Pengembangan Sistem Siem Terintegrasi Mitre Att&Ck Untuk Identifikasi Dan Analisis Insiden Keamanan Siber

1st Anbiya Sisda Yaridz
Fakultas Ilmu Terapan
Universitas Telkom
Bandung, Indonesia
yaridsans@student.telkomuniversity.ac.id

2nd Muhammad Iqbal
Fakultas Ilmu Terapan
Universitas Telkom
Bandung, Indonesia
miqbal@telkomuniversity.ac.id

***Abstrak* — Perkembangan teknologi informasi yang pesat membuat organisasi untuk memiliki sistem keamanan siber yang mampu mendeteksi dan merespons ancaman secara efisien. Salah satu pendekatan yang umum digunakan adalah pemanfaatan sistem deteksi intrusi berbasis host (HIDS) seperti Wazuh, yang terintegrasi dengan platform analisis log Elasticsearch. Namun, hasil monitoring terhadap studi kasus yang dilakukan menunjukkan bahwa alarm atau rule yang dihasilkan masih belum terhubung secara langsung dengan framework MITRE ATT&CK. Ketidakterhubungan ini menghambat proses identifikasi taktik dan teknik serangan karena tidak adanya pemetaan otomatis antara insiden yang terdeteksi dan struktur MITRE ATT&CK. Penelitian ini bertujuan untuk mengembangkan solusi berupa rule khusus pada Wazuh yang memungkinkan setiap alarm dikaitkan secara otomatis dengan taktik dan teknik MITRE ATT&CK. Hasilnya menunjukkan bahwa dengan pemetaan otomatis ini, proses klasifikasi insiden menjadi lebih cepat, akurat, dan kontekstual. Integrasi rule dengan MITRE ATT&CK mampu meningkatkan efektivitas dalam mendeteksi serta merespons insiden, sehingga memperkuat visibilitas dan kesiapan organisasi dalam menghadapi ancaman siber.1**

***Kata kunci*— MITRE ATT&CK, CIS controls, analisis log, deteksi intrusi, pemetaan taktik**

I. PENDAHULUAN

Dalam beberapa tahun terakhir, pertumbuhan pesat infrastruktur digital telah mendorong organisasi untuk mengandalkan teknologi informasi dalam mengelola proses operasional dan menyimpan data penting. Namun, di balik peningkatan efisiensi dan otomatisasi tersebut, muncul ancaman siber yang semakin kompleks, sistematis, dan sulit dideteksi oleh sistem keamanan konvensional. Serangan tidak lagi dilakukan secara acak, melainkan melalui pendekatan yang terstruktur dengan menggunakan taktik dan teknik canggih, yang mengharuskan organisasi untuk memiliki kemampuan deteksi serta respons yang adaptif dan kontekstual.

Simulasi serangan menjadi salah satu metode penting dalam mengukur kesiapan infrastruktur terhadap ancaman tersebut. Salah satu alat yang banyak digunakan untuk keperluan ini adalah Infection Monkey, sebuah tool open-source yang mampu mensimulasikan teknik serangan nyata seperti eksploitasi jaringan dan penyebaran lateral untuk mengidentifikasi potensi kerentanan sistem. Meskipun Infection Monkey berada di posisi menengah dalam studi perbandingan alat emulasi, keunggulannya dalam kemudahan penggunaan dan dukungan komunitas membuatnya populer sebagai alat uji coba keamanan.

Namun, dalam implementasi simulasi serangan yang dilakukan menggunakan Infection Monkey, ditemukan bahwa sistem deteksi berbasis Wazuh dan Elasticsearch belum sepenuhnya dapat memetakan hasil deteksi ke dalam taktik dan teknik pada framework MITRE ATT&CK. Hal ini menghambat proses analisis insiden secara cepat dan akurat karena kurangnya kontekstualisasi terhadap metode serangan.

