Inform : Jurnal Ilmiah Bidang Teknologi Informasi dan Komunikasi
Vol.9 No.1 January 2024, P-ISSN : 2502-3470, E-ISSN : 2581-0367

Information Security System Design Using XDR And EDR

Dedi Soleman[1], Benfano Soewito[2]
[1,2]*Computer Science Department, Universitas Bina Nusantara, Jakarta, Indonesia*
[1]dedi.soleman@binus.ac.id (*)
[2]bsoewito@binus.edu

Received: 2023-11-15; Accepted: 2023-12-29; Published: 2023-01-15

Abstract— Technology development has provided many benefits in providing services to the community and helping to manage government efficiently. However, increasing reliance on technology also indirectly increases the risk of cyberattacks. Every company faces the threat of cyber-attacks from hackers who try to access and possess important and confidential assets inside and outside the company. A cybersecurity system that can protect against various threats of attack from irresponsible parties is needed to protect these assets. A layered cybersecurity system is necessary to detect and respond to cyber-attacks that occur automatically. Extended detection and response (XDR) is a tool for detecting and responding to cyberattacks based on the data analysis results throughout the infrastructure to improve the efficiency of security operations. In addition, a system is also needed to detect, alert, investigate, isolate, and remove malicious software at endpoints in real time. This system is called Endpoint Detection and Response (EDR). Following the security system's implementation, the tests' results are systems that can monitor cyberattacks in real-time and provide an immediate response to protect information security on servers and endpoint devices.

Keywords— Cyber-attacks; Cyber Security; Firewall; XDR; EDR.

I. INTRODUCTION

Cybersecurity is a set of methods for protecting computers, networks, databases, and applications from attacks and unauthorized access, modification, or destruction referring to technologies, techniques, and procedures [1]. A vulnerability is a flaw in a system or design that allows an attacker to execute malicious commands, access data unlawfully, and/or perform various attacks that disrupt services. This vulnerability can pose a risk, namely the potential loss of information or system damage due to attacks that exploit the vulnerability [2].

In this era of rapid technological progress, new technologies have emerged. This article will cover the main topics of Cyber Security, XDR, and EDR components. As technology advances, improvements and refinements are designed to overcome the limitations of previous versions of technology [3][4]. System security has become a prominent topic in the network environment. Existing network technology and infrastructure must meet user needs. Most previous research has often discussed the basic concepts and features of Security Information and Event Management (SIEM), Security Orchestration, Automation and Response System (SOAR), and Intrusion Detection and Prevention System (IDPS). But what distinguishes this paper from previous research is that previous research emphasizes how useful the application of SIEM, SOAR, and IDPS as cybersecurity systems is.

As for its limitations, existing research has been done before [5] mentions SIEM, which can collect and analyze large event logs. However, it does not focus on log analysis to detect and respond to threats. Then, develop an endpoint security system, EDR, which still has a high false positive rate [6]. This paper proposes an efficient and integrated cybersecurity system solution where Extended Detection and Response (XDR) and Endpoint Detection and Response (EDR) will enhance corporate asset security measures.

Technology development has provided many benefits in providing services to the community and helping to manage government efficiently. However, increasing dependence on technology also indirectly increases the risk of cyber threats and attacks [7]. Over time, the development of cyberattacks today is like zero-day exploits, where these attacks work the same day before being detected because of their signature. The security system has not been created or repaired/updated.

In general, the cybersecurity system in organizations is in the form of an intruder detection system. However, this is not optimal because no system can detect and respond to cyber-attacks in real-time, automatically, and integrated by providing security. Multi-layered. In these conditions, the system still relies heavily on IT Security teams or administrators to respond to and deal with threats. Many endpoint security systems also use traditional antivirus that is not centralized on a single server and lacks analytical capabilities using machine learning and threat intelligence. The system can also not handle threats automatically, so it is less optimal in protecting endpoints from the threat of virus/malware attacks.

The proposed solution can effectively address the identified problem. Consequently, the research paper aims to fulfill its objectives by investigating the following questions: (1) the methodology for constructing a cybersecurity system with real-time functionality, automation, and integration using cloud-based XDR and EDR, (2) the processes by which XDR and EDR systems monitor, detect, and respond to cyberattacks, and (3) the specific approaches employed by XDR and EDR in monitoring, detecting, and responding to cyber threats.

The designated research questions are geared towards value creation. The corresponding research objectives for this study encompass understanding the methodology for constructing a real-time, automated, and integrated cybersecurity system employing cloud-based XDR and EDR, comprehending the monitoring, detection, and response mechanisms of XDR and EDR in the context of cyberattacks, and identifying strategies

DOI : https://doi.org/10.25139/inform.v9i1.7331

to enhance XDR performance and diminish false positives in the detection of cyberattacks.

