BAB II

LANDASAN TEORI

2.1 Security Information and Event Management (SIEM)

Menurut (IBM, 2024) *SIEM* adalah sebuah aplikasi *software* yang berfungsi mengumpulkan informasi dan *event* terkait dengan keamanan sebuah jaringan (*WAN* maupun *LAN*). *SIEM* merupakan gabungan dari sebuah produk yang sebelumnya terpisah, yaitu *Security Information Management (SIM)* dan *Security Event Management (SIEM*). Produk dari *SIEM*, bisa berupa peralatan,*software* ataupun *service* dan dapat digunakan untuk membuat log data keamanan dan mengenerate report sesuai dengan keadaan yang terjadi.

SIEM telah dikembangkan sebagai respons untuk membantu *administrator* merancang kebijakan keamanan dan mengelola peristiwa dari berbagai sumber. Secara umum, sebuah *SIEM* sederhana terdiri dari blok-blok terpisah (misalnya, perangkat sumber, pengumpulan log, penguraian normalisasi, mesin aturan, penyimpanan log, pemantauan peristiwa) yang dapat bekerja secara independen satu sama lain, tetapi tanpa semua bagian tersebut bekerja bersama, *SIEM* tidak akan berfungsi dengan baik (González-Granadillo et al., 2021).

2.2 Cyber Threat Intelligence

Menurut (Roberts, 2021) *Cyber Threat Intelligence* (CTI) dapat digambarkan sebagai proses pengambilan berbagai informasi tentang serangan siber, memahami bagaimana hal itu terjadi dan maknanya. Hal tersebut membantu untuk memprediksi dan mencegah serangan siber. Juga disebut sebagai intelijen ancaman, ini adalah metode untuk memperingatkan organisasi berdasarkan data

yang diperoleh dari berbagai sumber yang telah dianalisis. Sumber umum pelanggaran data adalah *malware*, ancaman orang dalam, rekayasa sosial, kredensial yang lemah dan dicuri, kerentanan aplikasi, konfigurasi yang salah, dan kesalahan dari pengguna. Kecerdasan ancaman itu sendiri merupakan evolusi dalam proses pengamanan data, file, dan infrastruktur.

Menurut (Abu et al., 2018) kecanggihan dalam serangan menyebabkan kemajuan dalam pengumpulan informasi dari berbagai sumber untuk melindungi aset dalam suatu lingkungan. Pertukaran intelijen ancaman memberikan dukungan yang kuat untuk menghadapi serangan siber di era baru. Dalam definisinya, *CTI* berbasis *adversary*, berfokus pada risiko, berorientasi pada proses dan disesuaikan untuk konsumen yang beragam. Berbasis *adversary* karena berusaha untuk mengidentifikasi motivasi dan niat serta metode para penyerang. *CTI* berfokus untuk meminimalkan risiko aset dan infrastruktur utama yang terpapar oleh aktivitas penyerang sehingga aktivitas bisnis tidak terpengaruh. *CTI* bertujuan untuk memberikan keunggulan pengetahuan atas pelaku ancaman *cyber* (Kaur et al., 2023). Definisi *CTI* tidak lengkap jika tidak menangkap data ancaman yang relevan yang mengalami tahap pengumpulan, analisis, dan pemrosesan yang mengarah pada intelijen yang dapat ditindaklanjuti yang membantu pengambilan keputusan, semuanya tepat waktu.

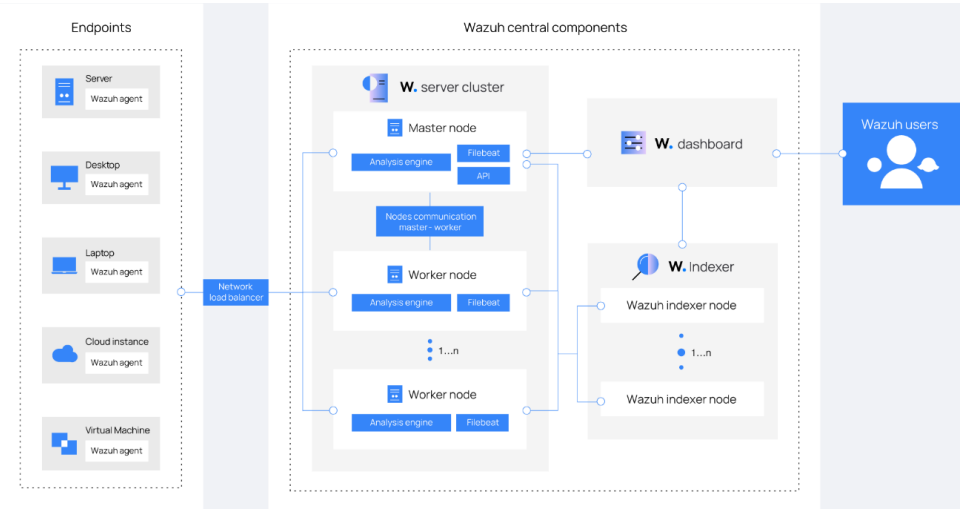
2.3 *Wazuh*

Wazuh adalah sebuah aplikasi *open-source* yang secara resmi didefinisikan sebagai *host-based intrusion detection system* (HIDS) (WAZUH, 2024). *Wazuh*

