INFOTECH: JOURNAL OF TECHNOLOGY INFORMATION
DOI: https://doi.org/10.37365/jti.v10i2.320

VOL. 10 No. 2 November 2024
P-ISSN : 2460-2108
E-ISSN : 2620-5181

MEMBANGUN *AGENT ENDPOINT DETECTION AND RESPONSE* (EDR) MENGGUNAKAN WAZUH DAN VIRUSTOTAL SEBAGAI SISTEM DETEKSI SERANGAN *RANSOMWARE* LOCKBIT 3.0

Muchammad Sholeh[1*], Almima Monalisa Putri[2]

[1,2]Teknik Informatika, Universitas Muhammadiyah Prof. DR. HAMKA Jakarta, Indonesia.
Correspondence email: m.sholeh@uhamka.ac.id

Article history: *Submission date: November-06-2024 Revised date: November-21-2024 Published date: November-30-2024*

ABSTRACT

Internet users who are still public with cyber threats can be the main target of cyber criminals who want to take away a variety of things that Internet users own, one of which is personal data. Ransomware is one of the most widely used types of cyber attacks today to lock data on the victim's computer and then ask for ransom in the amount of money so that the data can be reopened. The aim of this study is to detect the threat on the server from the LockBit 3.0 ransomware attack using the Wazuh open source platform with the VirusTotal API integration as well as to know the effectiveness of Endpoint Detection and Response (EDR) as a solution in detecting the ransumware attack and obtained the result that Wazuh with the integration of VirusTotal successfully implemented Endpoint detection and response that detects and deletes the LockBit 3.0 file from the server directory within average 0.7 seconds with 3 times trial tests.

Keywords: *Server Security Ransomware, Wazuh, Virustotal, Detection System, Monitoring.*

ABSTRAK

Pengguna internet yang masih awam dengan ancaman *cyber* dapat menjadi sasaran utama penjahat *cyber* yang ingin mengambil berbagai hal yang dimiliki pengguna internet salah satunya adalah data pribadi. *Ransomware* merupakan salah satu jenis serangan *cyber* yang paling banyak digunakan saat ini untuk mengunci data pada komputer korban kemudian meminta tebusan dalam jumlah besar agar data dapat dibuka kembali. Tujuan dari penelitian ini adalah dapat melakukan pendeteksian ancaman pada *server* dari serangan *ransomware* LockBit 3.0 menggunakan *platform* Wazuh berbasis *open source* dengan integrasi API VirusTotal serta mengetahui efesiensi dari *Endpoint Detection and Response* (EDR) sebagai solusi dalam mendeteksi serangan *ransomware* dan diperoleh hasil bahwa Wazuh dengan integrasi VirusTotal berhasil menerapkan *Endpoint Detection and Response* yaitu mendeteksi dan menghapus *file ransomware* LockBit 3.0 dari direktori *server* dalam rentang Waktu 0.7 detik dengan melakukan uji coba sebanyak tiga kali.

Kata Kunci: *Keamanan Server, Ransomware, Wazuh, Virustotal, Sistem Deteksi, Monitoring.*

PENDAHULUAN

Saat ini perkembangan teknologi khususnya internet telah melaju pesat di berbagai sektor. Penggunaan internet sangat dibutuhkan oleh banyak orang untuk mengakses informasi, media penyimpanan, mengunduh data, dan fasilitas internet lainnya pada masa kini (Sadya, 2023). Sejak tahun 2020, jumlah pengguna internet semakin meningkat diberbagai kalangan usia karena sebagian besar aktifitas mulai dialihkan menjadi tatap maya sehingga masyarakat semakin terbiasa dengan fasilitas internet.

Menurut Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), terdapat 215,63 juta jiwa di Indonesia yang telah menggunakan internet per Maret tahun 2023 (Asosiasi Penyelenggara Jasa Internet Indonesia, 2023).

Pada hasil survei yang berjudul "Penetrasi dan Perilaku Internet 2023" yang diselenggarakan oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), dari 8.510 responden pengguna internet di Indonesia diperoleh data pengguna internet di Indonesia didominasi dengan remaja berusia 13 hingga 18 tahun yaitu sebanyak 98,2% dengan kontribusi 12,15% dan remaja hingga dewasa dengan rentang usia 19 hingga 34 tahun sebanyak 97,17% dengan kontribusi 32,09%.

Berdasarkan informasi tersebut, dapat disimpulkan bahwa pengguna internet di Indonesia semakin tersebar diseluruh kalangan usia seiring dengan aksesbilitas masyarakat terhadap internet yang semakin mudah (Asosiasi Penyelenggara Jasa Internet Indonesia, 2023).

Disisi lain dari bertambahnya jumlah pengguna internet di Indonesia, terdapat banyak ancaman *cyber* yang mengintai semua orang yang menggunakan fasilitas internet. Pengguna internet yang masih awam dengan ancaman *cyber* dapat menjadi sasaran utama penjahat *cyber* yang ingin mengambil berbagai hal yang dimiliki pengguna internet salah satunya adalah data pribadi. Terdapat berbagai jenis ancaman *cyber* yang bisa membahayakan pengguna internet terutama untuk pengguna yang masih awam karena ancaman *cyber* dapat dilakukan melalui berbagai metode (Firman Pratama, 2023).

Ransomware adalah jenis *malware* yang menjadi salah satu ancaman *cyber* yang masih aktif menyerang perangkat pengguna internet hingga saat ini. *Ransomware* bekerja dengan cara mengenkripsi *file* serta meminta tebusan kepada korban untuk menebus *file* yang terenkripsi. Menurut Akamai Technologies, Inc., total korban serangan *ransomware* di kawasan Asia-Pasifik dan Jepang terus mengalami peningkatan hingga 204% pada tahun 2022 hingga 2023 dengan total kerugian hingga 50 juta USA dollar (Yuliardi, 2023). Menurut analisis yang dilakukan oleh The Record, sektor kesehatan menjadi korban utama dari serangan *ransomware* dengan total kasus sebanyak 593 kasus dan sebanyak 469 kasus serangan *ransomware* terjadi pada sektor pendidikan dalam periode tahun 2022 hingga 2023 (Janofsky, 2024).

