Daftar Pustaka

[1] redhat.com. "What is a Linux server?" Available at: https://www.redhat.com/en/topics/linux/linux-server [Accessed 31-01-2024].

[2] Abouabdalla O., El-Taj H., Ahmed M., & Sureswaran R.. 2009. "False positive reduction in intrusion detection system: A survey." In 2009 2nd IEEE International Conference on Broadband Network & Multimedia Technology. doi:10.1109/ICBNMT.2009.5348536.

[3] Al'aziz B.A.A., Sukarno P., & Wardana A.A.. 2020. "Blacklisted IP Distribution System to handle DDoS attacks on IPS Snort based on Blockchain." In 2020 6th Information Technology International Seminar (ITIS). doi:10.1109/ITIS50118.2020.9320996.

[4] Azodi A., Jaeger D., Cheng F., & Meinel C.. 2013. "A New Approach to Building a Multi-tier Direct Access Knowledgebase for IDS/SIEM Systems." In 2013 IEEE 11th International Conference on Dependable, Autonomic and Secure Computing. doi:10.1109/DASC.2013.48.

[5] Bartwal U., Mukhopadhyay S., Negi R., & Shukla S.. 2022. "Security Orchestration, Automation, and Response Engine for Deployment of Behavioural Honeypots." In 2022 IEEE Conference on Dependable and Secure Computing (DSC). doi:10.1109/DSC54232.2022.9888808.

[6] Chen Z., Chen Z., & Delis A.. 2007. "An Inline Detection and Prevention Framework for Distributed Denial of Service Attacks." The Computer Journal 50 (1): 7-40. doi:10.1093/comjnl/bxl042.

[7] Gibadullin R.F. & Nikonorov V.V.. 2021. "Development of the System for Automated Incident Management Based on Open-Source Software." In 2021 International Russian Automation Conference (RusAutoCon). doi:10.1109/RusAutoCon52004.2021.9537385.

[8] Hock F. & Kortiš P.. 2015. "Commercial and open-source based Intrusion Detection System and Intrusion Prevention System (IDS/IPS) design for an IP networks." In 2015 13th International Conference on Emerging eLearning Technologies and Applications (ICETA). doi:10.1109/ICETA.2015.7558466.

[9] Hristov M., Nenova M., Iliev G., & Avresky D.. 2021. "Integration of Splunk Enterprise SIEM for DDoS Attack Detection in IoT." In 2021 IEEE 20th International Symposium on Network Computing and Applications (NCA). doi:10.1109/NCA53618.2021.9685977.

[10] Laue T., Kleiner C., Detken K., & Klecker T.. 2021. "A SIEM Architecture for Multidimensional Anomaly Detection." In 2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS). doi:10.1109/IDAACS53288.2021.9660903.

[11] Majeed A., Rasool R., Ahmad F., Alam M., & Javaid N.. 2019. "Near-miss situation based visual analysis of SIEM rules for real time network security monitoring." Journal of Ambient Intelligence and Humanized Computing 10. doi:10.1007/s12652-018-0936-7.

[12] Muhammad A.R., Sukarno P., & Wardana A.A.. 2023. "Integrated Security Information and Event Management (SIEM) with Intrusion Detection System (IDS) for Live Analysis based on Machine Learning." Procedia Comput. Sci. 217: 1406–1415. doi:10.1016/j.procs.2022.12.339.

[13] Saad S., Traore I., & Brocardo M.L.. 2014. "Context-aware intrusion alerts verification approach." In 2014 10th International Conference on Information Assurance and Security. doi:10.1109/ISIAS.2014.7064620.

[14] Sridharan A. & Kanchana V.. 2022. "SIEM integration with SOAR." In 2022 International Conference on Futuristic Technologies (INCOFT). doi:10.1109/INCOFT55651.2022.10094537.

[15] Vasilyev V. & Shamsutdinov R.. 2020. "Security Analysis of Wireless Sensor Networks Using SIEM and Multi-agent Approach." In 2020 Global Smart Industry Conference (GloSIC). doi:10.1109/GloSIC50886.2020.9267830.

[16] Vast R., Sawant S., Thorbole A., & Badgujar V.. 2021. "Artificial Intelligence based Security Orchestration, Automation and Response System." In 2021 6th International Conference for Convergence in Technology (I2CT). doi:10.1109/I2CT51068.2021.9418109.

[17] Wazuh. "Network IDS integration - Proof of Concept guide · Wazuh documentation." Available at: https://documentation.wazuh.com/current/proof-of-concept-guide/integrate-network-ids-suricata.html [Accessed 31-01-2024].

[18] Yuan X., Li C., & Li X.. 2017. "DeepDefense: Identifying DDoS Attack via Deep Learning." In 2017 IEEE International Conference on Smart Computing (SMARTCOMP). doi:10.1109/SMARTCOMP.2017.7946998.

[19] Zhang B., Zhang T., & Yu Z.. 2017. "DDoS detection and prevention based on artificial intelligence techniques." In 2017 3rd IEEE International Conference on Computer and Communications (ICCC). doi:10.1109/CompComm.2017.8322748.

[20] Çakmakçı S.D., Hutschenreuter H., Maeder C., & Kemmerich T.. 2021. "A Framework For Intelligent DDoS Attack Detection and Response using SIEM and Ontology." In 2021 IEEE International Conference on Communications Workshops (ICC Workshops). doi:10.1109/ICCWorkshops50388.2021.94738