REFERENCES

[1] Chandola, V., Banerjee, A. and Kumar, V. (2009) 'Anomaly detection: A survey', ACM Computing Surveys, 41(3), pp. 1–58. Available at: https://doi.org/10.1145/1541880.1541882.

[2] Sharif, A. (2022). *What is Log Analysis? | CrowdStrike*. [online] crowdstrike.com. Available at: https://www.crowdstrike.com/cybersecurity-101/observability/log-analysis/.

[3] Joseph M. Carew (2020) How to choose between a rules-based vs. machine learning system | TechTarget, Enterprise AI. Available at: https://www.techtarget.com/searchenterpriseai/feature/How-to-choose-between-a-rules-based-vs-machine-learning-system (Accessed: 1 April 2023).

[4] Fürnkranz, J. (2013) 'Rule-based Methods', in W. Dubitzky et al. (eds) Encyclopedia of Systems Biology. New York, NY: Springer New York, pp. 1883–1888. Available at: https://doi.org/10.1007/978-1-4419-9863-7_610.

[5] Hansen, S. and Atkins, E.T. (1993) 'Automated System Monitoring and Notification with Swatch', in. LiSA. Available at: https://www.semanticscholar.org/paper/Automated-System-Monitoring-and-Notification-with-Hansen-Atkins/5ba262cc2173e4201df2406cde8c9e1078db7841 (Accessed: 1 April 2023).

[6] Hung, E. (2020) Machine Learning in Cyber Security— Windows User Anomaly Detection, Medium. Available at: https://medium.com/analytics-vidhya/cyber-security-in-machine-learning-Windows-user-anomaly-detection-e0d3457dea32 (Accessed: 1 April 2023).

[7] Legg, P.A. et al. (2017) 'Automated Insider Threat Detection System Using User and Role-Based Profile Assessment', IEEE Systems Journal, 11(2), pp. 503–512. Available at: https://doi.org/10.1109/JSYST.2015.2438442.

[8] Meng, W. et al. (2019) 'LogAnomaly: Unsupervised Detection of Sequential and Quantitative Anomalies in Unstructured Logs', in Proceedings of the Twenty-Eighth International Joint Conference on Artificial Intelligence. Twenty-Eighth International Joint Conference on Artificial Intelligence {IJCAI-19}, Macao, China: International Joint Conferences on Artificial Intelligence Organization, pp. 4739–4745. Available at: https://doi.org/10.24963/ijcai.2019/658.

[9] Farzad, A. and Gulliver, T.A. (2020) 'Unsupervised log message anomaly detection', ICT Express, 6(3), pp. 229–237. Available at: https://doi.org/10.1016/j.icte.2020.06.003.

[10] Dai, D. et al. (2020) 'Using machine learning and feature engineering to characterize limited material Datasets of high-entropy alloys', Computational Materials Science, 175, p. 109618. Available at: https://doi.org/10.1016/j.commatsci.2020.109618.

[11] Doreswamy, Hooshmand, M.K. and Gad, I. (2020) 'Feature selection approach using ensemble learning for network anomaly detection', CAAI Transactions on Intelligence Technology, 5(4), pp. 283–293. Available at: https://doi.org/10.1049/trit.2020.0073.

[12] Computer Forensic Investigator: 2023 Career Guide (2022) Coursera. Available at: https://www.coursera.org/articles/computer-forensic-investigator (Accessed: 1 April 2023).

[13] SearchWindowsServer. (n.d.). *What is Windows event log? - Definition from WhatIs.com*. [online] Available at: https://www.techtarget.com/searchwindowsserver/definition/Windows-event-log.

[14] Bradley, S. (2020) The most important Windows 10 security event log IDs to monitor, CSO Online. Available at: https://www.csoonline.com/article/3561889/the-most-important-Windows-10-security-event-log-ids-to-monitor.html (Accessed: 1 April 2023).

[15] Dutta, A. (2021) *System Failure Prediction using log analysis*, *Medium*. Available at: https://towardsdatascience.com/system-failure-prediction-using-log-analysis-8eab84d56d1 (Accessed: 1 April 2023).

[16] *How to Analyze Logs Using Artificial Intelligence* (2020) *LogicMonitor*. Available at: https://www.logicmonitor.com/blog/how-to-analyze-logs-using-artificial-intelligence (Accessed: 1 April 2023).

[17] Ryciak, P., Wasielewska, K. and Janicki, A. (2022) 'Anomaly Detection in Log Files Using Selected Natural Language Processing Methods', Applied Sciences, 12(10), p. 5089. Available at: https://doi.org/10.3390/app12105089.

[18] Bertero, C. et al. (2017) 'Experience Report: Log Mining Using Natural Language Processing and Application to Anomaly Detection', in 2017 IEEE 28th International Symposium on Software Reliability Engineering (ISSRE). 2017 IEEE 28th International Symposium on Software Reliability Engineering (ISSRE), Toulouse: IEEE, pp. 351–360. Available at: https://doi.org/10.1109/ISSRE.2017.43.