LockBit merupakan salah satu jenis *ransomware* yang sering digunakan oleh penjahat *cyber* untuk menyerang perangkat target ancaman *cyber*. Dilansir pada Kompas.com, Bank Syariah Indonesia (BSI) mengalami gangguan akibat serangan ransomware LockBit 3.0 pada tanggal 8 Mei 2023. Akibat serangan tersebut, Bank Syariah Indonesia (BSI) tidak dapat melakukan transaksi hingga server utama Bank Syariah Indonesia (BSI) berhasil dipulihkan pada tanggal 11 Mei 2023. Selain aktivitas transaksi menjadi terhambat, 15 juta data pribadi milik nasabah dan karyawan Bank Syariah Indonesia (BSI) terancam dibocorkan oleh peretas jika pihak bank tidak membayar tebusan sebesar 296.6 miliar rupiah kepada peretas (Priyatna Darmawan & Esti Pratiwi, 2023).

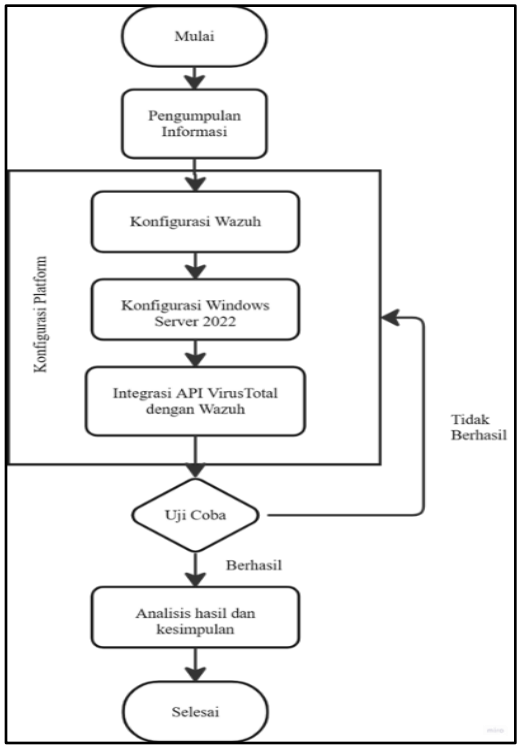
Tujuan penelitian ini untuk mendeteksi lebih dini terhadap *server* dari serangan *ransomware* LockBit 3.0 menggunakan *platform* Wazuh berbasis *open source* dengan integrasi API VirusTotal *dan* mengetahui cara kerja dari *Endpoint Detection and Response* (EDR) sebagai *agent* dalam mendeteksi serangan *ransomware* khususnya pada Windows Server 2022.

Penelitian ini menerapkan metode deteksi keamanan *endpoint server* dengan menggunakan *Endpoint Detection And Response* (EDR). *Endpoint Detection and Response* (EDR) merupakan salah satu solusi keamanan yang berfokus pada deteksi dan respons ancaman *cyber* pada *endpoint* seperti *server* (Karantzas & Patsakis, 2021) Solusi tersebut dapat dibangun dengan bantuan *platform* keamanan *cyber* berbasis *open source* yaitu Wazuh dengan integrasi API VirusTotal yang berfungsi sebagai mendeteksi jenis *malware* yang masuk ke dalam *server endpoint* (Budi et al., 2021).

METODE PENELITIAN

Alur Penelitian

Pada penelitian membangun *agent endpoint* menggunakan Wazuh dan VirusTotal sebagai sistem deteksi serangan *ransomware* LockBit 3.0, digunakan metode solusi keamanan *Endpoint Detection and Response* (EDR). *Endpoint Detection and Response* (EDR) menggabungkan pencegahan, deteksi, penyelidikan, dan respons, memberikan visibilitas, analitik, peringatan, dan respons otomatis untuk meningkatkan keamanan data dan mengatasi ancaman (Gorecki, 2020). Terdapat tiga tahapan yang peneliti lakukan dalam konfigurasi sistem yaitu:



Sumber : (Almima, 2024)
Gambar 1. Alur Penelitian

DOI: https://doi.org/10.37365/jti.v10i2.320
VOL. 10 No. 2 November 2024
P-ISSN : 2460-2108
E-ISSN : 2620-5181

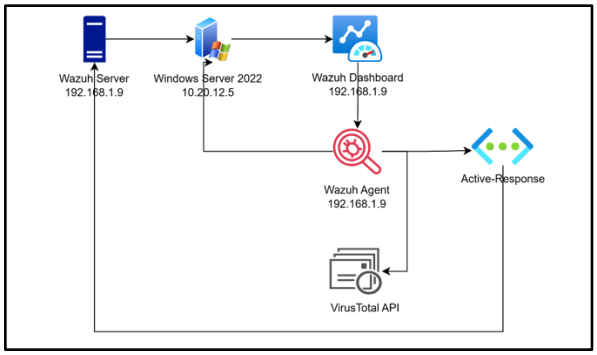
Adapun penjelasan alur penelitian pada gambar 1 sebagai berikut:

1. **Pengumpulan Informasi**
   Pada tahap pengumpulan informasi, peneliti mengumpulkan referensi yang memiliki keterkaitan dengan perancangan deteksi keamanan *server* menggunakan Wazuh untuk menambah pemahaman peneliti selama proses penelitian dilaksanakan (Irwansyah et al., 2022).
2. **Konfigurasi *Platform***
   Pada tahap konfigurasi platform, peneliti melakukan konfigurasi untuk pengujian deteksi ransomware LockBit 3.0 pada Windows Server 2022 menggunakan Wazuh dengan Integrasi API VirusTotal. Pada tahapan ini, terdapat tiga tahapan yang peneliti lakukan dalam konfigurasi sistem yaitu:
   a. **Konfigurasi Wazuh**
      Peneliti melakukan konfigurasi pada Wazuh *server* untuk mengetahui *IP Address* yang dapat digunakan Windows Server 2022 sebagai *endpoint* untuk mengakses Wazuh *dashboard* dan membuat Wazuh *agent* baru untuk memantau aktifitas *server* selama *server* dan *agent* dihidupkan (Retna Mulya & Tarigan, 2018).
   b. **Konfigurasi Windows Server 2022**
      Pada konfigurasi Windows Server 2022, peneliti membuat sebuah sistem *active-response* menggunakan Python IDLE agar *server endpoint* dapat menghapus *file* masuk yang dicurigai sebagai *ransomware* secara otomatis serta membuat *Key* API VirusTotal untuk diintegrasikan dengan Wazuh.
   c. **Integrasi API VirusTotal dengan Wazuh**
      Setelah *Key* API VirusTotal sudah dibuat dan Wazuh *agent* sudah berjalan dengan baik, peneliti melakukan integrasi antara VirusTotal dengan Wazuh melalui Wazuh *server* agar *active-response* dan API VirusTotal yang sudah dibuat dapat aktif mendeteksi *file* yang masuk ke dalam *server*.
3. **Uji Coba**
   Tahap uji coba dilakukan setelah seluruh tahapan dalam tahap konfigurasi sistem selesai. Peneliti melakukan simulasi serangan *ransomware* LockBit 3.0 pada Windows Server 2022 dengan mengunduh *file* berbentuk ZIP yang berisikan *ransomware* tersebut melalui internet untuk memastikan apakah sistem dapat mendeteksi *file* berbahaya. Jika belum berhasil, maka peneliti akan mengkaji ulang kembali apakah konfigurasi sudah dilakukan sesuai tahapan atau ada kesalahan yang peneliti lakukan dalam melakukan konfigurasi sebelumnya.
4. **Analisis Hasil dan Kesimpulan**
   Pada tahap ini, peneliti menganalisis hasil dari simulasi melalui Wazuh *dashboard* untuk mendapatkan informasi lebih lanjut mengenai hasil dari simulasi serangan *ransomware*. Jika hasil sudah tercapai, maka peneliti dapat membuat kesimpulan dari keseluruhan tahapan yang sudah peneliti laksanakan dari studi literatur hingga selesai (Irwansyah et al, 2024).