Penelitian ini berfokus pada pengembangan rule khusus yang terintegrasi dengan MITRE ATT&CK agar setiap alarm yang dihasilkan oleh sistem deteksi dapat secara otomatis dikaitkan dengan taktik dan teknik yang sesuai. Pendekatan ini diharapkan dapat memperkuat efektivitas sistem deteksi dan respons terhadap serangan siber. Selain itu, integrasi dengan CIS Controls digunakan untuk merancang strategi mitigasi yang sistematis dan terarah sesuai dengan kondisi organisasi.

II. KAJIAN TEORI

A. MITRE ATT&CK

Kerangka kerja MITRE ATT&CK (*Adversarial Tactics, Techniques, and Common Knowledge*) merupakan basis pengetahuan yang lengkap yang mendokumentasikan taktik, teknik, dan prosedur (TTP) yang biasa digunakan oleh penyerang siber pada berbagai tahap serangan.

B. CIS CONTROL

CIS Controls (*Center for Internet Security Controls*) adalah sekumpulan pedoman praktik terbaik (*best practices*) yang dirancang untuk membantu organisasi dalam meningkatkan keamanan siber mereka secara efektif. CIS

Controls disusun oleh *Center for Internet Security* (CIS) dan telah diakui secara luas sebagai kerangka kerja keamanan siber yang praktis, prioritas, dan dapat diimplementasikan di berbagai jenis organisasi, baik kecil maupun besar.

C. Elasticsearch, Kibana, Filebeat

Elasticsearch digunakan sebagai penyimpanan dan analisis log secara real-time dalam sistem SIEM. Filebeat berfungsi sebagai forwarder log dari endpoint ke Elasticsearch, sementara Kibana digunakan untuk visualisasi dan analisis data log secara interaktif.

D. Wazuh manager

Wazuh Manager berperan sebagai pusat analisis dan monitoring keamanan yang menerima log dari agen endpoint. Log tersebut dianalisis berdasarkan rule yang telah ditentukan untuk menghasilkan alert. Dalam sistem ini, rule set Wazuh telah terintegrasi dengan framework MITRE ATT&CK, sehingga setiap alert dapat langsung dipetakan ke taktik dan teknik serangan. Integrasi ini meningkatkan efektivitas deteksi dan pemahaman terhadap ancaman

E. WSL (*Windows Subsystem Linux*)

WSL adalah fitur di Windows yang memungkinkan pengguna menjalankan distribusi Linux secara langsung tanpa menggunakan mesin virtual. Dalam konteks implementasi sistem keamanan, WSL digunakan untuk menginstal dan menjalankan komponen seperti Wazuh Manager, Elasticsearch, dan Filebeat dalam lingkungan Linux di atas sistem operasi Windows.

F. NGINX

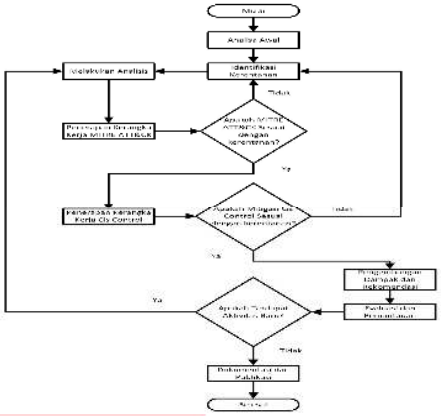
NGINX adalah web server open-source yang juga berfungsi sebagai reverse proxy dan load balancer. Dalam sistem ini, NGINX digunakan untuk mengamankan akses ke dashboard Wazuh dan Kibana melalui protokol HTTPS, serta menangani permintaan pengguna secara efisien.

III. METODE

Memberikan gambaran rancangan penelitian yang meliputi prosedur atau langkah-langkah penelitian, waktu penelitian, sumber data, cara perolehan data dan menjelaskan metode yang akan digunakan dalam penelitian [10 pts].

