VISA: Journal of Visions and Ideas
Vol 5 No 3 (2025) 1215–1230 E-ISSN 2809-2058 P-ISSN 2809-2643
DOI: 47467/visa.v5i3.9145

Implementasi *Extended Detection and Response* pada *Security Operation Center* dan *Computer Security Independent Response Team* dalam Peningkatan Sistem Keamanan Informasi Guna Meningkatkan Sistem Pertahanan Informasi

Fathan Luqman[1], H.A. Danang Rimbawa[2], Sunarta[3], Nugroho Wibisono[4]
[1234]Universitas Pertahanan Republik Indonesia
athanluqman2002@gmail.com[1]

ABSTRACT

The rapid development of digital technology increases the complexity of cyber threats, which are now increasingly sophisticated and organised, targeting individuals, enterprises and critical infrastructure. Therefore, an information security system capable of automatically detecting and responding to threats is an urgent need. This research aims to examine the implementation of Extended Detection and Response (XDR) in the Security Operation Centre (SOC) and Computer Security Incident Response Team (CSIRT) to improve the effectiveness of information security systems. The method used is experimental with testing in a controlled environment using Wazuh as the XDR platform. This study analyses how XDR collects, analyses and responds to log data in real-time to detect threats more accurately. The results show that XDR is able to improve threat detection by integrating logs from multiple sources, including endpoints, networks, and cloud services, and automating incident mitigation for faster response. The integration of Machine Learning in XDR is also proven to improve attack detection accuracy, reduce false positives, and speed up incident analysis. In conclusion, XDR is a comprehensive solution for modern information security systems, especially in the context of SOC and CSIRT, with its capabilities in detection-based analytics, multi-source data correlation, and automated response to threats. Based on this test, the efficiency of XDR in detecting and mitigating malware attacks is 98.3% using up to 60 malware and respons time under 10 second. Therefore, the implementation of XDR is recommended for organisations looking to enhance their security systems in a more adaptive and proactive manner in the face of evolving cyber threats.
Keywords: *Extended Detection and Response (XDR), Security Operation Center (SOC), Computer Security Incident Response Team (CSIRT), cybersecurity, threat detection, Wazuh*

ABSTRAK

Perkembangan teknologi digital yang pesat meningkatkan kompleksitas ancaman siber, yang kini semakin canggih dan terorganisir, menargetkan individu, perusahaan, dan infrastruktur kritis. oleh karena itu, sistem keamanan informasi yang mampu mendeteksi dan merespons ancaman secara otomatis menjadi kebutuhan mendesak. penelitian ini bertujuan mengkaji implementasi *extended detection and response (xdr*) dalam *security operation center (soc)* dan *computer security incident response* team *(csirt)* guna meningkatkan efektivitas sistem keamanan informasi. metode yang digunakan adalah eksperimen dengan pengujian dalam lingkungan yang dikontrol menggunakan wazuh sebagai platform xdr. studi ini menganalisis bagaimana xdr mengumpulkan, menganalisis, dan merespons data log secara *real-time* untuk mendeteksi ancaman dengan lebih akurat. hasil penelitian menunjukkan bahwa xdr mampu meningkatkan deteksi ancaman dengan mengintegrasikan log dari berbagai sumber, termasuk *endpoint*, jaringan, dan layanan *cloud*, serta mengotomatiskan

VISA: Journal of Visions and Ideas
Vol 5 No 3 (2025) 1215–1230 E-ISSN 2809-2058 P-ISSN 2809-2643
DOI: 47467/visa.v5i3.9145

mitigasi insiden untuk respons yang lebih cepat. integrasi *machine learning* dalam xdr juga terbukti meningkatkan akurasi deteksi serangan, mengurangi *false positives*, dan mempercepat analisis insiden. kesimpulannya, xdr menjadi solusi komprehensif bagi sistem keamanan informasi modern, terutama dalam konteks soc dan csirt, dengan kemampuannya dalam analitik berbasis deteksi, korelasi data multi-sumber, dan respons otomatis terhadap ancaman. berdasarkan pengujian ini juga dihasilkan bahwa efisiensi xdr dalam melakukan pendeteksian dan mitigasi serangan malware adalah sebesar 98,3% dengan menggunakan hingga 60 *malware* dan waktu respon kurang dari 10 detik. oleh karena itu, implementasi xdr direkomendasikan bagi organisasi yang ingin meningkatkan sistem keamanan mereka secara lebih adaptif dan proaktif dalam menghadapi ancaman siber yang terus berkembang.
kata kunci: *extended detection and response (xdr)*, s*ecurity operation center (soc)*, *computer security incident response team (csirt)*, keamanan siber, deteksi ancaman, wazuh

PENDAHULUAN

Perkembangan teknologi di dunia semakin dinamis dan tak terduga dalam hal keamanan komputer. Karena ancaman siber semakin sering terjadi, canggih, dan merusak, alat keamanan lama tidak lagi memadai. Solusi titik dan pertahanan yang terisolasi meninggalkan celah yang memungkinkan penyerang menembus jaringan dan mencuri data. Menurut laporan terbaru, biaya rata-rata pelanggaran data sekarang melebihi 4 juta USD. Dengan risiko keuangan dan reputasi yang begitu besar, organisasi membutuhkan kemampuan keamanan yang menyediakan visibilitas lengkap di seluruh infrastruktur mereka dan memungkinkan respons yang cepat dan terkoordinasi terhadap ancaman. Sangatlah penting untuk menggunakan solusi yang tepat yang meningkatkan perlindungan infrastruktur, baik lokal, di awan, atau hibrida (George *et al,* 2023; Brandao *et al,* 2021).