This research aims to determine and test the effectiveness and usefulness of the proposed solution based on the research questions and objectives, namely the application of XDR and EDR security systems. The proposed solution is expected to meet the demands of cybersecurity systems in one integrated platform to accelerate discovery and response to cyberattacks that will be used instead of traditional cybersecurity systems.

II. Research Methodology

In conducting research, it is essential to articulate the connections between each stage or process. This ensures that your research endeavors are characterized by increased concentration, specificity, and systematic progression. Figure 1 is the research framework to be carried out, and the stages will be carried out sequentially. There are four main stages of research: initiation, design, testing, and evaluation. This phase identifies common problems that occur in your company/organization.

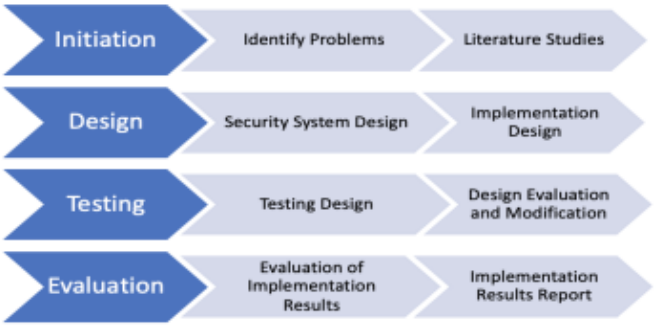

Figure 1. Research Framework

At this stage, the author also conducts literature studies or theoretical exploration by reviewing similar journals, reading various literature sources and papers related to similar topics, and being involved in other company matters. Literary research is conducted to obtain references and understand and complete theories and related information.

The next stage is to create a design based on existing problems in the company. Based on existing information, a layered and integrated information security system is needed, namely a system that can detect and respond to cyber-attacks in real-time, automatically, and integrated by providing security in layers. In the third stage, testing will be carried out on the design that has been implemented to determine whether the prototype's design and implementation are following what is expected. Finally, the author makes an evaluation plan for designing the security system built using several tools to conduct security testing on servers, applications, and endpoint devices.

In this study, the author combines two security systems with complementary functions: XDR and EDR. XDR is a comprehensive and optimized security system that integrates security systems and data security into a simplified system. XDR systems can incorporate protection for endpoint devices, servers, cloud applications, email, and more. In general, XDR functions to monitor, detect, warn, and respond to any cyber-attacks automatically.

The EDR is an endpoint security system that detects and responds to cyber-attacks based on the results of collecting endpoint traffic data. EDR helps predict potential threats and protect endpoints in advance by leveraging machine learning technology. EDR threat intelligence can detect and alert anomalies and repair internal networks that have been infected. This is because EDR combines elements of endpoint antivirus and endpoint management in detecting, investigating, and removing malicious software. In general, an overview of the topology security system proposed by the author can be seen in Figure 2.

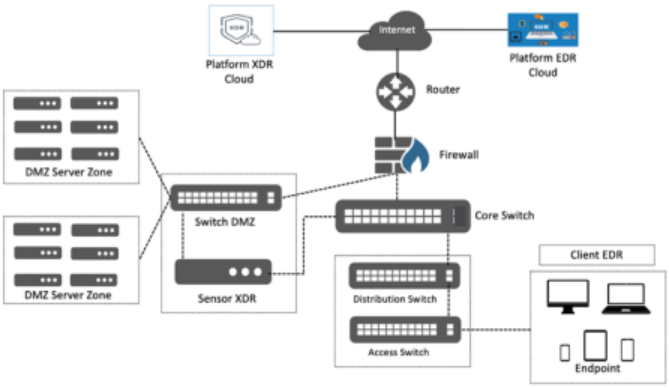

Figure 2. Topology Security System Using XDR and EDR

Based on Figure 2, the cyber security system design comprehensively detects internal and external attacks using XDR and EDR. The design is hybrid by integrating on-premise and cloud systems. The XDR sensor used on-premise will collect incoming and outgoing server traffic logs, then endpoint logs will be obtained from Cloud EDR using the Application Programming Interface (API). The collected logs will be analyzed using Big Data, Machine Learning, and Threat Intelligence technology contained in XDR, and several parameters used will be adjusted to the company's conditions. The aim is to improve system performance and reduce the occurrence of false positives. XDR integration will be carried out with IPS/Firewall and EDR devices via API in response to cyber-attacks.

