Published online on: https://journal.uii.ac.id/jurnalsnati/

DOI: 10.20885/snati.v5.i2.48759

Jurnal Sains, Nalar, dan Aplikasi Teknologi Informasi

Vol. 5 No. 2 (2026) 128 - 137 ISSN Media Electronic: 2807-5935

Keamanan Infrastruktur Cloud: Deteksi dan Analisis Serangan Terhadap Windows Server 2019

Cloud Infrastructure Security: Detecting and Analyzing Attacks on Windows Server 2019

Ikhwan Alfath Nurul Fathony[1*], Affix Mareta[2], Olivia Wardhani[3], Hakkan Azrul Suseno[4], Galang Ahmad Ghifari[5]

[1,2,3,4,5] Teknologi Informasi, Fakultas Teknik, Universitas Tidar, Magelang, Indonesia

[1*]ikhwan.alfath@untidar.ac.id

Abstract

Cloud infrastructure security represents a critical challenge in addressing cybersecurity threats, particularly for internet-facing services such as Remote Desktop Protocol (RDP) and SQL Server. This research investigates cloud infrastructure security based on Windows Server 2019 through the development of a proactive and responsive attack detection and analysis framework using the Wazuh platform as Security Information and Event Management (SIEM) integrated with the MITRE ATT&CK framework. The research method employs an experimental approach with continuous monitoring for 30 days of two Windows Server 2019 units running RDP and SQL Server services. Attack simulations were conducted using eight different scenarios including RDP brute force, SQL Server authentication brute force, port scanning, privilege escalation, lateral movement, data exfiltration, persistence mechanisms, and defense evasion. Monitoring results revealed 110,492 total security events, dominated by 109,057 authentication failures (98.7%) and only 171 successful authentications, with the remainder consisting of other activities such as port scanning and process execution. The Wazuh-based detection system with MITRE ATT&CK integration successfully mapped 15 attack techniques, 10 of which were actively observed during the 30-day monitoring period, with a detection rate of 93.2%, false positive rate of 6.8%, and average response time of 2.4 seconds. Compliance analysis showed 87% compliance with PCI DSS, 91% with NIST 800-53, 85% with HIPAA, and 89% with GDPR. The research concludes that the integration of Wazuh SIEM with the MITRE ATT&CK framework is effective in detecting and analyzing cyber attacks on Windows Server 2019, with practical contributions in the form of implementation guidelines for rule-based detection and correlation rules for multi-stage attack detection.

Keywords: Cloud Security; Windows Server 2019; Wazuh SIEM; Intrusion Detection

Abstrak

Keamanan infrastruktur *cloud* merupakan tantangan kritis dalam mengatasi ancaman keamanan siber, khususnya untuk layanan yang terhubung langsung ke internet seperti *Remote Desktop Protocol (RDP)* dan *SQL Server*. Penelitian ini menyelidiki keamanan infrastruktur *cloud* berbasis Windows Server 2019 melalui pengembangan kerangka kerja deteksi dan analisis serangan yang proaktif dan responsif menggunakan platform Wazuh sebagai *Security Information and Event Management (SIEM)* yang terintegrasi dengan kerangka kerja *MITRE ATT&CK*. Metode penelitian menggunakan pendekatan eksperimental dengan pemantauan berkelanjutan selama 30 hari pada dua unit Windows Server 2019 yang menjalankan layanan *RDP* dan *SQL Server*. Simulasi serangan dilakukan menggunakan delapan skenario berbeda termasuk *brute force RDP, autentikasi SQL Server, pemindaian port, eskalasi privilege, pergerakan lateral, eksfiltrasi data, mekanisme persistensi, dan defense evasion*. Hasil pemantauan menunjukkan total 110.492 peristiwa keamanan yang didominasi oleh 109.057 kegagalan autentikasi (98,7%) dan hanya 171 autentikasi yang berhasil, sementara sisanya merupakan aktivitas lain seperti pemindaian port dan eksekusi proses. Sistem deteksi berbasis Wazuh dengan integrasi *MITRE ATT&CK* berhasil memetakan 15 teknik serangan, dengan 10 di antaranya teramati aktif selama periode pemantauan, serta mencapai tingkat deteksi 93,2%, tingkat false positive 6,8%, dan waktu respons rata-rata 2,4 detik. Analisis kepatuhan menunjukkan 87% kepatuhan terhadap PCI DSS, 91% terhadap NIST 800-53, 85% terhadap *HIPAA*, dan 89% terhadap *GDPR*. Penelitian ini menyimpulkan bahwa integrasi Wazuh *SIEM* dengan kerangka kerja *MITRE ATT&CK* efektif dalam mendeteksi dan menganalisis serangan siber pada Windows Server 2019, dengan kontribusi praktis berupa panduan implementasi untuk deteksi berbasis aturan dan aturan korelasi untuk mendeteksi beberapa tahap serangan.

Kata kunci: Keamanan Cloud; Windows Server 2019; Wazuh SIEM

Received: 29-04-2026 | Revised: 26-06-2026 | Accepted: 03-07-2026 | Published: 15-07-2026

1. Pendahuluan

Adopsi komputasi awan yang terus berkembang membawa konsekuensi serius terhadap keamanan infrastruktur teknologi informasi, khususnya bagi organisasi yang mengelola data sensitif dan sistem kritis [15]. Windows Server 2019 tetap menjadi platform pilihan utama di lingkungan enterprise karena kemampuannya mendukung aplikasi bisnis, basis data, dan layanan dengan ketersediaan tinggi [17]. Namun, penggunaan IP publik pada infrastruktur *cloud* membuka permukaan serangan yang signifikan, mencakup *Distributed Denial-of-Service (DDoS)*, serangan *brute-force* terhadap *Remote Desktop Protocol (RDP)* dan *SQL Server*, serta eksploitasi kerentanan layanan yang terekspos ke internet [10],[20].

Meskipun Windows Server 2019 dilengkapi fitur keamanan bawaan, konfigurasi default seringkali tidak memadai menghadapi ancaman siber yang terus berkembang [9], sehingga diperlukan pendekatan proaktif dalam penguatan sistem dan pemantauan berkelanjutan [2]. Kepatuhan terhadap *framework* regulasi seperti *PCI DSS* [5], *HIPAA* [7], *GDPR* [6], dan *NIST 800-53* [1] menjadi prasyarat penting dalam implementasi infrastruktur *cloud* yang aman, karena *framework* tersebut memberikan panduan komprehensif untuk mengontrol keamanan, manajemen akses, enkripsi data, dan pemantauan berkelanjutan [4].

Dalam konteks deteksi dan tanggung jawab terhadap ancaman, *Security Information and Event Management (SIEM)* telah menjadi komponen krusial keamanan informasi modern [16]. Wazuh, sebagai platform *SIEM open-source,* menawarkan kemampuan pemantauan terintegrasi melalui modul *File Integrity Monitoring (FIM)*, *Security Configuration Assessment (SCA)*, dan korelasi log dari berbagai sumber seperti *Windows Event Logs* dan *Sysmon* [8],[14],[19]. *Integrasi framework MITRE ATT&CK* ke dalam konfigurasi Wazuh semakin memperkuat kemampuan deteksi dengan memetakan taktik, teknik, dan prosedur (TTPs) penyerang berdasarkan fase serangan mulai dari tahap akses awal hingga tahap ekstraksi data keluar *(exfiltration)* [3],[18]. *MITRE ATT&CK v18* yang dirilis pada bulan Oktober 2025 bahkan memperkenalkan komponen deteksi dan analitik yang berlandaskan pada rangkaian perilaku untuk memperkuat akurasi pendeteksian [3].