A. Deskripsi dan Alur Pekerjaan

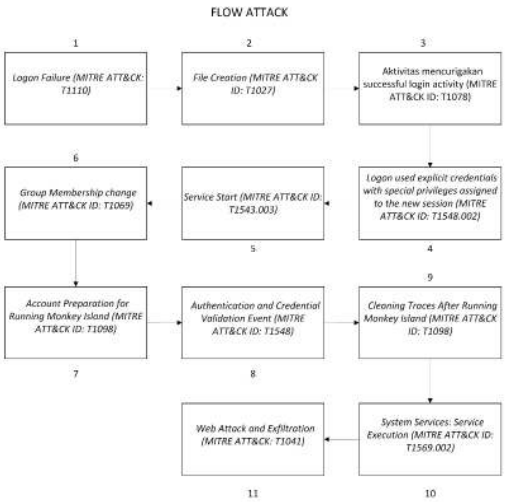
Proses analisis dimulai dengan identifikasi dan evaluasi awal terhadap potensi kerentanan pada sistem. Setelah kerentanan terdeteksi, dilakukan pemetaan terhadap framework MITRE ATT&CK untuk mengidentifikasi apakah teknik serangan yang ditemukan sesuai dengan taktik dan teknik yang terdokumentasi. Jika belum sesuai, dilakukan pengkajian ulang terhadap kerentanan yang ada. Apabila terdapat kesesuaian, tahap selanjutnya adalah penerapan CIS Controls untuk menentukan langkah mitigasi yang tepat. Penilaian terhadap efektivitas kontrol tersebut sangat penting untuk memastikan mitigasi berjalan optimal. Jika kontrol belum sesuai, proses identifikasi diulang hingga strategi mitigasi yang tepat ditemukan. Setelah mitigasi diterapkan, dilakukan pengembangan rekomendasi serta analisis dampak guna meningkatkan ketahanan sistem. Tahap akhir melibatkan proses evaluasi dan pemantauan guna mendeteksi aktivitas mencurigakan secara berkelanjutan. Apabila ditemukan indikasi ancaman lanjutan, dilakukan investigasi mendalam. Semua temuan dan proses dokumentasi disusun sebagai bentuk pelaporan insiden dan sebagai referensi untuk peningkatan keamanan di masa mendatang.



GAMBAR 1
Alur Kerja

B. Gambaran hasil analisis serangan Infection Monkey

Serangan dimulai dengan percobaan brute force terhadap akun pengguna, disusul keberhasilan login ke akun Administrator yang mengindikasikan kemungkinan penyerang telah memiliki kredensial. Setelah akses diperoleh, penyerang melakukan instalasi Infection Monkey melalui akun Administrator, menjalankan aplikasi Monkey Island, serta memanipulasi sistem untuk mempertahankan akses. Selanjutnya, penyerang menggunakan hak istimewa untuk membuat akun baru dengan hak administratif, mengaktifkan, memodifikasi, dan kemudian menghapusnya guna menyembunyikan jejak. Manipulasi juga dilakukan terhadap layanan sistem dan konfigurasi startup. Setelah kontrol penuh diperoleh, penyerang meluncurkan serangan ke server lain, ditandai dengan permintaan HTTP yang sukses (kode status 200), menunjukkan terjadinya penyebaran.



GAMBAR 2
Flow Attack

Dampak Serangan:

1. Kerugian Finansial – potensi pencurian data dan biaya pemulihan tinggi.
2. Kehilangan Data Sensitif – risiko kebocoran informasi pelanggan atau internal.
3. Gangguan Operasional – downtime dan kerugian produktivitas.
4. Kerusakan Reputasi – menurunnya kepercayaan publik.
5. Penyebaran Malware Lanjutan – digunakan sebagai titik serang ke sistem lain.
6. Eksploitasi Sumber Daya – misalnya untuk cryptojacking atau serangan DDoS.
7. Dampak Psikologis – menimbulkan stres pada staf dan pengguna.

