Do you want to build a career in Cyber Threat Intelligence?

Follow this guidance

V 2

Core Knowledge

Skills required for CTI

- ✔ The Intelligence Life Cycle
- ✔ Cyber Kill Chain
- ✔ Diamond Model
- ✔ Pyramid Of Pain
- ✔ IOCs
- ✔ MITRE ATT&CK
- ✔ Courses of Actions Matrix
- ✔ YARA
- ✔ STIX/TAXII
- ✔ Traffic Light Protocol (TLP)
- ✔ Logical Fallacies and Cognitive Biases

CTI Books

General CTI books I highly recommend

- 🕮 “Cyber Threat Intelligence 101” by Gary Ruddell
- 🕮 "Visual Threat Intelligence: An Illustrated Guide For Threat Researchers " by Thomas Roccia
- 🕮 "The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage" by Cliff Stoll
- 🕮 "Structured Analytic Techniques for Intelligence Analysis" by Richards J. Heuer Jr. and Randolph H. Pherson
- 🕮 "Psychology for intelligence analysis" by Richard J. Heuer Jr.
- 🕮 "The Art and Science of Intelligence Analysis" by Julian Richards

CTI Videos

General CTI videos I highly recommend

📺 The Cycle of Cyber Threat Intelligence https://www.youtube.com/watch?v=J7e74QLVxCk

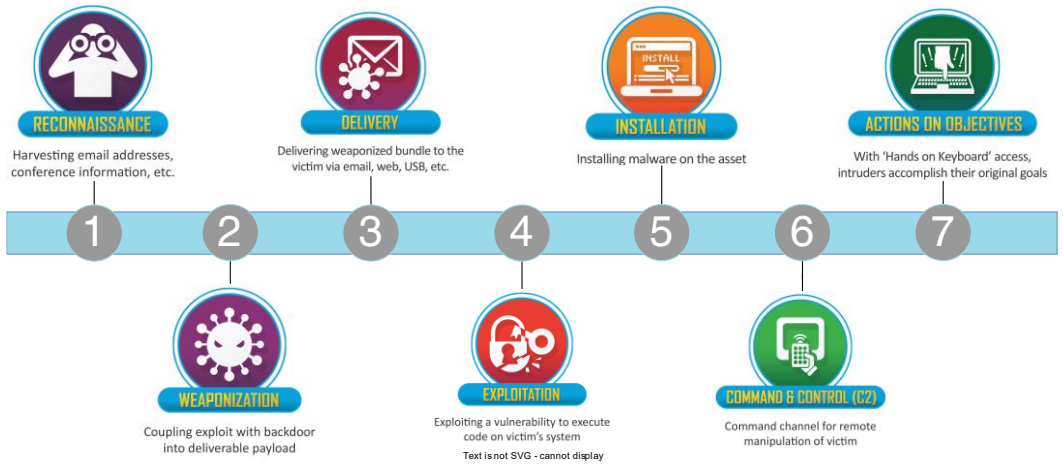
📺 Job Role Spotlight: Cyber Threat Intelligence https://www.youtube.com/watch?v=fvYb5-NxoDc

📺 You MUST understand Cyber Threat Intelligence to Blue Team https://www.youtube.com/watch?v=tWHqHy-MC1U

📺 Starting and Growing a Career in Cybersecurity, Digital Forensics, and Threat Intelligence https://www.youtube.com/watch?v=pykva0sI6u8

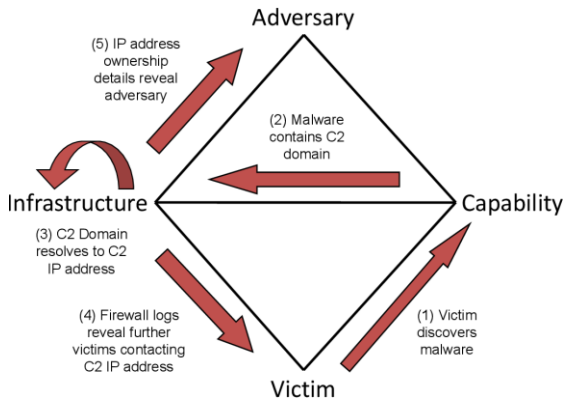
📺 SANS Cyber Threat Intelligence Summit 2023 https://www.youtube.com/playlist?list=PLfouvuAjspTpvL3nQFAxSq3oQCeCWfn5P