III. Result and Discussion

XDR is a security platform that collects and correlates data from various infrastructures. This includes email, endpoints, servers, cloud workloads, and networks, expanding global visibility and threat context. It allows you to analyze, prioritize, search for, and remediate threats to prevent data loss and security breaches. XDR combines multiple solutions into a cohesive and integrated security incident detection and response platform, developing automated endpoint detection and incident response solutions [8]. An overview of the security system proposed by the author can be seen in Figure 3.

DOI : https://doi.org/10.25139/inform.v9i1.7331

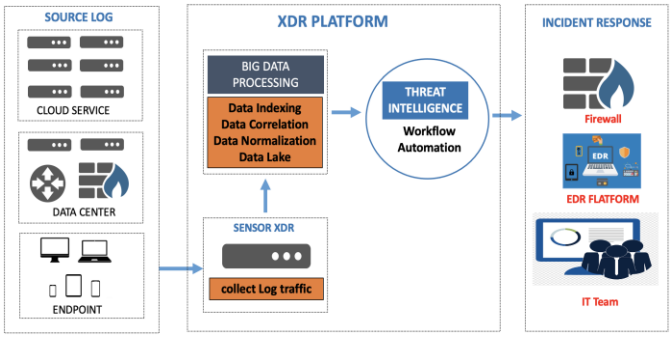

Figure 3. Proposed Cybersecurity System

Figure 3 shows that the cybersecurity system consists of three stages. The first stage captures all traffic logs on network devices, firewalls, endpoints, servers, and other devices. The second stage is that all logs will be stored in the XDR data lake, which will then be used to analyze and detect cyber-attacks. The final stage is to respond to cyber-attacks automatically and according to predetermined procedures, such as instructing IPS/Firewall/EDR to block. This security system is designed using XDR to carry out monitoring, detection, and response functions to cyberattacks.

Cisco states that XDR is a technology that uses a detection and response approach by providing a global view of the overall scope of the technology [9]. Figure 4 [9] shows that XDR has three layers: the first layer of data collection across the network, cloud, and endpoints, and then the analytics layer, which includes normalization data, data lake, and correlation data. Lastly is an automation layer to detect, analyze, track, and patch threats.

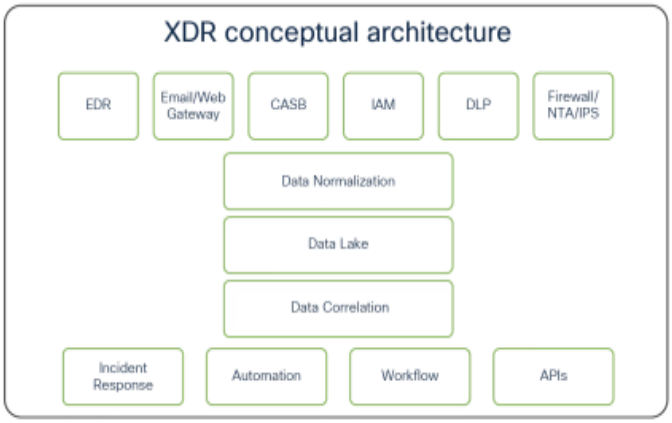

Figure 4. XDR Conceptual Architecture

The ability of XDR to detect and respond to cyberattacks is primarily determined by the availability of traffic logs collected in the XDR Data Lake. This data will be analyzed using Big Data models using Machine Learning, and this process includes cleaning, enrichment, and indexing processes that will produce data such as Source IP Address, Destination IP Address, time data, location data, and others. Furthermore, XDR detects attacks or anomalies according to existing workflows, including analysis, detection, and filter processes based on attack type.

Finally, XDR will conduct Threat Intelligence, which includes the process of identifying anomalies, correlation, and determining anomaly scores by combining parameters, namely fidelity parameters, namely the confidence value of XDR in the results of its analysis, and severity parameters, namely the value of the risk value of attack impact. The XDR can respond automatically if the attack exceeds the tolerance value set on the XDR platform. This response does not require instructions from the relevant IT team, so that it can save time and HR resources simultaneously. The expected benefits of using XDR are improving security operations' efficiency and cyber threat detection and response capabilities by combining visibility and control across endpoints, networks, and clouds [5]. It provides security teams with detailed information about:

a) Attack Detection: Critical threats will be combined with endpoint telemetry, and collected security events are further analyzed on complex platforms;

b) Attack Investigation: XDR enables correlation of all collected and relevant event information and supports identifying the problem's root cause.

c) Recommendation: XDR provides advice to deepen the investigation through further questioning and allow action to be taken to contain or remediate detected threats;

d) Threat Hunting: XDR enables querying data repositories containing sensor telemetry from various vendors to detect suspicious behavior and threats and take remedial action;

e) Block Attacks: Block known and unknown attacks by leveraging artificial intelligence-based analysis and behavioral threat protection to stop malware, exploits, and file-less attacks.