Strategi Mitigasi Berdasarkan CIS Controls:

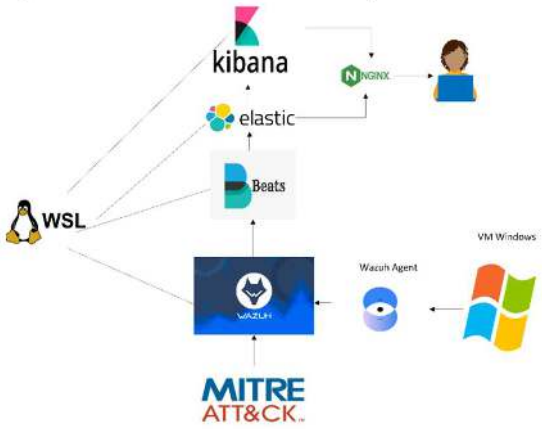
1. Manajemen Akun dan Aplikasi
2. Terapkan least privilege, MFA, dan nonaktifkan akun tidak terpakai.
3. Gunakan application allowlisting untuk mencegah instalasi aplikasi tidak sah.
4. Pemulihan Data
5. Lakukan backup rutin dan uji pemulihan secara berkala.
6. Manajemen Aset dan Software
7. Gunakan inventaris otomatis dan pastikan hanya software resmi yang digunakan.
8. Perlindungan Data Sensitif
9. Enkripsi data dan batasi akses berdasarkan peran.
10. Pelatihan Keamanan Pengguna
11. Edukasi tentang phishing, malware, dan praktik keamanan dasar.

C. Gambaran sistem lingkungan Uji coba

Lingkungan pengujian dibangun menggunakan WSL sebagai server utama, yang terdiri dari beberapa komponen inti: Elasticsearch, Filebeat, Kibana, Wazuh Manager, dan NGINX.

1. Elasticsearch menyimpan dan mengindeks log dari berbagai sumber.
2. Filebeat membaca log dari Wazuh Manager dan meneruskannya ke Elasticsearch.
3. Kibana menyajikan visualisasi data log untuk analisis interaktif.
4. Wazuh Manager menerima log dari Wazuh Agent (Windows VM), menganalisis, dan mengirimkan ke Filebeat.
5. NGINX berfungsi sebagai reverse proxy untuk mengamankan akses ke antarmuka Kibana dan Wazuh.

Log dari Windows VM dikirim oleh Wazuh Agent ke Wazuh Manager di WSL, diproses oleh Filebeat, lalu divisualisasikan di Kibana. Sistem ini diintegrasikan dengan MITRE ATT&CK, sehingga setiap alarm secara otomatis dipetakan ke taktik dan teknik yang relevan, guna meningkatkan efektivitas analisis dan respons insiden.



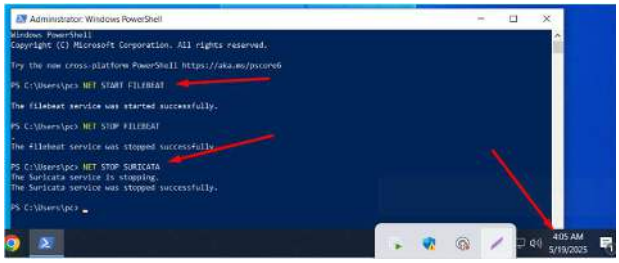
GAMBAR 3
Gambaran Sistem

IV. HASIL DAN PEMBAHASAN

Pada bab ini dibahas hasil pengujian sistem yang telah terintegrasi dengan framework MITRE ATT&CK untuk mengevaluasi efektivitas deteksi dan klasifikasi insiden secara otomatis. Permasalahan sebelumnya adalah insiden belum terhubung langsung dengan MITRE ATT&CK, sehingga identifikasi taktik dan teknik serangan kurang efektif. Sebagai solusi, dikembangkan sistem yang memetakan setiap alert secara otomatis ke dalam taktik dan teknik MITRE ATT&CK. Lingkungan uji coba menggunakan Elasticsearch sebagai pusat penyimpanan dan analisis log, serta Wazuh sebagai sistem deteksi host-based yang menghasilkan alert keamanan. Rule di Wazuh telah disesuaikan agar setiap insiden langsung terklasifikasi sesuai struktur MITRE ATT&CK.

