PEMBANGUNAN SISTEM PENGESANAN TITIK AKHIR BERASASKAN WAZUH

[1]Muhammad Akmal Hakim bin Aziz, [1]Khairul Akram Zainol Ariffin

[1]Fakulti Teknologi & Sains Maklumat
43600 Universiti Kebangsaan Malaysia

Abstrak

Projek ini memberi tumpuan kepada pembangunan sistem Pengesanan dan Respons Titik Akhir (EDR) berasaskan Wazuh bagi meningkatkan keselamatan sistem dalam organisasi berskala kecil dan sederhana. Titik akhir sering menjadi sasaran utama serangan siber kerana peranannya sebagai pintu masuk ke dalam rangkaian organisasi. Kajian ini mengenal pasti masalah utama iaitu keterbatasan perisian antivirus tradisional dalam mengesan ancaman canggih seperti Ancaman Berterusan Lanjutan (APT) serta ketiadaan mekanisme pemantauan masa nyata dan tindak balas automatik dalam banyak organisasi kecil. Ini meningkatkan risiko pencerobohan dan kerosakan sistem tanpa disedari. Sebagai penyelesaian, projek ini membangunkan sistem EDR menggunakan platform sumber terbuka Wazuh. Sistem ini dilengkapi dengan fungsi pemantauan integriti fail (FIM), pengesanan tingkah laku proses dan integrasi API VirusTotal untuk semakan reputasi fail secara automatik. Selain itu, mekanisme respons aktif turut dibangunkan bagi membolehkan sistem bertindak secara automatik terhadap ancaman yang dikenalpasti. Strategi pembangunan menggunakan pendekatan Agile dengan kitaran pembangunan beriterasi dan pengujian berterusan dalam persekitaran maya melibatkan sistem Windows 10, Windows 11 dan Kali Linux. Simulasi serangan seperti brute force, akses tidak sah dan penyalahgunaan proses sah digunakan untuk menilai keupayaan sistem. Hasil projek menunjukkan sistem yang dibangunkan berjaya mengesan, melaporkan dan bertindak balas terhadap pelbagai bentuk ancaman keselamatan dengan efektif. Sistem ini bukan sahaja memenuhi keperluan fungsi yang ditetapkan, malah sesuai diaplikasikan dalam persekitaran organisasi bersumber terhad bagi memperkukuh tahap keselamatan titik akhir.

Kata kunci: EDR, Wazuh, pemantauan masa nyata, respons automatik, VirusTotal.

Abstract

This project focuses on the development of a Wazuh-based Endpoint Detection and Response (EDR) system aimed at enhancing security within small and medium-sized organizational environments. Endpoints are frequent targets of cyberattacks due to their role as entry points into internal networks. The core problem addressed is the limitation of traditional antivirus software in detecting sophisticated threats such as Advanced Persistent Threats (APT), alongside the lack of real-time monitoring and automated response mechanisms especially in resource-constrained organizations. As a solution, this project develops an EDR system based on the open-source Wazuh platform, equipped with file integrity monitoring (FIM), behavioral process detection and API integration with VirusTotal to verify file reputations. In addition, an active response mechanism is implemented to automatically execute pre-defined actions against identified threats. The system was developed using an Agile methodology involving iterative development and continuous testing within a controlled virtual environment comprising Windows 10, Windows 11 and Kali Linux machines. Various attack scenarios such as brute-force login attempts, unauthorized access, and abuse of legitimate processes were simulated to evaluate the system's detection capabilities. The results demonstrate that the developed system successfully detects, logs, and responds to multiple types of security threats. The final product meets its functional goals and proves to be a practical and scalable solution for strengthening endpoint security, especially for organizations with limited resources.

Keywords: EDR, Wazuh, real-time monitoring, automated response, VirusTotal

1.0 PENGENALAN

Dalam era digital hari ini, organisasi semakin terdedah kepada pelbagai ancaman siber yang semakin canggih termasuk serangan perisian tebusan dan Ancaman Berterusan Lanjutan (APT) yang menyasarkan kelemahan titik akhir infrastruktur IT mereka. APT menggunakan teknik seperti perisian hasad polimorfik dan pengubahan log untuk mengelak daripada dikesan. Ini secara tak langsung menjadikannya sukar dicegah oleh sistem keselamatan tradisional (Wibowo et al. 2025). Menurut kajian daripada Ponemon Institute (2020), 68% daripada organisasi yang ditemu bual telah mengalami satu atau lebih serangan titik akhir yang berjaya membocorkan data infrastruktur IT mereka. Tambahan lagi, Morefield (2024) meramalkan peningkatan kekerapan serangan perisian tebusan pada tahun 2025 kerana kajian daripada BRITE (2024) menunjukkan jumlah mangsa serangan perisian tebusan telah meningkat daripada 2,700 syarikat pada tahun 2023 kepada hampir 4,900 syarikat pada tahun 2024.

Di antara ancaman siber yang wujud, serangan perisian tebusan adalah antara bentuk serangan yang popular. Menurut Shea dan Irei (2023), perisian tebusan merupakan sejenis perisian hasad yang mengenkripsi data, fail, peranti atau sistem mangsa menyebabkan ianya tidak dapat diakses dan tidak boleh digunakan sehingga penyerang menerima wang tebusan. Serangan ini boleh melumpuhkan organisasi dan menyebabkan kerugian yang banyak terutamanya apabila langkah pencegahan yang dilakukan tidak mencukupi ataupun tidak berkesan. Menurut kajian Ponemon Institute (2020), serangan titik akhir merupakan serangan yang paling biasa dihadapi oleh responden. Sebanyak 81% syarikat mengalami serangan yang melibatkan beberapa jenis perisian hasad manakala 28% syarikat mengalami serangan yang melibatkan peranti yang digodam atau dicuri.

Di samping itu, langkah-langkah keselamatan tradisional seperti penggunaan firewall dan perisian antivirus tidak lagi cukup untuk mengatasi kompleksiti ancaman siber yang semakin maju (Aslan et al. 2023; Peris.AI 2024). Kelemahan utama pendekatan ini ialah ketidakupayaannya untuk mengesan ancaman yang tidak diketahui atau teknik serangan yang lebih canggih. Hal yang demikian, sistem Pengesanan dan Respons Titik Akhir (EDR) telah diperkenalkan sebagai penyelesaian yang lebih maju dalam menangani cabaran ini. EDR adalah perisian yang mengumpul dan menganalisis data secara berterusan dari semua titik akhir dalam rangkaian termasuk komputer riba, pelayan, peranti mudah alih dan peranti Internet Pelbagai Benda (IoT). Sistem ini menggunakan analitik masa nyata dan automasi berasaskan

kecerdasan buatan untuk mengesan ancaman siber yang berjaya melepasi perisian antivirus dan alat keselamatan lain (IBM n.d.).

Titik akhir sering menjadi sasaran utama serangan siber kerana ia merupakan pintu masuk kritikal ke dalam rangkaian sesebuah organisasi. Namun, banyak organisasi terutamanya perusahaan kecil dan sederhana (SME), menghadapi cabaran dalam mengesan dan bertindak balas terhadap serangan siber secara masa nyata disebabkan oleh kekangan bajet dan keterbatasan sumber daya teknologi. Menurut laporan dari Cisco (2020), kebanyakan SME menyatakan kekangan bajet merupakan penghalang utama dalam meningkatkan keselamatan siber mereka. Kekangan ini menyebabkan mereka hanya mampu menggunakan antivirus tradisional sebagai lapisan pertahanan utama. Walaupun begitu, penyelesaian ini tidak mencukupi untuk menangani ancaman siber yang semakin kompleks. Menurut kajian Ponemon Institute (2020), perisian antivirus secara purata gagal mengesan 60% serangan siber sekaligus menunjukkan jurang ketara dalam keberkesanan penyelesaian keselamatan tradisional.

