Threat Intelligence Episode 5: Role Spotlight

**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: Jeremy Dallman** Principal Research Director, Microsoft Threat Intelligence; **Amy Bejtlich** Director of Intelligence Analysis, Dragos Inc; **Samuel Kimmons** Red Team Lead.

**Book to read:** Psychology of Intelligence Analysis

**YouTube Channel to follow:** Threat Intelligence Academy

**Keynotes:**

1. **Purpose of a CTI team:**

A group of people standing in front of a white background

Description automatically generated with low confidence

1. **Structuring your team to generate Intelligence:**



1. **Planning and Direction Fundamentals:** Intelligence Requirements [Strategic, Operational, Tactical], Threat Modeling, Collection Management Framework.
2. **Collection Management Framework:**

A close-up of a table

Description automatically generated with low confidence

1. **Key collection sources:** Intrusion Analysis, Malware, Domains, External Datasets, TLS certificates
2. **Understand about psychology of intelligence analysis**
3. **Correlating clusters:** threat actors, activity groups, campaigns, intrusion sets

One shortcut to clustering is simply applying the diamond model, the goal is to identify unique characteristics, map the unique characteristics to the diamond model,

1. **Key to sharing threat intelligence is to first know your audience**
2. **Threat Intelligence Application:**

A picture containing text, screenshot, businesscard, design

Description automatically generated

1. **Threat Intelligence Competencies:** Critical thinking, data collection & Examination, Communication & Collaboration, Technical exploitation, Information Security, Computing Fundamentals,
2. **Threat Intelligence paths:** Law Enforcement, National Security, Data Science, Military Intelligence, Journalism, Cyber Security.
3. **Threat Intelligence Resources:** Reading blogs and listening to podcasts from vendors and researchers will really help, IOC feeds inside MISP, CTI reports.

A picture containing text, screenshot, font

Description automatically generated

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>