memiliki keunggulan yakni memiliki fitur yang lebih banyak dibandingkan aplikasi serupa.

Gambar 2. 1 Logo WAZUH

Wazuh menggabungkan fungsi yang terpisah secara historis untuk menjadi single agent dan platform arsitektur. Perlindungan keamanan yang ditawarkan seperti untuk cloud public, cloud pribadi, dan pusat data. *Wazuh* juga memberikan analisis korelasi secara *real-time*, respons yang diberikan juga aktif dan bersifat granular, serta mencakup perbaikan pada perangkat sehingga *end point* akan tetap terjaga kebersihannya. Aplikasi *Wazuh* juga melakukan analisis log, pengecekan integritas, pemantauan *registry Windows*, deteksi *rootkit*, peringatan berbasis waktu, dan respons aktif secara *real-time* (WAZUH, 2024).



Gambar 2. 2 Arsitektur WAZUH

Berdasarkan Gambar 2.2 *Wazuh* terbagi atas 2 bagian, yaitu *Wazuh Server* dan *Wazuh Agent*. *Wazuh* Server adalah perangkat yang berfungsi untuk manajemen agen dan dasbor sistem monitoring baik berupa file integritas, *intrusion*, ataupun *log*. *Wazuh Agent* adalah perangkat yang dipasang pada perangkat *end point* untuk pembacaan sistem, pengumpulan log, dan mengirimkan data ke *Wazuh Server*.

Wazuh merupakan arsitektur berbasis *cloud* yang dirancang untuk mengurangi kompleksitas dan juga untuk meningkatkan keamanan sebagai bentuk perlindungan *end point* yang lebih kuat. Penggunaan *Wazuh* sangat penting untuk memastikan *file* ataupun data-data yang bersifat rahasia tetap aman dan terhindar dari perusakan maupun pencurian oleh pelaku kejahatan siber.

Selain kemampuan pemantauan berbasis agen, platform *Wazuh* dapat memantau perangkat tanpa agen seperti *firewall*, *switches*, *routers*, atau *IDS* jaringan. Misalnya, data log sistem dapat dikumpulkan melalui *Syslog*, dan konfigurasinya dapat dipantau melalui pemeriksaan data secara berkala, melalui *SSH* atau melalui *API*.

Perbedaan fitur antara SIEM Wazuh dan SIEM lainnya dapat dilihat dalam tabel hasil survei (Sheeraz et al., 2023). yang mencakup aspek seperti real-time monitoring, threat intelligence, behavior profiling, data dan user monitoring, application monitoring, analytics, log management, updates, reporting, GUI, detailed system description, serta database. Perbandingan ini membantu dalam

memahami keunggulan dan keterbatasan masing-masing sistem untuk menentukan solusi yang paling sesuai dengan kebutuhan keamanan.

Tabel 2. 1 Perbandingan SIEM

Fitur	OSSIM	Wazuh	MozDef	SIEMons	QRadar	Splunk	Securoni	Exabeam	LogRhyt
Real-time monitoring	✓	✓	✓	✓	✓	✓	✓	✓	✓
Threat intelligence	x	✓	x	✓	✓	✓	✓	✓	✓
Behavior profiling	✓	✓	x	✓	✓	✓	✓	✓	✓
Data monitoring	✓	✓	✓	✓	✓	✓	✓	✓	✓
User monitoring	✓	✓	✓	✓	✓	✓	✓	✓	✓
Application monitoring	✓	✓	✓	✓	✓	✓	✓	✓	✓
Analytics	✓	✓	✓	✓	✓	✓	✓	✓	✓

Log management	x	✓	✓	✓	✓	✓	✓	✓	✓
Updates	✓	✓	✓	✓	✓	✓	✓	✓	✓
Reporting	x	✓	x	✓	✓	✓	✓	✓	✓
GUI	x	✓	x	✓	✓	✓	✓	✓	✓
Detailed system description	x	x	x	x	✓	✓	✓	✓	✓
Database	MySQL	MySQL	ES	ES	Ariel	GZip-files	A.Hadoop	ES	SQL-server