A. Pengujian

Pengujian dilakukan pada VM Windows yang telah dikonfigurasi dengan Wazuh Agent dan Sysmon untuk memantau aktivitas sistem secara detail. Sysmon merekam aktivitas tingkat rendah, sementara Wazuh Agent mengirimkan log ke server untuk dianalisis. Simulasi serangan dilakukan berdasarkan framework MITRE ATT&CK, terutama teknik yang melibatkan eksekusi net.exe (S0039, T1027, T1049, T1077, T1135). Perintah seperti net user dan net view dijalankan melalui PowerShell untuk menguji apakah rule Wazuh yang terintegrasi dengan MITRE ATT&CK dapat mendeteksi dan mengklasifikasikan insiden secara otomatis.



GAMBAR 4
Pengujian

B. Hasil pada Elasticsearch

Berdasarkan hasil pengujian, dapat dilihat bahwa rule ATT&CK S0039 T1027 T1049 T1077 T1135: Net.exe Execution yang telah dikonfigurasi sebelumnya berhasil berjalan dengan baik. Aktivitas yang dilakukan pada mesin Windows, seperti penggunaan perintah net melalui PowerShell, berhasil terdeteksi dan dicatat sebagai event oleh Sysmon. Event ini kemudian dikirimkan melalui Wazuh Agent dan ditampilkan di Elasticsearch secara real-time. Keberhasilan ini ditandai dengan munculnya data log yang sesuai di Elasticsearch, lengkap dengan waktu kejadian yang akurat. Hal ini menunjukkan bahwa sistem deteksi telah mampu memantau dan mengidentifikasi aktivitas yang mencurigakan secara langsung, serta memetakannya ke dalam teknik dan taktik yang relevan dalam framework MITRE ATT&CK. Dengan demikian, proses analisis insiden dapat dilakukan lebih cepat dan berdasarkan konteks taktik serta teknik yang valid.

GAMBAR 5
Hasil Elasticsearch

C. Keluaran Sistem dan Integrasi Link MITRE ATT&CK

Hasil yang terlihat bahwa sistem berhasil menampilkan output hasil deteksi dari rule yang telah dibuat sebelumnya. Salah satu keunggulan dari rule ini adalah kemampuannya untuk tidak hanya mendeteksi aktivitas mencurigakan, tetapi juga secara otomatis menambahkan tautan (link output) yang mengarah langsung ke framework MITRE ATT&CK. Tautan ini mengacu pada halaman teknik atau taktik spesifik yang relevan dengan event yang terdeteksi, seperti T1027, T1049, dan lainnya.

GAMBAR 6
Link pada Elasticsearch

GAMBAR 7
Hasil link output MITRE ATT&CK

V. KESIMPULAN

Berdasarkan studi kasus serangan Infection Monkey, penyerang berhasil mengeksploitasi kerentanan dengan membuat akun administratif dan menjalankan aplikasi untuk menyebar ke host lain dalam subnet. Serangan ini menggunakan teknik canggih tanpa metode umum seperti brute-force. Analisis pemetaan ke 13 teknik MITRE ATT&CK dan integrasi CIS Controls menghasilkan 11 rekomendasi mitigasi, termasuk penguatan manajemen akun dan pelatihan keamanan. Penelitian ini juga mengembangkan rule Wazuh yang otomatis memetakan alarm ke MITRE ATT&CK, sehingga mempercepat analisis insiden secara real-time dan mendukung pengambilan keputusan keamanan yang lebih tepat.

REFERENSI

[1] M. Landauer, K. Mayer, F. Skopik, M. Wurzenberger, and M. Kern, “Red Team Redemption: A Structured Comparison of Open-Source Tools for Adversary Emulation,” *arXiv preprint arXiv:2408.15645*, pp. 1–12, 2024.

[2] A. Georgiadou, S. Mouzakitis, and D. Askounis, “Assessing MITRE ATT&CK Risk Using a Cyber-Security Culture Framework,” *Sensors*, vol. 21, no. 3267, p. 2, 2021.

