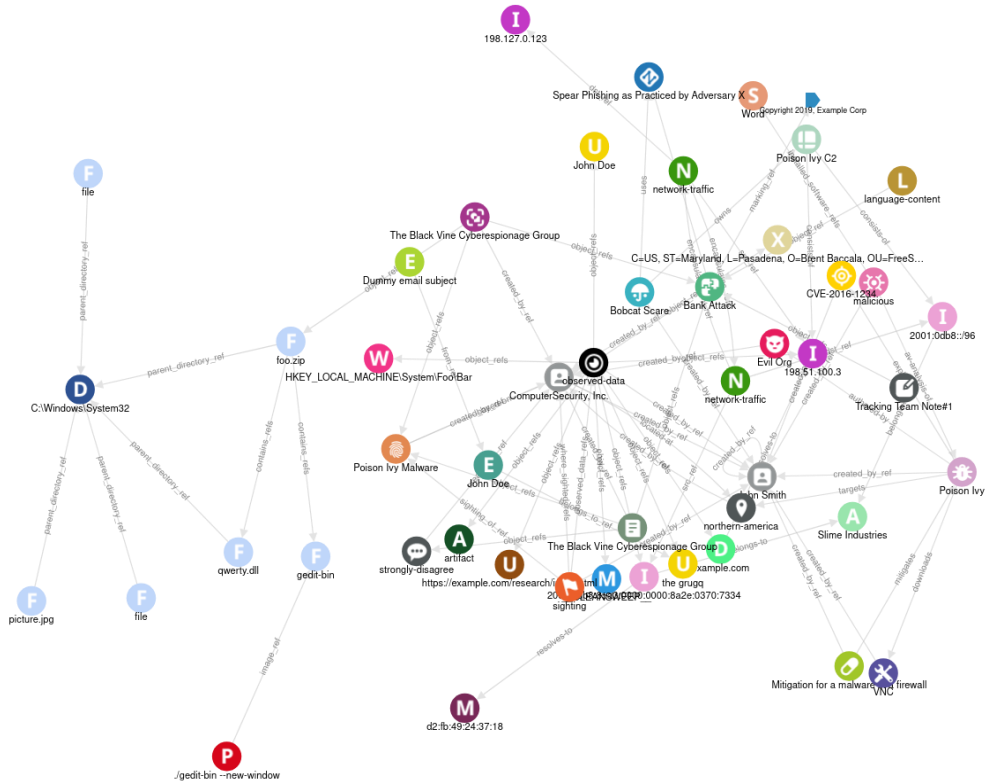


Figure 2:
Larger STIX graph example.
Taken from [3], visualised with [2].

The Problem

Figure 3:
Services offering threat detection and analysis [4].

The Problem

- Rating and ranking services
  - How good is the service quality?
  - How long does a service take to respond?
- Service data quality is hard to determine at implementation time.

The Goals

- How can data quality be measured within SOAR platforms?
  - What CTI measurements do already exist?
  - How can these be altered to work with CTI data of a SOAR platform?
  - How can a CTI rating framework be incorporated into a SOAR platform?

The Introduction

- Enodo…
  - … latin for 'untangle, explain, unfold'.
  - … is a CTI metrics framework.
  - … rates STIX sources based on multiple metrics.
  - … gives programmers and users an overview of the service quality.
  - … is embedded into the existing SOC-Toolkit.
  - … needs no human interaction.

Trust Indicator

- Tries to measure sources based on multiple data quality metrics.
- Based on multiple approaches from literature.
- Uses two papers as foundation:
  - Measuring and visualizing cyber threat intelligence quality [5]
  - Quantitative Evaluation of Trust in the Quality of Cyber Threat Intelligence Sources [6]
- Consists of 7 metrics.

The Metrics

- Extensiveness
  - Quantifies amount of information.
  - Based on required and optional parameters of objects.
- Compliance
  - Checks if objects are violating any restrictions of the STIX standard.
  - Not implemented due to incompatibility with framework.
- Representation Consistency
  - Checks if objects violate any logical restrictions.
  - Not implemented due to incompatibility with framework.
- Verifiability
  - Based on external references present in objects.
  - Counts the number of external references contained in each object.

The Metrics (cont.)

- Intelligence
  - Rates connectiveness of source.
  - Counts the links created by the source.
- Similarity
  - Shows how similar the objects of a source are to other sources.
- Completeness
  - Shows how much contribution the source has to the worldview.
  - Does so by calculating the overlap of source and worldview.
- Duration
  - Shows how long a service takes to respond to an API request.
  - Not a STIX metric, but a workflow metric.

