Cyber Threat Intelligence (CTI) SIG
2022 Annual Update

(TLP CLEAR)

Krassimir Tzvetanov (Purdue University)

Hendrik Adrian (LACERT)

James Chappell (Digital Shadows)

Overview

The Cyber Threat Intelligence (CTI) SIG

Established: February, 2018

Members: 216 registered, with 30+ active members

Meetings: Every second Wednesday in two time zones (alternating 8:00 and 3:30 pm UTC)

Goals:

- Standardize terminology across the industry
- Train new analysts and create educational and training material
- Help new teams build their program from scratch

Group philosophy and results

- **Philisophy:**

  Quality over quantity; point to the original materials

  We are not trying to gain numbers and want to make sure people who join are interested in contributing

Output:

- A common body of knowledge as **CTI Curriculum, Resources for starting a new team, Links to software, training, and education resources**
- Events: Online summits and contributions to FIRST technical events. CTI Training/Workshops, Briefing Papers and Shared Tools to help practitioners of Cyber threat Intelligence.

New Achievements, Projects & Goals

1. What is NEW in 2023's CTI SIG achievements:

- **Curriculum v3**
  - Building a new CTI team
    * With CTI Starter Kit slide for Business & Technical Stakeholders
  - Threat Intelligence program phases
  - Examples of Threat Modeling
  - CTI Tools setup reference

2. New projects we are working now (for 2024 goals)

- CTI Team Maturity Phases
- CTI Table Top Exercise
- Translation for Curriculum v3 to other languages

Maintaining previous works/projects

Maintenance & improving the previous projects:

- MITRE ATT&CK's threat techniques addition research on new technique Achievement:

  "TimeBomb" concept in malware sub-technique addendum at:
  T1124 "System Time Discovery"

- ICS/OT Indicator Taxonomy for MISP
  (updates in standard of maintenance section)

- Megalist Project maintenance
  (development version 0.4.07)

#FIRSTCON23

Thank you!

https://www.first.org/global/sigs/cti/

To subscribe to the mailing list for updates email:
cti-sig-news-subscribe@first.org