HASIL DAN PEMBAHASAN

Pada bab hasil dan pembahasan, peneliti memaparkan proses perancangan deteksi ancaman *ransomware* LockBit 3.0 pada *server* menggunakan Wazuh berbasis *open source* dengan integrasi *application programming interface* (API) VirusTotal sesuai dengan alur penelitian yang tertera dalam bab tiga metodologi penelitian.

Pada Gambar 2, terdapat topologi atau gambaran terkait perancangan Wazuh dan VirusTotal untuk mendeteksi serangan *ransomware* pada Windows Server 2022. Wazuh *server* akan membuat *IP address* yang dapat diakses oleh Windows Server 2022 untuk membuka Wazuh *dashboard* dan membuat Wazuh *agent* dengan *IP address* yang sama dengan Wazuh *server*. Kemudian dibuatkan *active-response* pada Windows Server 2022 sebagai media integrasi antara Wazuh *agent*, VirusTotal, dan Windows Server 2022 sehingga Wazuh dan VirusTotal dapat mendeteksi dan menghapus *file* yang mencurigakan.

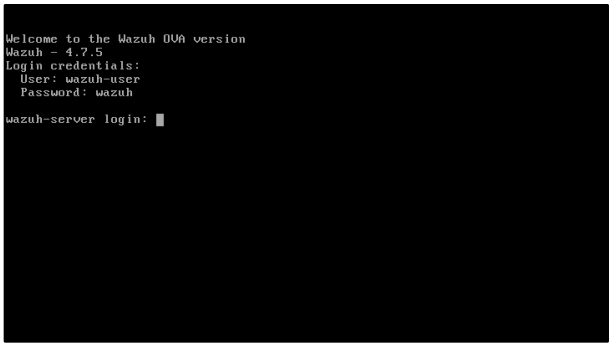


Sumber : (Almima, 2024)
Gambar 2. Topologi Wazuh dan Windows Server 2022

Konfigurasi Wazuh
Pada tahap konfigurasi Wazuh, peneliti melakukan kofigurasi pada Wazuh *server* dan Wazuh *Agent* dengan tujuan agar *server endpoint* yang akan dipantau dapat terhubung dengan Wazuh *dashboard* sebagai *endpoint detection and response*.

Login* Wazuh *Server
Pada tahap awal, peneliti melakukan *import file* Wazuh berbentuk OVA ke dalam Virtual Box agar peneliti dapat mengakses Wazuh *server* sebelum dilakukan konfigurasi

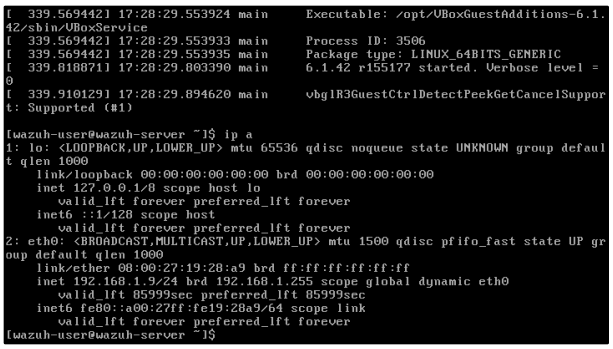
lebih dalam. Setelah proses *import* Wazuh OVA selesai, peneliti mulai menjalankan mesin virtual untuk membuka Wazuh OVA tersebut. Tampilan awal Wazuh akan muncul seperti gambar 3 yang selanjutnya peneliti dapat memasukkan *user* dan *password* yang tertera pada bagian *login credentials* untuk masuk ke dalam Wazuh *server*.



Sumber : (Almima, 2024)
Gambar 3. Tampilan Login Wazuh Server

Pengecekan *IP Address* Wazuh *Dashboard*

Setelah berhasil masuk ke dalam Wazuh *server*, tahapan berikutnya adalah memastikan *IP address* yang disediakan oleh Wazuh *server* agar peneliti dapat masuk ke dalam Wazuh *dashboard*. Pengecekan *IP address* dapat dilakukan dengan mengetik "ip a" pada Wazuh *server*. *IP address* yang dapat digunakan akan tertera pada eth2 yaitu 192.168.1.9 seperti yang tertera pada gambar 4.

