Threat Intelligence Episode 4: Career Build



**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:**

* **Eugene Levytskyi** [CEO at ParanoidLab | Cyber Threat Intelligence Analyst]
* [**Gary Ruddell**](https://uk.linkedin.com/in/garyruddell?trk=public_post_comment-text) is currently writing a 101 book about CTI and has some good content on LinkedIn and YouTube
* **Ashley Walker** OSINT | Threat Intel | Analyst | OPSEC | Firefighter | ThatThreatGuy |
* **Stewart K. Bertram** Head of Cyber Threat Intelligence
* **Gary Ruddell** I can help you get into cyber faster [Email: gary@garyruddell.com Twitter: @gary\_\_ruddell YouTube: @garyruddellofficial Instagram: garyruddellofficial ]

**Book to read:** [**Thomas Roccia**](https://au.linkedin.com/in/thomas-roccia?trk=public_post_comment-text) Visual Threat Intelligence [[Visual Threat Intelligence: An Illustrated Guide For Threat Researchers: Roccia, Thomas: 9798373228374: Amazon.com: Books](https://www.amazon.com/Visual-Threat-Intelligence-Illustrated-Researchers/dp/B0C7JCF8XD)]

**Learning material to build your career in CTI:**

**For absolute beginners**: ✅The Cycle of Cyber Threat Intelligence [**https://lnkd.in/di8BhrEz**](https://lnkd.in/di8BhrEz?trk=public_post-text) ✅Job Role Spotlight: Cyber Threat Intelligence [**https://lnkd.in/dzh7yX4j**](https://lnkd.in/dzh7yX4j?trk=public_post-text) ✅You MUST understand Cyber Threat Intelligence to Blue Team [**https://lnkd.in/dHEyV62n**](https://lnkd.in/dHEyV62n?trk=public_post-text) ✅Starting and Growing a Career in Cybersecurity, Digital Forensics, and Threat Intelligence [**https://lnkd.in/dVRQzvEW**](https://lnkd.in/dVRQzvEW?trk=public_post-text)

**More technically focused:** ✔️The Cyber Kill Chain [**https://lnkd.in/dprhKXGs**](https://lnkd.in/dprhKXGs?trk=public_post-text) ✔️Breaking The Kill Chain: A Defensive Approach [**https://lnkd.in/dxpUSmsa**](https://lnkd.in/dxpUSmsa?trk=public_post-text) ✔️Finding The MOST Valuable Data - The Pyramid Of Pain Explained [**https://lnkd.in/dkAxZVXy**](https://lnkd.in/dkAxZVXy?trk=public_post-text) ✔️The Secret Origins of the Pyramid of Pain [**https://lnkd.in/dNsDsbyE**](https://lnkd.in/dNsDsbyE?trk=public_post-text) ✔️Diamond Model of Intrusion Analysis - An Overview [**https://lnkd.in/dxd7hQmt**](https://lnkd.in/dxd7hQmt?trk=public_post-text) ✔️An Introduction to the Diamond Model of Intrusion Analysis by it's Co-Author Sergio Caltagirone [**https://lnkd.in/dtduCGPZ**](https://lnkd.in/dtduCGPZ?trk=public_post-text) ✔️What are Yara Rules (and How Cybersecurity Analysts Use Them) [**https://lnkd.in/dy3Y8Fjp**](https://lnkd.in/dy3Y8Fjp?trk=public_post-text) ✔️Malware Analysis Bootcamp - Creating YARA Rules [**https://lnkd.in/dwE8WmUt**](https://lnkd.in/dwE8WmUt?trk=public_post-text)

**Courses:** ✔️Intro to Cyber Threat Intelligence [**https://lnkd.in/d3d8uP5n**](https://lnkd.in/d3d8uP5n?trk=public_post-text) ✔️Cyber Threat Intelligence [**https://lnkd.in/driRRvvg**](https://lnkd.in/driRRvvg?trk=public_post-text) ✔️Cyber Threat Intelligence [**https://lnkd.in/dpkvF64d**](https://lnkd.in/dpkvF64d?trk=public_post-text) ✔️Using ATT&CK for Cyber Threat Intelligence Training [**https://lnkd.in/d6zzrNBy**](https://lnkd.in/d6zzrNBy?trk=public_post-text) ✔️Cyber Threat Intelligence 101 [**https://lnkd.in/d\_7m9-7f**](https://lnkd.in/d_7m9-7f?trk=public_post-text) ✔️MITRE ATT&CK Defender™ (MAD) ATT&CK® Fundamentals Badge Training [**https://lnkd.in/dbNyGtCV**](https://lnkd.in/dbNyGtCV?trk=public_post-text) ✔️MITRE ATT&CK Defender™ (MAD) ATT&CK® Cyber Threat Intelligence Certification Training [**https://lnkd.in/dsM\_\_Hqr**](https://lnkd.in/dsM__Hqr?trk=public_post-text) ✔️MITRE ATT&CK Defender™ (MAD) ATT&CK® SOC Assessments Certification Training [**https://lnkd.in/d2xwwEzM**](https://lnkd.in/d2xwwEzM?trk=public_post-text) ✔️Intermediate MITRE ATT&CK [**https://lnkd.in/d8u-JR5N**](https://lnkd.in/d8u-JR5N?trk=public_post-text)

**Keynotes:**

1. **Cycle:** Collect [integrate data] -> Process [put data in context] -> Analyze [Find insight and actions] -> Share [Inform decisions] to protect CIA triad
2. **Intelligence Areas:**

**A picture containing text, screenshot, font, menu

Description automatically generated**

1. **Link to learn -** [What is Cyber Threat Intelligence? [Beginner's Guide] (crowdstrike.com)](https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/)
2. **Threat Intelligence Sources –** Bleeping Computer, DARKReading, Trend Micro Vulnerabilities and Exploits, Krebson Security, InfoSecurity Magazine Threat Intelligence, IBM X-Force Exchange, Recorded Future Newsletter, DFIR Reports,
3. **Threat Intelligence Platforms-** Use [Collect -> Correlate -> Enrichment & Contextualization, Analyze, Integrate, Act]; Platforms like **Recorded Future**, **FireEye** [ subscription includes Fusion Intelligence, Strategic Intelligence, Operational Intelligence, Vulnerability Intelligence, Cyber Physical intelligence, Cyber Crime Intelligence, Cyber Espionage Intelligence], IBM X-Force Exchange, TruSTAR,
4. **Threat Intelligence Frameworks –** [Preparation -> Engagement -> Presence -> Effect/Consequence]
5. **Best Practices: Intelligent detection –** predict and prioritize security weakness, detect deviations to identify malicious activity, react in real time to exploits,

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>