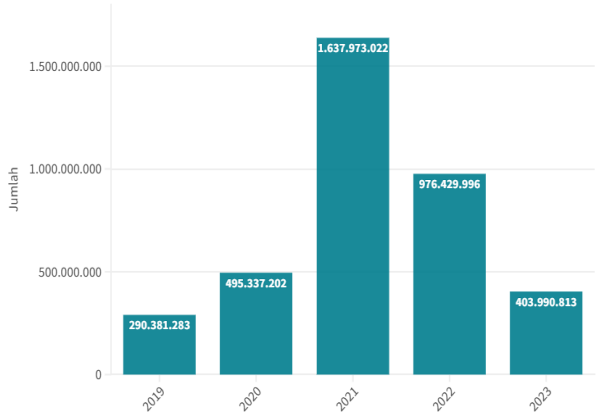
Berdasarkan Data statistik dari Badan Siber dan Sandi Negara (BSSN) yang dilampirkan pada gambar 1.1 mencatat bahwa telah terjadi 1,6 miliar serangan siber terhadap Indonesia pada tahun 2021. Dibandingkan dengan tahun sebelumnya (terjadi 495,33 juta serangan siber), jumlah ini meningkat sebesar 323,23%. Serangan yang dilancarkan diantaranya serangan terhadap aplikasi web, serangan terhadap bisnis, serangan terhadap identitas dan *malware*.

Pada tahun 2021 terjadi lonjakan yang dipengaruhi oleh adanya covid-19 yang kemudian pemerintah Indonesia menetapkan PPKM (Pemberlakuan Pembatasan Kegiatan Masyarakat). Dengan semua melakukan semua aktivitas melalui internet, maka muncul celah keamanan yang dapat dimanfaatkan oleh orang yang tidak bertanggung jawab untuk melakukan kejahatan melalui media internet atau yang sering kita sebut dengan istilah kejahatan *cyber (Cyber Crime)* (Atmojo *et al*, 2021).

Cybercrime dapat didefinisikan sebagai pelanggaran yang dilakukan terhadap perorangan atau sekelompok individu dengan motif kriminal untuk secara sengaja menyakiti reputasi korban atau menyebabkan kerugian fisik atau mental atau kerugian kepada korban baik secara langsung maupun tidak langsung, menggunakan jaringan telekomunikasi modern seperti Internet (jaringan termasuk namun tidak terbatas pada ruang *Chat, email, notice boards* dan kelompok) dan telepon genggam (Bluetooth / SMS / MMS) (Gani, 2018). Upaya untuk melindungi para pengguna dunia

VISA: Journal of Visions and Ideas
Vol 5 No 3 (2025) 1215–1230 E-ISSN 2809-2058 P-ISSN 2809-2643
DOI: 47467/visa.v5i3.9145

digital, pemerintah Indonesia telah mengeluarkan peraturan untuk melindungi sistem komputer dari serangan digital atau akses ilegal, seperti Undang-Undang Informasi Transaksi Elektronik (UU ITE). UU ITE tak hanya menjadi pelindung masyarakat di dunia digital namun menjadi aturan bersama bagi masyarakat yang beraktivitas di dunia digital.



Gambar 1.1 Data Statistik Serangan Siber di Indonesia
Sumber: Laporan Keamanan Siber BSSN, 2023

Dengan meningkatnya intensitas dan kompleksitas ancaman siber, kebutuhan akan pendekatan yang lebih komprehensif dalam menangani insiden keamanan informasi semakin krusial. Untuk menjawab tantangan ini, *Extended Detection and Response* (XDR) muncul sebagai solusi yang inovatif dan optimal dalam mendeteksi serta merespons ancaman siber dengan lebih cepat dan terintegrasi. XDR menggabungkan kemampuan *monitoring* dan analisis data dari berbagai sumber dalam satu platform untuk memperkuat operasional *Security Operations Center* (SOC) dan *Computer Security Incident Response Team* (CSIRT).

Pada penelitian ini, implementasi XDR diharapkan dapat meningkatkan kinerja SOC dan CSIRT, terutama dalam hal deteksi, investigasi, dan respons terhadap ancaman siber yang semakin canggih. Penelitian ini bertujuan untuk mengkaji penerapan XDR dalam konteks operasional SOC dan CSIRT guna mengevaluasi keefektifannya dalam meningkatkan keamanan siber.

METODE PENELITIAN

Metode penelitian yang digunakan adalah studi kasus dengan pendekatan *experimental research*.

a. Keterbatasan sumber data
   Penelitian ini terbatas pada data yang tersedia dari tempat penelitian dan tidak mencakup data dari organisasi lain yang mungkin memiliki pendekatan berbeda dalam implementasi XDR.
b. Keterbatasan deteksi
   Deteksi pada pengetesan atau uji ini dilakukan untuk mendeteksi *malware* dan serangan atau penetrasi terhadap domain server.
c. Pengujian

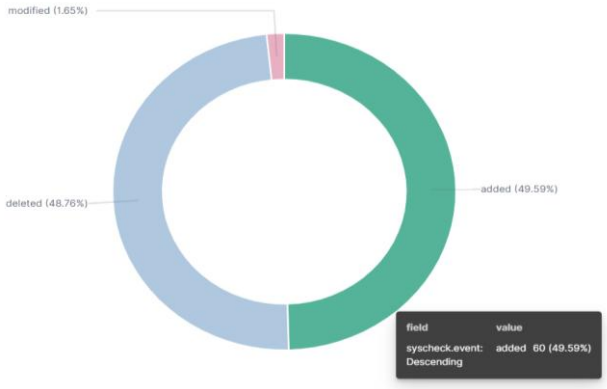
VISA: Journal of Visions and Ideas
Vol 5 No 3 (2025) 1215–1230 E-ISSN 2809-2058 P-ISSN 2809-2643
DOI: 47467/visa.v5i3.9145

Pengujian *malware detection* dilakukan dengan menggunakan *malware*. Pengujian *DoS attack* menggunakan *tools* hping3 dengan metode *SYN flood, ICMP flood* dan *UDP flood*. Pengujian *brute force* menggunakan *tools* hydra. Pengujian difokuskan pada *malware detection*, NIDS, dan *DoS attack.*

HASIL DAN PEMBAHASAN

Detection and Deleting *Malware*

Hasil daripada tes deteksi dan pengahapusan terhadap *malware* sebagai berikut:



Gambar 4.1 Diagram Hasil Pengujian
Sumber: diolah oleh penulis, 2025

Ditampilkan pada gambar 4.1 bahwa pengujian menggunakan 60 *malware* dengan cara menyimpan *file* yang terindikasi *malware* pada direktori yang kemudian *file* akan terdeteksi oleh dan dilakukan deleting atau penghapusan *file* yang terindikasi *malware* oleh sistem. Maka dengan itu dapat dilakukan penghitungan persentase efektifitas sistem berdasarkan deteksi dan penghapusan *file* dengan persamaan berikut.