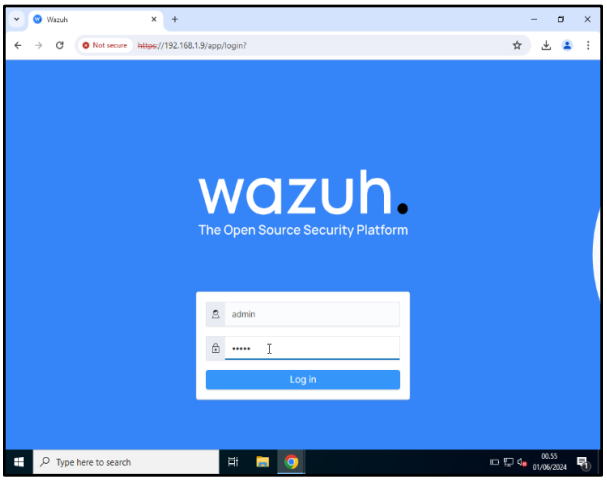


Sumber : (Almima, 2024)
Gambar 4. Pengecekan IP Address Untuk Mengakses Wazuh Dashboard

Login Wazuh *Dashboard*

Setelah *IP address* yang akan digunakan untuk masuk ke dalam Wazuh *dashboard* sudah ditemukan, peneliti melakukan tahapan berikutnya yaitu masuk ke dalam Wazuh *dashboard* menggunakan *IP address* yang disediakan melalui peramban *web* yang tersedia di *server endpoint*. Adapun peneliti menggunakan Chrome untuk masuk ke Wazuh *dashboard* dengan menggunakan https://192.168.1.9.

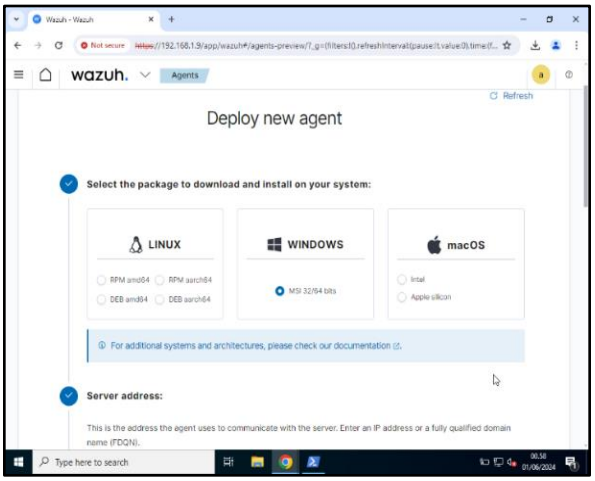
Setelah masuk menggunakan *IP address* yang disediakan, akan muncul tampilan *login* dari Wazuh *dashboard*. Peneliti menggunakan *username* dan *password default* yang disediakan oleh Wazuh yaitu "*admin*" untuk keduanya seperti yang tertera pada gambar 5.



Sumber : (Almima, 2024)
Gambar 5. Tampilan Login Wazuh Dashboard

Membuat Wazuh *Agent*

Setelah peneliti melakukan *login* pada Wazuh *dashboard*, peneliti membuat Wazuh *agent* baru melalui fitur *Deploy New Agent* agar Wazuh dapat terhubung dengan server *endpoint* untuk memantau aktifitas pada *server endpoint* tersebut. Pada gambar 6 peneliti memilih sistem operasi *endpoint* Windows sesuai *server endpoint* yang digunakan oleh peneliti dalam penelitian ini.

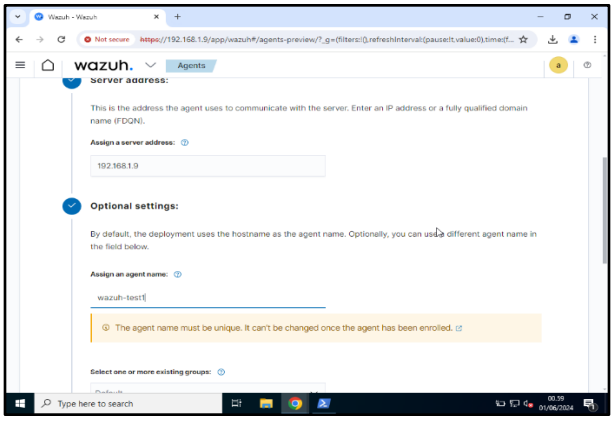


Sumber : (Almima, 2024)
Gambar 6. Pemilihan Sistem Operasi Endpoint Untuk Pembuatan Wazuh Agent Baru

Akreditasi Peringkat 4 (Sinta 4) Berdasarkan Keputusan Dirjen Pendidikan Tinggi, Riset, dan Teknologi Kemendikbudristek No.177/E/KPT/2024, 15 Oktober 2024. Diterbitkan oleh LPPM STMIK Widuri

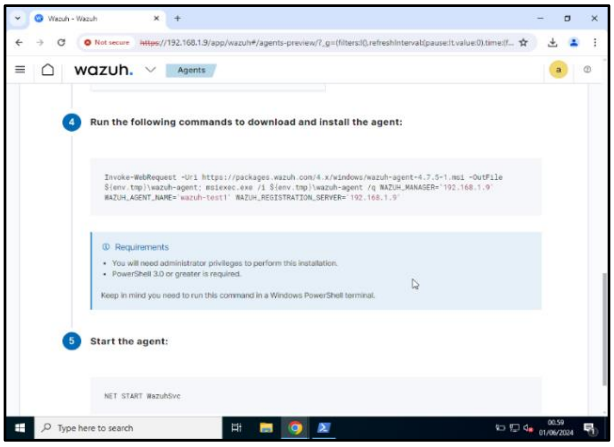
DOI: https://doi.org/10.37365/jti.v10i2.320
VOL. 10 No. 2 November 2024
P-ISSN : 2460-2108
E-ISSN : 2620-5181

Pada gambar 7, peneliti memasukkan *IP address* yang sama dengan *IP address* yang digunakan untuk mengakses Wazuh *dashboard* pada bagian *server address*. *Server address* dimasukkan ke dalam pembuatan Wazuh *agent* agar *agent* pada *server endpoint* dapat terhubung dengan Wazuh *server*. Pada bagian *Optional Settings*, peneliti menggunakan nama "Test-1" sebagai nama *agent* yang akan digunakan untuk memantau aktifitas *server endpoint*.



