## DAFTAR REFERENSI


Owaps.org. (2021). *Security Logging and Monitoring Failures*. Retrieved from owasp.org:https://owasp.org/Top10/A09_2021Security_Logging_and_Monitoring_Failures/

Negara, B. S. (2023). *Terbitkan Annual Report Berisi Prediksi Ancaman Siber 2023*. Retrieved from BSSN: Materi Literasi Budaya Keamanan Siber dan Buktikan Akuntabilitas Kinerja: https://www.bssn.go.id/annualreport2022/

Gartner.com. (n.d.). *Security Information and Event Management (SIEM)*. Retrieved fromGartner.com:https://www.gartner.com/en/informationtechnology/glossary/security-information-and-event-management-siem

IBM. (2023). *IBM QRadar Security Intelligence Platform*. Retrieved from ibm.com: https://www.ibm.com/docs/en/qsip/7.5?topic=quick-start-guide

Learning, I. (2023). *infinitelearning.id*. *About Infinite Learning*. Retrieved from www.infinitelearning.id

Ngrok. (2023). *ngrok.com/docs/*. Retrieved from ngrok.com: https://ngrok.com/

González-Granadillo, G., González-Zarzosa, S., & Díaz, R. (2021). Security Information and Event Management (SIEM): analysis, trends, and usage in critical infrastructures.

Chandra, B., Agnes. (2021). Pengaruh intellectual capital terhadap kinerja perusahaan pada perusahaan di indonesia. Journal.feb.unmul.ac.id. 402.

Arogundade, O. R. (2023). Network Security Concepts, Dangers, and Defense Best Practical. Computer Engineering and Intelligent Systems, Vol.14, 25-26.

Safi, F. (2020). Intrusion Detection System using Genetic Algorithm. International Research Journal of Engineering and Technology (IRJET), 452.

Alabady, S. (2009). Design and Implementation of a Network Security Model for Cooperative Network. International Arab Journal of ETechnology, 1(2), 26–36.

Wanjau, S. K., Wambugu, G. M., Kamau, G. N. (2021). SSH-Brute Force Attack Detection Model based on Deep . International Journal of Computer Applications Technology and Research, 42.

Takahash, T., Ndichu, S., Inoue, D. (2023). Breaking Alert Fatigue: AI-Assisted SIEM Framework for. Cybersecurity Research Institute, National Institute of Information and Communications Technology, 4.

Rikhtechi, L., Rave, V., Rezakhani, A. (2021). Secured Access Control in Security Information and Event . 69-70.

Chakrabarty, B., Patil, S. R., Shingornikar, S., Kothekar, A., Mujumdar, P., Raut, S., Ukirde, D., & Redbooks, I. (2021). Securing data on threat detection by using IBM Spectrum Scale and IBM QRADAR: an enhanced cyber resiliency solution.

Savola, A. (2021). Server Virtualization with VMware. Metropolia University of Applied Sciences, 3 - 10.

Kamal, M. R., Setiawan, M. A. (2021). Deteksi Anomali dengan Security Information and Event Management (SIEM) Splunk pada Jaringan UII.

Heluka, H. D., Sulistyo, W. (2023). Perancangan Dan Implementasi Security Information and Event Management (SIEM) pada Layanan Virtual Server. *Jurnal Ilmiah Komputer*.

Prasetyo, O. D., Trisnawan, P. H., Bhawiyuga, A. (2023). Uji Kinerja Host-Based Intrution Detection System WAZUH terhadap Serangan Brute Force dan Dos. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*.

I. Kotenko and A. Ulanov, "Agent-based simulation of DDOS attacks and defense mechanisms", Int. J. Comput., vol. 4, pp. 113-123, 2014.

Zargar, S. T., et al. “A Survey of Defense Mechanisms against Distributed Denial of Service (Ddos).” Ieee Communications Surveys & Tutorials, vol. 15, no. 4, 2013, pp. 2046–69.

PencilData. (2023, April). *Qradar Architecture.pdf* . Retrieved from slideshare.net: https://www.slideshare.net/PencilData/qradar-architecturepdf