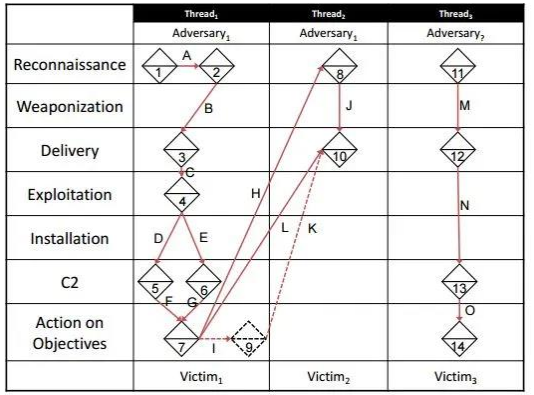
Cyber Kill Chain



- The Cyber Kill Chain https://www.youtube.com/watch?v=LqCbpiDyN8o
- Breaking The Kill Chain: A Defensive Approach https://www.youtube.com/watch?v=II91fiUax2g

Diamond Model



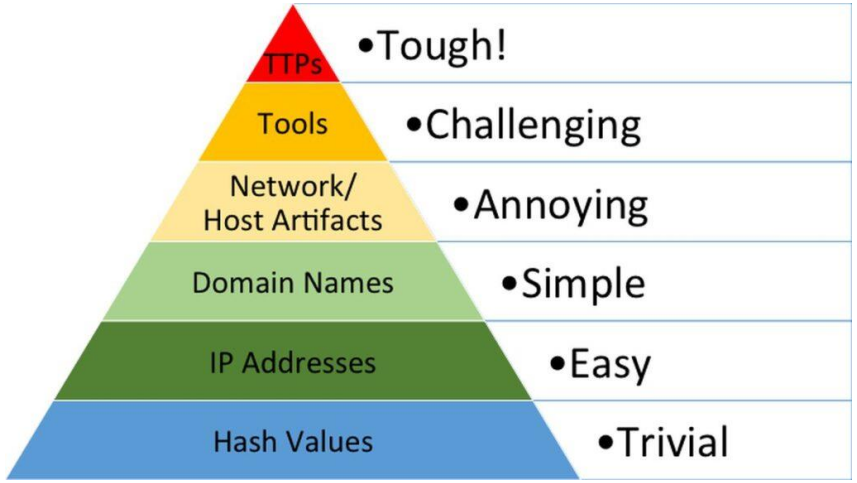


"The Diamond Model of Intrusion Analysis" by Sergio Caltagirone, Andrew Pendergast, and Chris Betz. A comprehensive guide that presents a structured method for analyzing cyber intrusions.

Diamond Model of Intrusion Analysis - An Overview https://www.youtube.com/watch?v=3PoQLOJr5WI

An Introduction to the Diamond Model of Intrusion Analysis by it's Co-Author Sergio Caltagirone https://www.youtube.com/watch?v=Yb4rg2NbgNw

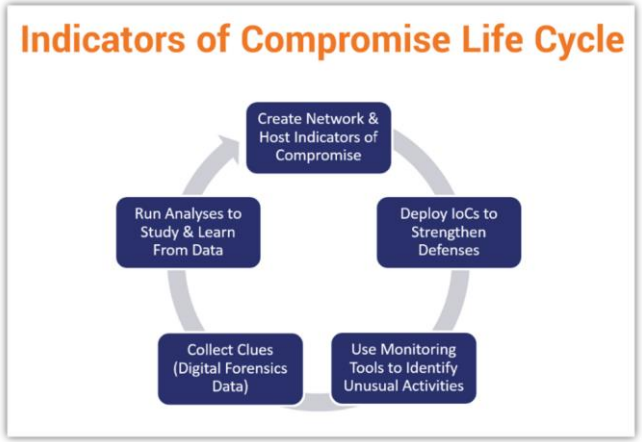
Pyramid Of Pain



- Finding The MOST Valuable Data - The Pyramid Of Pain Explained
  https://www.youtube.com/watch?v=O7PSKrgdHAI

