CYBRARY

Resources

Advanced Cyber Threat Intelligence

Created By: Alyssa Berriche, Instructor

Module 1: Introduction

• Threat Intelligence lifecycle
https://www.recordedfuture.com/threat-intelligence-lifecycle-phases/
https://www.recordedfuture.com/threat-intelligence-lifecycle/

• Building a Threat Intelligence Program, Anomali
https://www.anomali.com/files/white-papers/Securosis_ThreatIntelProgram.pdf

Module 2: Collection

• Threat Intelligence Feeds: Overview, Best Practices, and Examples
https://www.recordedfuture.com/threat-intelligence-feeds/

• What is an ISAC or ISAO? How do these cyber threat information sharing organizations improve security?
https://www.csoonline.com/article/3406505/what-is-an-isac-or-isao-how-these-cyber-threat-information-sharing-organizations-improve-security.html

• Assessment of the Information Sharing and Analysis Center Model
https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/812076-assessinfosharingmodel.pdf

• A curated list of Awesome Threat Intelligence resources
https://github.com/hslatman/awesome-threat-intelligence

• A curated list of amazingly awesome OSINT

https://github.com/jivoi/awesome-osint

• Threat Intelligence: Difference Between Platforms and Providers
https://www.recordedfuture.com/threat-intelligence-platform/

Module 3: Data management and Processing

• Standards and tools for exchange and processing of actionable information, Enisa
https://www.enisa.europa.eu/publications/standards-and-tools-for-exchange-and-processin-of-actionable-information

• Tools and Standards for Cyber Threat Intelligence Projects, SANS, Greg Farnham
https://www.sans.org/reading-room/whitepapers/warfare/tools-standards-cyber-threat-intelligence-projects-34375

• Threat Intelligence: the Importance of Human Analysis, Interpretation and Narrative, 2015, Ollie Whitehouse
https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2015/october/threat-intelligence-the-importance-of-human-analysis-interpretation-and-narrative/

Module 4: Analysis

• Assessing the Value of Structured Analytic Techniques in the U.S. Intelligence Community, by Stephen Artner, Richard S. Girven, James B. Bruce
https://www.analytic-education.com/resources-download/Artner_Assessment-of-SAT-effectiveness.pdf

• Applying Cyber Kill Chain® Methodology to Network Defense, Lockheed Martin
https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf

• The Diamond Model of Intrusion Analysis, Sergio Caltagirone
http://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf

• The Diamond Model For Intrusion Analysis: A Primer, 2014, by Andy Pendergast
https://digital-forensics.sans.org/summit-archives/cti_summit2014/The_Diamond_Model_for_Intrusion_Analysis_A_Primer_Andy_Pendergast.pdf

• Defensible Security Posture – Part 2
https://nigesecurityguy.wordpress.com/tag/cyber-kill-chain/

• Analysis of Competing Hypotheses, An Analytical Process by former CIA analyst Richards J Heuer, Jr.
https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1492185958.pdf

Module 5: Campaign Analysis

• Hands-on graph visualization: KeyLines & Neo4j
https://medium.com/neo4j/hands-on-graph-visualization-keylines-neo4j-9c5aeb7a8d3a

• Graph-Based Intelligence Analysis, Elise Devaux
https://linkurio.us/blog/graph-based-intelligence-analysis/

• Getting Started with ATT&CK: Threat Intelligence, Katie Nickels
https://medium.com/mitre-attack/getting-started-with-attack-cti-4eb205be4b2f

• Using ATT&CK to Advance Cyber Threat Intelligence — Part 1, Katie Nickels
https://medium.com/mitre-attack/using-att-ck-to-advance-cyber-threat-intelligence-part-1-c5ad14d59724

• Using ATT&CK to Advance Cyber Threat Intelligence — Part 2, Katie Nickels
https://medium.com/mitre-attack/using-att-ck-to-advance-cyber-threat-intelligence-part-2-6f21fdba80c

Module 6: Attribution

• APT Groups and Operations
https://docs.google.com/spreadsheets/d/1H9_xaxQHpWaa4O_Son4Gx0YOIzlcBWMsdvePFX68EKU/edit

• The Problems with Seeking and Avoiding True Attribution to Cyber Attacks, Rob M. Lee
https://www.robertmlee.org/the-problems-with-seeking-and-avoiding-true-attribution-to-cyber-attacks/

• Cognitive Bias Can Hamper Security Decisions, Kelly Sheridan
https://www.darkreading.com/threat-intelligence/cognitive-bias-can-help-shape-security-decisions/d/d-id/1334925

• 9 biases killing your security program
https://www.csoonline.com/article/3118746/9-biases-killing-your-security-program.html

• Logically Fallacious, Dr. Bo Bennett
https://www.logicallyfallacious.com/tools/lp/Bo/LogicalFallacies/3/Book-Contents

Module 7: Dissemination & Sharing

- How threat intelligence sharing can improve the security posture of whole industries
  https://www.csoonline.com/article/3387120/how-threat-intelligence-sharing-can-improve-the-security-posture-of-whole-industries.html

- What is Operational Threat Intelligence, Justin Swisher
  https://www.anomali.com/blog/what-is-operational-threat-intelligence

- How Tactical Threat Intelligence Helps Identify the Enemy
  https://www.recordedfuture.com/tactical-threat-intelligence/

- Security Intelligence at the Strategic, Operational and Tactical Levels, Bob Gourley
  https://securityintelligence.com/security-intelligence-at-the-strategic-operational-and-tactical-levels/

- What is Strategic Threat Intelligence, Steve Miller
  https://www.anomali.com/blog/what-is-strategic-threat-intelligence