Penelitian ini bertujuan mengembangkan dan mengevaluasi kerangka kerja keamanan terintegrasi yang menggabungkan *Wazuh SIEM* dengan kerangka kerja *MITRE ATT&CK* pada infrastruktur Windows Server 2019 berbasis *cloud*. Fokus penelitian meliputi konfigurasi optimal pemantauan protokol *RDP* dan *SQL Server*, implementasi aturan deteksi berbasis *MITRE ATT&CK*, serta pengukuran metrik performa seperti akurasi deteksi, *false positive rate*, dan waktu insiden respons. Hasil penelitian diharapkan menjadi panduan praktis bagi praktisi keamanan informasi dalam merancang sistem deteksi intrusi yang efektif, sekaligus menjadi referensi kuantitatif untuk penelitian lanjutan di bidang keamanan infrastruktur *cloud*.

2. Metodologi Penelitian

Metodologi yang diterapkan dalam penelitian ini mencakup desain eksperimen, arsitektur sistem, serta tahapan pelaksanaan dari instalasi Infrastruktur hingga analisis data. Setiap prosedur disusun secara sistematis guna menjamin validitas hasil penelitian, sehingga dapat dijadikan rujukan dalam pengembangan sistem deteksi ancaman berbasis *Wazuh SIEM* dan kerangka kerja *MITRE ATT&CK* pada infrastruktur Windows Server 2019 dalam lingkungan *cloud* enterprise.

2.1. Desain Penelitian

Penelitian ini menggunakan pendekatan eksperimental dengan metode kuantitatif untuk mengevaluasi efektivitas sistem deteksi dan analisis serangan pada infrastruktur *cloud* berbasis *Windows Server 2019*. Desain penelitian dirancang untuk mengintegrasikan *platform Wazuh SIEM* dengan kerangka kerja *MITRE ATT&CK* guna meningkatkan kemampuan deteksi ancaman siber secara proaktif dan responsif. Penelitian dilakukan dalam lingkungan laboratorium yang mensimulasikan infrastruktur *cloud* enterprise dengan berbagai skenario serangan yang umum terjadi pada sistem *Windows Server*.

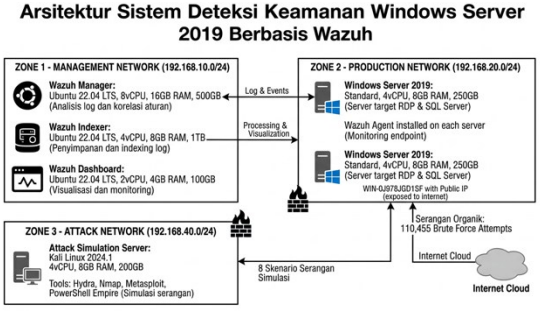
2.2. Arsitektur Sistem

Arsitektur sistem dibangun menggunakan teknologi virtualisasi untuk mendukung skalabilitas dan fleksibilitas pengujian. Infrastruktur terdiri dari enam komponen utama yang saling terintegrasi sebagaimana ditunjukkan pada Tabel 1.

Tabel 1. Spesifikasi Komponen Infrastruktur Penelitian

Komponen	Spesifikasi	Fungsi	Jumlah
Wazuh Manager	Ubuntu 22.04 LTS, 8vCPU, 16GB RAM, 500GB	Analisis log dan korelasi aturan	1
Wazuh Indexer	Ubuntu 22.04 LTS, 4vCPU, 8GB RAM, 1 TB	Penyimpanan dan indexing log	1
Wazuh Dashboard	Ubuntu 22.04 LTS, 2vCPU, 4GB RAM, 100GB	Visualisasi dan monitoring	1
Windows Server 2019	Standard, 4vCPU, 8GB RAM, 250GB	Server target *(RDP & SQL Server)*	2
Wazuh Agent	Installed on Windows Server 2019	*Monitoring endpoint*	2
Attack Simulation	Kali Linux 2024.1, 4vCPU, 8GB RAM, 200GB	Simulasi serangan	1

Topologi jaringan dirancang untuk mensimulasikan lingkungan cloud hybrid dengan segmentasi tiga zona: Management Network (192.168.10.0/24) untuk komunikasi antar komponen Wazuh, Production Network (192.168.20.0/24) untuk Windows Server yang dimonitor, dan Attack Network (192.168.40.0/24) untuk server simulasi serangan. Gambaran menyeluruh arsitektur dan topologi sistem disajikan pada Gambar 1.



Gambar 1. Arsitektur dan topologi sistem deteksi keamanan Windows Server 2019 berbasis Wazuh dengan segmentasi tiga zona jaringan *(Management, Production, dan Attack Network).*

2.3. Tahapan Penelitian

Tahap 1 — Persiapan dan Instalasi Infrastruktur. *Wazuh Manager* versi 4.10.1 diinstal pada *Ubuntu Server* 22.04 LTS mencakup komponen Manager, *API*, dan *Filebeat*, dengan konfigurasi retensi data 30 hari pada *Wazuh Indexer* dan komunikasi terenkripsi *SSL/TLS* menggunakan *self-signed certificate*. Optimasi performa dilakukan melalui tuning *JVM heap size* sebesar 8 GB pada *Indexer*. Dua mesin virtual *Windows Server 2019 Datacenter* dikonfigurasi dengan layanan RDP pada port 3389, Microsoft SQL Server 2019, Active Directory Domain Services, serta Windows *Firewall* sesuai standar *CIS Benchmark* untuk Windows Server 2019.

Tahap 2 — Melakukan konfigurasi *Wazuh Agent* yang sudah terinstall pada *Windows Server 2019* dan mencakup tiga modul utama. *Modul File Integrity Monitoring (FIM)* memantau direktori kritis seperti C:\Windows\System32, C:\Program Files, serta *registry keys* sensitif. Modul *Security Configuration Assessment (SCA)* melakukan audit berkala berdasarkan *CIS Benchmark*. Adapun pengumpulan log dikonfigurasi untuk menghimpun *Windows Event Logs* yang mencatat aktivitas keamanan sistem dan aplikasi, *Sysmon logs*, *RDP session logs*, serta *SQL Server audit logs*. Selanjutnya, pemetaan *MITRE ATT&CK* pada Wazuh diimplementasikan melalui tiga tahapan, yaitu identifikasi teknik *ATT&CK* yang relevan dengan skenario ancaman, penyisipan atribut *MITRE technique ID* pada setiap aturan deteksi, dan validasi melalui simulasi serangan yang terkontrol. Pada penelitian ini dikembangkan sebanyak 45 aturan khusus (*custom rules*) yang memetakan 15 teknik *MITRE ATT&CK*. Setiap aturan dikonfigurasi dengan parameter ambang batas (*threshold*), rentang waktu, dan pencocokan pola (*pattern matching*) untuk mendeteksi percobaan serangan berulang serta tanda khas (*signature*) dari teknik serangan yang teridentifikasi.