Suppose an attack occurs on a server where the hacker previously had direct access to the target server. In that case, XDR detects the attack after implementation by notifying XDR of the source IP, target IP, and the activity or type of attack used by the process.

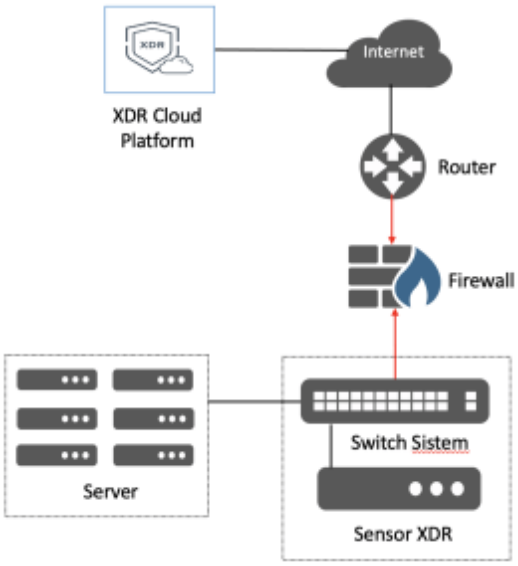

Figure 5. Topology when The Firewall Blocks Attacks

DOI : https://doi.org/10.25139/inform.v9i1.7331

Figure 5 shows the topology of a blocking attack with a target server in the DMZ zone. In the topology above, it is known that if there is an attack from inside and outside the XYZ Company network, all logs will be collected by the XDR sensor by mirroring. The topology is also known, such that if an attack targets the server, it will be detected by XDR and automatically blocked by IPS / Firewall devices so that inbound and outbound access cannot be done.

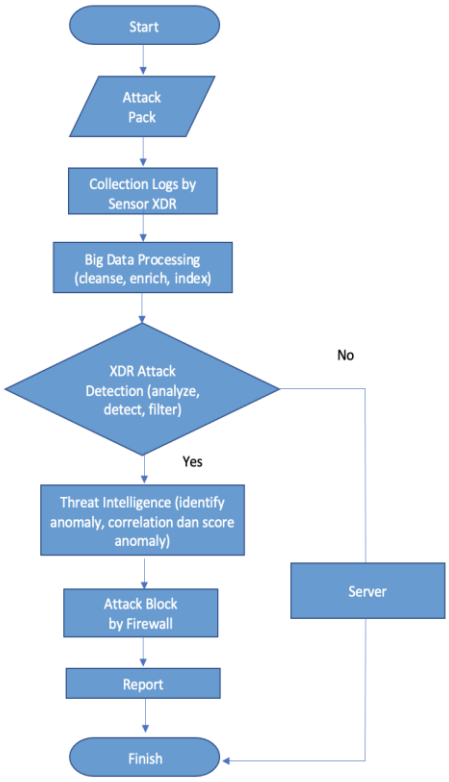

Figure 6. Flow When the Firewall Performs Block Attacks

Figure 6 shows the flow of blocking attacks IPS/Firewall devices performed, starting from receiving XDR logs and conducting analysis with Big Data models using Machine Learning. The XDR will detect attacks or anomalies according to existing workflows, including analysis, detection, and filter processes based on the type of attack. Finally, XDR will conduct Threat Intelligence, which includes identifying anomalies, correlation, and determining anomaly scores by combining fidelity parameters, namely XDR confidence values in the results of its analysis, and severity parameters, namely risk value impact of the attack. The XDR will respond automatically if the attack exceeds the tolerance value set on the XDR platform by instructing the IPS/Firewall to block [10].

The author's test simulated four different cyber-attacks, focusing on simulating attacks on servers, applications, and endpoint devices such as Denial of service (DoS), Structured Query Language (SQL) Injection, Port Scanning, and Trojan Viruses. This process focuses on its scope by analyzing the security system implemented and the performance of workflow parameters in the form of attack activities using the XDR security system [11]. Here are the results of the XDR security system performance test:

a) Port Scanning Attack: A port scan attack to detect active ports on the target system fails because the implemented security system detects it, and the hacker cannot find any information from the targeted system for hacking. Figure 7 shows that XDR can detect port-scanning attacks using the Nikto tools on the Kali Linux operating system. The firewall blocks it automatically so that hackers cannot obtain information from the target system to hack.

