Threat Intelligence Episode 3: CTI Goals

A picture containing diagram

Description automatically generated

**Disclaimer- Please use the below information only for learning, if the below information is used for any unethical activity, I am not accountable for that.**

**HELPFUL TO KNOW-**

**People you may want to connect with:** CyberSec\_Sai <https://link.medium.com/VbSq30Ujezb>

**To Recommend one book through every episode:** [Cyber Threat Intelligence No-Nonsense Guide](https://www.amazon.in/Cyber-Threat-Intelligence-No-Nonsense-Security/dp/1484272196/ref=asc_df_1484272196/?tag=googleshopdes-21&linkCode=df0&hvadid=586192038696&hvpos=&hvnetw=g&hvrand=7481315702143497430&hvpone=&hvptwo=&hvqmt=&hvdev=c&hvdvcmdl=&hvlocint=&hvlocphy=9062143&hvtargid=pla-1339488827948&psc=1), [Practical Threat Intelligence and Data-Driven Threat Hunting - Valentina Costa-Gazcó](https://yaksas.in/ycscblog/book-review-practical-threat-intelligence-and-data-driven-threat-hunting/#.ZEUIxnZBy3A),

**Links to Read/learn through every episode:** [SANS DFIR](https://www.youtube.com/@SANSForensics/playlists), [SANS CTI Summit](https://www.youtube.com/watch?v=Qy-19aRN58M&list=PLfouvuAjspTpvL3nQFAxSq3oQCeCWfn5P) , <https://github.com/BushidoUK/Open-source-tools-for-CTI/blob/master/Collections.md>

<https://medium.com/week-in-osint>

<https://socradar.io/top-open-source-solutions-for-building-security-operations-center-2/>

<https://socradar.io/how-to-build-a-soc-with-open-source-solutions/>

**Open-Source TI tools**: [MITRE ATT&CK](https://attack.mitre.org), [MITRE D3FEND](https://d3fend.mitre.org/), [URLscan.io](https://urlscan.io/), [Abuse.ch](https://abuse.ch/), [Malware Bazaar](https://bazaar.abuse.ch/), [Feodo Tracker](https://feodotracker.abuse.ch/), [URLHaus](https://urlhaus.abuse.ch/), [Threatfox](https://threatfox.abuse.ch/), [Yaraify](https://yaraify.abuse.ch/), [SSL Blacklist](https://sslbl.abuse.ch/), [AlienVault](https://otx.alienvault.com/browse/global/pulses?include_inactive=0&sort=-modified&page=1&limit=10), [OpenCTI](https://github.com/OpenCTI-Platform/opencti), [MISP](https://www.misp-project.org/),

**Threat Intel Feeds:** [Crowd strike Falcon](https://www.comparitech.com/go/crowdstrike-threat-intelligence-feeds-learn-more-best-threat-intelligence-feeds/l/list_dd_d__post__368152/u/2077720985.1670085930+1682237532+368152++d/), [AlienVault OTX](https://otx.alienvault.com/browse/global/pulses?include_inactive=0&sort=-modified&page=1&limit=10), [Anomali ThreatStream](https://www.anomali.com/products/threatstream), [Mandiant Threat Intelligence](https://www.mandiant.com/advantage/threat-intelligence)

**Useful Website:** [Virus Total](https://www.virustotal.com/gui/home/upload), [Open Source Tools for CTI](https://github.com/BushidoUK/Open-source-tools-for-CTI), [App.Any.Run](https://app.any.run/), [Hybrid Analysis](https://www.hybrid-analysis.com/), [FileScan.io](https://www.filescan.io/scan), [MITRE Group DB](https://attack.mitre.org/groups/), [Dragos Threat Groups](https://www.dragos.com/threat-activity-groups/),

**Resource:** [Malware samples sources](https://zeltser.com/malware-sample-sources/) , [Malware sources](https://infosecwriteups.com/malware-sample-sources-a3c7f306adea), [Adversary Intelligence](https://github.com/BushidoUK/Open-source-tools-for-CTI/blob/master/Adversary%20Intelligence.md), <https://start.me/p/ELY5By/technical-sources>

**Keynotes:**

**CTI Evolution:**

1. **Observable:** specific instance of “Bad”, Likely unique to the environment of compromise
2. **Indicator of Compromise:** compound statement of observables indicating breach, not used correctly in practice.
3. **Behavior**: How an adversary operates throughout the Kill Chain, most difficult to identify; most robust for detection

**CTI Goals:**

1. Build Understanding through Observables and IOCs
2. Transition Data into Adversary Behaviors
3. Build Detections and Defenses around Adversary Behaviors

**Malware Analysis Goals:**

Malware Sample -> Functionality & Purpose, Design & Structure, Signature & Detection

Malware Sources -> Incidents & IR Data, Shared Samples & Requested Analysis, 3rd Party Sources & Sample Gathering

Intrusion Event Components: (Security Incident)-> Host Data &Tools, Network Traffic & Protocols, Adversary intent & Purpose.

**Limitations:** Malware Analysis Provides Part of the Overall Picture; Overemphasis on Technical Binary Analysis Produces Skewed Conception; Context, Purpose, and Function are critical to understanding

**Tools vs. Actors-**

**Tool Continuity:**

**Dev Actor:** Dedicated Entities produce capabilities -> Capabilities transferred to command authorities to achieve strategic objectives.

**Planning Actor**: Capabilities transferred to command authorities to achieve strategic objectives -> Equities and exposure risk process determines entities for sharing and distribution.

**Operations Actor:** Equities and exposure risk process determines entities for sharing and distribution -> capabilities moved to operational teams to fulfil strategic missions.

**Malware Analysis Value-**

Malware Analysis is valuable and Important -> only one aspect of security event analysis, may lead to skewed perspectives, can indicate operational relationships where none exist.

**“Holistic” Threat Intelligence**: (Event Knowledge) ->Malware, binaries, tools; logs, artifacts, data; intent, purpose, objectives.

Please let me know if this has helped you in any way. You can also add your views through comments. I will be back next time with some more sharp insights on TI Episodes.

-by Shefali Kumai

For more cyber security learning follow me here-

<https://www.youtube.com/channel/UCf-F-eATCUXYaUVk8Xl7OOQ>

<https://www.instagram.com/cybersecurity.cyber_seek/>

<https://twitter.com/Shefali37920461>