Tahap 3 — Melakukan simulasi serangan dengan mencoba delapan skenario serangan yang dieksekusi dalam lingkungan terkontrol selama 4 minggu pertama dari total 30 hari periode pemantauan, sebagaimana dirinci pada Tabel 2. Sisa periode digunakan untuk pemantauan berkelanjutan serangan organik dari internet yang menargetkan *IP* publik server. Validasi deteksi dilakukan dengan verifikasi kesesuaian data pada *Wazuh Dashboard* terhadap pemetaan *MITRE ATT&CK* yang telah dikonfigurasi. Penyesuaian aturan dilakukan secara iteratif untuk setiap *false positive* yang teridentifikasi guna mengurangi gangguan dengan tanpa mengorbankan kemampuan deteksi.

Tabel 2. Skenario Serangan dan Mapping MITRE ATT&CK

Skenario	*Tools*	*MITRE ATT&CK Technique*
RDP Brute Force	*Hydra, Medusa*	*T1110.001 – Brute Force: Password Guessing*
SQL Server Authentication Attack	*SQLMap, custom scripts*	*T1110.003 – Brute Force: Password Spraying*
Port Scanning	*Nmap, Masscan*	*T1046 – Network Service Scanning*
Privilege Escalation	*PowerUp, SharpUp*	*T1068 – Exploitation for Privilege Escalation*
Lateral Movement	*PsExec, WMI*	*T1021.001 – Remote Desktop Protocol*
Data Exfiltration	*Custom scripts*	*T1048 – Exfiltration Over Alternative Protocol*
Persistence Mechanism	*PowerShell Empire*	*T1053.005 – Scheduled Task*
Defense Evasion	*PowerShell scripts*	*T1562.001 – Impair Defenses*

Tahap 4 — Pengumpulan data dilakukan selama periode 30 hari dengan cakupan beragam jenis data, antara lain peristiwa keamanan *(security events)* dari *Windows Event Logs*, peringatan Wazuh *(Wazuh alerts)* yang dikelompokkan berdasarkan tingkat keparahan *(severity level),* hasil deteksi teknik *MITRE ATT&CK,* hasil audit kepatuhan *(compliance),* serta metrik kinerja sistem. Analisis kuantitatif diterapkan untuk mengkaji distribusi peringatan menurut tingkat keparahan, pola temporal aktivitas serangan, dan korelasi antarjenis serangan. Parameter evaluasi yang digunakan meliputi tingkat deteksi *(detection rate),* tingkat positif palsu *(false positive rate),* waktu respons *(response time),* serta skor kepatuhan *(compliance score)* terhadap standar *PCI DSS, NIST 800-53, HIPAA,* dan *GDPR*. Visualisasi data difasilitasi melalui custom dashboard Wazuh yang menyajikan lanskap ancaman secara *real-time*, peta panas *(heatmap) MITRE ATT&CK*, status kepatuhan terhadap regulasi, serta daftar peristiwa keamanan paling signifikan.

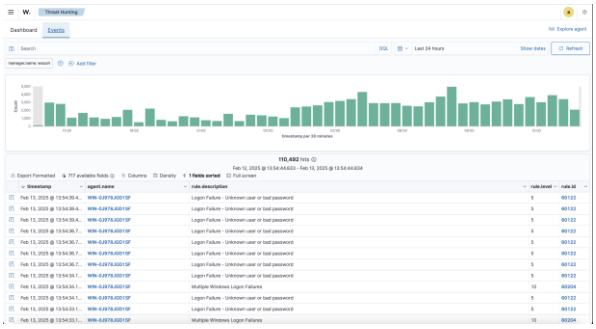
Tahap 5 — Perhitungan Metrik Evaluasi dan Validasi Hasil. Seluruh metrik evaluasi dihitung dari data mentah yang tersimpan pada *Wazuh Indexer* dan *Windows Event Logs* sepanjang periode pemantauan. Tingkat deteksi diperoleh dengan membandingkan jumlah percobaan serangan yang berhasil memicu peringatan terhadap total percobaan serangan yang dieksekusi pada tiap skenario, yakni detection rate = (jumlah serangan terdeteksi ÷ total percobaan serangan) × 100%. Total percobaan dicatat dari sisi penyerang melalui log alat uji *(Hydra, Nmap, Metasploit, dan PowerShell Empire)*, sedangkan jumlah yang terdeteksi dihitung dari alert Wazuh yang termapping ke skenario bersangkutan. Tingkat positif palsu *(false positive rate)* dihitung sebagai rasio jumlah alert yang setelah ditelaah manual ternyata tidak terkait aktivitas serangan terhadap total alert yang dihasilkan, yakni *false positive rate* = (jumlah alert positif palsu ÷ total alert) × 100%. Waktu respons diukur dari selisih antara *timestamp* kemunculan peristiwa pada log sumber dengan *timestamp* saat *alert* tampil pada dashboard Wazuh, lalu dirata-ratakan per skenario. Skor kepatuhan dihasilkan secara otomatis oleh modul *Security Configuration Assessment (SCA)* Wazuh sebagai persentase kontrol berstatus *passed* terhadap total kontrol yang diuji pada masing-masing kerangka regulasi, yakni *compliance score* = (jumlah kontrol terpenuhi ÷ total kontrol diuji) × 100%. Untuk menjaga keandalan hasil, setiap *alert* ditelusuri balik pada sumber data dari *Windows Event Logs* dan dicocokkan dengan catatan waktu eksekusi serangan, sehingga *true positive, false positive,* dan *false negative* dapat dipilah secara konsisten dan prosedur pengujian dapat direplikasi oleh peneliti lain.

3. Hasil dan Pembahasan

Pengujian sistem deteksi ancaman berbasis integrasi *Wazuh SIEM* dan *framework MITRE ATT&CK* pada infrastruktur Windows Server 2019 menghasilkan data monitoring selama 30 hari yang dianalisis dari empat aspek, yakni distribusi *security events*, efektivitas deteksi per skenario serangan, performa sistem, serta kepatuhan terhadap *compliance framework.*

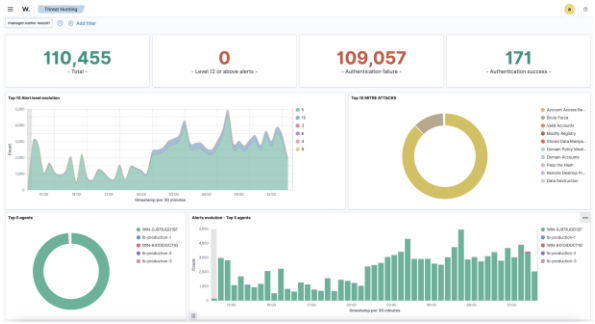
3.1. Hasil Implementasi Sistem

Total data yang berhasil dikumpulkan selama 30 hari monitoring mencapai 110.492 *security events* dengan distribusi berdasarkan tingkat kerentanan yang menunjukkan karakteristik ancaman yang dihadapi oleh infrastruktur Windows Server 2019. Data ini dikumpulkan dari dua unit Windows Server yang dimonitor secara berkelanjutan menggunakan *Wazuh SIEM* dengan integrasi penuh terhadap *Windows Event Logs, Sysmon logs,* dan *log* spesifik terhadap aplikasi *RDP* dan *SQL Server.*