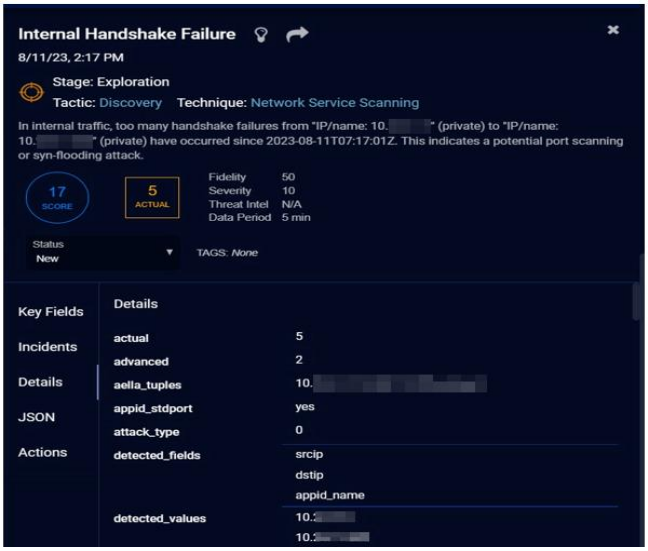

Figure 7. Port Scan Simulation Results Detected by XDR

b) SQL Injection Attacks: SQL injection attacks are carried out for hackers detected by XDR. The information captured is the type of attack, hacker IP, and target IP. The information is then passed to the IPS/WAF, where it can block the attack. Figure 8 shows that XDR can detect SQL Injection attacks using the SQL Map tool this tool can be used directly on the Kali Linux operating system, and then the firewall blocks it automatically so that attacks from hackers do not reach the target server.

Figure 8. SQL Injection Simulation Detected by *XDR*

DOI : https://doi.org/10.25139/inform.v9i1.7331

c) DoS Attack: DoS attacks carried out by hackers are detected by XDR. The information obtained is the type of attack, the hacker's IP, and the destination IP. The information is passed to IPS/Firewall to block the attack so that the server or system targeted by hackers does not experience interference as before. Figure 9 shows that XDR can detect a DoS attack using the Low Orbit Ion Cannon (LOIC). The firewall blocks it automatically so that the server or system targeted by hackers does not experience interference.

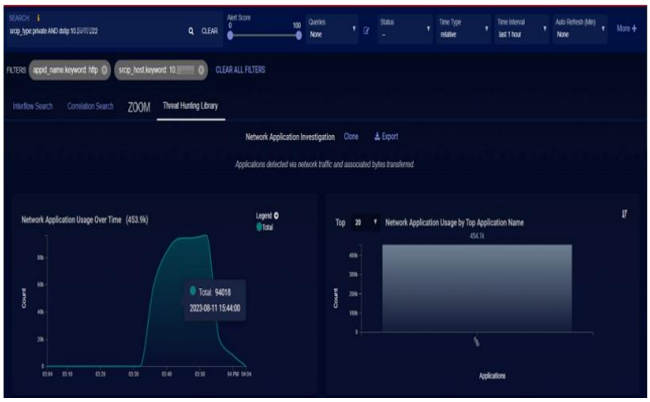

Figure 9. DoS Simulation Results Detected by XDR

The results of optimizing the XDR workflow for port scanning and DoS attacks. Table I logs port scan attacks that occur after XDR workflow parameters are applied. In the monitoring period, there were 10 attacks from internal to internal networks, and the XDR workflow parameters worked well in detecting anomalies with parameters with actual values of at least 3 handshake failures and no false positives [12].

TABLE I
PORT SCANNING ATTACK LOG ON XDR

Source IP	Destination IP	Actual	Severity	Fidelity
10.24.11.132	10.24.21.139	4	10	50
10.1.210.1	10.1.210.41	3	10	50
10.17.11.10	10.17.11.81	4	10	50
10.11.11.141	10.11.21.141	3	10	50
10.112.51.13	10.1.20.3	4	10	50
10.1.20.3	10.112.51.13	4	10	50
10.24.11.1	10.24.11.222	5	10	50
10.24.11.1	10.24.11.221	4	10	50
10.21.11.91	10.1.122.3	4	10	50
10.1.203.1	10.1.203.91	3	10	50

Table II logs DoS attacks before and after XDR workflow parameters were applied. In the monitoring period, there 6 attacks from external to internal networks, and the XDR workflow parameters were able to work well to detect anomalies with parameters [13] from the simulation conducted by the author with three types of cyber-attacks.

