FIRST Cyber Threat Intelligence (SIG)

2022 Annual Activity Report

(TLP WHITE)

Version: 1.3j - 5 to 10 minutes presentation

SIG Steering committee/Co-chairs:

James Chappell
Hendrik Adrian
Krassimir Tzvetanov

About Cyber Threat Intelligence SIG

The Cyber Threat Intelligence (CTI) SIG's

- **Goal:** Create common definitions of Cyber Threat Intelligence to enable useful discussion. Create best practice materials and resources.
- **Started:** 2018 in 30th Annual conference in KL. Originally proposed in February 2016 at TC in Munich,
- **Products:** A common body of knowledge called the **curriculum** and a **resources guide**. Online Summits and contributions to FIRST Technical Summits. CTI Training/Workshops, Briefing Papers and Shared Tools to help practitioners of Cyber threat Intelligence.
- **Membership:** 191 subscribed members across FIRST.

CTI SIG Mission and Goal

1. **Promote the benefits of** Cyber Threat Intelligence (CTI) and provide accessible and clear content to benefit FIRST members and attract new members to our community.

2. **Creation of** a FIRST wide common **body of knowledge (CBK) on Threat Intelligence** and establish it as an industry standard.
   This includes:
   - Definitions of commonly used terms
   - List of Tools that can be used by CTI Teams
   - List of Data Sources
   - Best practices / Methods

1. **Promote events through FIRST**
2. **Support CTI activities globally**
3. **Stay apolitical** - not a sharing forum
   We help members to develop maturity of CTI activities and connections instead.

Membership

- About the SIG: https://www.first.org/global/sigs/cti/
- How to apply: **Talk to SIG Chair, or use the "Request to Join" in FIRST Portal**
- Email Participants must be **willing to actively participate in CTI SIG activities**

No	Year	Membership	Growth
1	2018	100-	-
2	2019	150+	+ 50%
3	2020	171	+ 14%
4	2021	183	+ 7%
5	(up to June) 2022	191	+ 4%

- To set expectations - multiple roles:

  Reviewer, **Contributor** or **Curator.**

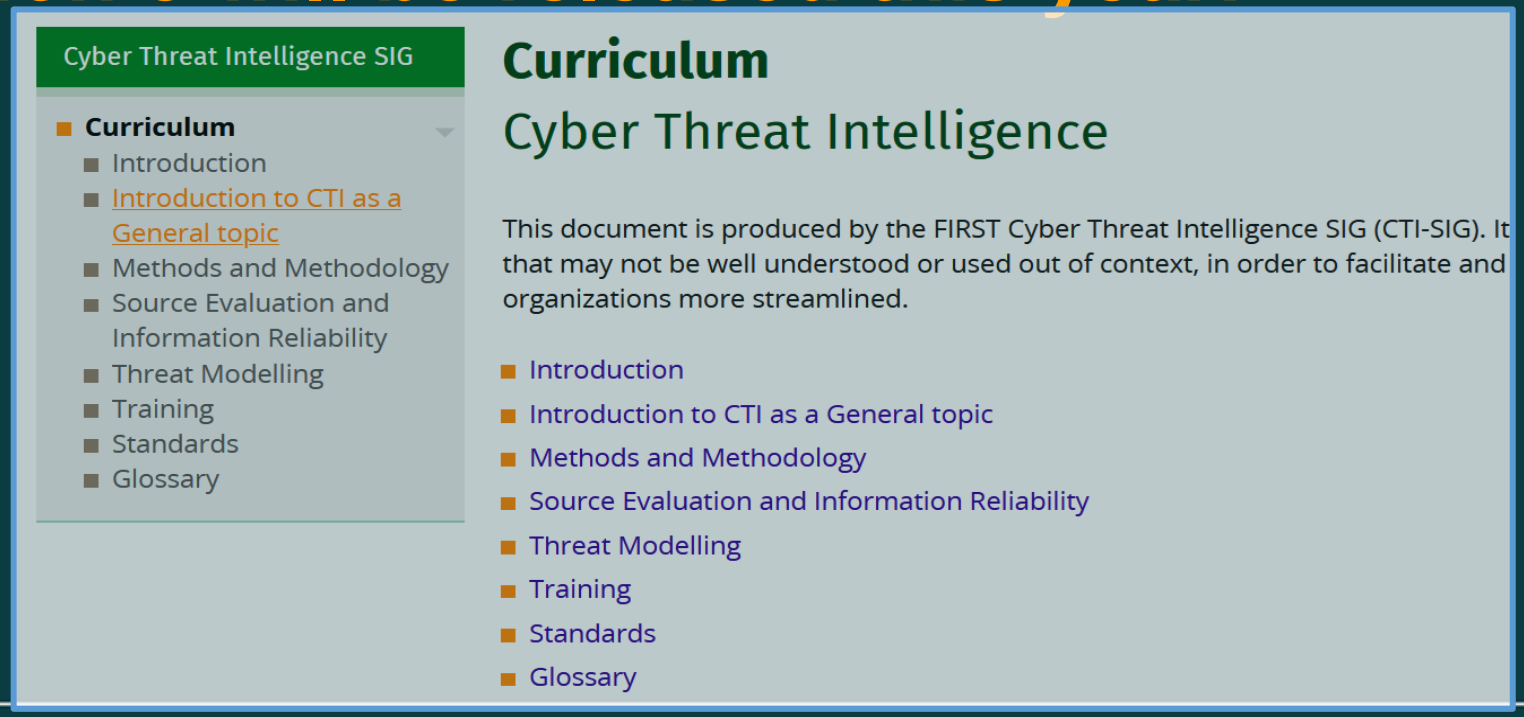
So what we have achieved in 2022?