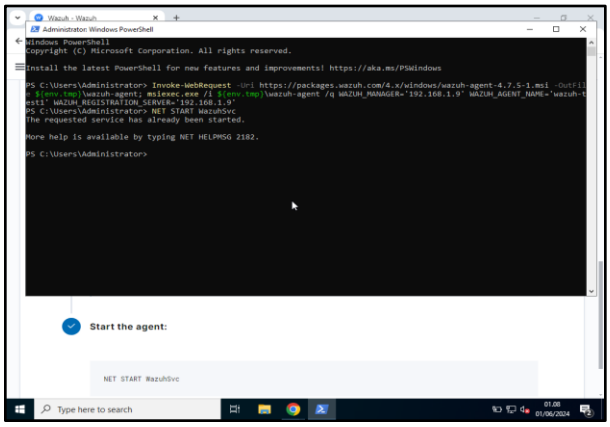
Sumber : (Almima, 2024)
Gambar 7. Input IP Server Address dan Nama Agent

Setelah pengisian *server address* dan nama *agent* selesai, Wazuh memberikan dua *command line* PowerShell yang berisikan installasi *software* Wazuh *agent* dan menjalankan *software* Wazuh *agent* yang sudah di*install* agar *agent* yang sudah dibuat di Wazuh *dashboard* sebelumnya dapat mulai berjalan memantau aktiftas *server endpoint* seperti yang tertera pada gambar 8.



Sumber : (Almima, 2024)
Gambar 8. Command Line Untuk Menjalankan Wazuh Agent Pada Windows Server Endpoint

Pada gambar 8, peneliti menjalankan kedua *command line* yang diberikan Wazuh menggunakan PowerShell Administrator untuk installasi dan mengaktifkan Wazuh *agent* agar dapat berfungsi pada *server endpoint*. Pada gambar 9 tertera bahwa *service* pada Wazuh *agent* sudah bisa berjalan setelah menjalankan kedua *command line* tersebut.



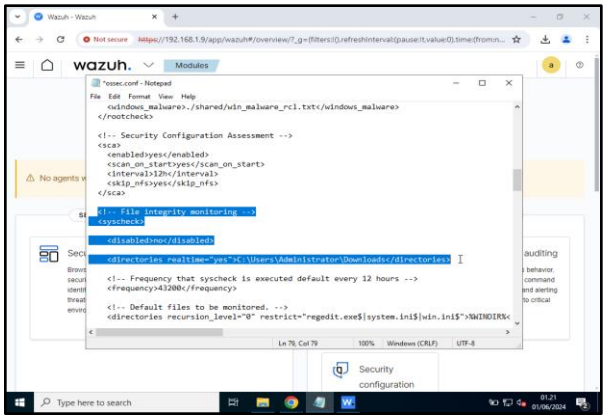
Sumber : (Almima, 2024)
Gambar 9. Mengaktifkan Wazuh Agent Pada Windows Server Endpoint

Konfigurasi Windows Server 2022

Setelah seluruh tahapan konfigurasi pada Wazuh selesai dan Wazuh *agent* sudah berjalan dengan baik, selanjutnya peneliti melakukan konfigurasi pada *server endpoint* yang peneliti gunakan yaitu Windows Server 2022.

Konfigurasi *File Integrity Monitoring*

Pada tahap konfigurasi *File Integrity Monitoring*, peneliti membuat syscheck pada Wazuh *agent* melalui direktori C pada *folder* ossec-agent bagian ossec.conf. Syscheck tersebut dibuat menjadi aktif agar Wazuh *agent* dapat melakukan *monitoring file* secara *real-time*. Pada gambar 10 peneliti membuat direktori yang dapat dilakukan *monitoring* oleh Wazuh *agent* secara *real-time* adalah pada direktori C:\Users\Administrator\Downloads.

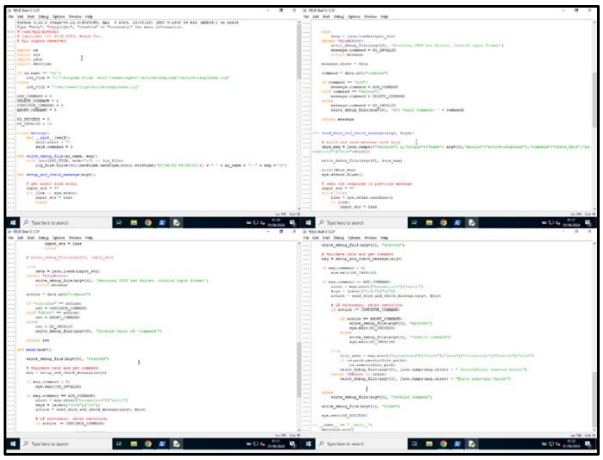


Sumber : (Almima, 2024)
Gambar 10. Mengaktifkan File Integrity Monitoring

Pembuatan *Active-Response*

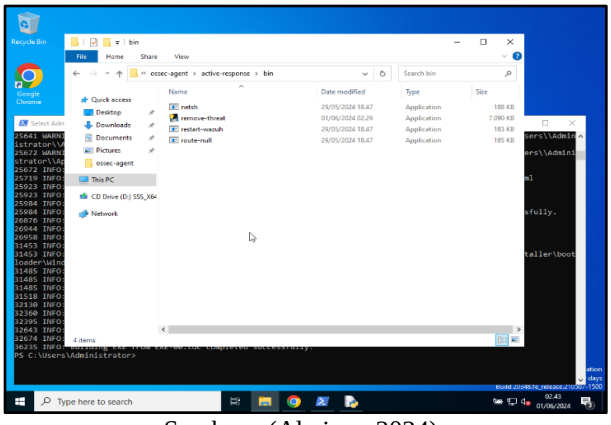
Pada tahapan membuat *active-response*, peneliti membuat *script* seperti pada gambar 11, agar *server endpoint* dapat membuang *file* secara *real-time* jika ada *file* berbahaya terdeteksi masuk ke dalam *server endpoint* menggunakan Python. Pada *script* yang dibuat, peneliti menentukan *log file* Wazuh *agent* berada yaitu pada direktori C pada *folder* ossec-agent bagian *active-response* agar aktifitas *active-response* menghapus *file* dapat masuk ke dalam *log* Wazuh *agent*.

\



Sumber : (Almima, 2024)
Gambar 11. Script Python Untuk Respon Remove File

Setelah *active-response* sudah dibuat dan sudah dipastikan tidak ada *error syntax*, peneliti menyimpan *file* dengan nama remove-threat.exe. Peneliti menggunakan format .exe agar *active-response* tersebut dapat berjalan sendiri ketika Wazuh *agent* sudah berjalan. *File active-response* yang sudah disimpan kemudian dipindahkan ke direktori Wazuh *agent* yaitu pada direktori C pada *folder* ossec-agent bagian *active-response* seperti pada gambar 12.



