## REFERENCES

Accenture. (2018). *AT-A-GLANCE Unlocking the value of improved cybersecurity protection THE EXPANDING THREAT LANDSCAPE AND NEW BUSINESS INNOVATION*. 2018–2019.

Almohannadi, H., Awan, I., Al Hamar, J., Cullen, A., Disso, J. P., & Armitage, L. (2018). Cyber threat intelligence from honeypot data using elasticsearch. *Proceedings - International Conference on Advanced Information Networking and Applications, AINA*, *2018-May*, 900–906. https://doi.org/10.1109/AINA.2018.00132

Ambre, A., & Shekokar, N. (2015). Insider threat detection using log analysis and event correlation. *Procedia Computer Science*, *45*(C), 436–445. https://doi.org/10.1016/j.procs.2015.03.175

Bahrami, P. N., Dehghantanha, A., Dargahi, T., Parizi, R. M., Choo, K. K. R., & Javadi, H. H. S. (2019). Cyber kill chain-based taxonomy of advanced persistent threat actors: Analogy of tactics, techniques, and procedures. *Journal of Information Processing Systems*, *15*(4), 865–889. https://doi.org/10.3745/JIPS.03.0126

Bhardwaj, A., & Goundar, S. (2019). A framework for effective threat hunting. *Network Security*, *2019*(6), 15–19. https://doi.org/10.1016/S1353-4858(19)30074-1

Caltagirone, S., Pendergast, A., & Betz, C. (2013). The Diamond Model of Intrusion Analysis. *Threat Connect*, *298*(0704), 1–61. Retrieved from http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA586960%5Cnhttps://www.threatconnect.com/wp-content/uploads/ThreatConnect-The-Diamond-Model-of-Intrusion-Analysis.pdf

Debnath, B., Solaimani, M., Gulzar, M. A. G., Arora, N., Lumezanu, C., Xu, J., … Khan, L. (2018). LogLens: A real-time log analysis system. *Proceedings - International Conference on Distributed Computing Systems*, *2018-July*, 1052–1062. https://doi.org/10.1109/ICDCS.2018.00105

Ertaul, L., & Mousa, M. (2018). Applying the Kill Chain and Diamond Models to

Microsoft Advanced Threat Analytics. *252 Int'l Conf. Security and Management SAM18*, 252–258.

Fernandes, G., Joel, J., Lemes, M., Jr, P., Fernando, L., & Jalal, C. (2018). A comprehensive survey on network anomaly detection. *Telecommunication Systems*. https://doi.org/10.1007/s11235-018-0475-8

Fiessler, A., Lorenz, C., Hager, S., Scheuermann, B., & Moore, A. W. (2017). HyPaFilter: Enhanced Hybrid Packet Filtering Using Hardware Assisted Classification and Header Space Analysis. *IEEE/ACM Transactions on Networking*, *25*(6), 3655–3669. https://doi.org/10.1109/TNET.2017.2749699

Fuchs, M., & Lemon, J. (2020). *A SANS Survey SANS 2020 Threat Hunting Survey Results*. (December).

Gao, P., Shao, F., Liu, X., Xiao, X., Qin, Z., Xu, F., … Song, D. (2020). *Enabling Efficient Cyber Threat Hunting With Cyber Threat Intelligence*. Retrieved from http://arxiv.org/abs/2010.13637

Hajisalem, V., & Babaie, S. (2018). A hybrid intrusion detection system based on ABC-AFS algorithm for misuse and anomaly detection. *Computer Networks*, *136*, 37–50. https://doi.org/10.1016/j.comnet.2018.02.028

He, P., Zhu, J., He, S., Li, J., & Lyu, M. R. (2016). An evaluation study on log parsing and its use in log mining. *Proceedings - 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2016*, 654–661. https://doi.org/10.1109/DSN.2016.66

Javeed, D., Khan, M. T., Ahmad, I., Iqbal, T., Badamasi, U. M., Ndubuisi, C. O., & Umar, A. (2020). An Efficient Approach of Threat Hunting Using Memory Forensics. *International Journal of Computer Networks and Communications Security*, *8*(5), 37–45. https://doi.org/10.47277/ijcncs/8(5)1

Jeon, K. S., Park, S. J., Chun, S. H., & Kim, J. B. (2016). A study on the big data log analysis for security. *International Journal of Security and Its Applications*, *10*(1), 13–20. https://doi.org/10.14257/ijsia.2016.10.1.02

Ju, A., Guo, Y., Ye, Z., Li, T., & Ma, J. (2019). HeteMSD: A Big Data Analytics Framework for Targeted Cyber-Attacks Detection Using Heterogeneous Multisource Data. *Security and Communication Networks*, *2019*. https://doi.org/10.1155/2019/5483918

Khan, M. A., Karim, M. R., & Kim, Y. (2019). A scalable and hybrid intrusion

detection system based on the convolutional-LSTM network. *Symmetry*, *11*(4). https://doi.org/10.3390/sym11040583

Kreps, J. (2015). *I ♥ Logs*. O'Reilly Media, Inc.

Le, T. (2015). A recommended framework for anomaly intrusion detection system (IDS). *Lecture Notes in Informatics (LNI), Proceedings - Series of the Gesellschaft Fur Informatik (GI)*, *246*, 1829–1840.

