Threat Intelligence Episode 1: Sharp Insights

A picture containing diagram

Description automatically generated

**HELPFUL TO KNOW-**

**People you may want to connect with:**

[Katie Nickels – Medium](https://medium.com/@likethecoins); [Adam Pennington – Medium](https://medium.com/@adamp_mitre); [Chad Warner – Medium](https://warnerchad.medium.com/);

**To Recommend one book through every episode:** [Mastering Cyber Intelligence](https://www.oreilly.com/library/view/mastering-cyber-intelligence/9781800209404/)

**Links to Read/learn through every episode:**

[“Mastering Cyber Intelligence” Notes | by Chad Warner | Medium](https://warnerchad.medium.com/mastering-cyber-intelligence-notes-985f6ead1b8a)

[Brief Review of 10 Threat Intel & Hunting Book Haul | by Unrivaled Rōnin | Medium](https://atrhein.medium.com/brief-review-of-10threat-intel-hunting-book-haul-55096d531545)

**Useful Website:** [pdfdrive-largest book database](https://pdfdrive.to/top-mastering-cyber-intelligence-books)

**Resource:** <https://academy.attackiq.com/> ; <https://ctf.cybersoc.wales/>

**KEY POINTS:** What to learn in Threat Intelligence-

1. You will want to learn **YARA**, **SNORT**, and **SIGMA**.” Sigma is for log files (to create detection rule) as Snort is for network traffic, and Yara is for files pattern match.
2. Having knowledge in the domain of Threat Hunting, Malware Analysis is a great help here to learn Threat Intelligence better.
3. Have some Understanding about Diamond model for intrusion analysis, MITRE ATT&CK framework, Cyber Kill Chain, Pyramid of Pain, Dark web Intelligence, and ATT&CK Navigator.
4. Understanding about Data, Information, and Intelligence helps to better analyse/process raw data – “**Data**” is discrete facts and stats gathered for analysis (e.g., IP addresses, URLs, hashes).“**Information**” is multiple data points combined to answer specific questions (e.g., answer to question, “How many times has my organization been mentioned on social media this month?”).“**Intelligence**” is result of analysing data and info to uncover patterns and provide context for decision-making. It must point toward specific decisions or actions and be tailored for easy use by a specific person, group, system that will use it to decide or act.
5. Have good knowledge of Cyber Threat Intelligence Life Cycle, and Threat Intel types (Strategic Intel, Tactical Intel, Technical Intel, and Operational Intel)
6. Do learn about how IOCs are utilised in TI, TTPs are mapped using raw data/TI finished report to MITRE ATT&CK framework. [**Tactics:** adversary’s technical goals; **Techniques**: how goals are achieved; and **Procedures:** specific implementations of techniques]. ATT&CK helps the public focus on known TTPs to better defend their data.
7. IOCs are reactive TI; Mapping TTPs are proactive TI. Read more on Threat Intel User Cases, APT reports, Publicly available TI reports (by Mandiant, DFIR report, , threat post, bleeping computers etc.)
8. If you are not willing to pay for any courses; feel free to avail this [self-guide on CTI](https://medium.com/katies-five-cents/a-cyber-threat-intelligence-self-study-plan-part-1-968b5a8daf9a) written by [**Kate Nickels**](https://medium.com/@likethecoins).
9. Make sure to read about STIX, TAXII, and CyBOX to better understand how TI is shared using standardised formats with consumers for proactive measures and take threat-informed decisions. Also learn about Threat Intel Platforms (commercial/Open source)
10. **Reporting** plays an important role in consuming and sharing TI well to better utilise it in proactive approaches. Reporting for-

* SOC: reporting, IOCs, TTPs, Courses of Action (CoA)
* Threat hunting: IOCs, TTPs, Yara rules, detection signatures
* CISO: Reporting
* Threat and vulnerability management: reporting, CVEs, CoAs
* Executives: reporting
* Broader security team: reporting
* Fraud: reporting, indicators
* Product owners: reporting, CVEs, CoAs
* Wider staff: awareness reporting

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 Malware Analysis 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>