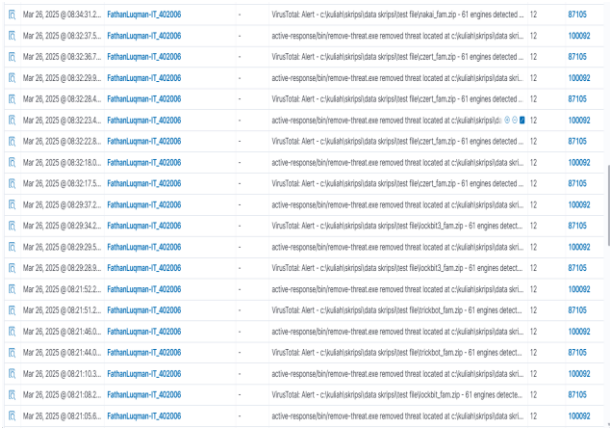
$$\frac{\text{deleted } file}{\text{added } file} \; x \; 100\% \tag{4.1}$$

$$\frac{48{,}76}{49{,}59} \; x \; 100 = \; 98.32\% \tag{4.2}$$

Berdasarkan persamaan 4.1 dan 4.2 , maka dapat dikatakan bahwa persentase efektifitas sistem berdasarkan deteksi dan penghapusan *file* dengan persamaan adalah sebesar 98,32% dengan total *file* yang di masukan berjumlah 60 sedangkan *file* yang terhapus berjumlah 59.

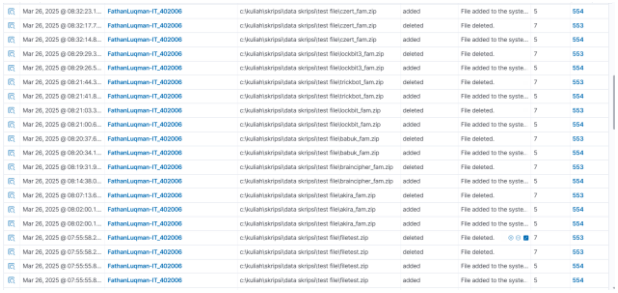
Log dari aktifivas direktori pada *endpoint* dicatat dan dimunculkan pada *log event* pada pada menu *File Integrity Monitoring* (FIM) dan juga pada menu *Malware Detection.* Tampilan dari log yang muncul pada *dashboard* dapat dilihat pada gambar berikut.

VISA: Journal of Visions and Ideas
Vol 5 No 3 (2025) 1215–1230 E-ISSN 2809-2058 P-ISSN 2809-2643
DOI: 47467/visa.v5i3.9145



Gambar 4.2 Log *Malware Detection*
Sumber : diolah oleh peneliti, 2025

Pada gambar 4.2 menampilkan log keamanan dari sistem XDR pada *dashboard malware detection* yang menunjukkan aktivitas *monitoring* dan respons terhadap ancaman yang terdeteksi yang memiliki beberapa parameter yang ditampilkan seperti *timestamp*, *agent name*, *rule description*, *rule level*, hingga *rule id.*



Gambar 4.3 Log *File Integrity Monitoring*
Sumber : diolah oleh peneliti, 2025

Pada gambar 4.3 menampilkan log keamanan dari sistem XDR pada *dashboard File integrity Monitoring* yang menunjukkan aktivitas *monitoring* dan respons terhadap ancaman yang terdeteksi yang memiliki beberapa parameter yang ditampilkan seperti *timestamp*, *agent name*, *syscheck path, syscheck event, rule description*, *rule level*, hingga *rule id.*

Deteksi Serangan Domain Server

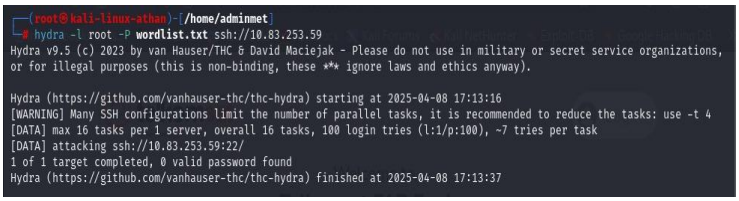
Pada bagian ini membahas mengenai hasil dari implementasi dan pengujian sistem XDR terhadap domain server yang dilakukan serangan berupa *Brute force, Dos Attack, Malware, Adware, Known bad CA's & Certificates, Tor .onion response and random Tor nodes connection*.*Simulate an outbound SSH scan, External IP Address Lookup website, URL Shortener* . Hasil dari pengujian ini ditampilkan dalam bentuk log yang di kumpulkan oleh Wazuh sebagai XDR dan SIEM.

Pada pengujian ini *Brute force, Dos Attack, Malware, External IP Address*

VISA: Journal of Visions and Ideas
Vol 5 No 3 (2025) 1215–1230 E-ISSN 2809-2058 P-ISSN 2809-2643
DOI: 47467/visa.v5i3.9145

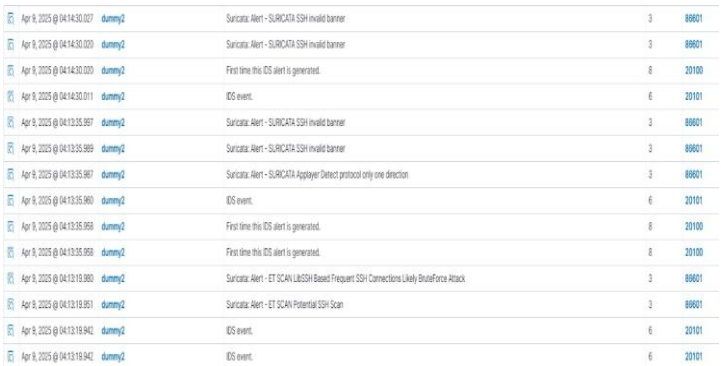
Lookup website, hingga *URL Shortener* yang dilakukan menggunakan metode manual dan serangan menggunakan berbagai *tools* pada Kali-Linux. Serangan dilakukan kepada server yang telah ditanamkan Wazuh-Agent dan *agent* sudah dipastikan berjalan.