The Architecture

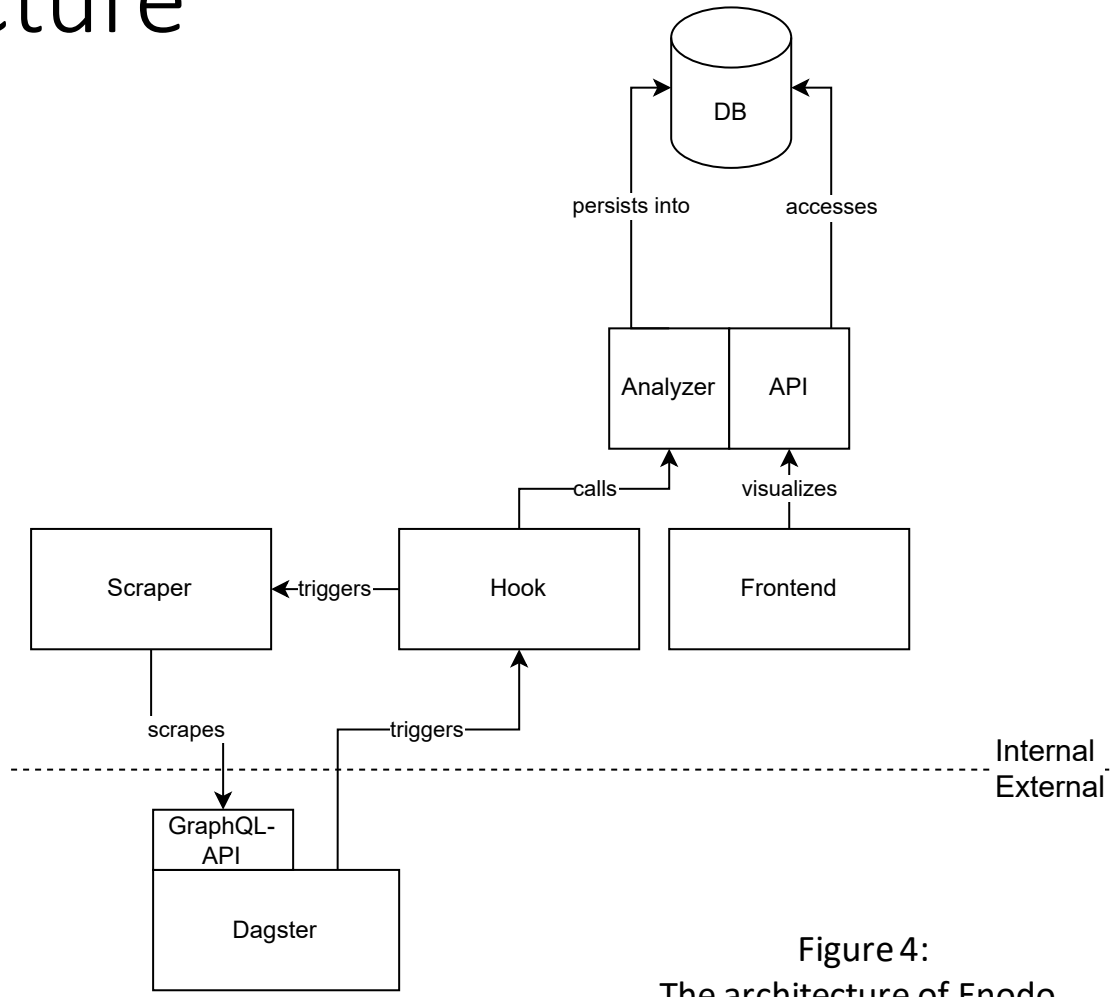


Figure 4:
The architecture of Enodo.