Kekangan bajet juga menyebabkan SME tidak mampu memperoleh kelengkapan keselamatan siber yang canggih seperti sistem berbayar yang menawarkan analisis ancaman lanjutan dan mekanisme pemulihan automatik. Tanpa sistem pemantauan yang berkesan, SME lebih mudah menjadi sasaran serangan (Fidel-Anyana et al. 2025). Kelemahan dalam pemantauan keselamatan dan ketidaktahuan terhadap aktiviti berniat jahat dalam sistem menjadikan SME sasaran yang lebih mudah bagi penyerang. Kajian terkini oleh Bhavsar dan Thakar (2025) menunjukkan bahawa penggunaan platform sumber terbuka seperti Wazuh dalam persekitaran SOC berjaya mengesan serangan seperti perisian hasad, serangan brute force dan DDoS secara berkesan dengan kos yang rendah dan tanpa kebergantungan kepada sistem berbayar. Ini menjadikan pendekatan sumber terbuka sebagai alternatif penting untuk SME. Tambahan pula, kaedah anomali baharu yang diperkenalkan oleh Zhao et al. (2025) menunjukkan keupayaan tinggi dalam mengesan corak serangan siber dalam data tabular menggunakan model berskala kecil yang sesuai dengan keperluan organisasi yang mempunyai sumber terhad.

Menyedari kelemahan antivirus tradisional dan keperluan untuk sistem keselamatan yang lebih maju, EDR telah diperkenalkan sebagai penyelesaian alternatif yang lebih canggih. Antivirus tradisional hanya bergantung pada pengesanan berasaskan corak. Sebaliknya, EDR menawarkan pemantauan masa nyata dan mekanisme respons automatik yang lebih berkesan. Namun, banyak sistem EDR sedia ada masih gagal mengesan dan mencegah ancaman yang lebih kompleks. Sebagai

contoh, kajian oleh Karantzas dan Patsakis (2021) menunjukkan bahawa lebih daripada separuh serangan APT yang disimulasikan berjaya memintas sistem EDR yang diuji sekaligus mendedahkan kekurangan dalam keupayaan pengesanan dan log. Kebergantungan pada peraturan statik tanpa integrasi data ancaman yang lebih luas menjadikan sistem ini kurang berkesan untuk menangani ancaman yang dinamik.

Berdasarkan masalah yang telah dikemukakan, projek ini akan membangunkan sistem EDR berasaskan Wazuh yang merupakan platform sumber terbuka dan percuma. Tidak seperti sistem EDR berbayar yang mahal, Wazuh menyediakan penyelesaian keselamatan yang lebih mampu milik sekaligus menjadikannya pilihan ideal untuk SME yang menghadapi kekangan bajet. Dengan menggunakan Wazuh, organisasi boleh mendapatkan sistem pengesanan ancaman yang lebih canggih tanpa menanggung kos pelesenan yang tinggi, menjadikannya satu penyelesaian yang lebih mampan dan fleksibel.

2.0 KAJIAN LITERATUR

Bahagian ini membincangkan kajian literatur yang berkaitan dengan pembangunan Sistem Pengesanan dan Respons Titik Akhir (EDR) berasaskan Wazuh. Tujuan utama bahagian ini adalah untuk menyediakan pemahaman yang mendalam mengenai teknologi, penyelidikan dan pendekatan terkini yang digunakan dalam sistem EDR untuk menangani ancaman siber yang semakin kompleks. Sorotan ini merangkumi kajian terhadap pelbagai penyelesaian EDR sama ada sumber terbuka mahupun berbayar dan menganalisis kekuatan, kelemahan serta cabaran yang berkaitan dengan pelaksanaannya. Bahagian ini dimulakan dengan membincangkan latar belakang peralatan siber dan fungsinya dalam ekosistem keselamatan diikuti oleh analisis teknologi dan sistem yang berkaitan. Seterusnya, penyelidikan terkini dan trend perkembangan dalam bidang EDR dibincangkan untuk memberikan konteks kepada pendekatan inovatif yang sedang diambil. Metodologi yang digunakan dalam kajian terdahulu turut dianalisis untuk memahami kelebihan dan kelemahan pendekatan yang berbeza diikuti oleh kritikan terhadap kajian lepas serta perbandingan teknologi sedia ada. Bahagian ini juga mengenal pasti jurang dalam penyelidikan yang menjadi asas kepada pembangunan projek, sebelum mengemukakan penyelesaian inovatif yang dapat memperkukuhkan sistem EDR. Akhirnya, bahagian ini dirumuskan dengan menghubungkan kajian literasi kepada objektif projek, memberikan justifikasi terhadap pemilihan teknologi dan menekankan kepentingan kajian ini dalam menangani cabaran keselamatan siber masa kini.

Dalam era digital masa kini, organisasi berdepan dengan pelbagai bentuk ancaman siber yang semakin kompleks, kerap berlaku, dan bersifat sukar dikesan. Kemunculan serangan yang lebih tersusun dan berterusan seperti APT telah mengubah landskap keselamatan digital. APT merujuk kepada serangan siber yang berprofil tinggi, dilakukan secara berterusan dan tersusun oleh penyerang yang mempunyai sumber dan kepakaran tinggi dengan matlamat untuk mencuri, memusnahkan atau mengganggu data sensitif secara senyap. Untuk menangani cabaran ini, organisasi perlu melaksanakan strategi pertahanan siber yang berlapis serta menggunakan peralatan keselamatan yang mampu bertindak secara pantas dan berkesan.

Antara peralatan keselamatan utama yang digunakan ialah firewall, antivirus, Sistem Pencegahan Pencerobohan (IPS), SIEM dan EDR. SIEM berfungsi sebagai pusat pengumpulan maklumat yang beroperasi secara pasif dengan menumpukan kepada pemantauan dan analisis data log daripada pelbagai sistem. Sebaliknya,

firewall melaksanakan tugas secara aktif dengan menapis dan menyekat trafik rangkaian yang mencurigakan bagi menghalang akses tidak sah daripada pihak luar (Tendikov et al. 2024). Antivirus mengenal pasti dan menghapus perisian hasad yang dikenali berdasarkan corak yang tersedia. IPS pula memantau trafik rangkaian secara aktif untuk mengesan dan menyekat aktiviti yang mencurigakan.

EDR pula merupakan sistem yang direka khusus untuk memantau, merekod, menganalisis dan memberi respons terhadap ancaman pada peringkat titik akhir seperti komputer pengguna dan pelayan. Menurut Kaur et al. (2024), EDR memainkan peranan penting dalam memastikan organisasi dapat mengesan, menyiasat dan memberi respons terhadap serangan siber dengan lebih berkesan melalui pemantauan tingkah laku dan analisis data secara mendalam. Sistem ini berupaya mengenal pasti kelakuan tidak normal yang mungkin menunjukkan kewujudan serangan yang belum dikenalpasti oleh sistem tradisional.

Dalam konteks Malaysia, SME menghadapi cabaran besar dalam mengadaptasi teknologi keselamatan siber disebabkan oleh kekangan kos, kurangnya kepakaran teknikal dan infrastruktur ICT yang terhad. Laporan semasa menyatakan bahawa banyak SME masih tidak memiliki sistem keselamatan yang lengkap dan bergantung kepada penyelesaian asas yang mudah dicerobohi. Oleh itu, pemilihan dan pelaksanaan peralatan keselamatan siber yang sesuai dengan tahap kematangan organisasi serta kemampuan sumber sedia ada adalah amat penting.

Kajian oleh Siji dan Uche (2023) menekankan keperluan untuk membanding dan menyesuaikan pemilihan sistem keselamatan seperti EDR berdasarkan keperluan dan tahap risiko organisasi. Pendekatan berlapis dan penggunaan sistem yang bersepadu bukan sahaja dapat meningkatkan ketahanan organisasi terhadap serangan APT, malah membolehkan tindakan respons yang lebih pantas dan efektif dilaksanakan.

Beberapa kajian terdahulu mengkaji keberkesanan pelaksanaan EDR dalam menangani ancaman APT dan perisian hasad. Park et al. (2022) menjalankan kajian terhadap gabungan GRR dan osquery dengan mensimulasikan empat vektor serangan APT berdasarkan kerangka MITRE ATT&CK. Mereka mendapati bahawa konfigurasi asal osquery hanya berjaya mengesan sekitar 28.5% daripada teknik serangan, yang menekankan keperluan penyesuaian mendalam bagi mencapai keberkesanan pengesanan sebenar. Karantzas dan Patsakis (2021) pula menilai keupayaan 11 sistem EDR terhadap APT melalui simulasi serangan berperingkat menggunakan Cobalt Strike. Hasil kajian menunjukkan banyak sistem gagal

mengesan atau menghasilkan amaran terhadap aktiviti kritikal terutamanya dalam kes serangan berprofil rendah dan serangan tanpa fail. Laporan Ponemon Institute (2020) turut menyokong kelemahan sistem tradisional apabila dilaporkan bahawa antivirus konvensional hanya mampu menghalang sekitar 40% serangan dengan kadar positif palsu yang tinggi.

