REFERENCES

Agnaou, A., El Kalam, A. A., and Ouahman, A. A., "Towards a collaborative architecture of Honeypots," in "2017 IEEE/ACS 14th International Conference on Computer Systems and Applications (AICCSA)," pp. 1299–1305, IEEE, 2017.

Agnaou, A., Kalam, A. A. E., and Ouahman, A. A., "Towards a collaborative architecture of honeypots," *Proceedings of IEEE/ACS International Conference on Computer Systems and Applications, AICCSA*, volume 2017-Octob pp. 1299–1305, 2018.

Ali, P. D. and Kumar, T. G., "Malware capturing and detection in dionaea honeypot," in "2017 Innovations in Power and Advanced Computing Technologies (i-PACT)," pp. 1–5, IEEE, 2017.

Angles, R. and Gutierrez, C., "Survey of graph database models," *ACM Computing Surveys (CSUR)*, volume 40(1) pp. 1–39, 2008.

Bailey, M., Cooke, E., Jahanian, F., Provos, N., Rosaen, K., and Watson, D., "Data reduction for the scalable automated analysis of distributed darknet traffic," in "Proceedings of the 5th ACM SIGCOMM conference on Internet Measurement," pp. 21–21, USENIX Association, 2005.

Baldwin, J. and Dehghantanha, A., "Leveraging support vector machine for opcode density based detection of crypto-ransomware," in "Cyber Threat Intelligence," pp. 107–136, Springer, 2018.

Barnum, S., "Standardizing cyber threat intelligence information with the Structured Threat Information eXpression (STIX)," *Mitre Corporation*, volume 11 pp. 1–22, 2012.

Barnum, S., Martin, R., Worrell, B., and Kirillov, I., "The cybox language specification," *The MITRE Corporation*, 2012.

Blackstock, M. and Lea, R., "Fred: A hosted data flow platform for the iot," in "Proceedings of the 1st International Workshop on Mashups of Things and APIs," pp. 1–5, 2016.

Boag, S., Chamberlin, D., Fernández, M. F., Florescu, D., Robie, J., Siméon, J., and Stefanescu, M., "XQuery 1.0: An XML query language," , 2002.

Canto, J., Dacier, M., Kirda, E., and Leita, C., "Large scale malware collection: lessons learned," in "IEEE SRDS Workshop on Sharing Field Data and Experiment Measurements on Resilience of Distributed Computing Systems," Citeseer, 2008.

cyware, "What is the difference between Cyber Situational Awareness and Cyber Awareness?" , 2018, URL https://cyware.com/educational-guides/cyber-situational-awareness/whats-the-difference-between-cyber-situational-awareness-and-cyber-a

D'Amico, A., Whitley, K., Tesone, D., O'Brien, B., and Roth, E., "Achieving cyber defense situational awareness: A cognitive task analysis of information assurance analysts," in "Proceedings of the human factors and ergonomics society annual meeting," volume 49, pp. 229–233, SAGE Publications Sage CA: Los Angeles, CA, 2005.

Danyliw, R., Meijer, J., and Demchenko, Y., "The Incident Object Description Exchange Format," , 2007, URL https://www.ietf.org/rfc/rfc5070.txt.

Debar, H., Curry, D., and Feinstein, B., "The intrusion detection message exchange format (IDMEF)," *Request for Comments (RFC)*, volume 4765, 2007.

Endo, P. T. and Sadok, D. F. H., "Whois based geolocation: A strategy to geolocate internet hosts," in "2010 24th IEEE International Conference on Advanced Information Networking and Applications," pp. 408–413, IEEE, 2010.

Fachkha, C. and Debbabi, M., "Darknet as a source of cyber intelligence: Survey, taxonomy, and characterization," *IEEE Communications Surveys & Tutorials*, volume 18(2) pp. 1197–1227, 2015.

Herr, T., "PrEP: A framework for malware & cyber weapons," *Journal of Information Warfare*, volume 13(1) pp. 87–106, 2014.

Hraiech, O., "Honeypot Deployment," , 2020, URL https://www.peerlyst.com/posts/honeypot-deployment-updated-oussema-hraiech-1.

internetworldstats.com, "INTERNET USAGE STATISTICS The Internet Big Picture," , 2020, URL https://www.internetworldstats.com/stats.htm.

Jabczynski, M., "Work report-CIF and GooSBA projects," Technical report, 2014.

Jamalpur, S., Navya, Y. S., Raja, P., Tagore, G., and Rao, G. R. K., "Dynamic malware analysis using cuckoo sandbox," in "2018 Second international conference on inventive communication and computational technologies (ICICCT)," pp. 1056–1060, IEEE, 2018a.

Jamalpur, S., Navya, Y. S., Raja, P., Tagore, G., and Rao, G. R. K., "Dynamic Malware Analysis Using Cuckoo Sandbox," *Proceedings of the International Conference on Inventive Communication and Computational Technologies, ICICCT 2018*, volume 1(Icicct) pp. 1056–1060, 2018b.

Jang-Jaccard, J. and Nepal, S., "A survey of emerging threats in cybersecurity," *Journal of Computer and System Sciences*, volume 80(5) pp. 973–993, 2014.