TABLE II
DOS ATTACK LOG ON XDR

Source IP	Destination IP	Actual	Severity	Fidelity
34.124.166.9	10.17.11.10	135,015	15	50
223.27.151.162	10.1.107.181	45,490	15	50
43.247.23.214	10.1.109.41	94,018	15	50
223.27.151.163	10.21.11.10	27,129	15	50
118.98.226.106	10.16.11.10	10,532	15	50
18.234.51.228	10.1.102.61	9,110	15	50

Table III shows that XDR can work well to monitor in real-time and detect and respond automatically to Port Scanning, DoS, and SQL Injection attacks so that it can secure data assets and systems in the company.

TABLE III
XDR SYSTEM TEST RESULTS

Attack Type	Performance XDR		Confusion Matrix	Information
	Detection	Response		
Port Scanning	Succeed	Succeed	True Positive	Attacks from Attackers can be detected by XDR and blocked by Firewall/IPS.
SQL Injection	Succeed	Succeed	True Positive	
DoS	Succeed	Succeed	True Positive	

EDR is an endpoint security solution that combines real-time monitoring, continuous data collection, and automated responses based on analytical results. EDR is a new security system that detects and investigates suspicious activity on hosts and endpoints and implements automation to help security teams detect and respond quickly to threats [14]. Therefore, EDR will only collect endpoint traffic data, and no network information will be collected [15].

EDR has Cyber Threat Intelligence that can detect and alert anomalies and repair internal networks that have been infected. So EDR works by combining endpoint antivirus and endpoint management elements to detect, scan, and remove malware that enters network devices [16]. EDR generates a large number of false positives with a large number of protocols, so it takes time to investigate the attack. In addition, the integrity of cyber-attack alerts must be validated manually [17]. Therefore, the presence of XDR complements the endpoint security system, namely EDR [5]. The following are key features in EDR that help manage endpoint device security [18]:

a) Threat Intelligence: Threat Intelligence in EDR makes it possible to warn or notify potential risks and threats based on the analysis results.

b) Continuous Monitoring: The best way to distinguish

DOI : https://doi.org/10.25139/inform.v9i1.7331

unusual endpoint conduct is to increment control. If an endpoint is tainted, EDR will immediately detect the activity and isolate it directly. EDRs can dynamically monitor endpoints by testing endpoints nonstop and automatically [19].

c) Remediation and Cleanup: Once the infected endpoints are cleaned and virus escalation is stopped to ensure no viruses remain, the damage caused by viruses, including APT, is repaired.

d) Machine Learning Proposed: By utilizing AI, EDR is likewise a "savvy" stage, another benefit. Prescient models use progressed examination methods, for example, profound figuring out how to comprehend malware qualities and anticipate the probability of obscure malware. Then, at that point, block never-before-seen assaults with a severe level of exactness [20].

When an attack occurs on an endpoint that programmers could go straightforwardly to the objective after carrying out a security framework, the assault can be recognized by EDR/XDR by illuminating the programmer's source IP, objective IP, and action or sort of assault. Utilized simultaneously [21].

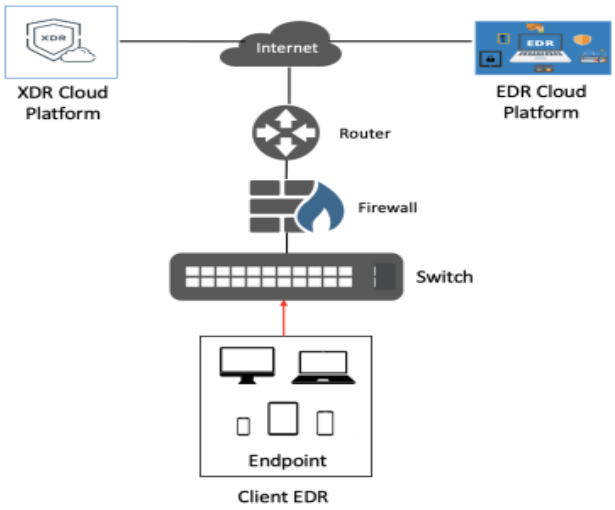

Figure 10. Topology when EDR Blocks Attacks

Figure 10 is the topology for a blocking attack targeting endpoints that use the network at Company XYZ. In the above topology, it is known that XDR will collect logs using the API if there is an attack on the XYZ Company endpoint. Then, from the topology, it is also known that if an attack is targeted at an endpoint, it will automatically be blocked by EDR devices [22]. The flow of blocking attacks performed by a device. First, XDR receives logs and analyzes them with Big Data models using Machine Learning. Then, XDR will detect attacks or anomalies according to existing workflows, including analysis, detection, and filter processes based on the type of attack. Finally, XDR will conduct Threat Intelligence, which includes identifying anomalies, correlation, and determining anomaly scores by combining fidelity parameters, namely XDR confidence values in the results of its analysis, and severity parameters, namely risk values impact of the attack [23]. Then, XDR will respond automatically if the attack is above the tolerance value set on the XDR platform by instructing EDR to block it so that endpoints cannot access the corporate network and spread viruses/malware [24]. The attacks carried out by hackers can be detected with XDR. The information obtained is the type of attack, IP Hacker, and IP destination. EDR blocked the attack. So that the endpoint or system targeted by hackers does not experience interference [25].