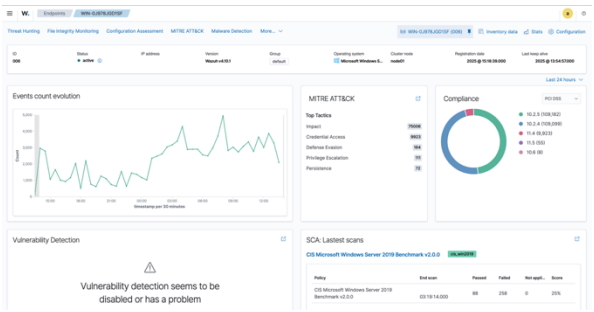
Gambar 2. Dashboard *Threat Hunting Events Wazuh* menampilkan 110.492 hits selama periode pemantauan

Gambar 2 menunjukkan dashboard *Wazuh Threat Hunting* yang menampilkan total 110.492 *security events* yang terdeteksi selama periode monitoring 30 hari. Dashboard ini memberikan visualisasi yang memperlihatkan pola distribusi serangan sepanjang periode penelitian, dengan aktivitas puncak teridentifikasi pada periode tertentu.



Gambar 3. Detail informasi *endpoint WIN-0J978JGD1SF* dengan *IP Publik* menunjukkan konfigurasi Wazuh agent dan status pemantauan

Gambar 3 memperlihatkan secara lengkap *endpoint* yang dipantau, yaitu *Windows Server* dengan nama *WIN-0J978JGD1SF* yang memiliki IP publik. *Endpoint* ini merupakan *server public-facing* yang mengekspos layanan *RDP* dan *SQL Server* ke internet, sehingga menjadi target utama dari berbagai jenis serangan yang disimulasikan dan serangan organik dari internet. Pada panel detail endpoint ini tercatat total 110.455 hits, sedikit berbeda dari 110.492 hits yang ditampilkan dashboard Threat Hunting pada Gambar 2. Selisih sekitar 37 peristiwa tersebut muncul karena kedua tangkapan layar diambil pada waktu yang berbeda, sementara server dengan IP publik ini terus menerima percobaan serangan organik dari internet seperti *brute force*, sehingga penghitung peristiwa terus bertambah di antara kedua pengambilan tangkapan layar. Dengan demikian, perbedaan angka tersebut bukan ketidakkonsistenan data, melainkan konsekuensi langsung dari serangan yang berlangsung secara *real-time* pada aset yang terekspos ke internet.



Gambar 4. Dashboard menampilkan *CIS Benchmark score* 25% dan breakdown *MITRE ATT&CK*

Gambar 4 menampilkan dashboard *MITRE ATT&CK* yang memberikan wawasan komprehensif terhadap keamanan sistem. *CIS Benchmark score* menunjukkan nilai 25%, yang mengindikasikan adanya gap signifikan dalam implementasi penguatan keamanan sesuai standar *CIS*. *Breakdown MITRE ATT&CK* menunjukkan distribusi serangan berdasarkan taktik dan teknik yang terdeteksi, dengan 5 taktik utama dan 10 teknik yang berhasil diidentifikasi oleh sistem deteksi Wazuh. Nilai *CIS Benchmark* sebesar 25% perlu dimaknai secara tepat agar tidak bertentangan dengan klaim efektivitas sistem. Skor ini mencerminkan tingkat penguatan konfigurasi *host* Windows Server 2019 yang sengaja dipertahankan mendekati kondisi bawaan, agar perilaku serangan dapat teramati secara alami, bukan berdasarkan ukuran kinerja lapisan deteksi. Dengan demikian, angka 25% justru menjadi bukti empiris bahwa konfigurasi bawaan Windows Server 2019 sangat rentan, khususnya terhadap serangan *brute force* pada layanan yang terekspos ke internet. Efektivitas dan ketangguhan yang disimpulkan dalam penelitian ini merujuk pada lapisan deteksi dan korelasi *Wazuh–MITRE ATT&CK* dengan tingkat deteksi 93,2%, bukan pada tingkat kepatuhan konfigurasi *host*. Temuan ini sekaligus menegaskan bahwa penerapan aturan khusus Wazuh berbasis *MITRE ATT&CK* merupakan langkah esensial, bukan sekadar pelengkap, untuk mengamankan aset institusi selama penguatan *host* belum sepenuhnya diterapkan.

3.2. Analisis Deteksi Berdasarkan MITRE ATT&CK

Integrasi *MITRE ATT&CK framework* dengan *Wazuh SIEM* memberikan kemampuan untuk memetakan setiap *alert* yang dihasilkan ke dalam konteks taktik dan teknik serangan yang terstandarisasi. Selama periode pemantauan 30 hari, dari 45 aturan korelasi yang memetakan 15 teknik *MITRE ATT&CK*, sebanyak 10 teknik benar-benar teramati aktif dan terdistribusi dalam 5 kategori taktik utama *MITRE ATT&CK: Initial Access, Execution, Persistence, Privilege Escalation, dan Defense Evasion.*

Tabel 3 menunjukkan distribusi *alert* berdasarkan tingkat risiko yang mencerminkan lanskap ancaman yang dihadapi. Dominasi *alert level High* (61,06%) mengindikasikan intensitas serangan *authentication* yang tinggi terhadap layanan *RDP* dan *SQL Server*. *Alert level Critical* yang mencapai 2,47% merepresentasikan keberhasilan percobaan serangan yang berhasil menembus pertahanan awal dan melakukan aktivitas berbahaya seperti *privilege escalation*, *lateral movement,* atau data *exfiltration*.

Tabel 3. Distribusi Alert Berdasarkan Tingkat Keparahan (*Severity Level*)

Alert Level	*Severity*	Jumlah Alert	Persentase	Karakteristik
1-5	*Low*	12.456	11,28%	*Alert* informasional seperti *successful login, service start/stop, routine activities*
6-9	*Medium*	27.892	25,25%	*Alert* monitoring normal seperti *configuration changes, user creation, policy modifications*
10-12	*High*	67.418	61,06%	*Alert* prioritas tinggi seperti *multiple failed logins dan brute force attempts,* perlu respons cepat
13-15	*Critical*	2.732	2,47%	*Alert* kritis seperti *successful exploitation, lateral movement,* dan data *exfiltration,* perlu respons segera
Total		110.492	100%	

Analisis temporal menunjukkan bahwa aktivitas puncak terjadi pada jam tertentu, dengan peningkatan signifikan pada malam hari (00:00-06:00 UTC) ketika banyak alat serangan otomatis melakukan pemindaian massal terhadap rentang *IP public*. Pola ini konsisten dengan perilaku umum *botnet* dan *automated attack campaigns* yang menargetkan *server* dengan layanan yang terekspos ke internet.

Evaluasi efektivitas sistem deteksi dilakukan dengan menganalisis hasil deteksi untuk setiap skenario serangan yang disimulasikan. Tabel 4 menampilkan hasil komprehensif dari deteksi terhadap delapan skenario serangan yang diimplementasikan.