Brute force



Gambar 4.4 konfigurasi *Script* Hydra
Sumber: diolah oleh penulis, 2025

Gambar 4.4, merupakan *script* yang dilakukan untuk melakukan penetrasi berupa *brute force. Script* dijalankan menggunakan *tools* Hydra dengan aplikasi Kali-Linux menggunakan operasi Linux. Hydra digunakan untuk melakukan serangan *brute-force* terhadap layanan SSH yang berjalan di IP 10.83.253.59 dengan menggunakan *username* root dan daftar *password* dari *file* wordlist.txt. *Hydra* mencoba masuk dengan menguji berbagai *password* dari *wordlist* yang diberikan. Namun, hasilnya menunjukkan bahwa tidak ada password yang cocok, sehingga serangan gagal. Selain itu, Hydra memberikan peringatan bahwa banyak konfigurasi SSH membatasi jumlah koneksi paralel.



Gambar 4.5 *Log Activity*
Sumber: diolah oleh peneliti, 2025

Pada gambar 4.5, menyajikan log activity yang mendeteksi adanya serangan *brute force* yang dilakukan terhadap agent test-svr. Sistem mendeteksi anomali dikarenakan user mencoba masuk untuk masuk berkali-kali dan menggunakan kredensial yang tidak sesuai dengan database yang ada.

Network Intrusion *Detection* System

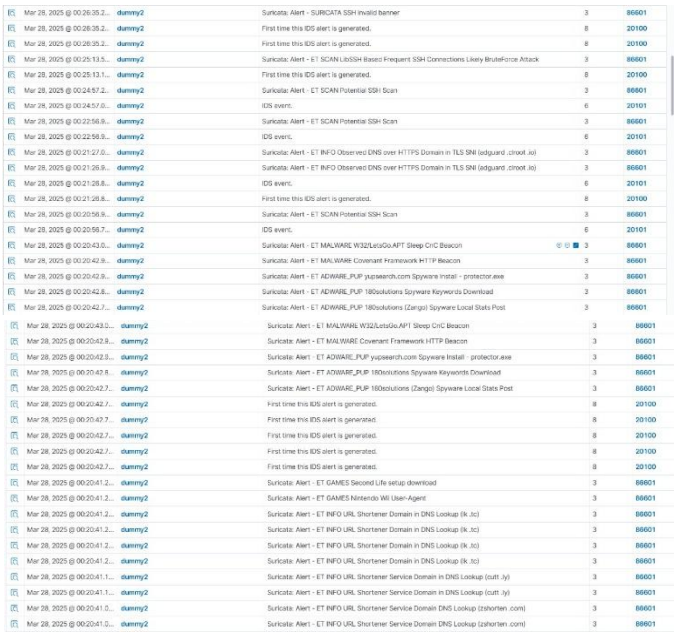
Pada pengujian IDS (*Intrusion Detection System*) dilakukan pegujian dengan

VISA: Journal of Visions and Ideas
Vol 5 No 3 (2025) 1215–1230 E-ISSN 2809-2058 P-ISSN 2809-2643
DOI: 47467/visa.v5i3.9145

tools tmNIDS untuk menguji NIDS pada domain server yang sudah disiapkan dengan pilihan pengujian seperti yang ditampilkan pada gambar berikut.

Gambar 4.6 Daftar Pengujian NIDS
Sumber : diolah oleh penulis, 2025

Berdasarkan gambar 4.6 ditampilkan bahwa ada 16 metode pengujian NIDS yang dapat diujikan kepada domain server yang dimana menggunakan *tools opensource* dari tmNIDS oleh *3CoreSec*. Dalam hal ini telah diujikan pada domain server yang sudah di *install* agent wazuh sebagai sistem keamanan XDR. Pada pengujian NIDS tersebut maka dihasilkan log sebagai berikut



Gambar 4.7 *Log Activity* IDS
Sumber: diolah oleh penulis, 2025

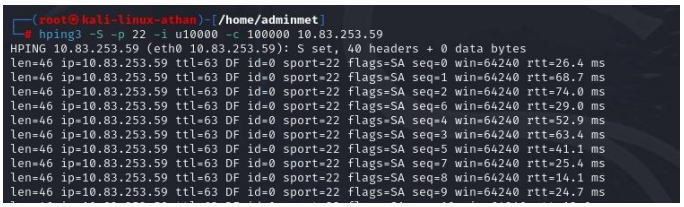
Pada gambar 4.7 ditampilkan *log activity* IDS yang memunculkan *alert* atau peringatan mengenai IDS *event* yang terdeteksi oleh sistem keamanan. Hasil dari pengujian IDS terlihat bahwa seluruh pengujian IDS oleh tmNIDS dapat terdeteksi sebagai anomali atau ancaman pada jaringan dan menampilkannya sebagai log alert pada *dashboard threat hunting* beserta data log detilnya mulai dari timestamp, rule

VISA: Journal of Visions and Ideas
Vol 5 No 3 (2025) 1215–1230 E-ISSN 2809-2058 P-ISSN 2809-2643
DOI: 47467/visa.v5i3.9145

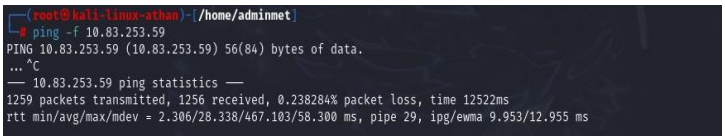
event hingga tingkat kerentanan berdasarkan NIST dan GDPI.