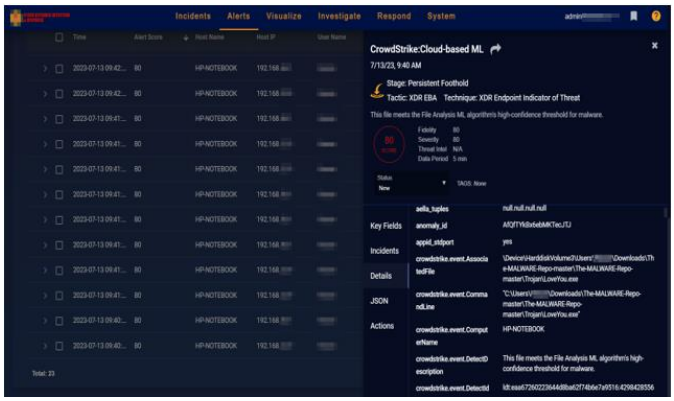

Figure 11. Log of Simulation Results of XDR Trojan Attacks Detected

Figure 11 shows that XDR can detect a simulated Trojan attack, and then EDR blocks it automatically so that the endpoint targeted by hackers does not experience interference. The simulation conducted by the author can be concluded in Table IV. XDR can work well to monitor in real-time and detect and respond automatically to Trojan Virus attacks so that it can secure data assets and endpoint devices in the company.

TABLE IV
XDR AND EDR SYSTEM TEST RESULTS

A. **Attack Type**	**Performance XDR**		*B.* **Confusion Matrix**	*C.* **Information**
	D. **Detection**	*E.* **Response**		
F. Trojan *G.*	*H.* Succeed *I.*	*J.* Succeed *K.*	*L.* True Positive *M.*	*N.* Attacks from Attackers can be detected by XDR and blocked by EDR.

IV. CONCLUSION

Based on the analysis of the results of Cyber Security System research using XDR and EDR, it can be concluded as follows. First, XDR security systems can integrate various security system platforms that can work in real time and automatically detect and respond to cyber-attacks. Second, Cybersecurity systems designed using XDR and EDR function well in

DOI : https://doi.org/10.25139/inform.v9i1.7331

detecting and responding to cyber-attacks such as Port Scanning, DoS, SQL Injection, and Trojan Viruses to reduce the risk of threats. Third, XDR security systems can complement endpoint security systems, namely EDR, which focuses on securing endpoint devices. The tests conducted on the XDR security system show that adjusting the XDR workflow according to organizational conditions can improve system performance and reduce false positives. The future research can be carried out by adapting the XDR workflow to other cyber-attacks such as Cross-Site Scripting (XSS), phishing, and other cyber-attacks so that the security system's performance is better and false positives are reduced.