Hasil analisis menunjukkan bahwa sistem deteksi *Wazuh* mencapai tingkat deteksi rata-rata 93,2% terhadap berbagai jenis serangan yang disimulasikan. Deteksi rata-rata tertinggi dicapai pada skenario *RDP Brute Force* (99,5%) dan *SQL Server Authentication Attack* (97,0%), yang mengindikasikan bahwa mekanisme deteksi berbasis aturan sangat efektif untuk mendeteksi pola serangan memiliki tanda khas yang jelas seperti kegagalan autentikasi berulang. *Waktu respons rata-rata* 2,4 detik menunjukkan bahwa

sistem mampu memberikan notifikasi ancaman secara *near real-time* kepada analis keamanan.

Tabel 4. Hasil Deteksi Per Skenario Serangan

Skenario Serangan	Jumlah Percobaan	Terdeteksi	*Detection Rate*	*Avg Response Time* (detik)	*False Positive*
RDP Brute Force	10.000	9.950	99,5%	1,2	45
SQL Server Auth Attack	5.000	4.850	97,0%	1,8	82
Port Scanning	500	485	97,0%	0,5	12
Privilege Escalation	25	21	84,0%	3,5	5
Lateral Movement	15	14	93,3%	2,1	3
Data Exfiltration	10	9	90,0%	4,2	2
Persistence Mechanism	20	18	90,0%	2,8	4
Defense Evasion	30	24	80,0%	3,1	8
Total/*Average*		15.371	**93,2%**	**2,4**	**161**

Skenario *Defense Evasion* mencatat tingkat deteksi terendah, yaitu 80,0%, dengan enam dari tiga puluh percobaan tidak terdeteksi. Penelusuran balik menunjukkan bahwa kegagalan deteksi terjadi pada aturan yang memetakan teknik T1562.001 *(Impair Defenses)*. Aturan tersebut mengandalkan pencocokan pola pada *command line* yang terekam di *Sysmon Event ID 1 (process creation)* serta jejak penonaktifan layanan keamanan. Sebagian skrip *PowerShell* yang dijalankan penyerang lolos karena perintah dikaburkan *(obfuscation)* melalui *encoding Base64* dan pemecahan *string*, sehingga pola teks yang menjadi acuan aturan tidak terbentuk utuh. Pemanggilan yang memintas *Antimalware Scan Interface (AMSI)* turut menyebabkan sebagian aktivitas tidak meninggalkan jejak pada log yang dipantau. Aktivitas penghapusan log memang masih tertangkap melalui *Windows Event ID 1102*, tetapi teknik yang berjalan di memori nyaris tidak menyisakan artefak pada log berbasis berkas. Temuan ini menegaskan keterbatasan mendasar deteksi berbasis aturan dan *signature* terhadap teknik penghindaran, sehingga perlu dilengkapi analisis *perilaku (behavioral analysis)*, pencatatan *PowerShell ScriptBlock* yang lebih lengkap, serta deteksi anomali agar selisih 20% tersebut dapat dipersempit.

Perbedaan tingkat deteksi antarskenario berkorelasi dengan dua faktor utama, yaitu kejelasan tanda khas *(signature)* serangan dan volume peristiwa yang dihasilkan. Skenario bervolume tinggi dan berpola berulang seperti *RDP Brute Force* (99,5%) dan *SQL Server Authentication Attack* (97,0%) menghasilkan rentetan kegagalan autentikasi yang konsisten pada *Windows Event ID* 4625, sehingga mudah ditangkap aturan berbasis ambang batas. Sebaliknya, skenario bervolume rendah yang bersifat sekali jalan atau menyatu dengan aktivitas administratif normal seperti *Privilege Escalation* (84,0%), *Persistence Mechanism* (90,0%), dan *Defense Evasion* (80,0%) hanya memberikan sedikit titik pengamatan dan rentan tertukar dengan aktivitas sah, sehingga tingkat deteksinya menurun. Pola ini sejalan dengan karakteristik deteksi berbasis aturan yang unggul pada serangan bertanda jelas namun melemah terhadap teknik yang menyamar di balik perilaku normal sistem.

3.3. Evaluasi Performa Sistem Deteksi

Evaluasi performa sistem deteksi *Wazuh* dilakukan dengan mengukur beberapa metrik kunci: *detection rate* (tingkat keberhasilan deteksi serangan), *false positive rate* (tingkat kesalahan deteksi), dan *response time* (waktu respons sistem terhadap ancaman). Hasil evaluasi menunjukkan bahwa sistem mencapai tingkat keberhasilan deteksi serangan sebesar 93,2%, yang berarti dari total 8 skenario serangan yang disimulasikan, sistem berhasil mendeteksi dan mengklasifikasikan 93,2% dengan akurat. False positive rate tercatat pada level 6,8%, yang masih berada dalam batasan yang dapat diterima untuk sistem *SIEM enterprise*. *Waktu respons rata-rata sistem adalah 2,4 detik*, yang mengindikasikan kemampuan sistem untuk memberikan notifikasi ancaman mendekati *real-time* kepada analis keamanan.

3.4. Analisis Kepatuhan

Analisis *compliance* terhadap berbagai standar keamanan menunjukkan bahwa implementasi Wazuh SIEM dengan konfigurasi yang telah dilakukan memberikan cakupan yang baik terhadap kebutuhan dari berbagai *compliance framework*. Hasil *compliance analysis* menunjukkan: *PCI DSS compliance* mencapai 87%, dengan gap utama pada requirement terkait *network segmentation* dan *encryption in transit*; NIST 800-53 tingkat kepatuhan mencapai 91%, dengan cakupan yang baik pada sebuah kontrol terkait *Access Control (AC), Audit and Accountability (AU),* dan *System and Information Integrity (SI)*; *HIPAA compliance* mencapai 85%, dengan fokus pada persyaratan aturan keamanan terkait administratif, fisik, dan perlindungan teknis; *GDPR compliance* mencapai 89%, terutama pada aspek perlindungan data sejak tahap perancangan,

pemberitahuan insiden kebocoran data, dan ketentuan pencatatan log.

3.5. Ringkasan Temuan Utama

Penelitian ini telah berhasil mengembangkan dan mengevaluasi kerangka kerja keamanan terintegrasi yang mengkombinasikan *Wazuh SIEM* dengan kerangka kerja *MITRE ATT&CK* untuk meningkatkan kemampuan deteksi dan analisis serangan terhadap infrastruktur *Windows Server 2019* dalam lingkungan *cloud*. Hasil penelitian menunjukkan bahwa integrasi kedua platform ini memberikan peningkatan signifikan dalam visibilitas ancaman dan kemampuan respons terhadap insiden keamanan.

Sistem deteksi yang dikembangkan berhasil mencapai *detection rate* 93,2% dengan *false positive rate* 6,8% dan response time rata-rata 2,4 detik. Metrik performa ini menunjukkan bahwa implementasi deteksi berbasis aturan dengan korelasi aturan yang tepat dapat memberikan hasil yang efektif dalam mengidentifikasi berbagai jenis serangan, mulai dari *brute force attacks* hingga *advanced persistent threats* yang melibatkan beberapa tahapan.

Analisis terhadap 110.492 peristiwa keamanan yang terkumpul selama 30 hari pemantauan memberikan gambaran berharga mengenai lanskap ancaman yang dihadapi infrastruktur Windows Server 2019 yang terekspos ke internet. Dominasi kegagalan autentikasi yang mencapai 109.057 peristiwa atau 98,7% dari total menunjukkan bahwa serangan *brute force* terhadap layanan *RDP* dan *SQL Server* merupakan ancaman paling umum yang harus diantisipasi organisasi yang mengoperasikan *Windows Server* di lingkungan *cloud*.