Denial of Service *Attack*

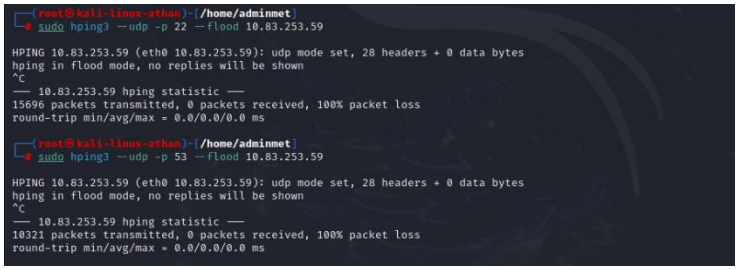
Pada pengujian ini dilakukan *denial of service* atau DoS *attack* dengan menggunakan 3 metode, yaitu SYN *flood*, ICMP *flood*, dan UDP *flood.* Berikut merupakan *command script* atau perintah yang digunakan untuk melakukan *DoS Attack.*



Gambar 4.8 *SYN Flood DoS Attack Command Script*
Sumber: diolah oleh penulis, 2025



Gambar 4.9 *ICMP Flood DoS Attack Command Script*
Sumber: diolah oleh penulis, 2025

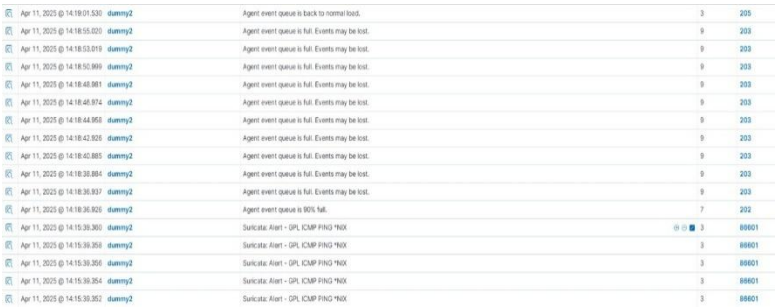


Gambar 4.10 *UDP Flood DoS Attack Command Script*
Sumber: diolah oleh penulis, 2025

Pada gambar 4.8, 4.9, 4.10 di tampilkan *command script* atau perintah yang digunakan untuk melakukan Dos *Attack* dengan menggunakan 3 metode yang berbeda dan hasil yang berbeda. Pada SYN Flood dan ICMP Flood, paket yang berhasil dikirimkan lebih dari 99% atau *loss* kurang dari 1%, sedangkan pada UDP Flood 100% paket yang dikirimkan pada setiap *port*-nya tidak sampai target atau *loss*. Hasil dari metode SYN *Flood* dan ICMP *Flood* dapat terdeteksi pada sistem keamanan yang kemudian akan muncul sebagai *log event* berupa *alert*, namun tidak dengan UDP Flood karena pada metode ini terjadi 100% *packet loss*.

VISA: Journal of Visions and Ideas
Vol 5 No 3 (2025) 1215–1230 E-ISSN 2809-2058 P-ISSN 2809-2643
DOI: 47467/visa.v5i3.9145

Gambar 4.11 ***Log Event SYN Flood***
Sumber: diolah oleh penulis, 2025



Gambar 4.12 ***Log Event ICMP Flood***
Sumber: diolah oleh penulis, 2025

Berdasarkan gambar 4.11 dan 4.12 maka pengujian dengan DoS *attack* dengan metode SYN *Flood* dan ICMP *Flood* berhasil dan dijabarkan secara spesifik dalam *log event* yang masuk pada *dashboard threat hunting*. Pada pengujian bahkan hingga dapat terjadi *lagging* karena terlalu banyak *packet* yang membanjiri server.

Pembahasan

Integrasi Wazuh dengan Suricata

Pada implementasi XDR selain integrasi VirusTotal, diperlukan juga integrasi Suricata guna dapat mengoptimalkan sistem keamanan informasi terutama pada hal yang behubungan dengan jaringan. Suricata merupakan sebuah layanan *open source* yang berfungsi sebagai *Network Intrusion Detection System* (NIDS). Suricata dirancang untuk menganalisis sebuah *network* secara *real-time*, mendeteksi sebuah serangan siber dan mengumpulkan informasi keamanan jaringan.

```
dummy@dummy2:~$ sudo apt-get install software-properties-common
sudo add-apt-repository ppa:oisf/suricata-stable
sudo apt update
sudo apt install suricata jq
```

Gambar 4.13 ***Command Script Install Suricata***
Sumber: diolah oleh penulis, 2025

Pada gambar 4.14 merupakan perintah pada server untuk mengunduh suricata agar dapat dijalankannya sistem IDS pada jaringan. Perintah dimulai pada mengunduh properti sistem, menambahkan repositori pada sistem, hingga melakukan *install* pada *endpoint*.

VISA: Journal of Visions and Ideas
Vol 5 No 3 (2025) 1215–1230 E-ISSN 2809-2058 P-ISSN 2809-2643
DOI: 47467/visa.v5i3.9145

```
vars:
  # more specific is better for alert accuracy and performance
  address-groups:
    HOME_NET: "[10.83.253.0/24]"
    #HOME_NET: "[192.168.0.0/16]"
    #HOME_NET: "[10.0.0.0/8]"
    #HOME_NET: "[172.16.0.0/12]"
    #HOME_NET: "any"
```

Gambar 4.14 ***Inform Routing Suricata to Network***
Sumber: diolah oleh penulis, 2025

Pada gambar 4.15 merupakan konfigurasi yang dibutuhkan agar suricata dapat terintegrasi dan terhubung pada jaringan terutama segmen yang akan di lakukan pemantauan dengan NIDS.

```
# Linux high speed capture support
af-packet:
  - interface: ens18
    # Number of receive threads. "auto" uses the number of cores
    #threads: auto
    # Default clusterid. AF_PACKET will load balance packets based on flow.
    cluster-id: 99
```

Gambar 4.15 ***Configuration Packet***
Sumber : diolah oleh penulis, 2025

Pada gambar 4.16 ditampilkan konfigurasi paket yang harus di atur agar tidak terjadi *miss packet* atau *loss packet.* Ditampilkan pada gambar bahwa "interfce : ens18", yang artinya bahwa script tersebut menentukan interface jaringan mana yang akan digunakan untuk menangkap atau menerima paket. Network Interface Card (NIC) yang digunakan pada konfigurasi tersebut adalah ens18.

Penambahan *Rule*

Pada konfigurasi dasar yang terdapat pada sistem yang diimplementasikan, belum terdapat *rule group* untuk integrasi dengan virustotal dan suricata untuk deteksi dan *response* terhadap ancaman yang terjadi pada *endpoint* dan jaringan pada infrastruktur. Konfigurasi ditambahkan pada *config file* yang terdapat pada server wazuh dan di *tunning* dengan *agent* agar *configurasi* yang ditambahkan dapat bekerja secara optimal sesuai dengan fungsinya.

