IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 8, April 2023

Cyber Attack Surface Management System

Vindhya L, Mahima B Gowda , Gowramma Gaari Sindhu, Keerthan V
Department of Information Science and Engineering
SJC Institute of Technology, Chikkaballapura, Karnataka, India

Abstract: *Defenders struggle to keep up with the pace of digital transformation in the face of an expanding modern enterprise attack surface and more sophisticated adversaries. A conceptual framework for relating attack surface management (ASM) to vulnerability management and cyber threat intelligence (CTI) improves cyber defense. The framework explains how ASM improves cyber resiliency in proactively detecting and responding to weaknesses that adversaries could exploit to cause unacceptable harm. Defenders should prioritize ASM aligning with the business continuity and enterprise risk management functions. A CTI-driven ASM conceptual framework (CTI-ASM) helps defenders achieve decision clarity on how best to prioritize preventing the most impactful exploitations based on adversaries' capabilities, opportunities, and intent. Security researchers have applied decision analysis methodology to solve various security challenges generally. Applying decision analysis methodology to CTI-ASM may improve the quality of its implementation and support higher quality CTI. Potentially helpful decision analysis tools and concepts include relevance diagrams, possibility and probability trees, sensitivity analysis, corporate risk attitudes, weighing imperfect information, and accounting for cognitive biases.*

Keywords: Threat Intelligence, Attack Surface Management (ASM), OpenSource Intelligence(OSINT), Penetration Testing, Spiderfoot (Tool Used)

REEFERENCES

[1]. HussenMaulud, D., Zeebaree, S. R., Jacksi, K., Mohammed Sadeeq, M. A., & Hussein Sharif, K. (2021). State of art for semantic analysis of natural language processing. *Qubahan Academic Journal*, *1*(2), 21-28.

[2]. Dashtipour, K., Poria, S., Hussain, A., Cambria, E., Hawalah, A. Y., Gelbukh, A., & Zhou, Q. (2016). Multilingual sentiment analysis: State of the art and independent comparison of techniques. *Cognitive Computation*, *8*(4), 757–771.

[3]. Charalambous, E., Kavallieros, D., Brewster, B., Leventakis, G., &Koutras, N. (2016). Combatting Cybercrime and Sexual Exploitation of Children: An Open Source Toolkit. In *Open source intelligence investigation: From strategy to implementation* (pp. 233–249). essay, Springer.

[4]. Pastrana, S., Hutchings, A., Caines, A., & Buttery, P. (2018). International Symposium on Research in Attacks, Intrusions, and Defenses. In *Research in attacks, intrusions, and Defenses:21ST International Symposium, RAID 2018, Heraklion, CRETE, Greece, September 10-12, 2018, proceedings* (Vol. 11050, pp. 207–227). Cham, Switzerland; Springer.

[5]. Ponder-Sutton, A. M. (2016). The Automating of Open Source Intelligence. In *Automating open source intelligence: Algorithms FOR OSINT* (pp. 1–20). essay, Elsevier/Syngress.

[6]. Benes, L. (2013). OSINT, New Technologies, Education: Expanding Opportunities and Threats. A New Paradigm. *Journal of Strategic Security*, *6*(3), 22–37.

[7]. Layton, R., & Watters, P. A. (2016). The Automating of Open Source Intelligence. In *Automating open source intelligence algorithms FOR OSINT* (pp. 1–17). essay, Syngress.

[8]. Santarcangelo, V., Oddo, G., Pilato, M., Valenti, F., &Fornaro, C. (n.d.). Social Opinion Mining: An Approach for Italian Language. In *Future internet of things and Cloud (FICLOUD), 2015 3rd International conference on* (pp. 693–697). Rome, Italy.

[9]. Hassan, N. A., & Hijazi, R. (2018). The evolution of open SourCeintelligenCe. In *Open source intelligence methods and tools a practical guide to online intelligence* (pp. 11–11). essay, APRESS.

DOI: 10.48175/IJARSCT-9533

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 8, April 2023

[10]. Azevedo, R., Medeiros, I., &Bessani, A. (2019). PURE: Generating Quality Threat Intelligence by Clustering and Correlating OSINT. In *2019 18th IEEE International Conference on Trust, Security and Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)* (pp. 483–490).

[11]. Bruwer, R. (H., & Rudman, R. (2015). Web 3.0: Governance, risks and safeguards. *Journal of Applied Business Research (JABR)*, *31*(3), 1037.

[12]. Glassman, M., & Kang, M. J. (2012). Intelligence in the internet age: The emergence and evolution of open source Intelligence (OSINT). *Computers in Human Behavior*, *28*(2), 673–682.

[13]. Klaus, S., Franziska, S., & Reiner, C. (2020). Conception and implementation of professional laboratory exercises in the field of open source intelligence (OSINT). *Society for Imaging Science and Technology*, *2020*(3), 1-99.

[14]. John, D. S. M., Goodchild, M. F., & Longley, P. (2007). In *Geospatial analysis: A guide to principles, techniques and software tools* (pp. 39–39). essay, Matador.

[15]. Nouh, M., Nurse, J. R. C., Webb, H., & Goldsmith, M. (2019). Cybercrime investigators are users too! understanding the socio-technical challenges faced by law enforcement. *Proceedings 2019 Workshop on Usable Security*, 1-11.

[16]. Koops, B.-J., Hoepman, J.-H., &Leenes, R. (2013). Open-source intelligence and privacy by design. *Computer Law & Security Review*, *29*(6), 676–688.

[17]. Layton, R., & Watters, P. A. (2016). The limitations of automating OSINT: understanding the question, not the answer. In *Automating open source intelligence algorithms FOR OSINT* (pp. 159–169). essay, Syngress.

[18]. Bar-Ilan, J. (2001). Data collection methods on the Web for infometric purposes — A review and analysis. *Scientometrics*, *50*(1), 7–32.

[19]. Gibson, H., Ramwell, S. S., & Day, T. (2016). Analysis, Interpretation and Validation of Open Source Data. In *Open source intelligence investigation from strategy to implementation* (pp. 95– 110). essay, Springer-Verlag.

[20]. Gibson, S. D. (2014). Exploring the Role and Value of Open Source Intelligence. In *Open source intelligence in the twenty-first century: New approaches and* (pp. 9–23). essay, Palgrave Macmillan.