Berdasarkan *tabel 2.1* diatas dapat dilihat perbandingan dari beberapa *SIEM Open-source* dan *SIEM* Komersil. Hasil perbandingan menunjukan fitur yang dibandingkan meliputi real-time monitoring, threat intelligence, behavior profiling, log management, analytics, hingga antarmuka GUI. Open-source SIEM, seperti Wazuh, menawarkan fleksibilitas dan biaya rendah dengan fitur yang mencakup log management, threat intelligence, dan GUI yang cukup memadai. Sebaliknya, proprietary SIEM, seperti Splunk dan QRadar, menyediakan fitur yang lebih komprehensif, termasuk analytics dan behavior profiling yang lebih canggih, meskipun membutuhkan biaya lebih besar. Pilihan menggunakan Wazuh

didasarkan pada kombinasi efisiensi biaya, fleksibilitas, dan fitur yang relevan untuk kebutuhan keamanan siber.

2.4 Malware Information Sharing Platform (*MISP*)

MISP merupakan singkatan dari *Malware Information Sharing Platform*, adalah platform intelijen ancaman sumber terbuka yang dirancang untuk memfasilitasi berbagi informasi terkait ancaman keamanan siber. Platform ini dikembangkan oleh *CIRCL (Computer Incident Response Center Luxembourg)* dengan kontribusi dari berbagai pihak lainnya (*MISP*, 2024).

MISP digunakan untuk menyimpan, membagikan, dan menerima informasi tentang *malware*, ancaman, dan kerentanan secara terstruktur. *MISP* digunakan secara luas oleh organisasi di berbagai sektor, termasuk keuangan, perawatan kesehatan, telekomunikasi, pemerintah, dan teknologi, untuk berbagi dan menganalisis informasi tentang ancaman terbaru (Gillard et al., 2023).

2.5 DFIR-IRIS

DFIR IRIS (*Digital Forensics and Incident Response Information Sharing*) Iris adalah platform *open-source* yang dirancang untuk mendukung respons insiden keamanan siber melalui kolaborasi, analisis bukti digital, dan manajemen informasi ancaman (DFIR IRIS, 2023). Platform ini memfasilitasi pengumpulan, analisis, dan berbagi data insiden keamanan untuk meningkatkan efisiensi respons terhadap ancaman siber. *DFIR-IRIS* menawarkan fitur manajemen insiden, pengelolaan bukti digital, dan integrasi dengan alat keamanan lainnya seperti *MISP*, sehingga memungkinkan respons lebih cepat dan terstruktur terhadap ancaman keamanan.

DFIR-IRIS juga mendukung dokumentasi untuk pelaporan dan kepatuhan terhadap regulasi.

2.6 Penelitian Terkait

Penelitian terkait yang menjadi acuan dalam penelitian ini berperan penting dalam memberikan landasan teori serta memperkuat analisis yang dilakukan. Berbagai penelitian sebelumnya digunakan sebagai referensi untuk memahami konsep, metode, serta hasil yang telah dicapai dalam bidang yang relevan. Dengan mengacu pada penelitian-penelitian tersebut, penelitian ini dapat mengidentifikasi kesenjangan penelitian serta mengembangkan pendekatan yang lebih tepat dalam mencapai tujuan yang telah ditetapkan. Rincian penelitian terkait yang digunakan dalam penelitian ini disajikan secara lebih sistematis dalam Tabel 2.2, sehingga memudahkan dalam melihat keterkaitan antara penelitian sebelumnya dengan penelitian yang sedang dilakukan.

Tabel 2. 2 Penelitian Terkait

NO	Penulis	Judul	Hasil Penelitian
1	(Sani, 2023)	Improved Log Monitoring using a Host-based Intrusion Detection System	Hasil penelitian tersebut menunjukkan bahwa penggunaan *WAZUH* sebagai solusi keamanan open-source dapat membantu dalam deteksi ancaman, memberikan pemahaman yang lebih baik terhadap isu yang muncul, serta meningkatkan kinerja sistem untuk