Achievements in 2022: CTI Curriculum

1. **Cyber Threat Intelligence Curriculum (version 2)**

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

Version 3 will be released this year!



Achievements in 2022: CTI Curriculum

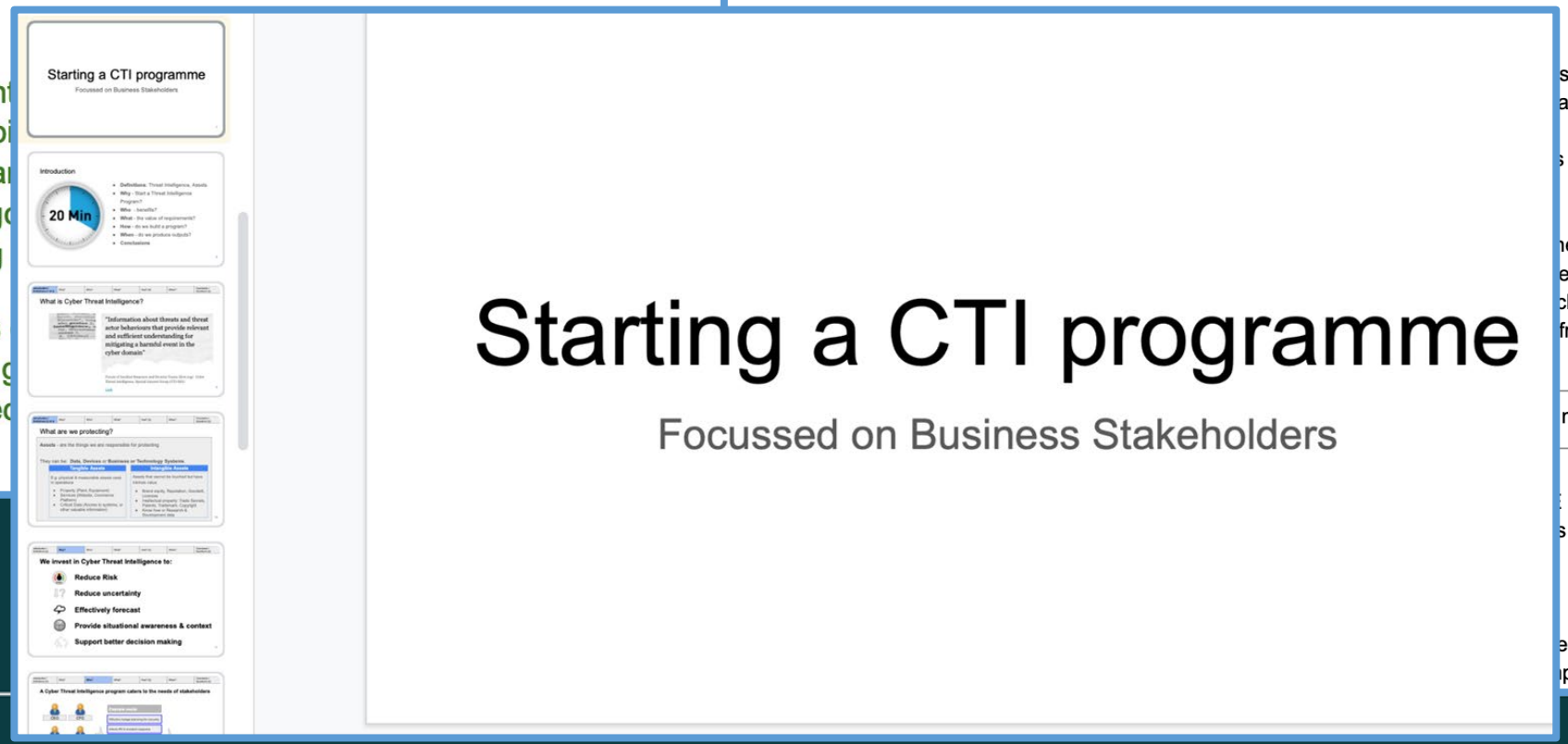
To be released:

1. Threat Intelligence Program Phases

Background

The goal of this document
Threat Intelligence capabi
greenfield efforts but it ca
in this space. The main g
capability without making

There are different levels
intended to be a general g
to fit your company's need



CTI Threat Modeling Example - Author: Adrian, Hendrik, Cyber Emergency Center, LAC/LACERT

Page 1

THREAT MODEL SECTOR: ONLINE GAME INDUSTRY

(presented on FIRST CTI SIG 20200214 by

- System exploitation (vulnerability)
  - DoS
  - Info leak
  - Elevation of privilege of game service

Possible *"exploit"*:

- tampering cookies in the game used device or from a service

to add permissive
s, dates)
ated (as per above

s access

ney
e (losses of trust)
claims)
from cookie abuse)

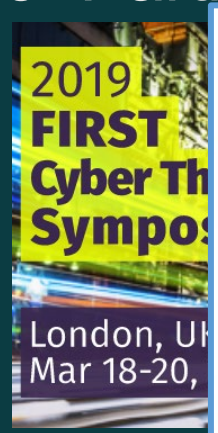
model & build trees

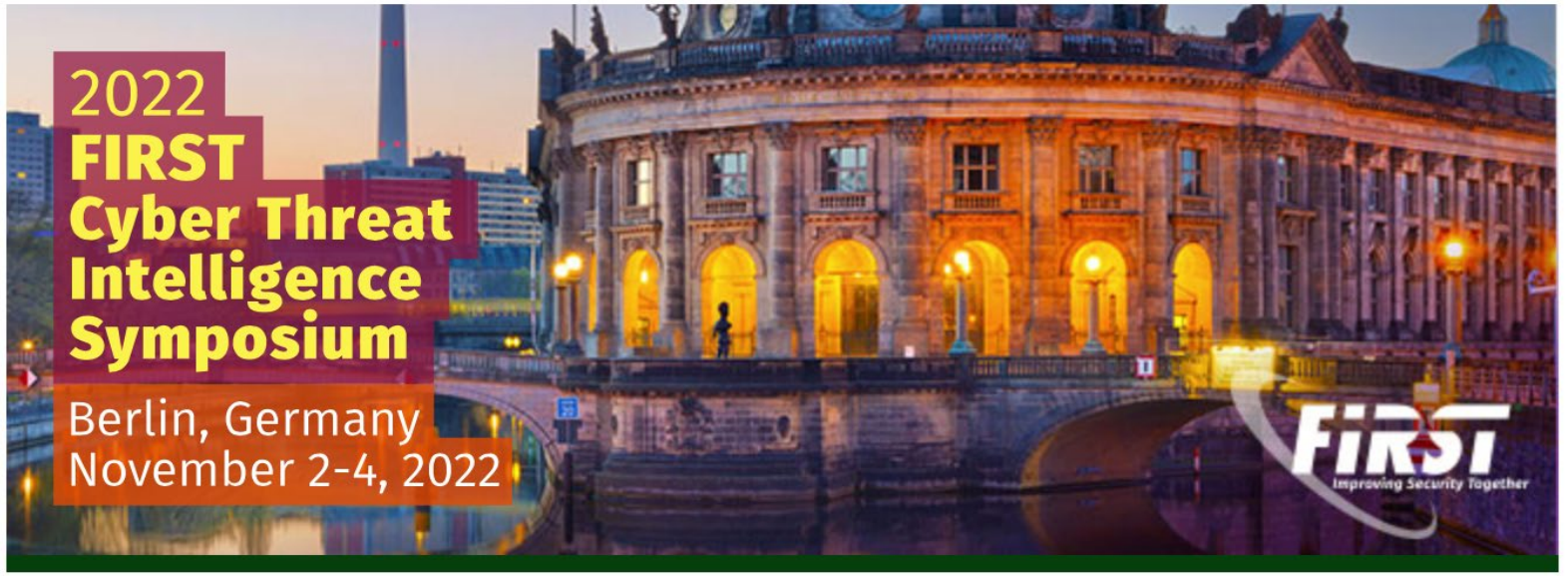
(based on definition