Beberapa sistem telah digunakan dalam pelbagai kajian untuk menilai keberkesanan EDR terutamanya sistem sumber terbuka seperti Wazuh, GRR dan osquery. Wazuh menyediakan pelbagai ciri seperti analisis log, pemantauan integriti fail, pengesanan aktiviti mencurigakan serta tindak balas automatik. Salah satu kekuatan utamanya ialah kebolehan untuk melaksanakan peraturan pengesanan khusus berdasarkan keperluan organisasi. Wazuh juga menyokong integrasi dengan platform maklumat ancaman pihak ketiga seperti VirusTotal. GRR pula sesuai digunakan dalam penyiasatan selepas insiden, tetapi kurang sesuai untuk pengesanan masa nyata. Osquery menggunakan struktur pertanyaan SQL untuk mendapatkan maklumat terperinci tentang sistem tetapi memerlukan konfigurasi mendalam bagi keberkesanannya.

Secara keseluruhannya, pemahaman terhadap fungsi, kekuatan dan had setiap komponen keselamatan siber perlu diberi perhatian serius. Di samping itu, faktor seperti kemampuan kewangan, keperluan operasi serta cabaran tempatan perlu diambil kira dalam merangka strategi pertahanan siber yang efektif dan bersesuaian dengan persekitaran organisasi masa kini. Melalui perbincangan menyeluruh ini, bahagian ini menyokong asas pembangunan sistem EDR berasaskan Wazuh yang lebih berkesan, adaptif dan berskala.

3.0 METODOLOGI

Metodologi dalam projek ini bertujuan menjelaskan pendekatan pembangunan, keperluan pengguna, keperluan sistem, model sistem serta algoritma yang digunakan bagi membangunkan sistem EDR berasaskan Wazuh. Bagi mencapai objektif yang telah ditetapkan, analisis terperinci terhadap keperluan pengguna dan keperluan sistem dijalankan terlebih dahulu. Keperluan pengguna yang dikenal pasti terdiri daripada dua peranan utama iaitu Pentadbir dan Penganalisis Keselamatan. Pentadbir bertanggungjawab dalam pengurusan konfigurasi keseluruhan sistem seperti pemasangan pelayan dan ejen Wazuh serta konfigurasi integrasi sistem dengan platform luar seperti VirusTotal. Penganalisis Keselamatan pula bertanggungjawab untuk memantau ancaman masa nyata, menganalisis log aktiviti ancaman, menyediakan laporan keselamatan serta mengemas kini peraturan pengesanan ancaman berdasarkan analisis yang dibuat.

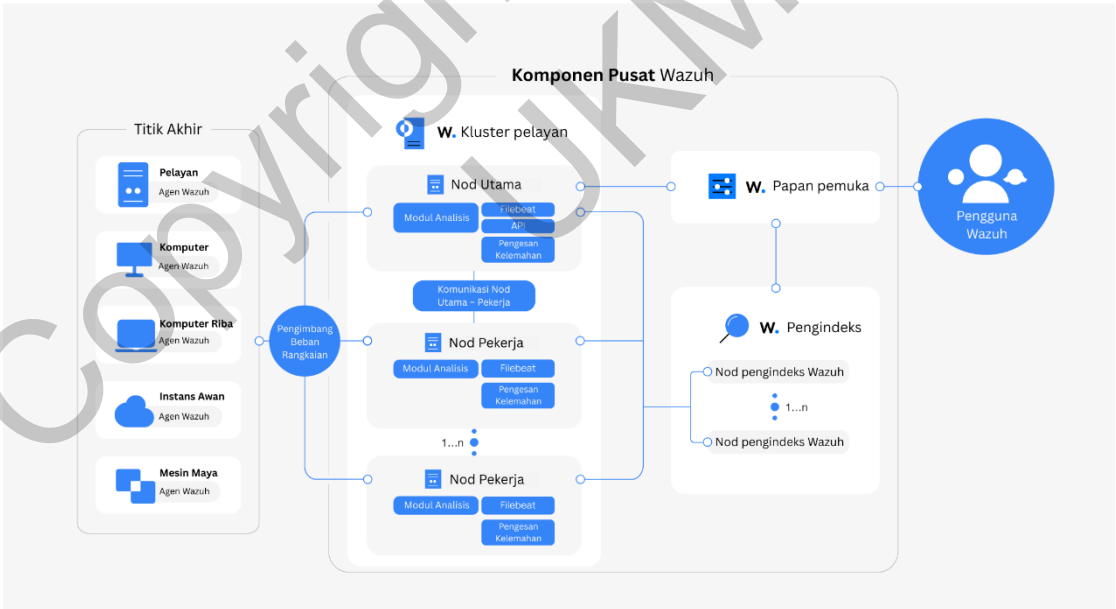
Bagi keperluan sistem, ia terdiri daripada keperluan fungsian, bukan fungsian, serta keperluan perkakasan dan perisian. Keperluan fungsian sistem ini merangkumi pemasangan pelayan dan ejen Wazuh, konfigurasi sistem bagi tujuan pemantauan ancaman masa nyata, integrasi dengan VirusTotal melalui penggunaan API untuk pengesanan automatik terhadap fail mencurigakan, serta keupayaan tindak balas automatik bagi menangani ancaman yang dikenal pasti secara segera. Keperluan bukan fungsian pula menumpukan kepada kebolehgunaan, kebolehpercayaan, dan prestasi sistem yang tinggi dalam mengendalikan pemprosesan log secara besar-besaran tanpa menjejaskan prestasi operasi keseluruhan. Spesifikasi perkakasan dan perisian sistem pula meliputi penggunaan pelayan dengan spesifikasi minimum seperti RAM 8 GB, storan SSD sekurang-kurangnya 100 GB, pemproses minimum 4 teras, sistem operasi Linux Ubuntu 22.04 LTS bagi pelayan Wazuh, serta sistem operasi Windows 10 dan Windows 11 bagi ejen titik akhir. Jadual 3.1 menunjukkan senarai keperluan perkakasan dan perisian

	Jenis	**Perincian**
Perkakasan	Komputer Riba	- 16 GB RAM - 1.5TB SSD Ruang simpanan (1TB + 512GB SSD)
Perisian	Sistem pengoperasian hos	Linux Mint 22.3 Cinamon
	Sistem pengoperasian agen	Windows 10 Windows 11

Perisian pengesanan dan respons	Wazuh versi 4.12.0
Perisian mesin maya	VirtualBox
Platform perisikan ancaman	VirusTotal

Jadual 3.1 Senarai Keperluan Perkakasan dan Perisian

Model sistem yang dibangunkan menggunakan seni bina pengguna-pelayan di mana pelayan pusat Wazuh bertanggungjawab untuk menerima, menyimpan serta menganalisis log aktiviti yang dihantar oleh ejen Wazuh pada titik akhir yang dipantau. Ejen-ejen yang dipasang pada mesin titik akhir bertugas mengumpul maklumat perubahan serta aktiviti sistem operasi pada titik akhir masing-masing, sebelum dihantar kepada pelayan pusat bagi tujuan analisis lanjut. Seni bina ini membolehkan komunikasi dua hala antara pelayan pusat dengan ejen-ejen titik akhir, yang seterusnya membolehkan sistem melaksanakan arahan tindak balas automatik terhadap ancaman secara serta-merta apabila ancaman dikenal pasti oleh sistem. Rajah 3.1 menunjukkan seni bina pengguna-pelayan Wazuh.