NO	Penulis	Judul	Hasil Penelitian
			deteksi ancaman. Selain itu, integrasi *WAZUH* dengan perangkat lunak antivirus dapat memberikan inspeksi yang lebih mendalam terhadap virus.
2	(Widyatono & Sulistyo, 2023)	Pemodelan Instrusion Prevention System Untuk Pendeteksi Dan Pencegahan Penyebaran Malware Menggunakan *WAZUH*	Hasil dari penelitian ini mencakup pengujian optimalisasi melalui simulasi serangan layanan pada server dan aplikasi web, serta pengujian dengan menghubungkan pengguna ke server untuk memeriksa log yang dikirimkan ke *Wazuh*. Penelitian ini berhasil mendeteki serangan malware namun memerlukan pengujian lebih lanjut.
3	(Spyros et al., 2022)	Towards Continuous Enrichment of Cyber Threat Intelligence: A Study on a Honeypot Dataset	Hasil penelitian menunjukkan hasil yang baik dengan algoritma ensemble machine learning dan bertujuan untuk memperkaya cyber threat intelligence dengan informasi tentang tingkat keparahan kejadian.

NO	Penulis	Judul	Hasil Penelitian
4	(Alanda et al., 2023)	Real-time Defense Against Cyber Threats: Analyzing *WAZUH*'s Effectiveness in Server Monitoring	Hasil penelitian menunjukkan bahwa *WAZUH* efektif dalam pertahanan real-time terhadap ancaman cyber dalam pemantauan server. *WAZUH* mampu mendeteksi integritas file, malware, dan merespons aktif terhadap ancaman.
5	(Murti Adi Santoso et al., 2022)	Monitoring Threats Menggunakan Huntbox dengan Metode MDR (Managed Detection and Response) pada Security Operation Center (SOC)	Hasil penelitian menunjukkan bahwa penggunaan Huntbox dengan metode MDR pada SOC dapat membantu dalam deteksi dan penanganan ancaman cyber. Metode MDR membantu dalam mengelola ancaman dan kerentanan keamanan dengan lebih efisien.
6	(Laksmiati, 2021)	Implementasi *WAZUH* 4.0 Untuk Perlindungan	Hasil pengujian menunjukkan bahwa setiap perubahan dalam registry tercatat dalam event log *WAZUH*. Event log dapat digunakan untuk keperluan

NO	Penulis	Judul	Hasil Penelitian
		Keamanan Integritas File	forensik digital dan pemenuhan standar FIM pada compliance.
7	(Alexandru STAN, 2021)	Automation of Log Analysis Using the Hunting ELK Stack	Penelitian ini membahas pentingnya alat manajemen log dalam keamanan cyber dan menunjukkan penggunaan tumpukan HELK untuk mengotomatisasi analisis log dan perburuan ancaman dalam lingkungan jaringan yang disimulasikan. Tumpukan HELK mencakup alat seperti Elasticsearch, Logstash, dan Kibana untuk mengumpulkan, mengurai, dan menganalisis data log.
8	(Dyan Heluka & Sulistyo, 2023)	Perancangan Dan Implementasi Security Information and Event Management (SIEM) pada Layanan Virtual Server	Hasil dan pembahasan menunjukkan bahwa SIEM *WAZUH* efektif dalam mendeteksi serangan web dan brute force SSH pada server. Diperlukan keterlibatan aktif dari administrator sistem untuk merancang aturan yang terus diperbarui pada SIEM.

NO	Penulis	Judul	Hasil Penelitian
9	(Mycek, 2023)	Monitoring, Management, and Analysis of Security Aspects of IaaS Environments	Penelitian ini membahas implementasi Sistem Deteksi Intrusi (IDS) berbasis cloud menggunakan alat sumber terbuka dan pendekatan Infrastructure as Code (IaC). IDS ini terdiri dari modul untuk pengambilan data, pemrosesan, analisis, peringatan, manajemen, prediksi, respons, dan pelaporan. Sistem ini dirancang untuk memantau dan merespons insiden keamanan di lingkungan cloud, memberikan fleksibilitas dan skalabilitas.
10	(Farrel et al., 2024)	Implementation of Security Information & Event Management (SIEM) *WAZUH* with Active Response and Telegram	mengimplementasikan dan menguji platform *WAZUH* Security Information and Event Management (SIEM) dengan Active Response serta mengintegrasikannya dengan Telegram untuk mendeteksi dan mengatasi serangan brute force pada sistem informasi GT-I2TI Usakti. Hasil pengujian menunjukkan efektivitas