- The Secret Origins of the Pyramid of Pain https://www.youtube.com/watch?v=3Xrl6ICxKxI

IOCs



- Understanding Indicators of Compromise for Incident Response
  https://www.youtube.com/watch?v=zs-AEaSd2vk

- Pyramid of Pain and Indicator of compromise
  https://www.youtube.com/watch?v=nQXtAv7EDrw

MITRE ATT&CK

- "MITRE ATT&CK™: Design and Philosophy" by Blake Strom, et al.
  A thorough exploration of the MITRE ATT&CK framework.

- The Anatomy of an ATT&CK https://www.youtube.com/watch?v=2icKi2q6NS4

- MITRE ATT&CK Framework for Beginners https://www.youtube.com/watch?v=GYyLnff2XRo

- Workshop: MITRE ATT&CK Fundamentals https://www.youtube.com/watch?v=1cCt2XZr2ms

Courses of Action Matrix

Kill-Chain Phases	Activity	Indicators	Courses of Action (COA)					
			Detect	*Deny*	*Disrupt*	*Degrade*	*Deceive*	*Destroy*
Reconnaissance	Research, Identification, and selection of targets	[Recipient List] Benign File: tcnom.pdf	Web Analytics	Firewall ACL				
Weaponization	Pairing remote access malware with exploit into a deliverable payload (e.g. Adobe PDF and Microsoft Office files	Trivial encryption algorithm: Key 1	NIDS	NIPS				
Delivery	Transmission of weapon to target (e.g. via email attachments, websites, or USB drivers)	dn...etto@yahoo.com Downstream IP: 60.abc.xyz.215 Subject: AIAA Technical Committees [Email body]	Vigilant User	Proxy Filter	In-line AV	Queuing		
Exploitation	Once delivered, the weapon's code is triggered, exploiting vulnerable applications or systems.	CVE-2009-0658 [shellcode]	HIDS	Patch	Data Execu-tion Pr-evention (DEP)			
Installation	The weapon installs a backdoor on a target's system allowing persistent access.	C:\...\fssm32.exe C:\...\IEUpd.exe C:\...\IEXPLORE.hlp	HIDS	"chroot" jail	AV			
C2	Outside server communicates with the weapons providing "hands on keyboard access" inside the target's network	202.abc.xyz.7 [HTTP request]	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objective	The attacker works to achieve the objective of the intrusion, which can include exfiltration or destruction of data, or intrusion of another target.	N/A	Audit Log			Quality of service	Honeypot	

Courses of Action Matrix in Cyber Threat Intelligence
https://warnerchad.medium.com/courses-of-action-matrix-in-cyber-threat-intelligence-82bf49243e46

YARA

- What are Yara Rules (and How Cybersecurity Analysts Use Them)
  https://www.youtube.com/watch?v=BM23_H2GGMA

- Writing YARA rules
  https://yara.readthedocs.io/en/stable/writingrules.html

STIX / TAXII

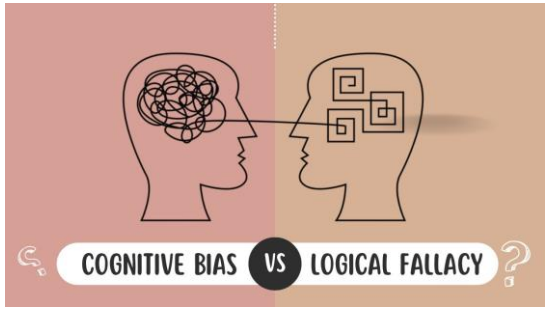
- What Are STIX/TAXII? https://www.youtube.com/watch?v=L7Ykky6Ntd0
- Introduction To STIX/TAXII 2 Standards https://www.youtube.com/watch?v=qAb7hL0HQ2M
- What are STIX/TAXII? https://www.anomali.com/resources/what-are-stix-taxii
- How STIX, TAXII and CybOX Can Help With Standardizing Threat Information https://securityintelligence.com/how-stix-taxii-and-cybox-can-help-with-standardizing-threat-information