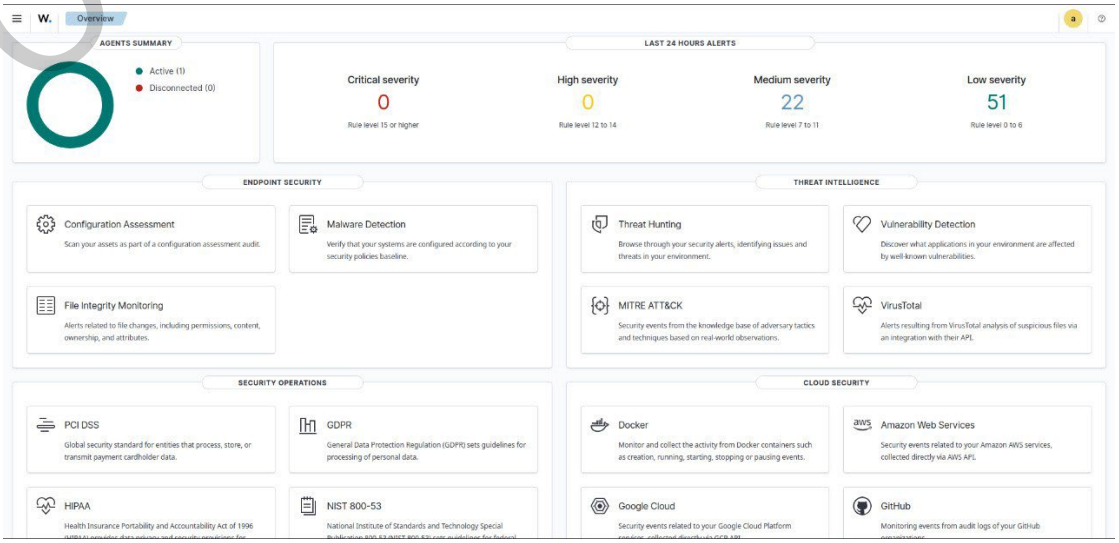
Rajah 3.1 Seni bina pengguna-pelayan Wazuh

Seterusnya, algoritma-algoritma khusus turut dibangunkan bagi meningkatkan keberkesanan sistem dalam pengesanan ancaman serta tindak balas terhadap aktiviti mencurigakan. Algoritma Pengesanan Kelemahan digunakan bagi mengesan kelemahan sistem berdasarkan analisis log aktiviti. Algoritma Pemantauan Integriti Fail pula digunakan bagi mengenal pasti perubahan yang berlaku pada fail-fail kritikal dalam sistem, yang boleh menandakan wujudnya pencerobohan atau ancaman keselamatan. Selain itu, Algoritma Respons Automatik pula dibangunkan bagi

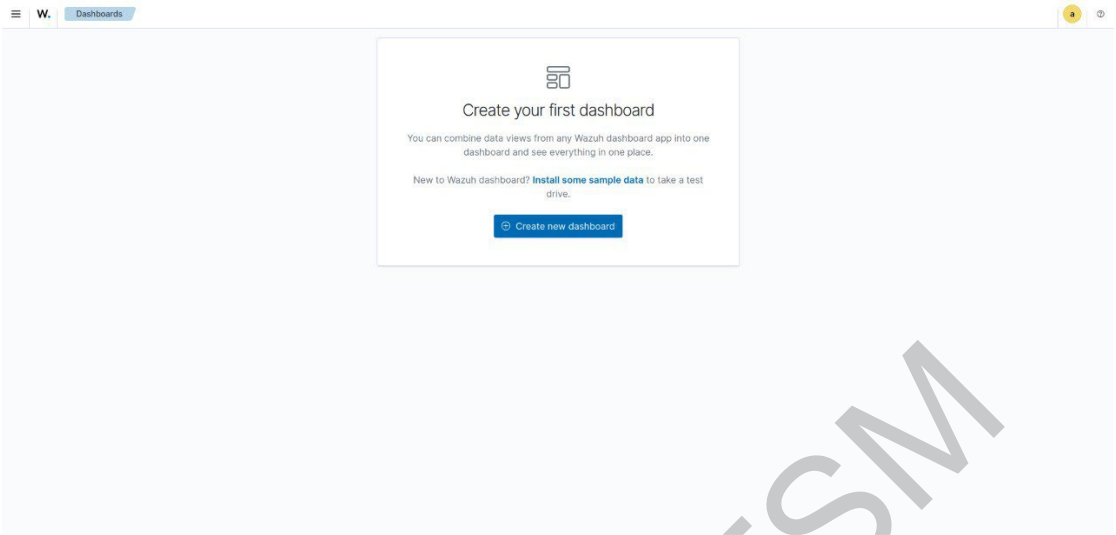
membolehkan sistem bertindak secara terus dengan menghapuskan fail mencurigakan daripada sistem titik akhir sejurus ancaman disahkan melalui maklumat yang diperoleh daripada VirusTotal. Akhir sekali, Algoritma Peraturan Pengesanan Perisian Hasad turut dibangunkan bagi mengesan kewujudan perisian hasad berdasarkan tingkah laku atau corak aktiviti yang mencurigakan dalam log aktiviti sistem

Antara muka sistem juga diberi perhatian dalam pembangunan sistem ini bagi memastikan kebolehgunaan serta kemudahan penggunaan oleh kedua-dua peranan pengguna yang telah dikenal pasti. Antara muka yang dibangunkan termasuk antara muka log masuk pengguna, menu utama, serta papan pemuka yang membolehkan visualisasi data ancaman serta laporan keselamatan dapat dipaparkan dengan jelas dan efektif kepada pengguna. Rajah 3.2 hingga 3.4 menunjukkan antara muka Wazuh.

Rajah 3.2 Antara muka log masuk Wazuh



Rajah 3.3 Antara muka menu utama Wazuh



Rajah 3.4 Antara muka papan muka Wazuh

Kesimpulannya, keseluruhan metodologi ini telah dirangka dengan teliti dan teratur bagi memastikan semua objektif projek dapat dicapai secara optimum. Daripada analisis awal, penentuan keperluan pengguna dan sistem, sehingga kepada pembangunan algoritma khusus serta reka bentuk seni bina pengguna-pelayan, setiap langkah diambil kira dengan penuh perhatian agar sistem ini mampu menyediakan penyelesaian yang efektif, praktikal dan bersesuaian dengan keperluan sebenar organisasi berskala kecil dan sederhana dalam memperkukuhkan keselamatan titik akhir mereka.

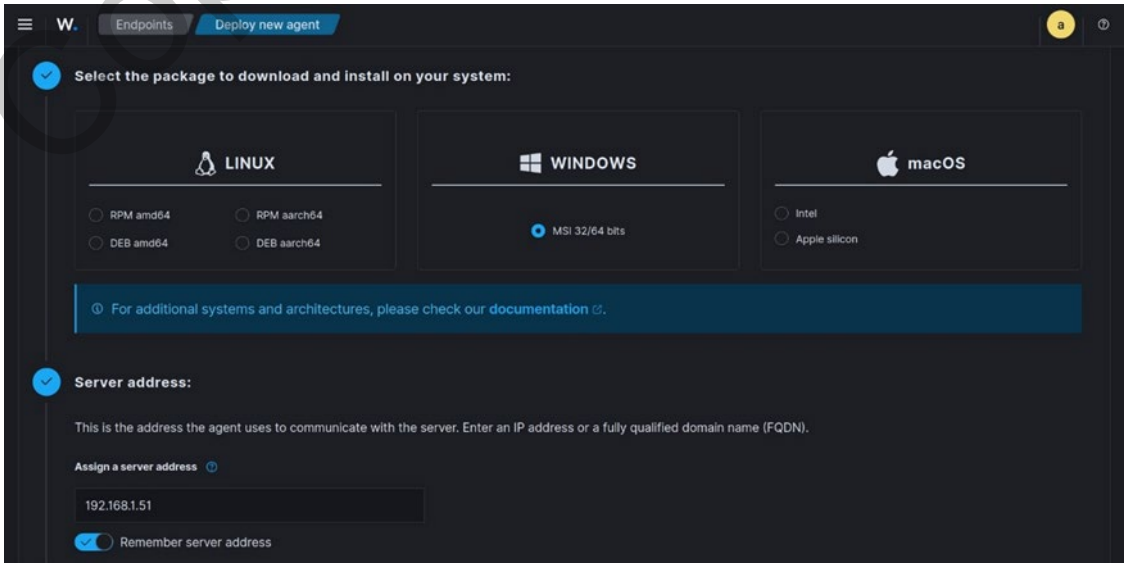
4.0 HASIL

Hasil projek ini memperincikan proses pembangunan sistem EDR berasaskan Wazuh termasuk pemasangan, konfigurasi, integrasi serta keputusan daripada ujian yang telah dijalankan. Dalam proses pembangunan, langkah pertama ialah pemasangan komponen pusat sistem Wazuh yang terdiri daripada pelayan Wazuh, pengindeks Wazuh, serta papan pemuka Wazuh. Pelayan Wazuh dipasang pada komputer hos menggunakan sistem operasi Linux Ubuntu 22.04 LTS dengan skrip arahan yang telah disediakan oleh dokumentasi rasmi Wazuh. Skrip pemasangan ini melibatkan konfigurasi asas seperti penetapan alamat IP serta penggunaan protokol komunikasi untuk ejen Wazuh yang akan berhubung dengan pelayan pusat. Rajah 4.1 menunjukkan skrip pemasangan Wazuh yang digunakan pada hos untuk pemasangan pelayan pusat, pengindeks serta papan pemuka Wazuh.

