Technical University of Denmark
Andreas Sfakianakis
References for the Guest Lectured titled "Welcome to the world of Cyber Threat Intelligence"

27/04/2021

Table of Contents

Highly recommended articles for an introduction to CTI

- A Cyber Threat Intelligence Self-Study Plan: Part 1
- FAQs on Getting Started in Cyber Threat Intelligence

Intro to CTI

1. Cuckoo's Egg - https://en.wikipedia.org/wiki/The_Cuckoo%27s_Egg_(book)
2. The KGB, the computer and me - https://www.youtube.com/watch?v=PGv5BqNL164
3. Intelligence driven incident response - https://www.amazon.com/Intelligence-Driven-Incident-Response-Outwitting-Adversary/dp/1491934948
4. SANS CTI Summit - https://www.sans.org/event/cyber-threat-intelligence-summit-2021
5. Intelligence cycle - https://en.wikipedia.org/wiki/Intelligence_cycle
6. Cybersecurity and the intelligence cycle - https://www.recordedfuture.com/cybersecurity-intelligence-cycle/
7. 3 Key Lessons that CTI Teams Should Learn from the Past - https://www.youtube.com/watch?v=kGqnCR6XOhQ
8. Intelligence collection priorities - https://medium.com/@sroberts/intelligence-collection-priorities-a80fa3ed73cd
9. The past, present and future of Threat Intelligence Platforms - https://www.youtube.com/watch?v=U7kuu7OFgYk

10. Exploring the opportunities and limitations of current Threat Intelligence Platforms - https://www.enisa.europa.eu/publications/exploring-the-opportunities-and-limitations-of-current-threat-intelligence-platforms
11. Kill chain - https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf
12. Diamond Model - https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf
13. MITRE's ATT&CK - https://attack.mitre.org/
14. Logical fallacies - https://yourlogicalfallacyis.com/
15. Psychology of intelligence analysis – https://www.cia.gov/static/9a5f1162fd0932c29bfed1c030edf4ae/Pyschology-of-Intelligence-Analysis.pdf
16. Structured Analytic Techniques for Intelligence Analysis - https://www.amazon.com/Structured-Analytic-Techniques-Intelligence-Analysis/dp/1608710181
17. Pyramid of pain - http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html
18. Words of Estimative Probability - https://www.cia.gov/static/0aae8f84700a256abf63f7aad73b0a7d/Words-of-Estimative-Probability.pdf
19. Traffic Light Protocol - https://www.first.org/tlp/

A view at the Threat Landscape

1. Ransomware - https://www.fireeye.com/current-threats/what-is-cyber-security/ransomware.html
2. Coveware ransomware marketplace report Q4 2020 - https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020
3. CrowdStrike 2021 Global Threat Report - https://www.crowdstrike.com/resources/reports/global-threat-report/
4. Ryuk Speed Run, 2 Hours to Ransom - https://thedfirreport.com/2020/11/05/ryuk-speed-run-2-hours-to-ransom/
5. Mitigating malware and ransomware attacks - https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks
6. Remembering when APT term became public - https://taosecurity.blogspot.nl/2018/01/remembering-when-apt-became-public.html
7. APT1 report - https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf
8. FireEye APT groups - https://www.fireeye.com/current-threats/apt-groups.html
9. CrowdStrike APT groups - https://adversary.crowdstrike.com/
10. Beyond Attribution: Seeking National Responsibility in Cyberspace - https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/beyond-attribution-seeking-national-responsibility-in-cyberspace/
11. The hacker and the state - https://www.amazon.com/Hacker-State-Attacks-Normal-Geopolitics/dp/0674987551

CTI Analyst Skillset

1. Cybersecurity domains mind map - https://www.linkedin.com/pulse/map-cybersecurity-domains-version-20-henry-jiang-ciso-cissp/
2. INSA Preparing cyber intelligence talent - https://www.insaonline.org/wp-content/uploads/2017/04/INSA_Cyber_Intel_PrepTalent.pdf
3. Maintaining External Situational Awareness
    a. Twitter - https://twitter.com/
        i. Twitter lists
            1. My precious Threat Intelligence - https://twitter.com/i/lists/106208332
            2. Cyber - https://twitter.com/i/lists/201875823
            3. Global CERTs - https://twitter.com/i/lists/222844774
    b. Reddit - https://www.reddit.com/
    c. Nuzzel - https://developers.nuzzel.com/
    d. RSS Aggregator
        i. Feedly – https://feedly.com/
        ii. Inoreader - https://www.inoreader.com/
    e. Podcasts
        i. CyberWire - https://thecyberwire.com/
    f. Newsletters
        i. CyberWire - https://thecyberwire.com/
        ii. TC Dragon News Bites - https://team-cymru.com/community-services/dnb/
        iii. SANS NewsBites - https://www.sans.org/newsletters/newsbites/
    g. Strategic sources
        i. The Economist – https://www.economist.com/
        ii. Council of Foreign Relations - https://www.cfr.org/
    h. Weekly summaries
        i. This Week in 4n6 - https://thisweekin4n6.com/
        ii. SANS @RISK - https://www.sans.org/newsletters/at-risk/