

DAFTAR PUSTAKA

- Antonio A. P, Candidate L, & Gracis R. (2022). Next Generation SOC: Automated Operations and Machine Learning in Cybersecurity.
- Arshad A, Rehman A U, Javaid S, Ali T. M, Sheikh J. A, & Azeem M. (2021). A Systematic Literature Review on Phishing and Anti-Phishing Techniques. <https://ieeexplore.ieee.org/>
- Atmojo W. T, Siregar E, & Audrey K. K. (2021). PENGENALAN CYBER SECURITY DALAM REVOLUSI INDUSTRI 4.0 DAN MENYONGSONG ERA SOCIETY 5.0 (Vol. 4).
- Bassey C, Chinda E. T, & Idowu S. (2024). Building a Scalable Security Operations Center: A Focus on Open-source Tools. Journal of Engineering Research and Reports, 26(7), 196–209. <https://doi.org/10.9734/jerr/2024/v26i71203>
- Bassey, C., Samuel, A. A., Imakuh, S., Oloruntola, O., & Onyia-Odike, I. (2024). Enhancing DDoS Attack Prevention And Detection Using IDS And XDR. In Journal of Multidisciplinary Engineering Science and Technology (JMEST) (Vol. 11). www.jmest.org
- Belcic, I. (2023, Agustus 25). *What Is Malware and How to Protect Against Malware Attacks?* From avast.com. <https://www.avast.com/c-malware>
- Budi, E., Wira, D., & Infantono, A. (2021). Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0. Prosiding Seminar Nasional Sains Teknologi Dan Inovasi Indonesia (SENASTINDO), 3, 223–234. <https://doi.org/10.54706/senastindo.v3.2021.141>
- Copeland, M. (2021). Cloud defense strategies with Azure Sentinel: Hands-on threat hunting in cloud logs and services. In Cloud Defense Strategies with Azure Sentinel: Hands-on Threat Hunting in Cloud Logs and Services. Apress Media LLC. <https://doi.org/10.1007/978-1-4842-7132-2>
- Dehran, B. (2024, Oktober 18). *Impact of zero-day attacks on a company's productivity.* From cloudkul.com: <https://cloudkul.com/blog/impact-of-zero-day-attacks-on-a-companys-productivity/>
- First. (2019). Computer Security Incident Response Team (CSIRT) Services Framework. <https://www.first.org>
- Firch, J. (2024, Feb 16). *What Is A Security Operations Center?* From purplesec.us: <https://purplesec.us/learn/security-operations-center-soc/>
- George, A. S., Hovan George, A. S., Baskar, T., & Pandey, D. (2021). XDR: The Evolution of Endpoint Security Solutions-Superior Extensibility and Analytics to Satisfy the Organizational Needs of the Future. Article in International Journal of Advanced Research in Science Communication and Technology, 8(1). <https://doi.org/10.5281/zenodo.7028219>
- George, A. S., Sagayarajan, S., Baskar, T., & Hovan George, A. S. (2023). Partners Universal International Innovation Journal (PUIIJ) Extending