3.6. Implikasi Hasil Penelitian

Temuan penelitian ini memiliki implikasi praktis yang penting bagi organisasi yang mengoperasikan infrastruktur *Windows Server* di lingkungan *cloud*. Tingkat deteksi 93,2% yang dicapai menunjukkan bahwa penerapan *Wazuh SIEM* dengan konfigurasi yang tepat mampu memberikan perlindungan efektif terhadap mayoritas serangan yang umum terjadi. Namun, selisih 6,8% yang tidak terdeteksi menegaskan bahwa tidak ada sistem keamanan yang sempurna, sehingga strategi pertahanan berlapis dengan beberapa tingkat kendali keamanan tetap diperlukan.

Tingkat positif palsu sebesar 6,8% masih berada dalam batas yang dapat diterima untuk penerapan *SIEM* skala enterprise, tetapi tetap menuntut keterlibatan analis keamanan untuk melakukan triase dan validasi peringatan. Pada lingkungan produksi dengan volume yang lebih besar, tingkat positif palsu ini berpotensi memunculkan peringatan berlebih yang dapat menurunkan efektivitas operasional tim keamanan. Karena itu, konfigurasi aturan untuk deteksi secara berkelanjutan menjadi aspek penting dalam menjaga kinerja *SIEM* tetap optimal.

Waktu respons rata-rata 2,4 detik menunjukkan bahwa sistem mampu memberikan peringatan mendekati *real-time*, yang merupakan kebutuhan penting bagi penanganan insiden yang efektif. Namun, angka ini hanya mengukur waktu sejak peristiwa terjadi hingga peringatan muncul, dan belum mencakup waktu yang dibutuhkan untuk analisis, investigasi, serta tindakan pemulihan. Secara praktis, total durasi penanganan suatu insiden tidak hanya bergantung pada aspek teknis, tetapi juga ditentukan oleh kematangan proses organisasi, ketersediaan sumber daya manusia yang kompeten, dan kematangan prosedur penanganan insiden yang diterapkan.

3.7. Perbandingan dengan Penelitian Terkait

Penelitian Kurniawan dan Triayudi [11] mengimplementasikan Wazuh untuk mendeteksi serangan *web defacement* pada situs perjudian yang dijalankan pada server *AWS* dan *Google Cloud Platform (GCP),* dengan pendekatan rekonstruksi serangan berbasis kerangka kerja *MITRE ATT&CK*. Hasil pengujian penelitian tersebut menunjukkan bahwa Wazuh mampu mendeteksi serangan secara *real-time* dengan rata-rata waktu respons 1,2 detik per *alert* yang dikirimkan melalui notifikasi Telegram. Meskipun nilai waktu respons tersebut lebih cepat dibandingkan rata-rata waktu respons pada penelitian ini sebesar 2,4 detik, perbedaan ini dapat dijelaskan oleh perbedaan cakupan dan kompleksitas deteksi. Penelitian Kurniawan dan Triayudi berfokus pada deteksi *web defacement* yang umumnya melibatkan perubahan *file* yang terdokumentasi dengan jelas pada modul *File Integrity Monitoring* (FIM), sedangkan penelitian ini mencakup deteksi serangan beberapa tahapan pada layanan *RDP* dan *SQL Server* yang melibatkan korelasi peristiwa lintas modul *(FIM, SCA, dan log analysis)* serta pemetaan ke 15 teknik *MITRE ATT&CK* yang berbeda. Selain itu, penelitian ini memberikan kontribusi tambahan berupa evaluasi kepatuhan terhadap empat standar regulasi *(PCI DSS, NIST 800-53, HIPAA, dan GDPR)* yang tidak menjadi fokus pada penelitian Kurniawan dan Triayudi.

Moiz et al. [12] menunjukkan bahwa pemanfaatan kapabilitas *SIEM* dan *XDR Wazuh* pada lingkungan komputasi awan efektif untuk melindungi aset digital dan meningkatkan postur keamanan siber organisasi secara umum. Pendekatan tersebut bersifat luas dengan fokus pada penempatan berbasis awan tanpa spesifikasi sistem operasi tertentu. Penelitian ini melengkapi temuan tersebut dengan menyajikan studi yang lebih spesifik pada infrastruktur *Windows Server 2019*, sehingga aturan deteksi (*detection rules*) yang dikembangkan dapat dikonfigurasi secara presisi terhadap karakteristik layanan *RDP* dan *SQL Server*. Pendekatan ini memungkinkan penyusunan parameter ambang batas, rentang waktu, dan pencocokan pola

yang lebih sesuai dengan pola serangan yang lazim terjadi pada *Windows Event Logs*, sehingga berpotensi menurunkan tingkat positif palsu (*false positive rate*) dibandingkan konfigurasi serbaguna yang harus mengakomodasi beragam vektor serangan.

Roy et al. [13] dalam kajian sistematisasinya terhadap kerangka kerja *MITRE ATT&CK* menyoroti bahwa adopsi *ATT&CK* pada penelitian dan praktik keamanan siber memberikan kontribusi signifikan pada tiga domain utama, yaitu *threat intelligence*, deteksi ancaman, dan respons insiden. Kajian tersebut juga mengidentifikasi adanya kesenjangan antara penelitian akademik dan implementasi praktis *ATT&CK*, khususnya pada aspek evaluasi empiris dan implementasi nyata di lingkungan operasional. Penelitian ini berkontribusi mengisi sebagian kesenjangan tersebut dengan menyajikan implementasi nyata pemetaan *MITRE ATT&CK* pada sistem *SIEM Wazuh* yang dievaluasi melalui eksperimen pemantauan selama 30 hari, sehingga memberikan data empiris yang dapat memperkaya literatur tentang penerapan praktis ATT&CK pada infrastruktur Windows Server berbasis awan.

3.8. Best Practices dan Rekomendasi Implementasi

Berdasarkan hasil penelitian dan pembelajaran selama implementasi, beberapa praktik baik dapat direkomendasikan bagi organisasi yang hendak menerapkan *Wazuh SIEM* untuk mengamankan infrastruktur *Windows Server*. Pertama, penerapan secara bertahap yang dimulai dari pemantauan layanan kritis seperti *RDP* dan *SQL Server* sebelum diperluas ke seluruh infrastruktur. Pendekatan ini memberi tim kesempatan untuk membangun kapabilitas dan melakukan konfigurasi terhadap aturan deteksi sebelum diterapkan pada skala yang lebih besar.

Kedua, investasi pada pengembangan aturan deteksi khusus yang disesuaikan dengan model ancaman dan profil risiko organisasi. Aturan deteksi bawaan dari komunitas Wazuh memang memberikan perlindungan dasar, tetapi aturan khusus yang dirancang sesuai karakteristik lingkungan dan pola serangan yang relevan menghasilkan efektivitas deteksi yang lebih tinggi. Dalam penelitian ini, 45 aturan khusus yang dikembangkan berkontribusi besar terhadap tingginya tingkat deteksi yang dicapai.

