DAFTAR PUSTAKA

Al-Duwairi, B., Al-Kahla, W., AlRefai, M. A., Abdelqader, Y., Rawash, A., & Fahmawi, R. (2020). SIEM-based detection and mitigation of IoT-botnet DDoS attacks. *International Journal of Electrical and Computer Engineering*, *10*(2), 2182–2191. https://doi.org/10.11591/ijece.v10i2.pp2182-2191

Arfanudin Citra, Sugiantoro Bambang, P. Y. (2019). *Analisis Serangan Router Dengan Security Information and Event Management Dan Implikasinya Pada Indeks Keamanan Informasi Analysis of Router Attack With Security Information and Event Management and Implications in Information Security Index*. *2*(1), 2615–8442.

Arman, M. (2020). Metode Pertahanan Web Server Terhadap Distributed Slow HTTP DoS Attack. *JATISI (Jurnal Teknik Informatika Dan Sistem Informasi)*, *7*(1), 56–70. https://doi.org/10.35957/jatisi.v7i1.284

Brooks, R. R., & Oz¸celik, I. (2020). *Distributed Denial of Service Attacks-Real-world Detection and Mitigation*. CRC Press.

ChaosSearch. (2021). *The Threat Hunter ' s Handbook*. 1–30.

Cinderatama, T. A., Alhamri, R. Z., & Yunhasnawa, Y. (2022). Implementasi Metode K-Means, Dbscan, Dan Meanshift Untuk Analisis Jenis Ancaman Jaringan Pada Intrusion Detection System. *INOVTEK Polbeng - Seri Informatika*, *7*(1), 169. https://doi.org/10.35314/isi.v7i1.2336

DDoS attacks in Q2 2022 | Securelist. (n.d.). Retrieved October 28, 2022, from https://securelist.com/ddos-attacks-in-q2-2022/107025/

Fauzi, A. (2020). Sistem Manajemen Dan Visualisasi Syslog Perangkat Jaringan Komputer Pada Ict Universitas Diponegoro Berbasis Elk Stack. *Jurnal Sistem*

Komputer, *10*(2), 42–46.

Fitri Nova, Pratama, M. D., & Prayama, D. (2022). Wazuh sebagai Log Event Management dan Deteksi Celah Keamanan pada Server dari Serangan Dos. *JITSI : Jurnal Ilmiah Teknologi Sistem Informasi*, *3*(1), 1–7. https://doi.org/10.30630/jitsi.3.1.59

Georgeta Catescu, Bs. (2018). *Detecting insider threats using Security Information and Event Management (SIEM)*. 1–107.

Gupta, B. B., & Dahiya, A. (2020). *Distributed Denial of Service (DDoS) Attacks Classification, Attacks, Challenges, and Countermeasures*. CRC Press.

Harahap, A. G. S., & Hutrianto, H. (2021). Intrusion Detection and Anomaly Menggunakan Wazuh Pada Universitas Muhammadiyah Palembang. *Bina Darma ...*, 324–328. https://conference.binadarma.ac.id/index.php/BDCCS/article/view/2150

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 Computer Science*, *217*(2022), 1406–1415. https://doi.org/10.1016/j.procs.2022.12.339

Murdoch, D. (2019). *Blue Team Handbook: SOC, SIEM, and Threat Hunting Use Cases* (pp. 39–59). https://www.amazon.co.uk/Blue-Team-Handbook-Condensed-Operations/dp/1091493898

Rahman, A. M., Seta, H. B., & Astriratma, R. (2020). Perancangan Bot Untuk Monitoring Server Dari Serangan *Distributed Denial Of Service* Dan Implementasi JSON Web Token Pada Sistem Notifikasi Serangan. *Informatik*, *16*(2), 116–127. https://ejournal.upnvj.ac.id/index.php/informatik/article/view/2008

Skopik, F., Wurzenberger, M., & Landauer, M. (2021). *Smart Log Data Analytics*. Springer International Publishing. https://doi.org/10.1007/978-3-030-74450-2

Tanang Anugrah, F., Ikhwan, S., & Gusti A.G, J. (2022). Implementasi Intrusion Prevention System (IPS) Menggunakan Suricata Untuk Serangan SQL Injection. *Techné : Jurnal Ilmiah Elektroteknika*, *21*(2), 199–210. https://doi.org/10.31358/techne.v21i2.320

Tiara Sakinah, . (2022). *ANALISIS LOG SISTEM PADA SECURITY INFORMATION AND EVENT MANAGEMENT UNTUK MENDETEKSI DATA EXFILTRATION*.

What is Syslog server and its working ? - GeeksforGeeks. (n.d.). Retrieved October 28, 2022, from https://www.geeksforgeeks.org/what-is-syslog-server-and-its-working/

Yasin, A., & Mohidin, I. (2019). Monitoring DDOS Pada Openflow Switch Dengan Alienvault Ossim. *Jurnal Teknologi Informasi Indonesia (JTII)*, *3*(2), 23. https://doi.org/10.30869/jtii.v3i2.260