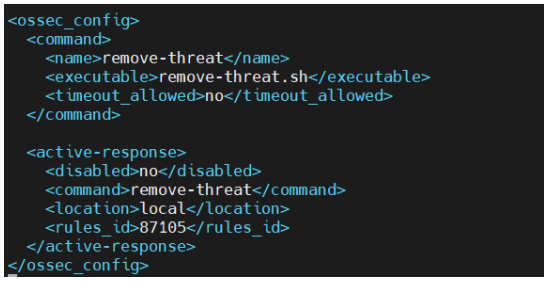
```
<ossec_config>
  <localfile>
    <log_format>syslog</log_format>
    <location>/var/log/suricata/fast.log</location>
  </localfile>


  <localfile>
    <log_format>json</log_format>
    <location>/var/log/suricata/eve.json</location>
  </localfile>

</ossec_config>
```

Gambar 4.16 ***Config Rule Suricata***
Sumber : diolah oleh penulis, 2025

VISA: Journal of Visions and Ideas
Vol 5 No 3 (2025) 1215–1230 E-ISSN 2809-2058 P-ISSN 2809-2643
DOI: 47467/visa.v5i3.9145



Gambar 4.17 *Config Rule VirusTotal*
Sumber : diolah oleh peneliti, 2025

Pada tahapan ini akan dilakukan implementasi berdasarkan kebutuhan dan perancangan desain yang sudah dijabarkan pada tabel 4.1 dan gambar 3.4. Implementasi sistem Wazuh sebagai XDR dilakukan dengan *install* Wazuh *manager* pada server dan *install* Wazuh *agent* pada endpoint agen. Pada penelitian ini implementasi difokuskan pada deteksi *malware* dan respon terhadap *malware*. Wazuh di integrasikan dengan VirusTotal dengan menggunakan API (*Application Programming Interface*) agar kemudian *file* dengan *malware* dapat dideteksi dan dilakukan penghapusan dengan respon aktif seperti yang disajikan pada gambar 4.1 dan gambar 4.2.

Cara kerja dari pendeteksian *malware* itu sendiri dimulai dari *Wazuh-Agent* yang sudah ditanamkan pada *endpoint* akan memantau perubahan pada *directory* atau penyimpanan, kemudian akan melakukan *scan* atau pemindaian otomatis terhadap *file* yang ada pada *directory*, bila sistem mendeteksi adanya indikasi *malware* , maka sistem akan segera melakukan respon aktif dengan menghapus *file* tersebut.

Pengujian Detecting and Deleting *Malware*

Pengujian dilakukan dengan cara menambahkan *file* yang mengandung *malware* ke dalam sistem yang dipantau oleh XDR (Wazuh) guna deteksi dan respon terhadap *malware* yang dapat membahayakan perangkat. Pada pengujian ini dilakukan dengan menambahkan 60 *file* yang mengandung *script* berbahaya atau yang biasa disebut *malware*. Berdasarkan gambar 4.1 bahwa hasil dari pengujian tersebut menunjukkan persentase efektifitas sistem berdasarkan deteksi dan penghapusan *file* dengan persamaan adalah sebesar 98,32% dengan total *file* yang di masukan berjumlah 60 sedangkan *file* yang terhapus berjumlah 59.

Berdasarkan gambar 4.2 *log malware detection* pada *dashboard malware detection* dalam Wazuh menunjukkan adanya respons aktif terhadap ancaman yang ditemukan dalam sistem yang kemudian disajikan dengan parameter sebagai berikut:

1. Peringatan dari VirusTotal (*Alert*)
   Wazuh memanfaatkan integrasi dengan VirusTotal, yang memungkinkan *file* diuji dalam *database* global. Beberapa *file* yang diuji dikonfirmasi sebagai *malware* oleh 61 mesin deteksi antivirus. Contohnya, *file* "nakai_fam.zip" dideteksi oleh 61 *engine* antivirus sebagai ancaman.
2. Respons otomatis

VISA: Journal of Visions and Ideas
Vol 5 No 3 (2025) 1215–1230 E-ISSN 2809-2058 P-ISSN 2809-2643
DOI: 47467/visa.v5i3.9145

Wazuh secara otomatis menjalankan *active-response/bin/remove-threat.exe*, yang menghapus *file* yang telah terdeteksi berbahaya.

3. Tingkat keparahan ancaman
   Tingkat ancaman yang ditunjukan berdasarkan hasil analisis file yang terindikasi *malware* oleh mesin deteksi *malware*, menunjukkan hingga *level* 12. Ancaman tersebut dikategorikan sebagai ancaman yang tinggi karena memiliki nilai hinggal lever 12 yang langsung ditangani dengan penghapusan otomatis. Berikut tabel mengenai klasifikasi tingkat ancaman dalam bentuk skala level.

Tabel 4.1 *Rule Level*

Level	**Kategori**	**Deskripsi**
0-3	Infomasi	Tidak berbahaya, log biasa, aktivitas normal.
Level	**Kategori**	**Deskripsi**
4-6	Peringatan rendah	Sesuatu yang mencurigakan, perlu diperhatikan.
7-9	Peringatan sedang	Aktivitas beresiko, mungkin serangan ringan.
10-13	Ancaman tinggi	Tanda-tanda kuat adanya serangan.
14-15	Ancaman sangat tinggi	Serangan aktif atau berbahaya, memerlukan tindakan segera.

Sumber : diolah oleh penulis, 2025

4. ID aturan (*rule.id*)
   Beberapa ID aturan ditemukan dalam log, seperti:
   a. 100092, Berhubungan dengan proses penghapusan ancaman oleh Wazuh.
   b. 87105, Terkait dengan deteksi ancaman oleh VirusTotal.

Dari hasil log, dapat disimpulkan bahwa Wazuh berhasil mendeteksi ancaman secara *real-time* dan melakukan mitigasi dengan menghapus *file* berbahaya secara otomatis.