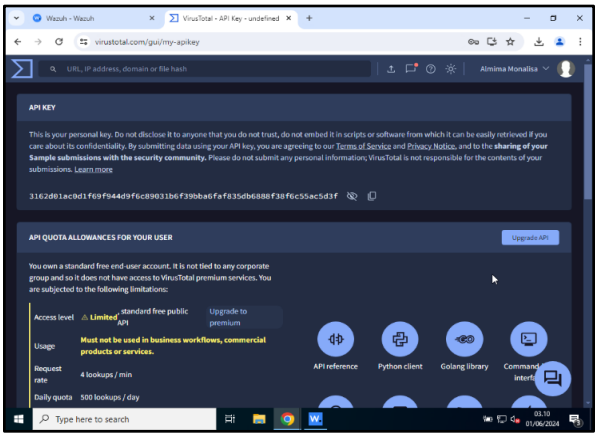
Sumber : (Almima, 2024)
Gambar 12. Memindahkan File Active-Response ke Direktori Wazuh Agent

Integrasi API VirusTotal dengan Wazuh

Setelah tahapan konfigurasi pada *endpoint* Windows Server 2022 selesai, peneliti melakukan integrasi API VirusTotal dengan Wazuh *server* agar VirusTotal dapat mendeteksi *file* yang masuk ke dalam direktori pada *server endpoint*.

Pembuatan API *Key* VirusTotal

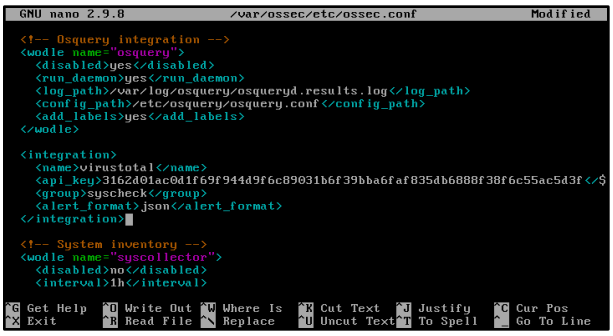
Pada tahap ini, peneliti membuat akun VirusTotal terlebih dahulu untuk mendapatkan API *Key personal use*. Adapun API *Key* yang peneliti dapatkan adalah 3162d011c0d1f69f944d9f6c89031b6f39bba6faf835db6888f38f6c55ac5d3f . API *Key* tersebut peneliti gunakan untuk integrasi dengan Wazuh *server*.



Sumber : (Almima, 2024)
Gambar 13. API Key VirusTotal

Konfigurasi Integrasi VirusTotal

Setelah mendapatkan API *Key* VirusTotal, peneliti membuka kembali Wazuh *server* dan masuk ke direktori /var/ossec/etc/ossec.conf. Pada direktori ini, peneliti menambahkan konfigurasi Wazuh pada bagian *integration* dengan tujuan agar VirusTotal dapat ikut aktif secara otomatis ketika *File Integrity Monitoring* pada syscheck yang telah peneliti aktifkan sebelumnya berjalan ketika ada *file* mencurigakan masuk.



Sumber : (Almima, 2024)
Gambar 14. Konfigurasi Integrasi VirusTotal Dan Wazuh Server

DOI: https://doi.org/10.37365/jti.v10i2.320
VOL. 10 No. 2 November 2024
P-ISSN : 2460-2108
E-ISSN : 2620-5181

Integrasi VirusTotal Dengan *Active-Response*

Pada tahapan ini, peneliti melakukan integrasi antara VirusTotal dengan *file active-response* yang sudah peneliti buat sebelumnya dengan nama *file* remove-threat.exe pada direktori yang sama dengan konfigurasi integrasi API *Key* VirusTotal yaitu direktori /var/ossec/etc/ossec.conf seperti yang tertera pada gambar 15, Integrasi ini bertujuan agar *file* remove-threat.exe dapat berjalan otomatis menghapus *file* ketika Wazuh dan VirusTotal mendeteksi adanya *file* berbahaya yang masuk ke dalam *server endpoint*.

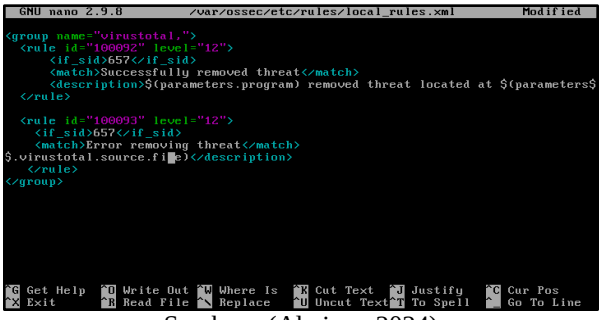
Pada bagian *command*, Peneliti mengubah *timeout allowed* menjadi *no* agar *file* remove-threat.exe dapat terus berjalan menghapus *file* selama VirusTotal terus mendeteksi adanya *file* berbahaya. Pada bagian *active-response*, peneliti mengubah bagian *disabled* menjadi *no* agar *command remove threat* diatas tidak berhenti.

Sumber : (Almima, 2024)

Gambar 15. Mengaktifkan *Active-Response*

Membuat *Rules* VirusTotal Pada Wazuh *Server*

Pada tahapan ini, peneliti masuk ke dalam direktori Wazuh *server* /var/ossec/etc/rules/local_rules.xml. Peneliti membuat *rules* VirusTotal dengan *level alert* yaitu 12 yang memiliki arti bahwa ada indikasi serangan pada sistem *endpoint*. Dengan dibuatnya *rules alert*, serangan yang terdeteksi oleh VirusTotal secara otomatis akan masuk ke dalam alert level 12 dan administrator dapat memeriksa secara *filtering alert level* 12 ke atas.