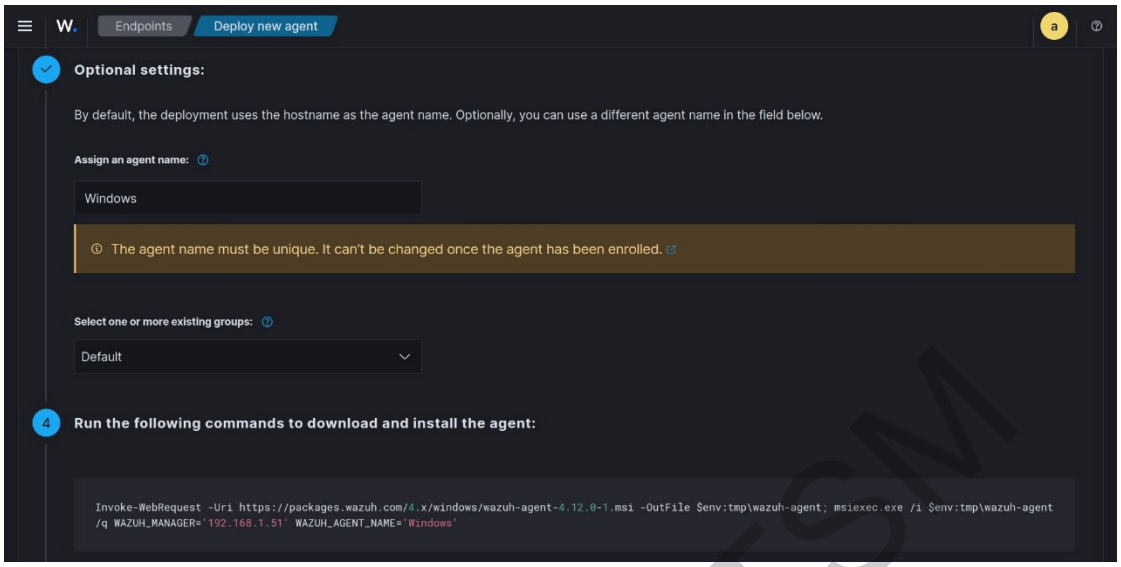
```
$ curl -sO https://packages.wazuh.com/4.12/wazuh-install.sh && sudo bash ./wazuh-install.sh -a
```

Rajah 4.1 Skrip arahan pemasangan Wazuh

Selepas pemasangan pelayan pusat selesai, proses seterusnya adalah pemasangan dan konfigurasi ejen Wazuh pada titik akhir menggunakan sistem operasi Windows 10 dan Windows 11. Proses ini bermula dengan menjana skrip pemasangan melalui papan pemuka Wazuh dengan menentukan sistem operasi serta alamat pelayan Wazuh yang digunakan.

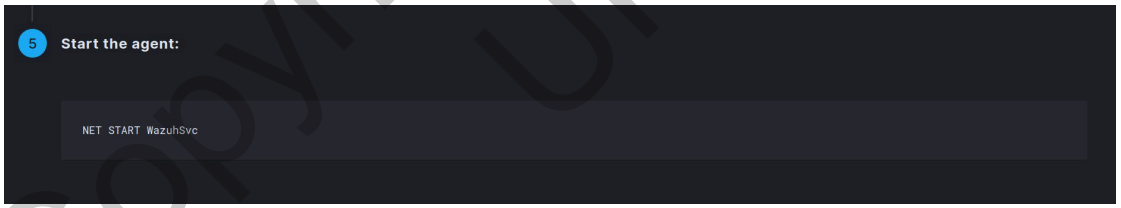


Rajah 4.2 Antara muka pemilihan sistem operasi dan alamat pelayan

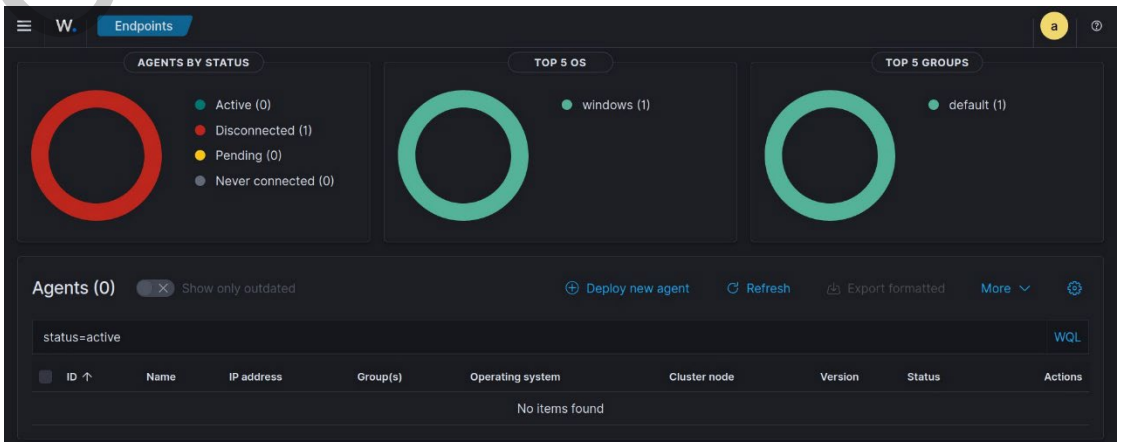


Rajah 4.3 Antara muka konfigurasi nama agen dan penjanaan skrip pemasangan

Rajah 4.2 menunjukkan antara muka pemilihan sistem operasi dan alamat pelayan Wazuh, manakala Rajah 4.3 menunjukkan antara muka konfigurasi nama agen serta penjanaan skrip pemasangan untuk pemasangan ejen. Selepas ejen berjaya dipasang, perkhidmatan Wazuh pada ejen titik akhir perlu diaktifkan bagi memastikan komunikasi dengan pelayan pusat berjalan lancar. Status sambungan ejen kemudian disahkan melalui papan pemuka Wazuh untuk memastikan ejen telah berhubung dengan pelayan pusat.



Rajah 4.4 Arahan untuk memulakan perkhidmatan agen Wazuh



Rajah 4.5 Status sambungan agen dalam papan pemuka Wazuh

Rajah 4.4 menunjukkan arahan untuk memulakan perkhidmatan ejen Wazuh, manakala Rajah 4.5 menunjukkan status sambungan ejen yang dipaparkan dalam papan pemuka Wazuh selepas pemasangan berjaya dilakukan.