NO	Penulis	Judul	Hasil Penelitian
		Notification for Mitigating Brute Force Attacks on The GT-I2TI USAKTI Information System	solusi yang diimplementasikan dalam mendeteksi dan mengatasi serangan brute force melalui berbagai protokol.
11	(Fernandes et al., 2023)	On the Performance of Secure Sharing of Classified Threat Intelligence between Multiple Entities	Penelitian ini berhasil mengimplementasikan prototipe berbagi intelijen ancaman menggunakan teknik enkripsi yang dapat dicari, menunjukkan peningkatan kinerja melalui sistem caching, dan memastikan kerahasiaan informasi dengan analisis keamanan menggunakan AVISPA.
12	(Anam et al., 2023)	Implementation of Security Information and Event Management (SIEM) for	Penelitian ini menunjukkan bahwa implementasi Alienvault OSSIM sebagai sistem SIEM di Unit Sumber Daya Informasi (USDI) Universitas Udayana efektif untuk memantau dan menganalisis log aset TI selama 3

NO	Penulis	Judul	Hasil Penelitian
		Monitoring IT Assets Using Alienvault OSSIM (Case Study: Udayana University Information Resources Unit)	bulan, mencatat 230.622 kejadian dengan server DNS sebagai penyumbang log terbanyak. Alienvault OSSIM berhasil memberikan notifikasi email real-time kepada administrator tentang potensi serangan atau aktivitas mencurigakan, meskipun tidak ditemukan serangan signifikan dan semua risiko dikategorikan rendah.

2.7 Keterbaruan Penelitian

Kebaruan dari penelitian yang dilakukan yaitu penerapan C*yber Threat Intelligence* pada *SIEM WAZUH* dengan melakukan integrasi *DFIR IRIS* dan *MISP* untuk mempermudah proses *incident response*. Perbedaan dengan penelitian sebelumnya ditunjukan pada tabel 2.2

Tabel 2. 3 Matriks Penelitian

NO	Penelitian	Judul	Ruang Lingkup					
			SIEM		CTI	Incident Response	Skema Serangan	
			WAZUH	Lainya			Malware	Lainya
1	(Sani, 2023)	Improved Log Monitoring using a	✓	-	-	-	-	✓

NO	Penelitian	Judul	Ruang Lingkup					
			SIEM		CTI	Incident Response	Skema Serangan	
			WAZUH	Lainya			Malware	Lainya
		Host-based Intrusion Detection System						
2	(Widyatono & Sulistyo, 2023)	Pemodelan Instrusion Prevention System Untuk Pendeteksi Dan Pencegahan Penyebaran Malware Menggunakan *WAZUH*	✓	-	-	-	✓	
3	(Spyros et al., 2022)	Towards Continuous Enrichment of Cyber Threat Intelligence: A Study on a Honeypot Dataset	-.	✓	✓	-	✓	✓
4	(Alanda et al., 2023)	Real-time Defense Against Cyber Threats: Analyzing *WAZUH*'s Effectiveness in Server Monitoring	✓	-	-	-	✓	✓
5	(Murti Adi Santoso et al., 2022)	Monitoring Threats Menggunakan Huntbox dengan Metode MDR (Managed Detection and Response) pada	-	✓	✓	-	✓	✓

NO	Penelitian	Judul	Ruang Lingkup					
			SIEM		CTI	Incident Response	Skema Serangan	
			WAZUH	Lainya			Malware	Lainya
		Security Operation Center (SOC)						
6	(Laksmiati, 2021)	IMPLEMENTASI *WAZUH* 4.0 UNTUK PERLINDUNGAN KEAMANAN INTEGRITAS FILE	. ✓	-	-	-	-	✓
7	(Alexandru STAN, 2021)	Automation of Log Analysis Using the Hunting ELK Stack	.-	-	✓	✓	-	✓
8	(Dyan Heluka & Sulistyo, 2023)	Perancangan Dan Implementasi Security Information and Event Management (SIEM) pada Layanan Virtual Server	✓.	-	-	-	-	✓
9	(Mycek, 2023)	Monitoring, Management, and Analysis of Security Aspects of IaaS Environments	. ✓	-	-	-	-	✓
10	(Farrel et al., 2024)	Implementation of Security Information & Event Management (SIEM) *WAZUH* with Active	. ✓	-	-	-	-	✓

NO	Penelitian	Judul	Ruang Lingkup					
			SIEM		CTI	Incident Response	Skema Serangan	
			WAZUH	Lainya			Malware	Lainya
		Response and Telegram Notification for Mitigating Brute Force Attacks on The GT-I2TI USAKTI Information System-						
11	(Fernandes et al., 2023)	On the Performance of Secure Sharing of Classified Threat Intelligence between Multiple Entities	-	-	✓	-	-	✓
12	(Anam et al., 2023)	Implementation of Security Information and Event Management (SIEM) for Monitoring IT Assets Using Alienvault OSSIM (Case Study: Udayana University Information Resources Unit)	-	✓	-	-	-	✓
13	Our Research		✓	-	✓	✓	✓	-