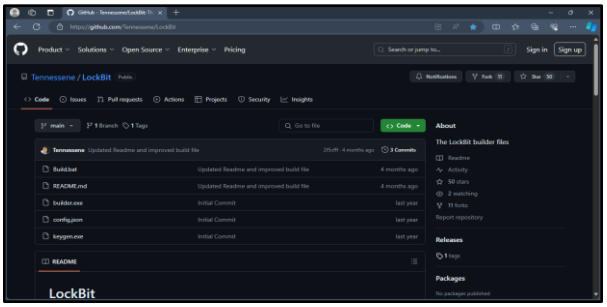


Sumber : (Almima, 2024)

Gambar 16. Rules VirusTotal

Uji Coba

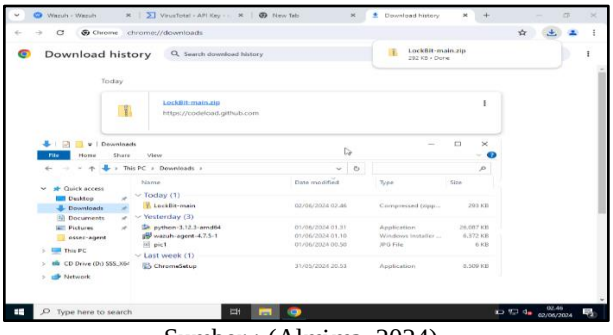
Setelah konfigurasi secara keseluruhan selesai, peneliti melakukan *test* atau uji coba dengan cara mengunduh *file* dengan format ZIP yang berisikan *ransomware* LockBit 3.0 melalui laman internet. Peneliti menyiapkan *link* untuk mengunduh *file* berisikan *ransomware* LockBit 3.0 dan peneliti menggunakan *link* GitHub seperti yang tertera pada gambar 17.



Sumber : (*https://github.com/Tennessene/LockBit*)

Gambar 17. File Ransomware LockBit 3.0 Di GitHub

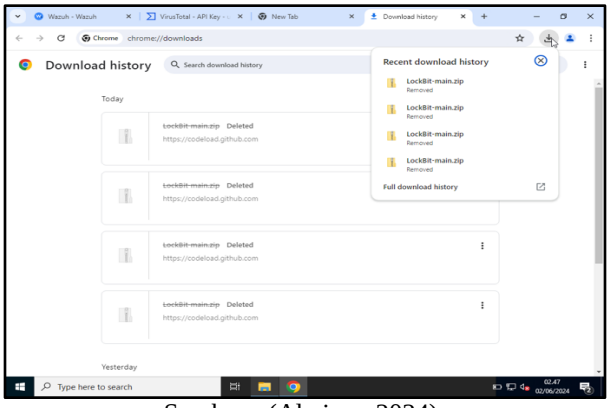
Setelah peneliti sudah menyiapkan *link file* yang akan peneliti gunakan, berikutnya peneliti melakukan uji coba dengan mengunduh *file* tersebut pada peramban *web* menggunakan *link* yang sudah disiapkan. Pada gambar 18, tertera bahwa *file* dengan format *file* ZIP yang berisikan *ransomware* LockBit 3.0 berhasil masuk ke dalam direktori C:\Users\Administrator\Downloads.



Sumber : (Almima, 2024)

Gambar 18. File Ransomware LockBit 3.0 Berhasil diunduh

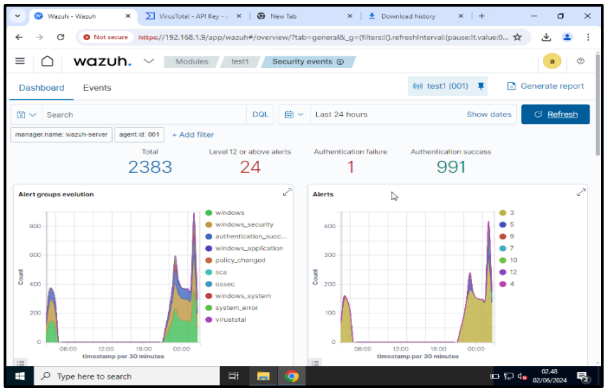
Setelah *file ransomware* LockBit 3.0 berhasil diunduh, peneliti melakukan *refresh* pada direktori C:\Users\Administrator\Downloads. *File* yang berisikan *ransomware* LockBit 3.0 tersebut hilang baik pada direktori C:\Users\Administrator\Download setelah peneliti melakukan *refresh* pada File Explorer.



Sumber : (Almima, 2024)
Gambar 19. File Ransomware LockBit 3.0 Dihapus Secara Otomatis

Hasil Uji Coba

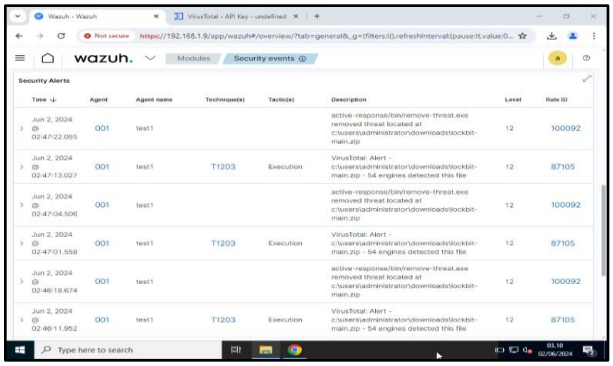
Setelah peneliti melakukan uji coba, peneliti kembali membuka Wazuh *Dashboard* pada bagian *Security Events*. Pada gambar 20, tertera bahwa terdapat *alert* atau peringatan keamanan terhadap *server endpoint* yang peneliti gunakan yaitu Windows Server 2022. Terdapat 24 *alert* dengan *level alert* 12 keatas dan terdapat *alert groups* VirusTotal pada bagian *Alert Groups Evolution* yang artinya bahwa API VirusTotal sudah berjalan dengan baik selama peneliti melakukan uji coba sebelumnya.



Sumber : (Muchammad Sholeh, 2024)
Gambar 20. Tampilan Wazuh Dashboard Bagian Alerts

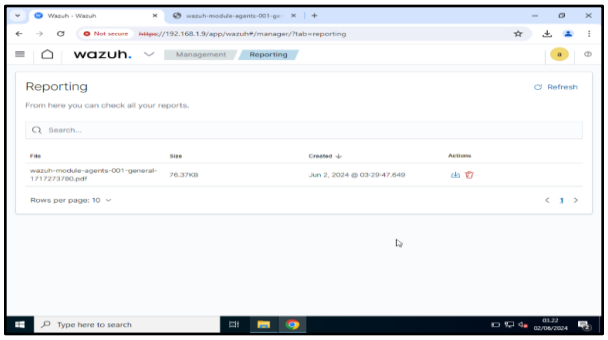
Pada bagian *Security Alerts*, terdapat penjelasan terkait *alerts* keamanan terhadap *server endpoint* yang diberikan oleh Wazuh secara *real-time*. Pada gambar 4.20 terdapat bahwa Wazuh dan VirusTotal berhasil mendeteksi *file* ZIP berisikan *ransomware* LockBit 3.0 pada direktori C:\Users\Administrator\Downloads pada pukul 02:46:11 setelah peneliti mengunduh *file* tersebut. Dalam selang waktu 0.7 detik pada pukul 02:46:18, *active-response* pada Wazuh *server* yang telah peneliti buat sebelumnya mulai merespon Wazuh dan VirusTotal kemudian menjalankan remove-threat.exe untuk menghapus *file* yang terdeteksi oleh VirusTotal pada direktori C:\Users\Administrator\Downloads.