Proses konfigurasi pemantauan ancaman pula melibatkan penggunaan Sysmon yang berfungsi sebagai pemantau aktiviti sistem operasi Windows secara mendalam. Konfigurasi Sysmon dijalankan melalui fail XML khas yang menentukan jenis aktiviti sistem yang perlu dipantau, seperti pelaksanaan arahan PowerShell atau sebarang perubahan konfigurasi sistem kritikal.

```
<Sysmon schemaversion="4.90">
  <HashAlgorithms>*</HashAlgorithms>
  <!-- This now also determines the file names of the files preserved (String) -->
  <CheckRevocation>False</CheckRevocation>
  <!-- Setting this to true might impact performance -->
  <DnsLookup>False</DnsLookup>
  <!-- Disables lookup behavior, default is True (Boolean) -->
  <ArchiveDirectory>Sysmon</ArchiveDirectory>
  <!-- Sets the name of the directory in the C:\ root where preserved files will be saved (String)-->
  <EventFiltering>
    <!-- Event ID 1 == Process Creation - Includes -->
    <RuleGroup groupRelation="or">
      <ProcessCreate onmatch="include">
        <ParentImage name="technique_id=T1546.008,technique_name=Accessibility Features" condition="image">sethc.exe</ParentImage>
        <ParentImage name="technique_id=T1546.008,technique_name=Accessibility Features" condition="image">utilman.exe</ParentImage>
```

Rajah 4.6 Contoh konfigurasi XML Sysmon

```
<localfile>
<location>Microsoft-Windows-Sysmon/Operational</location>
<log_format>eventchannel</log_format>
</localfile>
```

Rajah 4.7 Konfigurasi untuk membaca log Sysmon dalam sistem Windows

```
<group name="sysmon,">
 <rule id="255000" level="12">
 <if_group>sysmon_event1</if_group>
 <field name="sysmon.image">\\powershell.exe||\\.ps1||\\.ps2</field>
 <description>Sysmon - Event 1: Bad exe: $(sysmon.image)</description>
 <group>sysmon_event1,powershell_execution,</group>
 </rule>
</group>
```

Rajah 4.8 Peraturan untuk mengesan pelaksanaan PowerShell melalui Sysmon

Rajah 4.6 menunjukkan konfigurasi XML untuk pemantauan mendalam menggunakan Sysmon, Rajah 4.7 menunjukkan konfigurasi membaca log Sysmon di dalam sistem Windows dan Rajah 4.8 menunjukkan peraturan khusus untuk mengesan aktiviti mencurigakan melalui Sysmon, iaitu pelaksanaan PowerShell.

Selain itu, konfigurasi sistem turut melibatkan penetapan direktori untuk pemantauan integriti fail (FIM) serta direktori yang akan dihantar kepada VirusTotal secara automatik bagi semakan reputasi fail.

```
<directories whodata="yes" report_changes="yes">C:\Users\Public</directories>
```

Rajah 4.9 Direktori yang dipantau oleh FIM

```
<directories realtime="yes">C:\Users\akmal\Downloads</directories>
```

Rajah 4.10 Direktori yang dipantau oleh VirusTotal

Rajah 4.9 menunjukkan senarai direktori yang dipantau secara berterusan oleh FIM, manakala Rajah 4.10 menunjukkan direktori khusus yang dipantau oleh integrasi VirusTotal untuk pengesanan automatik fail mencurigakan.

Integrasi dengan VirusTotal dijalankan melalui penggunaan API yang disediakan oleh VirusTotal dan konfigurasi aktif respons dalam sistem Wazuh. Integrasi ini membolehkan semakan automatik ke atas fail mencurigakan berdasarkan reputasi global yang disediakan oleh VirusTotal. Jika fail tersebut disahkan berniat jahat, sistem secara automatik akan menghapuskan fail tersebut daripada titik akhir tanpa memerlukan campur tangan manusia.

```
<ossec_config>
  <integration>
    <name>virustotal</name>
    <api_key>ed1bc6fdf8b8fe8051bddd29016ddf4de1c6cc0cd502d6185c4e8b665971a46f</api_key>
    <group>syscheck</group>
    <alert_format>json</alert_format>
  </integration>
</ossec_config>

<ossec_config>
  <command>
    <name>remove-threat</name>
    <executable>remove-threat.exe</executable>
    <timeout_allowed>no</timeout_allowed>
  </command>

  <active-response>
    <disabled>no</disabled>
    <command>remove-threat</command>
    <location>local</location>
    <rules_id>87105</rules_id>
  </active-response>
</ossec_config>
```

Rajah 4.11 Konfigurasi Integrasi VirusTotal dan Respons Aktif

```
<group name="virustotal,">
  <rule id="100092" level="12">
      <if_sid>657</if_sid>
      <match>Successfully removed threat</match>
      <description>$(parameters.program) removed threat located at $(parameters.alert.data.virustotal.source.file)</description>
  </rule>

  <rule id="100093" level="12">
    <if_sid>657</if_sid>
    <match>Error removing threat</match>
    <description>Error removing threat located at $(parameters.alert.data.virustotal.source.file)</description>
  </rule>
</group>
```

Rajah 4.12 Peraturan untuk Menyatakan Hasil Tindakan Respons Aktif

Rajah 4.11 menunjukkan konfigurasi integrasi antara Wazuh dengan VirusTotal, manakala Rajah 4.12 menunjukkan peraturan respons aktif yang digunakan apabila ancaman disahkan.

Tambahan lagi, konfigurasi untuk menyekat akses alamat IP yang dikenal pasti

berbahaya turut dilaksanakan bagi meningkatkan lagi perlindungan terhadap ancaman dari luar rangkaian organisasi.

```
<localfile>
  <log_format>syslog</log_format>
  <location>C:\Apache24\logs\access.log</location>
</localfile>
```

Rajah 4.13 Konfigurasi Pemantauan Log Akses Apache di Windows

```
<group name="attack,">
  <rule id="100100" level="10">
    <if_group>web|attack|attacks</if_group>
    <list field="srcip" lookup="address_match_key">etc/lists/blacklist-alienvault</list>
    <description>IP address found in AlienVault reputation database.</description>
  </rule>
</group>
```

Rajah 4.14 Peraturan untuk Pengesanan Alamat IP Berisiko

```
<ossec_config>
  <active-response>
    <disabled>no</disabled>
    <command>netsh</command>
    <location>local</location>
    <rules_id>100100</rules_id>
    <timeout>60</timeout>
  </active-response>
</ossec_config>
```

Rajah 4.15 Konfigurasi untuk Menyekat IP pada Titik Akhir Windows menggunakan netsh

Rajah 4.13 menunjukkan konfigurasi log akses Apache yang dipantau, Rajah 4.14 menunjukkan peraturan khusus untuk pengesanan alamat IP berisiko, manakala Rajah 4.15 menunjukkan konfigurasi penyekatan IP secara automatik di titik akhir Windows melalui arahan netsh.

Seteusnya, pengujian sistem dijalankan dengan enam ujian khusus bagi mengesahkan keberkesanan sistem dalam pengesanan, pelaporan serta tindak balas terhadap pelbagai bentuk ancaman keselamatan. Jadual 4.2 menunjukkan ringkasan reka bentuk kes ujian yang dijalankan sepanjang proses pengujian sistem.

Jadual 4.1 Reka Bentuk Kes Ujian

No	Nama Ujian	Objektif	Kriteria Lulus/Gagal
1	Pemasangan Agen Wazuh	Memastikan agen dipasang dan aktif dalam papan pemuka Wazuh.	LULUS: Agen muncul sebagai aktif dalam papan pemuka. GAGAL: Agen tidak muncul atau tidak menghantar log.
2	Pemantauan Integriti Fail (FIM)	Cipta, ubah dan padam fail fim_test.txt dalam direktori yang dipantau.	LULUS: Semua tindakan (cipta, ubah, padam) direkod dalam log Wazuh. GAGAL: Tiada log dikesan untuk salah satu atau semua tindakan.
3	Pengesanan dan Pemadaman Fail Perisian Hasad melalui Integrasi VirusTotal	Mengesan fail EICAR, imbasan melalui VirusTotal dan pemadaman automatik oleh respons aktif	LULUS: Fail dikesan sebagai berbahaya dan dipadam secara automatik. GAGAL: Fail tidak dikesan atau tidak dipadam.
4	Serangan Brute Force (Hydra)	Mengesan cubaan log masuk berulang ke perkhidmatan SMB dari sistem luar	LULUS: Log aktiviti log masuk berulang dikesan. GAGAL: Tiada log berkaitan aktiviti dikesan.
5	Akses curl dari Kali ke Apache Windows	Mengesan cubaan log masuk berulang ke perkhidmatan SMB dari sistem luar	LULUS: Sambungan pertama berjaya, sambungan seterusnya disekat dan log dikesan. GAGAL: Sambungan tidak disekat atau tiada log.
6	Simulasi T1218.010 (Regsvr32 – Signed Binary Proxy Execution)	Mengesan eksploitasi proses sah (regsvr32.exe) untuk melaksanakan skrip jauh	LULUS: Log berkaitan regsvr32 direkod oleh Wazuh. GAGAL: Tiada log berkaitan dikesan.