[3] M. I. Abdullah, A. I. Abas, and A. I. Hajamydeen, “Effective SOC Response Strategies Using MITRE ATT&CK,” *Malaysia Board of Technologists (MBOT)*, vol. 3, no. 1, pp. 1–7, Jun. 2024.

[4] H. Irawan, A. H. Muhammad, and A. Nasiri, “Design of Cybersecurity Maturity Assessment Framework Using NIST CSF v1.1 and CIS Controls v8,” *INOVTEK POLBENG - SERI INFORMATIKA*, vol. 9, no. 1, pp. 1–14, 2024.

[5] “Akamai ‘Infection Monkey’, 2 Januari 2025. [Online]. Available: https://www.akamai.com/infectionmonkey. [Accessed 2 Januari 2025].”

[6] “M. ATTACK, ‘MITRE ATT&CK ID: T1078,’ The MITRE Corporation, 2 Januari 2025. [Online]. Available: https://attack.mitre.org/techniques/T1078/. [Accessed 2 Januari 2025].”

[7] “M. ATTACK, ‘MITRE ATT&CK ID: T1548.002,’ The MITRE Corporation, 2 Januari 2025. [Online]. Available: https://attack.mitre.org/techniques/T1548/002/. [Accessed 2 Januari 2025].”

[8] “M. ATTACK, ‘MITRE ATT&CK ID: T1543.003,’ The MITRE Corporation, 2 Januari 2025. [Online]. Available: https://attack.mitre.org/techniques/T1543/003/. [Accessed 2 Januari 2025].”

[9] “M. ATTACK, ‘MITRE ATT&CK ID: T1069,’ The MITRE Corporation, 2 Januari 2025. [Online]. Available: https://attack.mitre.org/techniques/T1069/. [Accessed 2 Januari 2025].”

[10] “M. ATTACK, ‘MITRE ATT&CK ID: T1098,’ The MITRE Corporation, 2 Januari 2025. [Online]. Available: https://attack.mitre.org/techniques/T1098/. [Accessed 2 Januari 2025].”

[11] "M. ATTACK, 'MITRE ATT&CK ID: T1548,' The MITRE Corporation, 2 Januari 2025. [Online]. Available: https://attack.mitre.org/techniques/T1548/. [Accessed 2 Januari 2025]."
[12] "M. ATTACK, 'MITRE ATT&CK ID: T1027,' The MITRE Corporation, 2 Januari 2025. [Online]. Available: https://attack.mitre.org/techniques/T1027/. [Accessed 2 Januari 2025]."
[13] "M. ATTACK, 'MITRE ATT&CK ID: T1569.002,' The MITRE Corporation, 2 Januari 2025. [Online]. Available: https://attack.mitre.org/techniques/T1569/002/. [Accessed 2 Januari 2025]."
[14] "M. ATTACK, 'MITRE ATT&CK ID: T1021,' The MITRE Corporation, 2 Januari 2025. [Online]. Available: https://attack.mitre.org/techniques/T1021/. [Accessed 2 Januari 2025]."
[15] "M. ATTACK, 'MITRE ATT&CK ID: T1041,' The MITRE Corporation, 2 Januari 2025. [Online]. Available: https://attack.mitre.org/techniques/T1041/. [Accessed 2 Januari 2025]."
[16] "M. ATTACK, 'MITRE ATT&CK ID: T1110,' The MITRE Corporation, 2 Januari 2025. [Online]. Available: https://attack.mitre.org/techniques/T1110/. [Accessed 2 Januari 2025]."
[17] "M. ATTACK, 'MITRE ATT&CK ID: T1046,' The MITRE Corporation, 2 Januari 2025. [Online]. Available: https://attack.mitre.org/techniques/T1046/. [Accessed 2 Januari 2025]."
[18] "M. ATTACK, 'MITRE ATT&CK ID: TA0008,' The MITRE Corporation, 2 Januari 2025. [Online]. Available: https://attack.mitre.org/tactics/TA0008/. [Accessed 2 Januari 2025]."
[19] "CIS Critical Security Controls Version 8.1, 2024. [Online]. Available: https://www.cisecurity.org/controls/v8-1."