s applicable score is

eering
pered cookie

in 2022: CTI Events

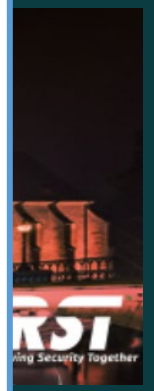
3. Participation in planning and organizing FIRST CTI events

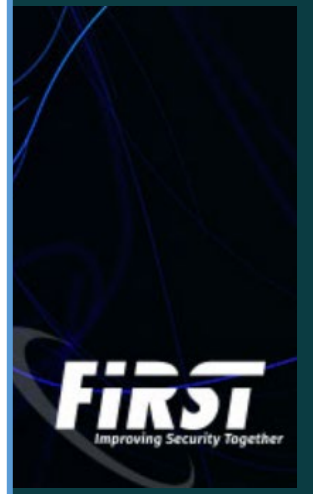




2022 FIRST Cyber Threat Intelligence Symposium | #FIRSTCTIBerlin22

Berlin (DE), November 2-4, 2022





What...in 2022: Standard bodies work

On projects, previously we had achieved these..

Tools **Categories (C)**	no	description	index code
	1	Intel Collection	C1
Status: Discussed, Applied	2	Intel Analysis	C2
Explanation:	3	RE & Malware	C3
"C" defines CATEGORY of the pointed tools or feeds or links, not its data	4	Triage	C4
	5	General	C5
	6	DFIR Artifacts Acquiring	C6
	7	Offensive tool (RAT/rootkit/vuln-scan)	C7

Search your desired category

C2, C3, C6 16 of 21

INTERNAL USE ONLY | (LEGEND: SOFT R... OFFENSIVE TOOL, REVMARK FOR ANALYSED ITEM)