Pengujian yang dijalankan merangkumi enam senario ancaman yang telah dipilih berdasarkan fungsi utama sistem EDR seperti yang dirancang dalam dokumen keperluan dan reka bentuk sistem. Aspek yang diuji termasuk pemasangan ejen, pemantauan fail, pengesanan fail mencurigakan, serangan brute force, ujian akses tidak sah serta eksploitasi proses sah menggunakan teknik MITRE ATT&CK. Setiap ujian dilaksanakan secara terkawal oleh responden dengan menggunakan sistem yang telah disediakan dan dipantau melalui log serta amaran keselamatan yang dijana oleh sistem Wazuh.

Sebelum menilai keberkesanan sistem dari aspek teknikal, penting untuk difahami bahawa latar belakang responden dari segi pengetahuan keselamatan siber

memainkan peranan dalam interpretasi hasil pengujian. Jadual 4.2 menunjukkan tahap pengetahuan keselamatan siber bagi lima orang responden yang terlibat.

Jadual 4.2 Tahap Pengetahuan Keselamatan Siber Responden (n=5)

Tahap Pengetahuan	**Bilangan Responden**	**Peratus (%)**
Tiada	2	40
Asas	3	60
Pertengahan	0	0
Mahir	0	0

Keputusan menunjukkan bahawa daripada lima responden yang terlibat dalam pengujian, majoriti sebanyak 60% memiliki pengetahuan asas dalam keselamatan siber manakala 40% tidak mempunyai pengalaman atau pengetahuan dalam bidang tersebut.Tiada responden yang melaporkan tahap pertengahan atau mahir. Keadaan ini mencerminkan profil pengguna sebenar dalam konteks SME yang mungkin tidak mempunyai kepakaran mendalam dalam keselamatan siber. Oleh itu, kebolehan responden untuk melaksanakan ujian dengan jayanya menjadi petunjuk awal bahawa sistem EDR yang dibangunkan bersifat mesra pengguna dan tidak memerlukan tahap kemahiran teknikal yang tinggi. Seterusnya, keputusan pengujian bagi setiap kes ujian diringkaskan dalam Jadual 4.3.

Jadual 4.3 Ringkasan Keputusan Ujian Sistem EDR (n=5)

No.	**Ujian**	**Bilangan Responden**	**Bilangan Lulus**	**Bilangan Gagal**	**Peratus Lulus (%)**
1	Pemasangan Ejen Wazuh	5	5	0	100%
2	Pemantauan Integriti Fail	5	5	0	100%
3	Pengesanan dan Pemadaman Fail Perisian Hasad melalui Integrasi	5	5	0	100%

	VirusTotal				
4	Serangan Brute Force menggunakan Hydra	5	5	0	100%
5	Akses curl dari Kali ke Apache Windows	5	5	0	100%
6	Simulasi T1218.010 (Regsvr32 – Signed Binary Proxy Execution)	5	5	0	100%

Semua responden berjaya melaksanakan kesemua enam ujian dengan hasil yang menunjukkan keberkesanan sistem dalam mengesan dan bertindak balas terhadap aktiviti yang mencurigakan. Keputusan yang konsisten ini menggambarkan bahawa sistem telah dibangunkan dengan baik dari segi kefungsian teknikal serta mudah difahami dan digunakan oleh pengguna yang bukan dari latar belakang keselamatan siber profesional. Dalam ujian pemasangan ejen, responden melaporkan bahawa proses pemasangan berjalan tanpa ralat dan ejen berjaya muncul sebagai aktif dalam papan pemuka sistem. Ini menandakan kestabilan sambungan antara ejen dan pelayan serta kejelasan arahan pemasangan.

Seterusnya, dalam ujian pemantauan fail, sistem dapat mengesan tiga jenis aktiviti terhadap fail iaitu penciptaan, pengubahsuaian dan penghapusan fail. Log yang dihasilkan lengkap dan muncul secara masa nyata di papan pemuka Wazuh, membuktikan ketepatan modul FIM dalam merekod aktiviti kritikal. Untuk pengesanan fail perisian hasad, sistem berjaya mengenal pasti fail EICAR sebagai berbahaya dan bertindak memadam fail tersebut secara automatik menggunakan respons aktif. Responden turut menyatakan bahawa proses ini berlaku dengan pantas dan tanpa memerlukan input lanjut daripada pengguna yang menunjukkan kecekapan integrasi sistem dengan perkhidmatan VirusTotal.

Ujian serangan brute force turut menunjukkan hasil yang memuaskan, di mana sistem berjaya merekod cubaan log masuk berulang dari alat Hydra yang dijalankan pada mesin Kali Linux. Log yang dipaparkan dalam papan pemuka menunjukkan butiran berkaitan aktiviti serangan, membolehkan pentadbir mengenal pasti pola

serangan secara jelas. Bagi ujian akses luar menggunakan curl, sistem bertindak menyekat sambungan kedua dan seterusnya daripada IP yang sama. Sambungan pertama dibiarkan berjaya seperti yang dirancang bagi tujuan penilaian. Mekanisme sekatan ini berjaya dilaksanakan melalui modul respons aktif berdasarkan senarai reputasi IP yang ditentukan. Akhir sekali, simulasi serangan berdasarkan teknik T1218.010 daripada MITRE ATT&CK menggunakan regsvr32.exe turut berjaya dikesan. Sistem menjana log berkaitan aktiviti regsvr32 secara tepat.

Sebagai pelengkap kepada aspek teknikal, satu bahagian khusus turut diberikan kepada responden untuk menilai sistem secara keseluruhan dari perspektif pengguna. Penilaian ini penting bagi memastikan sistem bukan sahaja berfungsi dengan baik tetapi juga mudah digunakan dan boleh diterima oleh pengguna sasaran seperti pentadbir rangkaian atau kakitangan teknikal di SME. Maklum balas responden terhadap aspek kebolehgunaan sistem diringkaskan dalam dua jadual iaitu jadual 4.4 dan 4.5.

Jadual 4.4 Penilaian Sistem – Soalan Jenis Ya/Tidak (n=5)

Soalan Penilaian	**Ya**	**Tidak**	**Peratus (%)**
Adakah sistem ini mudah digunakan dan difahami?	5	0	100%
Adakah sistem ini mesra pengguna?	5	0	100%

Keputusan jadual 4.4 menunjukkan bahawa kesemua responden bersetuju bahawa sistem adalah mudah difahami dan mesra pengguna. Ini menunjukkan bahawa sistem EDR yang dibangunkan mempunyai antara muka yang intuitif serta menyediakan pengalaman penggunaan yang positif walaupun dalam kalangan pengguna yang mempunyai pengetahuan teknikal asas.

Seterusnya, maklum balas terbuka yang diberikan oleh responden turut menunjukkan penerimaan positif terhadap sistem EDR yang dibangunkan. Semua responden memberikan pandangan yang menyokong keberkesanan sistem termasuk menyatakan bahawa sistem ini mudah digunakan, mesra pengguna sangat membantu dalam kawalan keselamatan komputer dan mampu mengelakkan insiden keselamatan dengan kos yang minimum. Seorang responden secara khusus menekankan bahawa sistem ini sesuai untuk syarikat kecil kerana ia dapat

melindungi keselamatan organisasi tanpa memerlukan perbelanjaan tambahan. Pandangan ini mencerminkan nilai tambah sistem dalam konteks organisasi yang mempunyai sumber terhad seperti SME.

Dari segi penambahbaikan, dua daripada lima responden menyatakan bahawa tiada penambahbaikan diperlukan, menandakan tahap kepuasan yang tinggi terhadap sistem dalam bentuk sedia ada. Namun begitu, selebihnya mencadangkan beberapa penambahbaikan seperti peningkatan aspek keselamatan sedia ada serta penambahan fungsi berasaskan kecerdasan buatan. Cadangan ini memperlihatkan kesedaran responden terhadap keperluan jangka panjang dan potensi pengembangan sistem sejajar dengan teknologi keselamatan siber semasa.