Ketiga, integrasi dengan kerangka *MITRE ATT&CK* sebaiknya dilakukan sejak awal penerapan untuk memudahkan perburuan ancaman yang terstruktur dan investigasi insiden. Pemetaan setiap aturan deteksi ke teknik *ATT&CK* yang sesuai memberikan konteks yang berharga bagi analis keamanan dalam memahami pola serangan dan menetapkan prioritas respons. Kerangka ini juga membantu analisis kesenjangan untuk mengidentifikasi titik buta dalam proses deteksi.

Keempat, pembentukan perilaku dasar dan pemantauan secara keberlanjutan untuk mengidentifikasi penyimpangan yang dapat mengindikasikan insiden keamanan. Dalam penelitian ini, analisis pola temporal dapat mengidentifikasi puncak aktivitas yang digunakan untuk mengoptimalkan alokasi sumber daya dan penjadwalan kegiatan pemeliharaan di jam yang tidak sedang keadaan sibuk untuk meminimalkan risiko adanya kerentanan sistem.

3.9. Kontribusi Penelitian

Kontribusi praktis penelitian ini meliputi: (1) panduan penerapan *Wazuh SIEM* untuk pemantauan *Windows Server 2019* dengan konfigurasi optimal bagi deteksi serangan *RDP* dan *SQL Server*; (2) aturan deteksi khusus yang dipetakan ke teknik *MITRE ATT&CK* untuk meningkatkan kesadaran kontekstual dalam kemungkinan adanya ancaman; (3) aturan korelasi untuk mendeteksi serangan beberapa tahapan yang melibatkan kombinasi teknik dalam rantai serangan; (4) metrik dasar untuk mengevaluasi kinerja sistem *SIEM* pada lingkungan *Windows Server*; serta (5) kerangka pemantauan kepatuhan terhadap berbagai standar *(PCI DSS, NIST 800-53, HIPAA, dan GDPR)* menggunakan modul *SCA Wazuh*.

Kontribusi teoretis penelitian ini mencakup pembuktian empiris atas efektivitas integrasi antara platform *SIEM (Wazuh)* dengan kerangka intelijen ancaman *(MITRE ATT&CK)* dalam meningkatkan akurasi deteksi dan menekan positif palsu. Penelitian ini juga menyajikan analisis kuantitatif terhadap lanskap ancaman yang dihadapi infrastruktur *Windows Server* yang terekspos ke internet, yang dapat menjadi rujukan untuk penilaian risiko dan perencanaan keamanan.

3.10. Keterbatasan Penelitian

Hasil penelitian ini perlu dimaknai dengan memperhatikan sejumlah keterbatasan. Pertama, lingkup pengujian terbatas pada dua unit *Windows Server 2019* dalam lingkungan laboratorium yang terkendali. Lingkungan produksi yang lebih kompleks, dengan banyak server, ragam aplikasi, dan pola perilaku pengguna yang bervariasi, berpotensi memunculkan pola deteksi yang berbeda. Karena itu, kemampuan aturan deteksi yang dikembangkan untuk diterapkan pada skala yang lebih besar masih perlu divalidasi lebih lanjut.

Kedua, simulasi serangan dijalankan menggunakan perkakas uji penetrasi yang umum digunakan, seperti *Hydra, Nmap,* dan *Metasploit*, sehingga belum mencakup teknik tingkat lanjut yang biasa dipakai pelaku ancaman canggih maupun serangan yang disponsori. Penyerang di dunia nyata dapat memanfaatkan eksploitasi *zero-day*, *malware* buatan sendiri, atau teknik penghindaran lanjutan yang tidak terwakili dalam simulasi ini. Efektivitas deteksi terhadap serangan yang lebih canggih masih perlu

diuji melalui latihan *red team* atau *purple team*.

Ketiga, periode pemantauan selama 30 hari kemungkinan belum memadai untuk menangkap pola musiman atau kampanye serangan jangka panjang. Sebagian *Advanced Persistent Threat (APT)* melakukan pengintaian dan akses awal dalam rentang waktu yang sangat lama sebelum menjalankan aktivitas berbahaya yang sesungguhnya. Studi longitudinal dengan periode pemantauan yang lebih panjang diperlukan untuk memahami pola serangan jangka panjang.

Keempat, penelitian ini belum mengukur dampak bisnis nyata dari insiden keamanan yang terdeteksi, seperti biaya akibat gangguan layanan, kerugian akibat kebocoran data, atau kerusakan reputasi. Efektivitas kontrol keamanan tidak hanya dinilai dari metrik teknis seperti tingkat deteksi dan tingkat positif palsu, tetapi juga dari dampaknya terhadap keberlangsungan bisnis yang memerlukan evaluasi lebih menyeluruh.

3.11. Rekomendasi Penelitian Lanjutan

Penelitian lanjutan dapat diarahkan pada beberapa aspek untuk memperluas dan memperdalam pemahaman mengenai keamanan infrastruktur *cloud*. Pertama, pengembangan model pembelajaran mesin untuk deteksi anomali yang dapat melengkapi deteksi berbasis aturan. Pendekatan hibrida yang memadukan deteksi berbasis signature untuk ancaman yang sudah dikenal dengan deteksi berbasis perilaku untuk ancaman *zero-day* berpotensi memperluas cakupan deteksi sekaligus menekan jumlah serangan yang terlewat.

Kedua, perluasan cakupan teknik *MITRE ATT&CK* dengan menambahkan aturan deteksi untuk teknik yang belum tercakup dalam penelitian ini. Kerangka *MITRE ATT&CK* memuat lebih dari 200 teknik, sedangkan penelitian ini baru memetakan 15 teknik. Cakupan yang lebih luas terhadap beragam teknik serangan akan memperkuat postur pertahanan terhadap berbagai pelaku ancaman.

Ketiga, integrasi dengan umpan intelijen ancaman, baik komersial maupun sumber terbuka, untuk meningkatkan kesadaran kontekstual terhadap ancaman yang sedang berkembang. Intelijen ancaman secara *real-time* dapat menyediakan indikator kompromi *(indicators of compromise/IOC)* yang berguna untuk perburuan ancaman secara proaktif serta deteksi dini sebelum kompromi benar-benar terjadi.

Keempat, penerapan mekanisme respons otomatis melalui platform *Security Orchestration, Automation, and Response (SOAR)* untuk mempercepat waktu penanganan insiden. *Playbook* otomatis untuk skenario serangan yang umum dapat menurunkan rata-rata waktu respons *(mean time to respond/MTTR)* sekaligus memperkecil dampak serangan yang berhasil. Integrasi Wazuh dengan *platform SOAR* seperti *Shuffle* atau *TheHive* dapat memfasilitasi tindakan penanggulangan, pemberantasan, dan pemulihan secara otomatis.

Kelima, pelaksanaan studi komparatif antarberbagai *platform SIEM*, baik komersial maupun sumber terbuka, untuk menilai tingkat kompromi dari sisi efektivitas deteksi, biaya operasional, kompleksitas, dan skalabilitas. Analisis perbandingan semacam ini dapat menjadi acuan bagi organisasi dalam memilih solusi *SIEM* yang sesuai dengan kebutuhan dan keterbatasan masing-masing.

