BAB 1

PENDAHULUAN

1.1. Latar Belakang

Ancaman serangan siber semakin meningkat seiring dengan pesatnya perkembangan teknologi informasi. Salah satu bentuk ancaman siber adalah *malicious software* (*malware*), yakni kode berbahaya yang dirancang untuk mengeksploitasi celah keamanan pada sistem operasi, situs web, aplikasi, maupun jaringan. Celah keamanan (*vulnerability*) merupakan kesalahan dalam kode atau konfigurasi yang membuka peluang bagi pihak tidak bertanggung jawab untuk melakukan eksploitasi yang merugikan (Hapsari & Pambayun, 2023). Dalam era serangan siber yang semakin kompleks, penting bagi organisasi untuk memiliki sistem keamanan yang dapat secara proaktif mendeteksi dan merespons ancaman tersebut.

Salah satu solusi efektif dalam keamanan siber adalah *Security Information and Event Management (SIEM)*. *SIEM* memungkinkan pengumpulan, analisis, dan respons terhadap data keamanan dari berbagai sumber. Efektivitas *SIEM* dapat ditingkatkan dengan mengintegrasikan *Cyber Threat Intelligence (CTI),* yang menyediakan informasi mendalam dan terkini tentang ancaman siber, termasuk indikator kompromi *(IOC)*, taktik, teknik, dan prosedur (TTP) yang digunakan oleh pelaku ancaman. Menurut (Roberts, 2021). *CTI* membantu memprediksi dan mencegah serangan dengan memanfaatkan data ancaman siber yang dianalisis secara strategis. *CTI* juga berperan dalam mengurangi *false negative* yaitu ancaman

yang tidak terdeteksi sebagai ancaman, sehingga fokus dapat diberikan pada ancaman yang benar-benar signifikan.

Salah satu platform *CTI* yang banyak digunakan adalah *Malware Information Sharing Platform* (*MISP*). *MISP* memungkinkan organisasi untuk menyimpan, berbagi, dan menerima informasi tentang *malware*, ancaman, dan kerentanan secara terstruktur (Gillard et al., 2023). *MISP* adalah solusi *CTI open-source* yang unggul karena memungkinkan berbagi informasi ancaman secara *real-time*, yang mempercepat identifikasi dan penanganan ancaman. *MISP* memfasilitasi pertukaran data ancaman yang aman dan efisien, baik di sektor publik maupun swasta. Selain itu, *MISP* menyediakan integrasi yang mudah dengan berbagai alat keamanan lainnya, seperti *SIEM, IDS*, dan solusi keamanan lainnya, yang memungkinkan otomatisasi analisis ancaman dan respons yang lebih cepat. (Gupta et al., 2021).

SIEM berfungsi sebagai sistem pemantauan dan analisis keamanan yang bekerja secara *real-time* atau melalui *history log*. Sistem ini mengumpulkan *log* dari berbagai perangkat, seperti *firewall, server,* dan *endpoint*, untuk mendeteksi pola aktivitas mencurigakan yang dapat mengindikasikan serangan *malware* (González-Granadillo et al., 2021). Salah satu perangkat lunak *SIEM* berbasis *open-source* yang populer adalah *Wazuh*. *Wazuh* merupakan solusi pemantauan keamanan yang komprehensif, menyediakan fitur deteksi ancaman, pemantauan insiden, respons insiden, serta memastikan kepatuhan terhadap kebijakan keamanan. Sebagai *Host Intrusion Detection System (HIDS), Wazuh* berfokus pada pemantauan aktivitas di level *endpoint*. Salah satu fitur unggulannya adalah *File Integrity Monitoring*

(FIM), yang memungkinkan pemantauan menyeluruh terhadap setiap perubahan yang terjadi pada file di endpoint, sehingga membantu dalam mendeteksi aktivitas mencurigakan atau potensi serangan siber.(Sheeraz et al., 2023).