[19] Du, M. et al. (2017) 'DeepLog: Anomaly Detection and Diagnosis from System Logs through Deep Learning', in Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. CCS '17: 2017 ACM SIGSAC Conference on Computer and Communications Security, Dallas Texas USA: ACM, pp. 1285–1298. Available at: https://doi.org/10.1145/3133956.3134015.

[20] Pande, A. and Ahuja, V. (2017) 'WEAC: Word embeddings for anomaly classification from event logs', in 2017 IEEE International Conference on Big Data (Big Data). 2017 IEEE International Conference on Big Data (Big Data), Boston, MA: IEEE, pp. 1095–1100. Available at: https://doi.org/10.1109/BigData.2017.8258034.

[21] Customers clustering: K-Means, DBSCAN and AP (2022). Available at: https://kaggle.com/code/datark1/customers-clustering-k-means-dbscan-and-ap (Accessed: 1 April 2023).

[22] Sohn, K. et al (2021) *Discovering Anomalous Data with Self-Supervised Learning*. Available at: https://ai.googleblog.com/2021/09/discovering-anomalous-data-with-self.html (Accessed: 1 April 2023).

[23] Apap, F. et al. (2002) 'Detecting Malicious Software by Monitoring Anomalous Windows Registry Accesses', in A. Wespi, G. Vigna, and L. Deri (eds) Recent Advances in Intrusion Detection. Berlin, Heidelberg: Springer Berlin Heidelberg (Lecture Notes in Computer Science), pp. 36–53. Available at: https://doi.org/10.1007/3-540-36084-0_3.

[24] Stolfo, S.J., Apap, F., Eskin, E., Heller, K., Hershkop, S., Honig, A. and Svore, K. (2005). A comparative evaluation of two algorithms for Windows Registry Anomaly Detection. *Journal of Computer Security*, 13(4), pp.659–693. doi: https://doi.org/10.3233/jcs-2005-13403.

[25] Host-Based Anomaly Detection Using Wrapping File Systems (2004). Available at: https://apps.dtic.mil/sti/citations/ADA451576 (Accessed: 1 April 2023).

[26] Anaconda | Anaconda Training: A Learning Path for Data Scientists (no date) Anaconda. Available at: https://www.anaconda.com/blog/anaconda-training-a-learning-path-for-data-scientists (Accessed: 1 April 2023).

[27] Root, D. (2020) An Overview of The Anaconda Distribution, Medium. Available at: https://towardsdatascience.com/an-overview-of-the-anaconda-distribution-9479ff1859e6 (Accessed: 1 April 2023).

[28] Hoffman, C. (2016). *What Is the Windows Event Viewer, and How Can I Use It?* [online] How-To Geek. Available at: https://www.howtogeek.com/123646/htg-explains-what-the-windows-event-viewer-is-and-how-you-can-use-it/.

[29] vinaypamnani-msft (2023) *View the security event log (Windows 10)*. Available at: https://learn.microsoft.com/en-us/Windows/security/threat-protection/auditing/view-the-security-event-log (Accessed: 1 April 2023).

[30] Lancaster, L. (n.d.). *Log Anomaly Detection Using Machine Learning | Zebrium*. [online] www.zebrium.com. Available at: https://www.zebrium.com/blog/using-machine-learning-to-detect-anomalies-in-logs.

[31] Lutkevich, B. (2021). *What is Natural Language Processing? An Introduction to NLP*. [online] TechTarget. Available at: https://www.techtarget.com/searchenterpriseai/definition/natural-language-processing-NLP.

[32] Juluru, K. *et al.* (2021) 'Bag-of-Words Technique in Natural Language Processing: A Primer for Radiologists', *RadioGraphics*, 41(5), pp. 1420–1426. Available at: https://doi.org/10.1148/rg.2021210025.

[33] Alkhalifa, S. (2020). *Fraud and Anomaly Detection with Artificial Neural Networks using Python3 and Tensorflow. | by Saleh Alkhalifa | Towards Data Science*. Available at: https://towardsdatascience.com/fraud-and-anomaly-detection-with-artificial-neural-networks-using-python3-and-tensorflow-44b73d8b1240 (Accessed: 1 April 2023).

[34] Nieto Juscafresa, A. (2022). An introduction to explainable artificial intelligence with LIME and SHAP. Treballs Finals de Grau (TFG) - Matemàtiques. [online] Available at: https://diposit.ub.edu/dspace/handle/2445/192075.

[35] Wang, Q. *et al.* (2021) 'Log Sequence Anomaly Detection Method Based on Contrastive Adversarial Training and Dual Feature Extraction', *Entropy*, 24(1), p. 69. Available at: https://doi.org/10.3390/e24010069.