Selain itu, responden turut diminta memberikan pandangan sama ada terdapat mana-mana fungsi atau ujian yang dirasakan sukar difahami. Majoriti responden menyatakan bahawa semua fungsi adalah mudah difahami dan dilaksanakan.

Jadual 4.5 Penilaian Sistem Berdasarkan Skala Likert (n=5)

Soalan Penilaian	1	2	3	4	5
Kebarangkalian untuk menggunakan sistem ini di masa hadapan	0	0	2 (40%)	2 (40%)	1 (20%)
Tahap kepuasan keseluruhan terhadap sistem	0	0	0	3 (60%)	2 (40%)

Berdasarkan jadual 4.5, analisis penilaian dilakukan menggunakan skala Likert lima mata. Bagi soalan berkaitan kebarangkalian menggunakan sistem ini pada masa akan datang, skala yang digunakan ialah seperti berikut 1 = sangat tidak setuju, 2 = tidak setuju, 3 = neutral, 4 = setuju dan 5=sangat setuju. Manakala bagi soalan tahap kepuasan keseluruhan terhadap sistem, skala yang digunakan ialah 1 = sangat tidak berpuas hati, 2 = tidak berpuas hati, 3 = neutral, 4 = berpuas hati dan 5 = sangat berpuas hati.

Bagi penilaian terhadap kebarangkalian menggunakan sistem, sebanyak 40% responden memilih nilai 4 dan 20% memilih nilai maksimum 5. Dua orang responden memberikan skor 3 dan tiada responden memberikan skor 1 atau 2.

Secara keseluruhan, dapatan ini menunjukkan bahawa kesemua responden menunjukkan kecenderungan positif terhadap potensi penggunaan sistem ini dalam konteks sebenar terutamanya dalam persekitaran SME.

Dari segi tahap kepuasan keseluruhan terhadap sistem, 60% responden memberikan skor 4, manakala 40% lagi memberikan skor 5. Tiada responden memberikan skor 3 atau lebih rendah. Hal ini menunjukkan bahawa sistem ini bukan sahaja berfungsi dengan baik dari sudut teknikal tetapi turut memberikan pengalaman penggunaan yang memuaskan kepada pengguna akhir sepanjang sesi pengujian dijalankan

5.0 KESIMPULAN

Secara keseluruhannya, sistem yang dibangunkan menunjukkan prestasi yang memuaskan dan telah berjaya memenuhi objektif yang ditetapkan. Sistem mampu mengesan perubahan fail, mengimbas fail berisiko tinggi melalui integrasi dengan VirusTotal, memadam fail secara automatik serta mengesan aktiviti mencurigakan seperti serangan brute force dan penyalahgunaan proses sah. Pengujian juga menunjukkan bahawa sistem ini mudah digunakan, mesra pengguna serta sesuai diaplikasikan dalam konteks SME yang mempunyai sumber kewangan dan teknikal yang terhad.

Namun begitu, terdapat beberapa kekangan yang dikenalpasti sepanjang pelaksanaan projek. Antaranya termasuk had pengujian yang terhad kepada sistem operasi Windows sahaja serta kekangan masa yang mengehadkan pengujian dalam persekitaran sebenar berskala besar. Selain itu, integrasi sistem dengan sumber perisikan ancaman awam seperti VirusTotal bergantung kepada had penggunaan API percuma yang mungkin tidak sesuai untuk penggunaan berskala perusahaan. Dari sudut teknikal, sistem juga masih bergantung kepada peraturan statik dan belum mengintegrasikan sebarang bentuk kecerdasan buatan untuk pengesanan dinamik. Tambahan lagi, akses kepada Wazuh bergantung kepada alamat IP hos yang digunakan. Sekiranya hos menggunakan peruntukan alamat IP secara dinamik melalui DHCP, terdapat risiko alamat IP akan berubah yang boleh menyukarkan akses kepada papan pemuka Wazuh serta menjejaskan komunikasi dengan ejen titik akhir.

Sebagai cadangan penambahbaikan pada masa hadapan, sistem ini boleh penggunaan teknik kecerdasan buatan seperti pembelajaran mesin boleh

dimanfaatkan untuk menganalisis corak log secara dinamik sekali gus meningkatkan keupayaan sistem dalam mengenal pasti ancaman yang tidak diketahui. Sekiranya berkemampuan, sistem ini juga wajar dipertimbangkan untuk dilaksanakan dalam persekitaran berasaskan awan bagi menjamin skalabiliti, mobiliti dan aksesibiliti sistem secara lebih fleksibel terutamanya dalam persekitaran kerja moden

6.0 RUJUKAN

Aslan, Ö., Aktuğ, S.S., Ozkan-Okay, M., Yilmaz, A.A. & Akin, E. 2023. A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. Electronics (Switzerland). MDPI.

Bhavsar, R. & Thakar, V. 2025. Design and Implementation of an Open-Source Security Operations Center for Effective Cyber Threat Detection and Response.

BRITE. 2024. State of Ransomware 2024: A Year of Surges and Shuffling. https://blackkite.com/wp-content/uploads/2024/05/BlackKite_Report_Ransomware-2024.05.14.pdf

Cisco. 2020. Cisco Cybersecurity Report Series 2020 Small and Medium-Sized Business.

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. Article in International Journal of Advanced Research in Science Communication and Technology 8(1).

IBM. 2024. What is endpoint detection and response (EDR)? https://www.ibm.com/topics/edr

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.

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 Vol. 556. EDP Sciences.

Morefield. 2024. 5 Cybersecurity Predictions for 2025. https://morefield.com/blog/5-cybersecurity-predictions-for-2025/

Park, S.H., Yun, S.W., Jeon, S.E., Park, N.E., Shim, H.Y., Lee, Y.R., Lee, S.J., Park, T.R., Shin, N.Y., Kang, M.J. & Lee, I.G. 2022. Performance Evaluation of Open-Source Endpoint Detection and Response Combining Google Rapid Response and Osquery for Threat Detection. IEEE Access 10: 20259–20269.

Peris.AI. 2024. Why Antivirus Software Is No Longer Enough – Here's What You Need. https://www.linkedin.com/pulse/why-antivirus-software-longer-enough-heres-what-nmj3c

Ponemon Institute. 2020. The Third Annual Study on the State of Endpoint Security Risk. https://www.morphisec.com/hubfs/2020%20State%20of%20Endpoint%20Security%20Final.pdf

Prasad, M.D., Sindusha, M.S.N.V.R.S., Jahnavi, N., Ali, M.W. & Devi, S.A. 2024. Enabling Cybersecurity Defenses: Advanced Endpoint Detection, Data Breach Identification, and Anomaly Resolution. Proceedings - 2024 8th International Conference on Inventive Systems and Control, ICISC 2024 hlm. 461–468. Institute of Electrical and Electronics Engineers Inc.

Shea, S. & Irei, A. 2023. What is ransomware? How it works and how to remove it. https://www.techtarget.com/searchsecurity/definition/ransomware

Siji, F.G. & Uche, O.P. 2023. An improved model for comparing different endpoint detection and response tools for mitigating insider threat. Indian Journal of Engineering 20(53)

Tendikov, N., Rzayeva, L., Saoud, B., Shayea, I., Azmi, M.H., Myrzatay, A. & Alnakhli, M. 2024. Security Information Event Management data acquisition and analysis methods with machine learning principles. Results in Engineering

Wazuh. 2024. Documentation Index. https://documentation.wazuh.com/current/index.html

Wibowo, B., Nurrohman, A. & Hafiz, L. 2025. Deep Learning in Wazuh Intrusion Detection System to Identify Advanced Persistent Threat (APT) Attacks. International Journal of Science Education and Cultural Studies 4(1): 1–10.

Zhao, X., Leng, X., Wang, L., Wang, N. & Liu, Y. 2025. Efficient anomaly detection in tabular cybersecurity data using large language models. Scientific Reports 15(1).

Muhammad Akmal Hakim bin Aziz (A193460)
Dr. Khairul Akram Zainol Ariffin
Fakulti Teknologi & Sains Maklumat
Universiti Kebangsaan Malaysia