DFIR IRIS merupakan platform open-source yang mendukung investigasi dan respons insiden keamanan siber. *DFIR IRIS* memungkinkan pengelolaan data insiden secara terorganisir dengan menyediakan fitur pengumpulan, visualisasi, dan analisis data yang terstruktur ancaman (DFIR IRIS, 2023). Platform ini memfasilitasi investigasi terperinci, termasuk pencatatan data log dan analisis insiden siber yang komprehensif, sehingga meningkatkan kemampuan deteksi dan respons terhadap ancaman. Integrasi (Zohra & Zerrouk, 2024). *DFIR IRIS* dengan *SIEM* seperti *Wazuh* memberikan solusi yang lebih kuat untuk mendeteksi ancaman secara *real-time* dan memastikan analisis data yang lebih baik.

Penelitian sebelumnya telah menunjukkan efektivitas *Wazuh* dalam pertahanan real-time terhadap ancaman siber, termasuk deteksi integritas file dan malware (Alanda et al., 2023; Widyatono & Sulistyo, 2023). Namun, terdapat kelemahan dalam deteksi *malware*, di mana *Wazuh* memerlukan integrasi lebih lanjut dengan threat sharing dan manajemen log untuk meningkatkan kemampuan deteksinya. Penelitian lain menyoroti pentingnya *log management* serta *incident response* dan berbagi ancaman untuk memperluas cakupan deteksi serangan (Alexandru STAN, 2021; Fernandes et al., 2023; Jeon et al., 2023).

Berdasarkan permasalahan yang ada, penelitian ini bertujuan untuk mengoptimalkan penggunaan *SIEM Wazuh* dalam deteksi *malware* dengan

menerapkan *CTI*. Pendekatan ini dilakukan melalui integrasi *SIEM Wazuh* dengan *MISP* dan *DFIR IRIS* untuk meningkatkan efektivitas deteksi ancaman dan respons keamanan siber.

1.2. Rumusan Masalah

Berdasarkan latar belakang masalah yang telah dipaparkan, adapun rumusan masalah pada penelitian ini yaitu:

1. Bagaimana kinerja *SIEM Wazuh* dalam mendeteksi malware?
2. Bagaimana dampak integrasi *MISP* terhadap peningkatan akurasi dan deteksi ancaman *Malware*?
3. Bagaimana pengaruh *DFIR-IRIS* dalam mempercepat respons insiden?

1.3. Tujuan Penelitian

Berdasarkan latar belakang masalah yang telah dipaparkan, adapun tujuan pada penelitian ini yaitu:

1. Mengukur kinerja *SIEM Wazuh* dalam mendeteksi ancaman *Malware.*
2. Mengevaluasi dampak integrasi *MISP* pada deteksi ancaman *Malware*.
3. Menganalisis peran *DFIR-IRIS* dalam mendukung respons insiden secara *real-time*.

1.4. Manfaat Penelitian

Adapun manfaat penelitian yang dilakukan sebagai berikut:

1. Diharapkan dapat membantu mengoptimalkan proses deteksi dan respons insiden melalui integrasi *Cyber Threat Intelligence* dengan *SIEM Wazuh*.

2. Menyediakan panduan praktis bagi pengguna dan peneliti untuk mengintegrasikan *MISP* dan *DFIR IRIS* dengan *SIEM Wazuh* guna meningkatkan efektivitas deteksi *malware*.

1.5. Batasan Masalah

Adapun batasan masalah yang dilakukan sebagai berikut:

1. Penelitian ini menggunakan sampel *malware* dari repositori *github.com/ThatSINEWAVE*.
2. Fokus penelitian adalah integrasi *Cyber Threat Intelligence* dengan *SIEM Wazuh*, *MISP*, dan *DFIR-IRIS*.
3. Evaluasi efektivitas penerapan *Cyber Threat Intelligence* dilakukan dalam lingkungan simulasi atau percobaan, tanpa implementasi langsung di lingkungan produksi organisasi.
4. Penelitian ini bersifat jangka pendek sehingga tidak mencakup analisis dinamika jangka panjang dalam deteksi dan respons ancaman keamanan.