REFERENCES

[1] C. Schröer, F. Kruse, and J. M. Gómez, "A systematic literature review on applying CRISP-DM process model," *Procedia Comput. Sci.*, vol. 181, no. 2019, pp. 526–534, 2021, doi: 10.1016/j.procs.2021.01.199.
[2] E. Sindiren and B. Ciylan, "Privileged account management approach for preventing insider attacks," *Int. J. Comput. Sci. Netw. Secur.*, vol. 18, no. 1, pp. 33–42, 2018.
[3] L. Santos, C. Rabadao, and R. Gonçalves, "Intrusion detection systems in Internet of Things: A literature review," in *2018 13th Iberian Conference on Information Systems and Technologies (CISTI)*, IEEE, 2018, pp. 1–7.
[4] N. Mazhar, R. Salleh, M. A. Hossain, and M. Zeeshan, "SDN based intrusion detection and prevention systems using manufacturer usage description: A survey," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 12, 2020.
[5] P. R. Brandao and J. Nunes, "Extended Detection and Response".
[6] D. A. S. GEORGE, A. S. H. George, T. Baskar, and D. Pandey, "XDR: The Evolution of Endpoint Security Solutions-Superior Extensibility and Analytics to Satisfy the Organizational Needs of the Future," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 8, no. 1, pp. 493–501, 2021.
[7] M. A. Halim, A. Abdullah, and K. A. Z. Ariffin, "Recurrent neural network for malware detection," *Int. J. Adv. Soft Compu. Appl*, vol. 11, no. 1, pp. 43–63, 2019.
[8] J. Mcafee, "'What Is XDR? Extended Detection and Response,'" 2021. [Online]. Available: https://www.mcafee.com/enterprise/en-us/security-awareness/endpoint/what-is-xdr.html
[9] Cisco. (n.d.)., "Understanding Extended Detection and Response (XDR)," 2023. [Online]. Available: https://www.cisco.com/c/en/us/products/collateral/security/securex/xdr-buyer-guide.html
[10] I. Bachane, Y. I. K. Adsi, and H. C. Adsi, "Real time monitoring of security events for forensic purposes in Cloud environments using SIEM," in *2016 Third International Conference on Systems of Collaboration (SysCo)*, IEEE, 2016, pp. 1–3.
[11] C. Arfanudin, B. Sugiantoro, and Y. Prayudi, "Analisis Serangan Router Dengan Security Information and Event Management Dan Implikasinya Pada Indeks Keamanan Informasi," *CyberSecurity dan Forensik Digit*, vol. 2, no. 1, pp. 1–7, 2019.
[12] M. Palmieri, N. Shortland, and P. McGarry, "Personality and online deviance: The role of reinforcement sensitivity theory in cybercrime," *Comput. Human Behav.*, vol. 120, p. 106745, 2021.
[13] C. Nilă, I. Apostol, and V. Patriciu, "Machine learning approach to quick incident response," in *2020 13th International Conference on Communications (COMM)*, IEEE, 2020, pp. 291–296.
[14] G. Karantzas and C. Patsakis, "An empirical assessment of endpoint detection and response systems against advanced persistent threats attack vectors," *J. Cybersecurity Priv.*, vol. 1, no. 3, pp. 387–421, 2021.
[15] B. T. O'hara and B. Malisow, *Ccsp (ISC) 2 certified cloud security professional official study guide*. John Wiley & Sons, 2017.
[16] M. Chopra and C. Mahapatra, "Significance of security information and event management (SIEM) in modern organizations," *Int. J. Innov. Technol. Explor. Eng*, vol. 8, no. 7, pp. 432–435, 2019.
[17] S. Chandel, M. Yan, S. Chen, H. Jiang, and T.-Y. Ni, "Threat intelligence sharing community: A countermeasure against advanced persistent threat," in *2019 IEEE Conference on Multimedia Information Processing and Retrieval (MIPR)*, IEEE, 2019, pp. 353–359.
[18] S. Chandel, S. Yu, T. Yitian, Z. Zhili, and H. Yusheng, "Endpoint protection: Measuring the effectiveness of remediation technologies and methodologies for insider threat," in *2019 international conference on cyber-enabled distributed computing and knowledge discovery (cyberc)*, IEEE, 2019, pp. 81–89.
[19] J. M. Biju, N. Gopal, and A. J. Prakash, "Cyber attacks and its different types," *Int. Res. J. Eng. Technol.*, vol. 6, no. 3, pp. 4849–4852, 2019.
[20] M. I. Alghamdie, "WITHDRAWN: A novel study of preventing the cyber security threats." Elsevier, 2021.
[21] J. Kinyua and L. Awuah, "AI/ML in Security Orchestration, Automation and Response: Future Research Directions.," *Intell. Autom. Soft Comput.*, vol. 28, no. 2, 2021.
[22] A. A. Aziz and Z. Amtul, "Developing Trojan horses to induce, diagnose and suppress Alzheimer's pathology," *Pharmacol. Res.*, vol. 149, p. 104471, 2019.
[23] D. Al Shaer, O. Al Musaimi, B. G. de la Torre, and F. Albericio, "Hydroxamate siderophores: Natural occurrence, chemical synthesis, iron binding affinity and use as Trojan horses against pathogens," *Eur. J. Med. Chem.*, vol. 208, p. 112791, 2020.
[24] D. C. Patel *et al.*, "Paradoxical motion on sniff test predicts greater improvement following diaphragm plication," *Ann. Thorac. Surg.*, vol. 111, no. 6, pp. 1820–1826, 2021.
[25] C. Topping, A. Dwyer, O. Michalec, B. Craggs, and A. Rashid, "Beware suppliers bearing gifts!: Analysing coverage of supply chain cyber security in critical national infrastructure sectorial and cross-sectorial frameworks," *Comput. Secur.*, vol. 108, p. 102324, 2021.

DOI : https://doi.org/10.25139/inform.v9i1.7331