Liao, H. J., Richard Lin, C. H., Lin, Y. C., & Tung, K. Y. (2013). Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications*, *36*(1), 16–24. https://doi.org/10.1016/j.jnca.2012.09.004

Mansfield-Devine, S. (2017). Threat hunting: assuming the worst to strengthen resilience. *Network Security*, *2017*(5), 13–17. https://doi.org/10.1016/S1353-4858(17)30050-8

Martínez-Álvarez, R. P., Giraldo-Rodríguez, C., & Chaves-Diéguez, D. (2018). Large scale anomaly detection in data center logs and metrics. *ACM International Conference Proceeding Series*, 1–4. https://doi.org/10.1145/3241403.3241442

Rahayu, S. S., & Robiah, Y. (2018). *An Enhancement of Cyber Threat Intelligence Framework Comparative Study of Cyber Threat Intelligence Framework Framework An Enhancement of Cyber Threat Intelligence*. (November).

Rastogi, R., Akash, S., Shobha, G., Poonam, G., Pratiba, D., & Singh, A. (2017). Design and development of generic web based framework for log analysis. *IEEE Region 10 Annual International Conference, Proceedings/TENCON*, 232–236. https://doi.org/10.1109/TENCON.2016.7847996

Sakr, S., Maamar, Z., Awad, A., Benatallah, B., & Van Der Aalst, W. M. P. (2018). Business process analytics and big data systems: A roadmap to bridge the gap. *IEEE Access*, *6*, 77308–77320. https://doi.org/10.1109/ACCESS.2018.2881759

Services, E. E. (2015). *Data Sciene and Big Data Analytics*. Retrieved from http://library1.nida.ac.th/termpaper6/sd/2554/19755.pdf

Shah, N., Willick, D., & Mago, V. (2018). A framework for social media data analytics using Elasticsearch and Kibana. *Wireless Networks*, (December). https://doi.org/10.1007/s11276-018-01896-2

Shamimul Islam, Haidar Ali, Ahsan Habib, Nur Nobi, Mahbub Alam, D. H. (2018). Threat minimization by design and deployment of secured networking model. *Journal of Electronics and Information Engineering*, *8*(2), 96–106. Retrieved

from http://ijeie.jalaxy.com.tw/contents/ijeie-v8-n2/ijeie-v8-n2.pdf

Shin, H. (2016). *13.2018_네트워크 보안 관제를 위한 로그 시각화 방법-A log Visualization method for network security monitoring*.

Skopik, F., Settanni, G., & Fiedler, R. (2016). A problem shared is a problem halved: A survey on the dimensions of collective cyber defense through security information sharing. *Computers and Security*, *60*, 154–176. https://doi.org/10.1016/j.cose.2016.04.003

Strom, B. E., Battaglia, J. A., Kemmerer, M. S., Kupersanin, W., Miller, D. P., Wampler, C., … Wolf, R. D. (2017). *Finding cyber threats with ATT&CK-based analytics*. (June), 1–47. Retrieved from https://www.mitre.org/sites/default/files/publications/16-3713-finding-cyber-threats with att%26ck-based-analytics.pdf

Subba, B., Biswas, S., & Karmakar, S. (2017). Enhancing performance of anomaly based intrusion detection systems through dimensionality reduction using principal component analysis. *2016 IEEE International Conference on Advanced Networks and Telecommunications Systems, ANTS 2016*. https://doi.org/10.1109/ANTS.2016.7947776

Terzi, D. S., Terzi, R., & Sagiroglu, S. (2017). Big data analytics for network anomaly detection from netflow data. *2017 International Conference on Computer Science and Engineering (UBMK)*, *9*(5), 592–597. https://doi.org/10.1109/UBMK.2017.8093473

Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers and Security*, *72*, 212–233. https://doi.org/10.1016/j.cose.2017.09.001

Yen, T. F., Oprea, A., Onarlioglu, K., Leetham, T., Robertson, W., Juels, A., & Kirda, E. (2013). Beehive: Large-scale log analysis for detecting suspicious activity in enterprise networks. *ACM International Conference Proceeding Series*, 199–208. https://doi.org/10.1145/2523649.2523670

Yoo, S., Jo, J., Kim, B., & Seo, J. (2020). Hyperion: A Visual Analytics Tool for an Intrusion Detection and Prevention System. *IEEE Access*, *8*, 133865–133881. https://doi.org/10.1109/ACCESS.2020.3010789

Zhang, L., & Huang, M. (2016). A firewall rules optimized model based on service-grouping. *Proceedings - 2015 12th Web Information System and Application*

*Conference, WISA 2015*, 142–146. https://doi.org/10.1109/WISA.2015.47

Zhu, J., He, S., Liu, J., He, P., Xie, Q., Zheng, Z., & Lyu, M. R. (2019). Tools and Benchmarks for Automated Log Parsing. *Proceedings - 2019 IEEE/ACM 41st International Conference on Software Engineering: Software Engineering in Practice, ICSE-SEIP 2019*, 121–130. https://doi.org/10.1109/ICSE-SEIP.2019.00021