Megalist Resource

Title	[C]ategory	[P]urpose	LastUpdate	Summary	
Vfeed	C4, C5	P1, P2	25-Nov-2017	VFeed Core collects the basis xml feed which is generated by a reliable reference and correlates it across multiple information sources.	http://www. https://githu
Viper	C3, C6	P1, P2	24-Oct-2018	Viper is a python based binary analysis and management framework, that works well with Cuckoo and YARA	https://githu
VirusShare	C2, C3, C6	P1, P2	N/A (online tool	VirusShare.com is a repository of malware samples to provide security researchers, incident responders, forensic analysts, and the morbidly curious access to samples of malicious code.	https://virus
Virustotal	C2, C3, C6	P1, P2	N/A (online tool	Virustotal, a subsidiary of Google, is a free online service that analyzes files and URLs enabling the identification of viruses, worms, trojans and other kinds of malicious content detected by antivirus engines and website scanners	https://www
Visualize_Logs	C2, C3, C6	P1, P2	12-Nov-2016	Open source visualization library and command line tools for logs. (Cuckoo, Procmon, more to come...)	https://githu
Vlany	C3, C6, C7	P1, P3	11-Aug-2017	vlany is a Linux LD_PRELOAD rootkit.	https://githu

FIRST.ORG CTI SIG - MISP Proposal for ICS/OT Threat Attribution (IOC) Project

*) Based on agreed CTI SIG new project draft proposed in 20190717: https://docs.google.com/document/d/1EVMAR8T0-E0X0798PqPzYRybUpoUA2TIJhG0_dCrC5k/edit#

ICS/OT MISP Taxonomy

Item 01 ICS/OT Components Categories	OT Components Category	Description	MISP Proposed Impl
	Programmable Logic Controller (PLC)	1. Computing device with user-programmable memory to storing instructions to operate a physical process. 2. Various PLC types for different processses	Taxonomies
	Remote Terminal Unit (RTU)	1. Data aquisitionand control unit designedto support field sites and remote 2. [illegible] and wireless communication capabilities 3. No st[illegible] program log	
	Human-Machine Interface (HMI)	1. Hardware/software that operators used to interact with control system. 2. From physical control panels to a complete cpmputer systems	
	Sensors	Pressure, Temperature, Flow, Voltage, Optical, Proximity	
	Actuators	Variable Frequency Drive, Servo Drive, Valve, Circuit Breaker	
	Communications	Modems, Routers, Serial - Ethernet Converters, Swtiches	
	Supervisory Level Devices	1. Control Server (Supervisory systems that hosts control software to manage lower level control devices like PLC). 2. Data Historian (Centralized database for information about process, control activity and status record). 3. Engineering workstations (Creating and revising control systems anbd programs, incl. project files).	

References	Description	MISP Proposed Impl
RTOS https://en.wikipedia.org/wiki/Comparison_of_real-time_operating_systems	Please see the URL reference, there are a lot of it to be listed in here . These OS are also referred as Firmware.	Taxonomy
Linux Embedded Base OS	Yocto Buildroot OpenWRT B & R Linux Scientific Linux Raspbian	

FIRST CTI SIG PROJECT FRAMEWORK TO ENRICH MITRE ATT&CK® MATRIX

Version5 release date: 08.28.2020 (firstly presented in FIRST.ORG CTI SIG on 07.29.2020)

What...in 2022: Standard bodies work

4. **Maintenance & improve the projects we had achieved:**

New Projects:

- CTI Curriculum Translation Project (to support multiple languages)
- Research to improve CTI Platform related products/tools

Maintaining Previous Developed Projects:

- MITRE ATT&CK's CTI SIG threat techniques addition framework on new technique
  Achievement: "TimeBomb" concept in malware sub-technique addendum at T1124 "System Time Discovery"

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

- Megalist Project second version released (dev v0.4.07) (updates)

What's next? Road map to 2023

Members:

- Keep encouraging members for more contribution and collaboration
- Finding new ways of working to engage with busy FIRST membership

Curriculum:

- Cyber Threat Intelligence Curriculum fourth version
  - additional chapters to fill more gaps in details in published curriculum

Events:

- FIRST Cyber Threat Intelligence Conferences in 2023
- Workshop and training for 2023 during the FIRST events

New **Project:**

- CTI TTX Plan, Re-activation for a lot of pending ideas to develop! Stay tune!

Questions?