Traffic Light Protocol (TLP)

📺 How to protect secrets https://www.youtube.com/watch?v=h6IpyZ-YCPs

▨ Traffic Light Protocol (TLP) Definitions and Usage https://www.cisa.gov/news-events/news/traffic-light-protocol-tlp-definitions-and-usage

Logical Fallacies and Cognitive Biases



- Deconstructing the Analyst Mindset https://www.youtube.com/watch?v=Qy-19aRN58M
- 12 Cognitive Biases Explained https://www.youtube.com/watch?v=wEwGBIr_RIw
- 31 logical fallacies in 8 minutes https://www.youtube.com/watch?v=Qf03U04rqGQ
- The Most Common Cognitive Bias https://www.youtube.com/watch?v=vKA4w2O61Xo

Courses

🎓 Courses:

- ✔ Intro to Cyber Threat Intelligence
  https://www.cybrary.it/course/intro-cyber-threat-intelligence
- ✔ Cyber Threat Intelligence (IBM)
  https://www.coursera.org/learn/ibm-cyber-threat-intelligence
- ✔ Cyber Threat Intelligence
  https://tryhackme.com/module/cyber-threat-intelligence
- ✔ Using ATT&CK for Cyber Threat Intelligence Training
  https://attack.mitre.org/resources/training/cti/
- ✔ Cyber Threat Intelligence 101
  https://arcx.io/courses/cyber-threat-intelligence-101

Courses

🎓 Courses:

✔ MITRE ATT&CK Defender™ (MAD) ATT&CK® Fundamentals Badge Training
https://www.cybrary.it/course/mitre-attack-defender-mad-attack-fundamentals

✔ MITRE ATT&CK Defender™ (MAD) ATT&CK® Cyber Threat Intelligence Certification Training
https://www.cybrary.it/course/mitre-attack-defender-mad-attack-for-cyber-threat-intelligence

✔ MITRE ATT&CK Defender™ (MAD) ATT&CK® SOC Assessments Certification Training
https://www.cybrary.it/course/mitre-attack-defender-mad-attack-for-soc-assessments

✔ Intermediate MITRE ATT&CK
https://www.academy.attackiq.com/learning-path/intermediate-mitre-attck

Certifications

My list of Top Cyber Threat Intelligence Certifications

✔ GCTI: GIAC Cyber Threat Intelligence https://www.giac.org/certifications/cyber-threat-intelligence-gcti

✔ CPTIA, CRTIA, CCTIM by CREST
https://www.crest-approved.org/certification-careers/crest-certifications/crest-practitioner-threat-intelligence-analyst

https://www.crest-approved.org/certification-careers/crest-certifications/crest-registered-threat-intelligence-analyst

https://www.crest-approved.org/certification-careers/crest-certifications/crest-certified-threat-intelligence-manager

✔ MITRE's MAD https://mitre-engenuity.org/cybersecurity/mad

Certifications

✔ CCIP, CCTIA, and Cyber Intelligence Tradecraft Certification by CISA
https://niccs.cisa.gov/education-training/catalog/mcafee-institute/certified-cyber-intelligence-professional-ccip

https://niccs.cisa.gov/education-training/catalog/cybertraining-365/certified-cyber-threat-intelligence-analyst

https://niccs.cisa.gov/education-training/catalog/treadstone-71/cyber-intelligence-tradecraft-certified-cyber-intelligence

✔ CTIS-I and CTIS-II by Center for Threat Intelligence https://www.centerforti.com/certification

✔ CTIA: Certified Threat Intelligence Analyst by EC-Council https://www.eccouncil.org/train-certify/certified-threat-intelligence-analyst-ctia

Bonus

Lists of awesome Threat Intelligence resource

✔ Awesome Intelligence
https://github.com/ARPSyndicate/awesome-intelligence

✔ awesome-threat-intelligence
https://github.com/hslatman/awesome-threat-intelligence

Contact

Follow me and ParanoidLab if you want more content like this!

Eugene Levytskyi

linkedin.com/in/eugene-levytskyi

ParanoidLab

linkedin.com/company/paranoidlab

https://paranoidlab.com