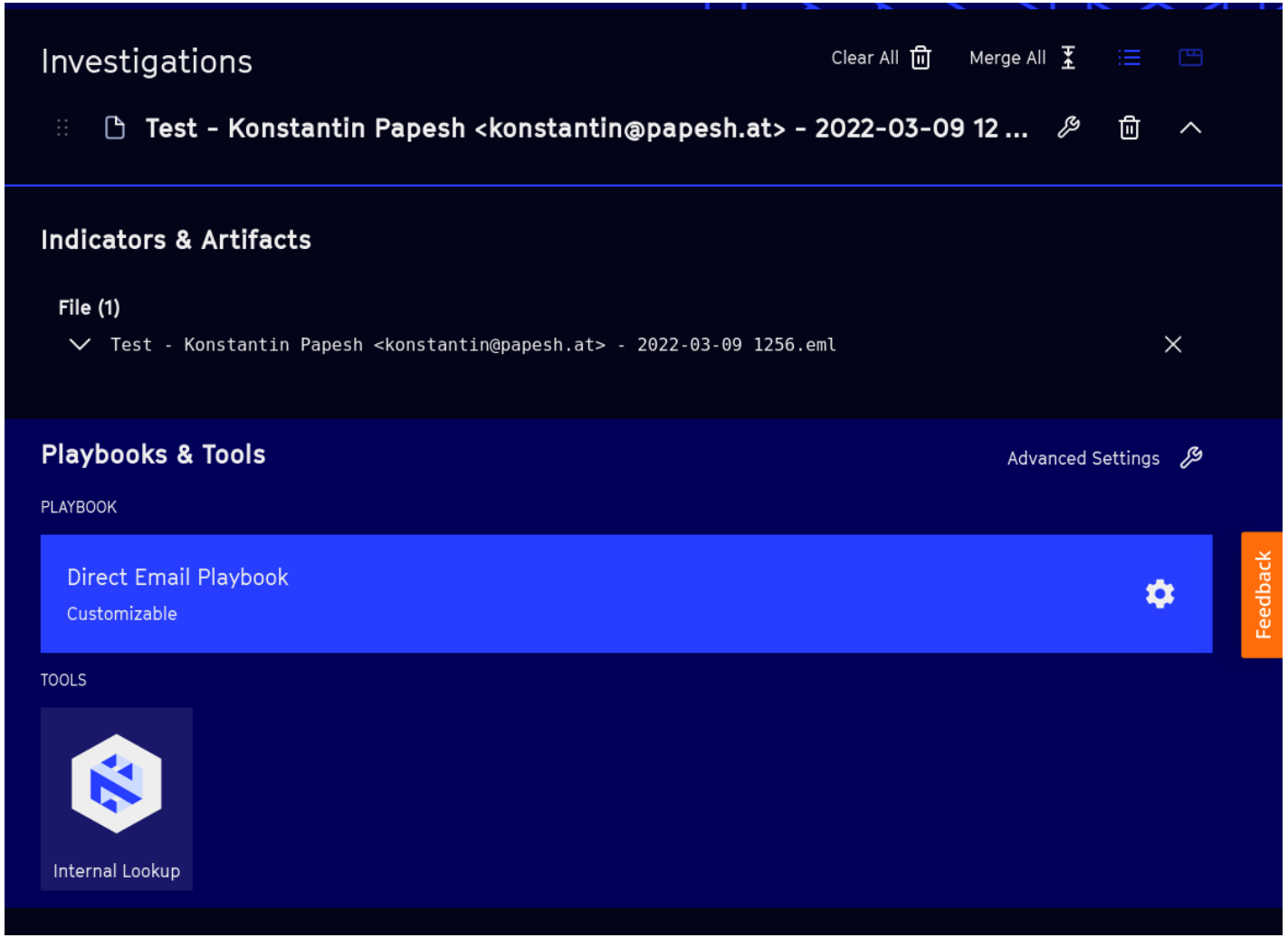


Figure 5:
Frontend example
of the SOC-Toolkit.

Figure 6:
Metric visualisation via the Enodo frontend.

The Results

- What CTI measurements do already exist?
  - Multiple feasible metrics found.
- How can these be altered to work with CTI data of a SOAR platform?
  - Removal of metrics requiring multiple snapshots, adding API response time and comparing objects more in-depth.
- How can a CTI rating framework be incorporated into a SOAR platform?
  - Integration of CTI rating framework into SOAR platform no major problem.

- Comparison between metrics of different services is possible.
- Further research directions
  - Include historic data
  - Incorporate user feedback
  - Include more metadata into calculation

References

[1] https://docs.oasis-open.org/cti/stix/v2.1/stix-v2.1.html

[2] https://traut.github.io/stixview/dist/demos/viewer.html

[3] https://gist.githubusercontent.com/traut/05d70be673133b0b4c938057fb38da04/raw/821424986917ab3e3ddb0a78ef3dfc9ad9f1b9bb/stix21-sample-bundle.json

[4] https://www.optiv.com/navigating-security-landscape-guide-technologies-and-providers

[5] D. Schlette, F. Böhm, M. Caselli, and G. Pernul, „Measuring and visualizing cyber threat intelligence quality“, International Journal of Information Security, vol. 20, no. 1, pp. 21–38, Feb. 2021. doi: 10.1007/s10207-020-00490-y.

[6] T. Schaberreiter, V. Kupfersberger, K. Rantos, A. Spyros, A. Papanikolaou, C. Ilioudis, and G. Quirchmayr, „A Quantitative Evaluation of Trust in the Quality of Cyber Threat Intelligence Sources“, in Proceedings of the 14th International Conference on Availability, Reliability and Security, New York, NY, USA: ACM, Aug. 2019, pp. 1–10, isbn: 9781450371643. doi: 10.1145/3339252.3342112.

AIST