Kim, E., Kim, K., Shin, D., Jin, B., and Kim, H., "CyTIME: Cyber Threat Intelligence ManagEment framework for automatically generating security rules," in "Proceedings of the 13th International Conference on Future Internet Technologies," pp. 1–5, 2018.

Kumar, S., Janet, B., and Eswari, R., "Multi Platform Honeypot for Generation of Cyber Threat Intelligence," *Proceedings of the 2019 IEEE 9th International Conference on Advanced Computing, IACC 2019*, pp. 25–29, 2019.

Kumar, S., Janet, B., and Eswari, R., "Automated Cyber Threat Intelligence Generation from Honeypot Data," in "Inventive Communication and Computational Technologies," pp. 591–598, Springer, 2020.

Kumar, S., Sehgal, R., Singh, P., and Chaudhary, A., "Nepenthes honeypots based botnet detection," *arXiv preprint arXiv:1303.3071*, 2013.

Lee, A., Varadharajan, V., and Tupakula, U., "On malware characterization and attack classification," in "Proceedings of the First Australasian Web Conference-Volume 144," pp. 43–47, 2013.

Lekić, M. and Gardašević, G., "IoT sensor integration to Node-RED platform," in "2018 17th International Symposium INFOTEH-JAHORINA (INFOTEH)," pp. 1–5, IEEE, 2018.

Liao, X., Yuan, K., Wang, X., Li, Z., Xing, L., and Beyah, R., "Acing the ioc game: Toward automatic discovery and analysis of open-source cyber threat intelligence," in "Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security," pp. 755–766, 2016.

Lim, C., Marcello, M., Japar, A., Tommy, J., and Kho, I. E., "Development of Distributed Honeypot Using Raspberry Pi," in "International Conference on Information, Communication Technology and System," , 2014.

Mavroeidis, V. and Bromander, S., "Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence," *Proceedings - 2017 European Intelligence and Security Informatics Conference, EISIC 2017*, volume 2017-Janua pp. 91–98, 2017.

Milajerdi, S. M., Eshete, B., Gjomemo, R., and Venkatakrishnan, V., "Poirot: Aligning attack behavior with kernel audit records for cyber threat hunting," in "Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security," pp. 1795–1812, 2019.

MITRE, "TAXII: An Overview," , 2013, URL http://taxii.mitre.org/about/documents/TAXII_Overview_briefing_July_2013.pdf.

Morrison, J. P., *Flow-based programming : a new approach to application development*, Van Nostrand Reinhold, 1994, URL http://gen.lib.rus.ec/book/index.php?md5=695ac19e3debab49e7ee0db11abbb79f.

Naveen, S. and Kumar, T. G., "Ransomware Analysis Using Reverse Engineering," in "International Conference on Advances in Computing and Data Sciences," pp. 185–194, Springer, 2019.

Nellums, K., "Alienvault launches open threat exchange, largest community-sourced information security threat feed," , 2012, URL https://cybersecurity.att.com/who-we-are/press-releases/.

Noel, S., "Interactive visualization and text mining for the capec cyber attack catalog," in "Proceedings of the ACM Intelligent User Interfaces Workshop on Visual Text Analytics," , 2015.

Oosterhof, M., "Cowrie," , 2010, URL https://github.com/cowrie/cowrie.

Project, T. H., "Kippo," , 2010, URL https://www.honeynet.org/projects/old/kippo/.

Purplesec, "Honeypot Deployment," , 2019, URL https://purplesec.us/resources/cyber-security-statistics/.

Roundy, K. A. and Miller, B. P., "Hybrid analysis and control of malware," in "International Workshop on Recent Advances in Intrusion Detection," pp. 317–338, Springer, 2010.

Rouse, M., "Verizon VERIS (Vocabulary for Event Recording and Incident Sharing) Framework," , 2014, URL https://searchsecurity.techtarget.com/.

Singh, Y. K., *Fundamental of research methodology and statistics*, New Age International, 2006.

Spitzner, L., "Honeypots: Catching the insider threat," pp. 170– 179, 2004.

Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., and Thomas, C. B., "Mitre att&ck: Design and philosophy," *Technical report*, 2018.

Tounsi, W. and Rais, H., "A survey on technical threat intelligence in the age of sophisticated cyber attacks," *Computers & security*, volume 72 pp. 212–233, 2018.

US-CERT, "Traffic Light Protocol (TLP) Definitions and Usage," , 2013, URL https://www.us-cert.gov/tlp.

Van Rossum, G. et al., "Python Programming Language." in "USENIX annual technical conference," volume 41, p. 36, 2007.

Wagner, C., Dulaunoy, A., Wagener, G., and Iklody, A., "Misp: The design and implementation of a collaborative threat intelligence sharing platform," in "Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security," pp. 49–56, 2016.

Will Gibb, D. K., "Threat Research OpenIOC: Back to the Basics," , 2013, URL https://www.fireeye.com/blog/threat-research/2013/10/openioc-basics.html.

Yadav, T. and Rao, A. M., "Technical aspects of cyber kill chain," in "International Symposium on Security in Computing and Communication," pp. 438–452, Springer, 2015.