KESIMPULAN DAN SARAN

Berdasarkan hasil penelitian, penelitian ini berhasil membuktikan bahwa *Extended Detection and Response* (XDR) dapat meningkatkan efektivitas deteksi dan mitigasi ancaman dalam *Security Operation Center* (SOC) dan *Computer Security Incident Response Team (*CSIRT). Kesimpulan penelitian ini dibagi menjadi tiga bagian sesuai dengan tujuan penelitian, yaitu analisis dan evaluasi kinerja XDR dalam mendeteksi *malware*, identifikasi jenis serangan utama pada domain server, serta strategi peningkatan efisiensi tim SOC dan CSIRT melalui implementasi XDR.

Vol 5 No 3 (2025) 1215–1230 E-ISSN 2809-2058 P-ISSN 2809-2643
DOI: 47467/visa.v5i3.9145

Analisis dan Evaluasi Kinerja XDR dalam Deteksi *Malware* dan Respons terhadap Ancaman

Hasil penelitian menunjukkan bahwa XDR memiliki akurasi deteksi *malware* sebesar 98,3% dan mampu merespons ancaman dalam waktu kurang dari 3 detik, jauh lebih cepat dibandingkan metode tradisional yang membutuhkan 10 hingga 15 detik dalam mengkorelasikan data log dan mendeteksi serangan. Dalam skenario serangan ransomware, sistem XDR berhasil memblokir eksekusi *malware* dengan tingkat keberhasilan >98%, membuktikan bahwa XDR tidak hanya mendeteksi ancaman tetapi juga mampu melakukan mitigasi otomatis secara real-time. Selain itu, implementasi automasi berbasis AI dalam XDR berhasil mengurangi false positive hingga 40%, yang selama ini menjadi salah satu kendala dalam sistem keamanan berbasis aturan seperti SIEM. Dengan demikian, penelitian ini membuktikan bahwa XDR dapat meningkatkan kecepatan deteksi ancaman dan efektivitas mitigasi *malware* secara signifikan dalam SOC dan CSIRT.

Identifikasi Jenis Serangan Utama pada Domain Server dan Faktor Penyebabnya

Berdasarkan analisis terhadap insiden keamanan yang diamati selama penelitian, terdapat tiga jenis serangan utama yang sering terjadi pada domain server, yaitu *brute force attack*, DOS *attack*, dan *ransomware* atau *malware*. Serangan *brute force attack* terjadi akibat kelemahan dalam kebijakan kata sandi serta kurangnya implementasi sistem otentikasi multi-faktor (MFA). Serangan Ransomware, yang menjadi ancaman utama bagi domain server, sering kali disebabkan oleh kurangnya deteksi dini terhadap *malware* berbasis *file* dan rendahnya kesadaran pengguna terhadap phishing email. Hasil penelitian menunjukkan bahwa XDR mampu mendeteksi ketiga jenis serangan ini dengan efektivitas tinggi, terutama dalam mendeteksi pola serangan berbasis anomali yang sulit dideteksi oleh sistem keamanan tradisional. Oleh karena itu, implementasi XDR dalam SOC dan CSIRT menjadi solusi yang efektif untuk mengidentifikasi dan mengatasi serangan utama pada domain server.

Strategi Peningkatan Optimalisasi Tim SOC dan CSIRT melalui Implementasi XDR

Hasil penelitian ini menunjukkan bahwa implementasi XDR dapat meningkatkan optimalisasi kerja tim SOC dan CSIRT dengan mengurangi waktu analisis dan respon terhadap insiden keamanan. Dengan mengotomatiskan proses deteksi, analisis, dan mitigasi ancaman, tim SOC dapat memfokuskan sumber daya mereka pada investigasi insiden tingkat tinggi, daripada menangani false positive yang berlebihan. Selain itu, dashboard berbasis website dalam XDR memungkinkan pemantauan ancaman secara real-time, memberikan visibilitas yang lebih luas terhadap keamanan jaringan. Rekomendasi utama untuk meningkatkan efisiensi kerja tim SOC dan CSIRT meliputi penggunaan teknologi AI yang lebih canggih, seperti *Vision Transformer* (ViT) untuk deteksi ancaman zero-day, serta integrasi dengan IoT Security untuk memperluas cakupan pemantauan ancaman. Dengan strategi ini, XDR

Vol 5 No 3 (2025) 1215–1230 E-ISSN 2809-2058 P-ISSN 2809-2643
DOI: 47467/visa.v5i3.9145

dapat menjadi fondasi utama bagi sistem keamanan yang lebih efisien, adaptif, dan tangguh terhadap ancaman siber.

Secara keseluruhan, penelitian ini membuktikan bahwa XDR merupakan inovasi yang lebih unggul dalam mendeteksi, menganalisis, dan merespons ancaman dibandingkan metode keamanan konvensional. Dengan integrasi kecerdasan buatan (AI), korelasi data *multi-layer*, serta respons otomatis, sistem ini dapat mempercepat deteksi ancaman, mengurangi false positive, serta meningkatkan efektivitas pengawasan real-time dalam SOC dan CSIRT.

Rekomendasi pengembangan yang diusulkan dalam penelitian ini, adalah penggunaan Vision Transformer (ViT) untuk meningkatkan deteksi serangan zero-day, integrasi dengan teknologi IoT Security, serta pengujian dalam skenario jaringan yang lebih kompleks, menjadi arah penting untuk memastikan bahwa XDR terus berkembang sebagai solusi keamanan siber yang lebih tangguh dan adaptif.

Saran

Berdasarkan hasil penelitian, berikut beberapa saran yang dapat dipertimbangkan untuk pengembangan lebih lanjut:

1. Optimalisasi Algoritma K-Means
   Perlu dilakukan pengujian dengan parameter yang lebih variatif dalam algoritma K-Means untuk meningkatkan akurasi dalam mengelompokkan data log SIEM.
2. Integrasi dengan *Machine Learning* Lanjutan
   Untuk meningkatkan akurasi deteksi, sistem dapat dikembangkan lebih lanjut dengan mengintegrasikan metode *machine learning* lain seperti *Random Forest* atau *Deep Learning*.
3. Peningkatan Sistem Notifikasi dan Automasi
   Implementasi sistem notifikasi *real-time* yang lebih responsif dapat membantu administrator dalam menangani ancaman lebih cepat dan efisien.
4. Evaluasi False Positives dan False Negatives
   Perlu dilakukan analisis lebih lanjut terhadap *false positives* dan *false negatives* yang terjadi dalam sistem agar deteksi ancaman menjadi lebih akurat dan tidak mengganggu operasional normal sistem.