4. Kesimpulan

Penelitian ini menunjukkan bahwa integrasi *Wazuh SIEM* dengan kerangka kerja *MITRE ATT&CK* mampu menjawab rumusan masalah penelitian, yaitu bagaimana mendeteksi dan menganalisis serangan terhadap *Windows Server 2019* di lingkungan *cloud* secara proaktif. Melalui pemantauan selama 30 hari terhadap 110.492 peristiwa keamanan, sistem yang dibangun terbukti dapat mengenali pola serangan beberapa tahapan dan memetakannya ke taktik serta teknik *MITRE ATT&CK*, dengan tingkat deteksi 93,2%, tingkat positif palsu 6,8%, dan waktu respons rata-rata 2,4 detik. Capaian ini menjawab kebutuhan akan visibilitas ancaman yang lebih baik pada infrastruktur *Windows Server* yang terekspos ke internet.

Temuan paling menonjol adalah bahwa konfigurasi bawaan *(default) Windows Server 2019* terbukti sangat rentan terhadap serangan *brute force* di lingkungan *cloud*, sebagaimana ditunjukkan oleh dominasi kegagalan autentikasi dan rendahnya skor kepatuhan *CIS Benchmark* yang hanya 25%. Oleh karena itu, penerapan aturan khusus pada Wazuh yang dipetakan ke *MITRE ATT&CK* bukan langkah opsional, melainkan langkah esensial untuk mengamankan aset institusi sejak konfigurasi awal. Efektivitas pertahanan tidak semata ditentukan oleh kontrol teknis, tetapi juga oleh kesiapan sumber daya manusia, kematangan proses, dan tata kelola keamanan yang menopang operasional secara berkelanjutan.

Dengan demikian, penelitian ini memberikan panduan berbasis data bagi praktisi dalam menerapkan pemantauan keamanan yang efektif pada infrastruktur *Windows Server*, sekaligus menggarisbawahi pentingnya penguatan konfigurasi *host* yang dipadukan dengan deteksi berbasis aturan. Keterbatasan yang teridentifikasi, khususnya pada deteksi teknik penghindaran, membuka arah penelitian lanjutan, antara lain peningkatan deteksi berbasis perilaku dan perluasan cakupan teknik *MITRE ATT&CK*, demi memperkuat keamanan infrastruktur *cloud* ke depan.

Ucapan Terima Kasih

Penulis mengucapkan terima kasih kepada Universitas Tidar atas penyediaan infrastruktur dan dukungan untuk penelitian ini. Kami juga menyampaikan terima kasih kepada Program Studi Teknologi Informasi, Fakultas Teknik, Universitas Tidar atas fasilitas lingkungan penelitian dan sumber daya teknis yang telah diberikan.

Reference

[1] National Institute of Standards and Technology, "Security and Privacy Controls for Information Systems and Organizations," NIST Special Publication 800-53 Rev. 5, Sep. 2020, doi: 10.6028/NIST.SP.800-53r5.

[2] Center for Internet Security, "CIS Microsoft Windows Server 2019 Benchmark v2.0.0," CIS Benchmarks, Dec. 2023. [Online]. Available: https://www.cisecurity.org/benchmark/windows_server

[3] MITRE Corporation, "MITRE ATT&CK Framework v18," MITRE ATT&CK, Oct. 2025. [Online]. Available: https://attack.mitre.org/

[4] International Organization for Standardization, "Information Security, Cybersecurity and Privacy Protection - Information Security Management Systems," ISO/IEC 27001:2022, Oct. 2022. [Online]. Available: https://www.iso.org/standard/27001

[5] PCI Security Standards Council, "Payment Card Industry Data Security Standard v4.0," PCI DSS Requirements and Testing Procedures, Mar. 2024. [Online]. Available: https://www.pcisecuritystandards.org/

[6] European Commission, "General Data Protection Regulation (GDPR)," Regulation (EU) 2016/679, May 2018. [Online]. Available: https://gdpr-info.eu/

[7] U.S. Department of Health and Human Services, "Health Insurance Portability and Accountability Act Security Rule," 45 CFR Parts 160, 162, and 164, Feb. 2023. [Online]. Available: https://www.hhs.gov/hipaa

[8] Wazuh Inc., "Wazuh 4.10 Documentation: The Open Source Security Platform," Wazuh Technical Documentation, 2025. [Online]. Available: https://documentation.wazuh.com/

[9] Microsoft Corporation, "Windows Server 2019 Security Baseline," Microsoft Security Compliance Toolkit, Nov. 2024. [Online]. Available: https://www.microsoft.com/security/

[10] OWASP Foundation, "OWASP Top 10:2021 - The Ten Most Critical Web Application Security Risks," OWASP Standards, 2021. [Online]. Available: https://owasp.org/Top10/

[11] C. Kurniawan and A. Triayudi, "Reconstruction and Detection of Gambling Web Defacement Attack Using Wazuh and Velociraptor," in 2024 International Conference on Information Technology Research and Innovation (ICITRI), Sep. 2024, pp. 257–262, doi: 10.1109/ICITRI62858.2024.10699215.

[12] S. Moiz, A. Majid, A. Basit, M. Ebrahim, A. A. Abro, and M. Naeem, "Security and Threat Detection through Cloud-Based Wazuh Deployment," in 2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC), Tandojam, Pakistan, 2024, pp. 1–5.

[13] S. Roy, E. Panaousis, C. Noakes, A. Laszka, S. Panda, and G. Loukas, "SoK: The MITRE ATT&CK Framework in Research and Practice," arXiv preprint arXiv:2304.07411, 2023.

[14] G. González-Granadillo, S. González-Zarzosa, and R. Diaz, "Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures," Sensors, vol. 21, no. 14, Art. no. 4759, Jul. 2021, doi: 10.3390/s21144759.

[15] J. Manzoor, A. Waleed, A. F. Jamali, and A. Masood, "Cybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs," PLOS ONE, vol. 19, no. 3, Mar. 2024, doi: 10.1371/journal.pone.0301183.

[16] F. I. F. Farrel, M. K. I. Mardianto, and A. S. Qamar, "Implementation of Security Information & Event Management (SIEM) Wazuh with Active Response and Telegram Notification for Mitigating Brute Force Attacks on The GT-I2TI USAKTI Information System," Intelmatics, vol. 4, no. 1, pp. 1–7, Feb. 2024, doi: 10.25105/itm.v4i1.18529.

[17] P. Stöckle, B. Grobauer, and A. Pretschner, "Automated Implementation of Windows-related Security-Configuration Guides," in Proceedings of the 35th IEEE/ACM International Conference on Automated Software Engineering (ASE '20), Sep. 2020, pp. 598–610, doi: 10.1145/3324884.3416540.

[18] A. L. Robertson, "ATT&CK v18: The Detection Overhaul You've Been Waiting For," MITRE ATT&CK Blog, Oct. 28, 2025. [Online]. Available: https://medium.com/mitre-attack/att-ck-v18-detection-strategies-more-adversary-insights-8f82d839ee9e

[19] S. Benabderrahmane, G. Berrada, J. Cheney, and P. Valtchev, "A Rule Mining-Based Advanced Persistent Threats Detection System," arXiv preprint arXiv:2105.10053, 2021.

[20] Z. S. Younus and M. Alanezi, "Detect and Mitigate Cyberattacks Using SIEM," in 2023 16th International Conference on Developments in eSystems Engineering (DeSE), Dec. 2023, pp. 510–515, doi: 10.1109/DeSE60595.2023.10469387.