- Detection and Response: How MXDR Evolves Cybersecurity.*
<https://doi.org/10.5281/zenodo.8284342>
- Gunawan, F., Fadhillah, A., & Malays Sari, E. (2024). Membangun Benteng Digital Untuk Memperkuat Etika Cyber Security Melawan Ancaman Cyber Crime. 25. <https://doi.org/10.37817/tekinfo.v25i1>
- Haryanto, B., & Chandra, D. W. (2024). Implementasi Wazuh Integritas File untuk Perlindungan Keamanan Berdasarkan Aktivitas Log di BTSI UKSW. Jurnal Indonesia : Manajemen Informatika Dan Komunikasi, 5(1), 183–192. <https://doi.org/10.35870/jimik.v5i1.447>
- Itmanagement. (2023, Mei 31). *Penjelasan tentang ITSM (IT Service Management)*. From itmanagement.id: <https://www.itmanagement.id/2023/05/penjelasan-tentang-itsm-it-service.html>
- Itmtech. (2022, Mei 12). *Is Your Business Ready To prevent, Detect And Respond To Cyber Attacks?* From itmtech.ie: <https://itmtech.ie/managed-detection-and-response-kildare/>
- Kasturi, S., Li, X., Li, P., & Pickard, J. (2024). A Proposed Approach to Integrate Application Security Vulnerability Data with Incidence Response Systems. American Journal of Networks and Communications, 13(1), 19–29. <https://doi.org/10.11648/j.ajnc.20241301.12>
- Kaur, H., Sanjaiy, D., Paul, T., Kumar Thakur, R., Kumar, K. V., Jay, R., & Kaviti Naveen, M. (2024). Evolution of Endpoint Detection and Response (EDR) in Cyber Security: A Comprehensive Review. E3S Web of Conferences, 556. <https://doi.org/10.1051/e3sconf/202455601006>
- KEMHAN. (n.d.). *Aduan Siber*. Retrieved 2024 from csirt.kemhan.go.id: <https://csirt.kemhan.go.id/portal/aduan>
- Lakshmi Narayanan Kaliyaperumal. (2021). The-Evolution-of-Security-Operations-and-strategies-for-Building-an-Effective-SOC_joa_Eng_1021. ISACA, 5.
- Make Computer Science Great Again. (2023, Agustus 20). *Understanding the CIA Triad: The Foundation of Network Security*. From medium.com: <https://medium.com/@MakeComputerScienceGreatAgain/understanding-the-cia-triad-the-foundation-of-network-security-ceb8d839d7c2>
- Microsoft. (2024). *Optimize SOC operations with Microsoft Defender XDR*. Retrieved 2024 from microsoft.com: <https://www.microsoft.com/en-us/security/business/solutions/extended-detection-response-xdr#diagram-cta-popup>
- Mughal, A. A., & Mughal, A. A. (2022). Building and Securing the Modern Security Operations Center (SOC). <https://orcid.org/0009-0006-8460-8006>
- Novikov, I. (2024, Juni 21). *XDR vs. SIEM*. From lab.wallarm.com: <https://lab.wallarm.com/what/xdr-vs-siem-unveiling-the-next-generation-of-threat-detection-and-response/>

- Padangsambian Kota Denpasar. (2023, Juli 25). *Cara Menghindari Dan Melindungi Diri Dari PHISHING*. From padangsambian.denpasarkota.go.id: <https://www.padangsambian.denpasarkota.go.id/berita/cara-menghindari-dan-melindungi-diri-dari-phishing>
- Ramos Brandao, P., & Nunes, J. (2021). Extended *Detection* and Response Importance of Events Context. <https://doi.org/10.31112/kriativ-tech-2021-10-58>
- Robin Ruefle, A. D. (2014). Computer Security Incident Response Team Development and Evolution. *IEEE Security & Privacy*, 16-26.
- Tahir R. (2018). A Study on *Malware* and *Malware Detection* Techniques. *International Journal of Education and Management Engineering*, 8(2), 20–30. <https://doi.org/10.5815/ijeme.2018.02.03>
- Tanczer L. M., Brass, I., & Carr, M. (2018). CSIRTs and Global Cybersecurity: How Technical Experts Support Science Diplomacy. *Global Policy*, 9, 60–66. <https://doi.org/10.1111/1758-5899.12625>
- Terabit Komputer. (2023, Juli 27). *Mengenal Serangan DDOS Pada Komputer*. From terabitkomputer.com: <https://terabitkomputer.com/category/teknologi/>
- Waheed A, Seegolam B, Jowaheer M. F, Sze C. L. X, Hua E. T. F, & Sindiramutty S R. (2024). Zero-Day Exploits in Cybersecurity: Case Studies and Countermeasure. <https://doi.org/10.20944/preprints202407.2338.v1>
- Wazuh. (2025). *Active XDR protection from modern threats*. Retrieved 2025 from Wazuh.com: <https://wazuh.com/platform/xdr/>
- Yuniarto, T. (2024, Juli 31). *Tantangan Keamanan Siber Indonesia: Ancaman dan Dampaknya*. From kompaspedia.kompas.id: <https://kompaspedia.kompas.id/baca/paparan-topik/tantangan-keamanan-siber-indonesia-ancaman-dan-dampaknya#:~:text=Tren%20Trafik%20Anomali%20Serangan%20Siber&text=Laporan%20dari%20Badan%20Siber%20dan,1%20miliar%20anomali%20trafik%20serangan>.
- Zones. (n.d.). *Network Operations Center*. Retrieved 2024 from Zones.com: https://www.zones.com/site/statics/static_page.html?name=networking/network-operations-center