Vol 5 No 3 (2025) 1215–1230 E-ISSN 2809-2058 P-ISSN 2809-2643
DOI: 47467/visa.v5i3.9145

DAFTAR PUSTAKA

Antonio A. P., Candidate L, & Gracis R. (2022). Next Generation SOC: Automated Operations and Machine Learning in Cybersecurity.

Arshad A., Rehman A U., Javaid S., Ali T. M., Sheikh J. A., & Azeem M. (2021). A Systematic Literature Review on Phishing and Anti-Phishing Techniques. https://ieeexplore.ieee.org/

Atmojo W. T., Siregar E, & Audrey K. K. (2021). Pengenalan Cyber Security Dalam Revousi Industri 4.0 Dan Menyongsong Era Society 5.0 (Vol. 4).

Bassey C., Chinda E. T., & Idowu S. (2024). Building a Scalable Security Operations Center: A Focus on Open-source *Tools*. *Journal of Engineering Research and Reports,* 26(7), 196–209. https://doi.org/10.9734/jerr/2024/v26i71203

Bassey, C., Samuel, A. A., Imakuh, S., Oloruntola, O., & Onyia-Odike, I. (2024). Enhancing DDoS *Attack* Pr*event*ion And *Detection* Using IDS And XDR. *Journal of Multidisciplinary Engineering Science and Technology (JMEST),* 11. www.jmest.org

Belcic, I. (2023, Agustus 25). *What Is Malware and How to Protect Against Malware Attacks? avast.com.* https://www.avast.com/c-malware

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

Copeland, M. (2021). Cloud defense strategies with Azure Sentinel: Hands-on threat hunting in cloud logs and services. In Cloud Defense Strategies with Azure Sentinel: Hands-on Threat Hunting in Cloud Logs and Services. *Apress Media LLC.* https://doi.org/10.1007/978-1-4842-7132-2

Dehran, B. (2024, Oktober 18). *Impact of zero-day attacks on a company's productivity*. *cloudkul.com.* https://cloudkul.com/blog/impact-of-zero-day-attacks-on-a-companys-productivity/

Firch, J. (2024, Feb 16). *What Is A Security Operations Center? purplesec.us.* https://purplesec.us/learn/security-operations-center-soc/

First. (2019). Computer Security Incident Response Team (CSIRT) Services Framework. https://www.first.org

George, A. S., Hovan George, A. S., Baskar, T., & Pandey, D. (2021). XDR: The Evolution of Endpoint Security Solutions-Superior Extensibility and Analytics to Satisfy the Organizational Needs of the Future. *International Journal of Advanced Research in Science Communication and Technology,* 8(1). https://doi.org/10.5281/zenodo.7028219

George, A. S., Sagayarajan, S., Baskar, T., & Hovan George, A. S. (2023). Partners Universal International Innovation Journal (PUIIJ) Extending *Detection* and Response: How MXDR Evolves Cybersecurity. https://doi.org/10.5281/zenodo.8284342

Gunawan, F., Fadhilah, A., & Malays Sari, E. (2024). Membangun Benteng Digital Untuk Memperkuat Etika Cyber Security Melawan Ancaman Cyber Crime. 25. https://doi.org/10.37817/tekinfo.v25i1

Vol 5 No 3 (2025) 1215–1230 E-ISSN 2809-2058 P-ISSN 2809-2643
DOI: 47467/visa.v5i3.9145

Haryanto, B., & Chandra, D. W. (2024). Implementasi Wazuh Integritas *File* untuk Perlindungan Keamanan Berdasarkan Aktivitas Log di BTSI UKSW. *Jurnal Indonesia : Manajemen Informatika Dan Komunikasi,* 5(1), 183–192. https://doi.org/10.35870/jimik.v5i1.447

Itmanagement. (2023, Mei 31). *Penjelasan tentang ITSM (IT Service Management)*. itmanagement.id. https://www.itmanagement.id/2023/05/penjelasan-tentang-itsm-it-service.html

Itmtech. (2022, Mei 12). *Is Your Business Ready To prevent, Detect And Respond To Cyber Attacks? itmtech.ie*. https://itmtech.ie/managed-detection-and-response-kildare/

Kaliyaperumal, Lakshmi Narayanan. (2021). The-Evolution-of-Security-Operations-and-strategies-for-Building-an-Effective-SOC_joa_Eng_1021. ISACA, 5.

Kasturi, S., Li, X., Li, P., & Pickard, J. (2024). A Proposed Approach to Integrate Application Security Vulnerability Data with Incidence Response Systems. *American Journal of Networks and Communications,* 13(1), 19–29. https://doi.org/10.11648/j.ajnc.20241301.12

Kaur, H., Sanjaiy, D., Paul, T., Kumar Thakur, R., Kumar, K. V., Jay, R., & Kaviti Naveen, M. (2024). Evolution of Endpoint *Detection* and Response (EDR) in Cyber Security: A Comprehensive Review. E3S Web of Conferences, 556. https://doi.org/10.1051/e3sconf/202455601006

KEMHAN. (n.d.). *Aduan Siber*. Retrieved 2024 from csirt.kemhan.go.id: https://csirt.kemhan.go.id/portal/aduan

Make Computer Science Great Again. (2023, Agustus 20). *Understanding the CIA Triad: The Foundation of Network Security*. From medium.com: https://medium.com/@MakeComputerScienceGreatAgain/understanding-the-cia-triad-the-foundation-of-network-security-ceb8d839d7c2

Microsoft. (2024). *Optimize SOC operations with Microsoft Defender XDR*. Retrieved 2024 from microsoft.com: https://www.microsoft.com/en-us/security/business/solutions/extended-detection-response-xdr#diagram-cta-popup

Mughal, A. A., & Mughal, A. A. (2022). Building and Securing the Modern Security Operations Center (SOC). https://orcid.org/0009-0006-8460-8006

Novikov, I. (2024, Juni 21). *XDR vs. SIEM*. From lab.wallarm.com: https://lab.wallarm.com/what/xdr-vs-siem-unveiling-the-next-generation-of-threat-detection-and-response/