Agenda

- Welcome
- Transitions
- Engagements
- CTI TC Working Group Calls
Welcome

Be sure to record your attendance
This meeting does count towards voting rights

If you have any questions, please contact workspace-transition-questions@oasis-open.org

Working with OASIS and Higher Logic to troubleshoot issues with the new platform. Please ensure emails from the following domains are not sent to the your spam folders: (1) ConnectedCommunity.org (2) mail.groups.oasis-open.org.

There have been cases where emails from the system where not sent to users and other cases where system emails were sent to spam folders.
Transitions - Stepping Down

- **Emily Ratliff** is stepping down as **STIX co-chair**
  - Emily will remain an **editor** and **maintainer**

- **Jonathan Matkowsky** is stepping down as **Secretary**
  - Jonathan is actively for **Microsoft** representation

Thank you again to Emily and Jonathan for your contribution to the TC!
Transitions - Stepping Up

- **Steve Relitz** is stepping up as STIX co-chair
  - Involved in STIX since 2014
  - Hosted Interop Plugfest and CASP Village

Thank you Steve for your willing to serve the TC in this capacity!
CTI Engagements

Adoption & Awareness Events
# Upcoming Engagement Opportunities

<table>
<thead>
<tr>
<th>Event</th>
<th>Location</th>
<th>Date</th>
<th>Submission Deadline</th>
</tr>
</thead>
<tbody>
<tr>
<td>CASP Cybersecurity Automation Village</td>
<td>Reston, VA</td>
<td>April 10-12</td>
<td></td>
</tr>
<tr>
<td>FIRST CTI</td>
<td>Berlin, Germany</td>
<td>April 15-17</td>
<td>Dec 21-2023</td>
</tr>
<tr>
<td>RSA 2024</td>
<td>San Francisco, CA</td>
<td>May 6-9</td>
<td>Oct 13-2023</td>
</tr>
<tr>
<td>FIRST Conference</td>
<td>Fukuoka, Japan</td>
<td>June 9-14</td>
<td>Nov 30-2023</td>
</tr>
<tr>
<td>Blue Team Con</td>
<td>Chicago, IL</td>
<td>September 6-8</td>
<td>Mar 17-2024</td>
</tr>
<tr>
<td>InfoSec World 2024</td>
<td>Lake Buena Vista, FL</td>
<td>September 23-25</td>
<td>Feb 26-2024</td>
</tr>
<tr>
<td>National Cyber Summit</td>
<td>Huntsville, AL</td>
<td>September 24-26</td>
<td>May 10-2024</td>
</tr>
</tbody>
</table>

Let us know if you are tracking any events not on this list.
FIRST CTI

April 15-17, 2024
Berlin, Germany
The conference serves as a hub for experts to exchange knowledge, share innovative ideas, and learn about the latest proactive strategies in threat intelligence.

Different talks were directly mentioning the STIX standard and some talks did more advanced analysis:

- Solving CTI Sector Incoherence in a Living Growing OpenCTI Repository: Extend STIX 2.1 FTW
  - Explaining all the challenges with duplicated entries, label misused, misspellings,...
  - Sectors are different between STIX 2.1 and US CISA (e.g. Academic versus Education)
  - Many other issues were described
- Multiple talks about LLM/AI/ML mentioning STIX as an export format without going into much detail

In Session #1:
We discussed where there were current successful examples of LLM/AI/ML to generate valid STIX 2.1 content. There are limitation gaps with only simple examples (e.g. one object) being generated by some models. ChatGPT was mentioned as a known model with simple examples.

We also discussed the ability to leverage STIX as structured inputs for LLM/AI/ML models to generate knowledge and content.
FIRST Conference 2024
Fukuoka, Japan

• NeuroCTI - A Custom Fine-Tuned LLM For CTI
  • Benchmarking, successes and lessons learned to build an open LLM model for CTI analysts. An open model was also published. STIX and MISP standard were mentioned as an output format to facilitate the integration with threat intelligence platforms. A significant number of challenges were in the clean-up of the original threat intelligence reports usually in PDF or HTML. Standard like STIX were lacking in the original data source to facilitate the building of the model.
  • Online demo and classification: https://test.cti.tools/
  • First model published: https://huggingface.co/ctitools/neurocti-small

• Information Sharing SIG
  • STIX version 1 and version 2 - what's the current deprecation level for version 1 and the communication sent to vendors still using STIX 1 only.
  • Request for sample STIX 2.1 dataset - The following dataset was mentioned but https://codeberg.org/adulau/misp-circl-feed but the cybersecurity community is actively searching for more.

• Standards SIG
  • Interested to improve the STIX2 Incident Reporting data model, including between documentation, collecting and defining more realistic sample data, and developing training materials.

In Session #1:
We discussed establishing a stronger relationship with FIRST and updates to CTI Extension Process Policy which supports all extension work including the STIX Incident Object.
Open Source Community

A few recent new initiatives and updates to projects using STIX
Open Source Community

- [https://github.com/AbuseTotal/openstix-python](https://github.com/AbuseTotal/openstix-python)
  - OpenSTIX is an **unofficial STIX 2.1 library and toolkit** built upon the foundations of the STIX2 library, aimed at enhancing the efficiency and productivity of cybersecurity professionals. It is developed and maintained by AbuseTotal, a startup committed to delivering high-quality software solutions in the cybersecurity domain.
  - Built-in datasets to facilitate the use of external references such as MITRE ATT&CK

- [https://github.com/MISP/misp-stix](https://github.com/MISP/misp-stix)
  - MISP-STIX is the python library used in MISP to convert MISP ↔ STIX
  - Many improvements in the recent releases were done to have a full coverage and mapping (ideas for the future STIX 2.2)

- If you know about other Open Source projects relying/using STIX 2.1, let us know.

In Session #2:
Another tool was mentioned [txt2stix](https://github.com/muchdogesec/txt2stix). txt2stix is a Python script that is designed to identify and extract IoCs and TTPs from text files, identify the relationships between them, convert them to STIX 2.1 objects, and output as a STIX 2.1 bundle. [https://github.com/muchdogesec/txt2stix](https://github.com/muchdogesec/txt2stix)
CTI TC Working Group

Fridays 8:30-9:30 AM EST will transition CTI TC Working Group sessions. The CTI TC Working Group will provide an opportunity for the TC to continue collaboration and discussion of related topics.

Let us know if
- you have any topics you would like to bring up so we can coordinate the agenda
- you want to attend but the current time slot doesn’t work for you

The following topics were mentioned:
- Playbook Extension
- OASIS ITU response - to be discussed during the July Monthly meeting
- FIRST Collaboration and Liaisons
- ITU Liaison