**REFERENCES**

[1] S. Samtani, M. Abate, V. Benjamin, and W. Li, Cybersecurity as an Industry:

A Cyber Threat Intelligence Perspective, pp. 1–20. Cham: Springer

International Publishing, 2019.

[2] R. McMillan, “Definition: threat intelligence.” https://www.gartner.

com/doc/2487216/definition-threat-intelligence, 2013. Retrieved January,

2019.

[3] D. Bianco, “The Pyramid of Pain.” http://detectrespond.

blogspot.com/2013/03/the-pyramid-of-pain.html, 2013.

[4] A. Modi, Z. Sun, A. Panwar, T. Khairnar, Z. Zhao, A. Doupé, G.-J.

Ahn, and P. Black, “Towards automated threat intelligence fusion,” in

IEEE 2nd International Conference on Collaboration and Internet Computing

(CIC), pp. 408–416, IEEE, 2016.

[5] A. Boukhtouta, D. Mouheb, M. Debbabi, O. Alfandi, F. Iqbal, and

M. El Barachi, “Graph-theoretic characterization of cyber-threat infrastructures,”

Digital Investigation, vol. 14, pp. S3–S15, 2015.

[6] C. Sillaber, C. Sauerwein, A. Mussmann, and R. Breu, “Data quality

challenges and future research directions in threat intelligence sharing

practice,” in Workshop on Information Sharing and Collaborative Security,

pp. 65–70, ACM, 2016.

[7] S. Lee, H. Cho, N. Kim, B. Kim, and J. Park, “Managing cyber threat

intelligence in a graph database: Methods of analyzing intrusion sets,

threat actors, and campaigns,” in International Conference on Platform

Technology and Service (PlatCon), pp. 1–6, IEEE, 2018.

[8] X. Liao, K. Yuan, X. Wang, Z. Li, L. Xing, and R. Beyah, “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, ACM, 2016.

[9] G. Husari, E. Al-Shaer, M. Ahmed, B. Chu, and X. Niu, “TTPDrill: Automatic

and Accurate Extraction of Threat Actions from Unstructured

Text of CTI Sources,” in Proceedings of the 33rd Annual Computer Security

Applications Conference, pp. 103–115, ACM, 2017.

[10] F. Böhm, F. Menges, and G. Pernul, “Graph-based visual analytics for

cyber threat intelligence,” Cybersecurity, vol. 1, no. 1, p. 16, 2018.

[11] U. Noor, Z. Anwar, A. W. Malik, S. Khan, and S. Saleem, “A machine

learning framework for investigating data breaches based on semantic

analysis of adversary’s attack patterns in threat intelligence repositories,”

Future Generation Computer Systems, 2019.

[12] C. Shi, Y. Li, J. Zhang, Y. Sun, and S. Y. Philip, “A survey of heterogeneous

information network analysis,” IEEE Transactions on Knowledge

and Data Engineering, vol. 29, no. 1, pp. 17–37, 2017.

[13] P. K. Manadhata, S. Yadav, P. Rao, and W. Horne, “Detecting malicious

domains via graph inference,” in European Symposium on Research in

Computer Security, pp. 1–18, Springer, 2014.

[14] X. Kong, B. Cao, and P. S. Yu, “Multi-label classification by mining label

and instance correlations from heterogeneous information networks,”

in Proceedings of the 19th ACM SIGKDD international conference on

Knowledge discovery and data mining, pp. 614–622, ACM, 2013.

[15] M. Ji, J. Han, and M. Danilevsky, “Ranking-based classification of

heterogeneous information networks,” in Proceedings of the 17th ACM

SIGKDD international conference on Knowledge discovery and data mining,

pp. 1298–1306, ACM, 2011.

[16] W. Tounsi and H. Rais, “A survey on technical threat intelligence in the

age of sophisticated cyber attacks,” Computers & Security, 2017.

[17] S. Barnum, “Standardizing cyber threat intelligence information with

the structured threat information eXpression (STIXTM),” MITRE Corporation,

vol. 11, pp. 1–22, 2012.

[18] R. Danyliw, J. Meijer, and Y. Demchenko, “The incident object description

exchange format,” tech. rep., 2007.

[19] Mandiant, “Sophisticated indicators for the modern threat landscape:

An introduction to OpenIOC.” Technical report, Mandiant Whitepaper,

2013.

[20] T. Yadav and A. M. Rao, “Technical aspects of cyber kill chain,” in

International Symposium on Security in Computing and Communication,

pp. 438–452, Springer, 2015.

[21] H. Gascon, B. Grobauer, T. Schreck, L. Rist, D. Arp, and K. Rieck,

“Mining attributed graphs for threat intelligence,” in Proceedings of the

Seventh ACM on Conference on Data and Application Security and Privacy,

pp. 15–22, ACM, 2017.

[22] B. Hooi, H. A. Song, A. Beutel, N. Shah, K. Shin, and C. Faloutsos,

“Fraudar: Bounding graph fraud in the face of camouflage,” in Proceedings

of the 22nd ACM SIGKDD International Conference on Knowledge

Discovery and Data Mining, pp. 895–904, ACM, 2016.

[23] Y. Shi, G. Chen, and J. Li, “Malicious domain name detection based

on extreme machine learning,” Neural Processing Letters, vol. 48, no. 3,

pp. 1347–1357, 2018.

[24] M. Iannacone, S. Bohn, G. Nakamura, J. Gerth, K. Huffer, R. Bridges,

E. Ferragut, and J. Goodall, “Developing an ontology for cyber security

knowledge graphs,” in Proceedings of the 10th Annual Cyber and Information

Security Research Conference, pp. 1–4, 2015.

[25] S. Noel, E. Harley, K. Tam, M. Limiero, and M. Share, “CyGraph: graphbased

analytics and visualization for cybersecurity,” in Handbook of

Statistics, vol. 35, pp. 117–167, Elsevier, 2016.