Peneliti melakukan uji coba secara berulang sebanyak tiga kali dan lama waktu Wazuh dan VirusTotal untuk mendeteksi hingga *active-response* aktif menghapus *file ransomware* LockBit 3.0 relatif sama yaitu kurang dari 1 detik seperti yang tertera pada gambar 21.



Sumber : (Muchammad Sholeh, 2024)
Gambar 21. Tampilan *Security Alerts* Pada Wazuh Dashboard

Pada Wazuh *dashboard*, peneliti dapat mengunduh laporan dokumentasi dalam bentuk grafik yang dapat digunakan sebagai bahan evaluasi terhadap keamanan *server endpoint*. Peneliti mengunduh laporan melalui *tools* yang ada pada Wazuh *Dashboard* yaitu pada bagian *management*. Laporan dokumentasi ini dapat digunakan untuk melakukan evaluasi terkait keamanan pada *server endpoint* atau melakukan mitigasi jika diperlukan.



Sumber : (Muchammad Sholeh, 2024)
Gambar 22. Mengunduh Laporan Dokumentasi Wazuh Dashboard

DOI: https://doi.org/10.37365/jti.v10i2.320
VOL. 10 No. 2 November 2024
P-ISSN : 2460-2108
E-ISSN : 2620-5181

KESIMPULAN

Kesimpulan pada penelitian ini sebagai berikut: Setelah dilakukan uji coba sebanyak tiga kali, Wazuh *Agent* dengan integrasi API VirusTotal berhasil mendeteksi seluruh serangan *ransomware* dan terhapus secara otomatis melalui *active-response* yang sudah dibuat dalam rentang waktu 0.7 detik setelah *file* masuk ke dalam direktori *downloads* dan *Endpoint Detection and Response* (EDR) pada wazuh bekerja dengan mendeteksi aktivitas mencurigakan pada Windows Server 2022 melalui pemantauan integritas *file* pada *File Integrity Monitoring* yang terhubung dengan Wazuh *Agent* yang sudah terintegrasi dengan API VirusTotal.

DAFTAR PUSTAKA

Asosiasi Penyelenggara Jasa Internet Indonesia. (2023). *Survei Penetrasi & Perilaku Internet 2023*.

Budi, E., Wira, D., & Infantono, A. (2021). Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0. *Prosiding Seminar Nasional Sains Teknologi Dan Inovasi Indonesia (SENASTINDO)*, *3*, 223–234. https://doi.org/10.54706/senastindo.v3.2021.141

Firman Pratama, N. (2023). Perancangan Sistem Deteksi Dini Keamanan Informasi DISKOMINFO Kabupaten Bandung. *Jurnal Teknik Informatika Dan Sistem Informasi*, *10*(1), 808–820. https://doi.org/https://doi.org/10.35957/jatisi.v10i1.3488

Gorecki, A. (2020). Cyber Breach Response That Actually Works. In A. Brand & R. Gregory Taylor-Broun (Eds.), *Cyber Breach Response That Actually Works* (p. 129). Wiley.

Irwansyah, Akhmad Rizal Dzikrillah, Muhammad Rifky Aditya, Syafira Nadia Al-Fadillah, M. M. M. (2024). Impelementasi Wireless Sebagai Media Komunikasi Pada Software Kendali Manipulator Mobile Multi Lengan. *Infotech: Journal of Technology Information*, *10*(1), 21–26. https://doi.org/https://doi.org/10.37365/jti.v10i1.242

Irwansyah, I., Wiranata, A. D., Muryono, T. T., & Budiyantara, A. (2022). Sistem Pakar Deteksi Kerusakan Jaringan Local Area Network (Lan) Menggunakan Metode Beckward Chaining Berbasis Web. *Infotech: Journal of Technology Information*, *8*(2), 135–142. https://doi.org/https://doi.org/10.37365/jti.v8i2.150

Janofsky, A. (2024, January 15). *Ransomware tracker: The latest figures [January 2024]*.

Karantzas, G., & Patsakis, C. (2021). An Empirical Assessment of Endpoint Detection and Response Systems against Advanced Persistent Threats Attack Vectors. *Journal of Cybersecurity and Privacy*, *1*(3), 387–421. https://doi.org/10.3390/jcp1030021

Muchammad Sholeh, A. M. P. (2024). *Membangun Agent Endpoint Detection And Response (Edr) Menggunakan Wazuh Dan Virustotal Sebagai Sistem Deteksi Serangan Ransomware Lockbit 3.0*.

Priyatna Darmawan, A., & Esti Pratiwi, I. (2023, May 13). Hacker Ransomware LockBit Klaim Curi 15 Juta Data BSI, Pakar: Diperkirakan sejak Libur Lebarab. *Kompas.Com*.

Retna Mulya, B. W., & Tarigan, A. (2018). Pemeringkatan Risiko Keamanan Sistem Jaringan Komputer Politeknik Kota Malang Menggunakan Cvss Dan Fmea. *ILKOM Jurnal Ilmiah*, *10*(2), 190–200. https://doi.org/10.33096/ilkom.v10i2.311.190-200

Sadya, S. (2023, March 9). *APJII: Pengguna Internet Indonesia 215,63 Juta pada 2022-2023*. Dataindonesia.Id.

Yuliardi, S. (2023, August 16). Akamai: di Kawasan APJ Kerentanan Meluas, Jumlah Korban Ransomware Meningkat 204 Persen. *WartaEkonomi.Co.Id*.

VOL. 10 No. 2 November 2024
P-ISSN : 2460-2108
E-ISSN : 2620-5181

DOI: https://doi.org/10.37365/jti.v10i2.320

Akreditasi Peringkat 4 (Sinta 4) Berdasarkan Keputusan Dirjen Pendidikan Tinggi, Riset, dan Teknologi Kemendikbudristek No.177/E/KPT/2024, 15 Oktober 2024. Diterbitkan oleh LPPM STMIK Widuri