BAB I
PENDAHULUAN

1.1 Latar Belakang

PT Sekuriti Siber Indonesia adalah perusahaan yang berfokus pada layanan keamanan sistem informasi, seperti penetration testing, security assessment, pendampingan ISO 27001, PCI DSS, SOC monitoring, dan pelatihan. Dengan visi menjadi pemimpin dalam industri keamanan siber di Indonesia dan misi memberikan solusi keamanan yang inovatif dan efektif, perusahaan ini berkomitmen untuk melindungi aset aset kritikal milik kliennya.

Salah satu layanan PT SSI adalah *Security Operation Center (SOC)* yaitu membantu klien dalam monitoring endpoint endpoint Linux (server), infrastruktur aplikasi dan jaringan dari berbagai ancaman dan potensi serangan siber. Dalam proses monitoring dibutuhkan sebuah sistem atau aplikasi yang saling terintegrasi agar dapat mendeteksi berbagai jenis serangan dan ancaman secara akurat termasuk serangan malware.

Magang di PT Sekuriti Siber Indonesia memberi saya kesempatan untuk berkontribusi dalam proyek SOC PT Sekuriti Siber Indonesia. Tujuan utama magang ini yaitu membantu mengembangkan aplikasi integrasi SIEM dengan Platform *Threat Intelligence Malware Bazaar*

Malware Bazaar adalah platform open source untuk berbagi sampel malware. Tujuannya adalah membantu peneliti keamanan, profesional IT, dan organisasi untuk menganalisis, mendeteksi, dan melawan ancaman siber yang disebabkan oleh malware. Platform ini berfungsi sebagai repositori pusat yang memungkinkan pengguna untuk mengunggah, mengunduh, dan mencari sampel malware.

Threat Intelligence adalah proses pengumpulan, analisis, dan penyampaian informasi terkait ancaman siber untuk membantu organisasi memahami,

mencegah, dan merespons ancaman keamanan dengan lebih efektif. Informasi ini digunakan untuk mengidentifikasi potensi risiko, memahami pola serangan, dan merumuskan langkah mitigasi yang lebih baik.

Oleh karena itu menghubungkan SIEM dengan *Threat Intelligence* seperti *Malware Bazaar* sangat dibutuhkan oleh tim SOC untuk membantu dalam mendeteksi dini serangan Malware.

Pengalaman magang ini tidak hanya memberikan pemahaman praktis tentang Security Operation Center, tetapi juga mendukung misi PT Sekuriti Siber Indonesia dalam meningkatkan keamanan informasi untuk setiap organisasi yang menggunakan jasa SOC PT Sekuriti Siber Indonesia

1.2 Deskripsi Pekerjaan

Pada penelitian ini penulis melakukan proyek pengembangan Integrasi Wazuh dengan platform *Malware Bazaar* dengan memanfaatkan API yang sudah disediakan. Adapun ruang lingkup dari penelitian ini sebagai berikut:

1. Penelitian ini berfokus pada Integrasi *Malware Bazaar* dengan Wazuh untuk mendeteksi aktifitas malware melalui fitur *File Integrity Monitoring (FIM)*
2. Proses integrasi memanfaatkan API yang disediakan oleh *Malware Bazaar*
3. Metode deteksi mencakup pencocokan hashing file pada database platform *Malware Bazaar* pada sistem operasi Linux.
4. Sampel malware yang diuji berjumlah lima. tiga sampel diperoleh dari database *Malware Bazaar* dua dari sumber lain
5. Hasil pengujian akan dibandingkan dengan platform berbayar seperti VirusTotal

1.3 Tujuan

Tujuan dari penelitian adalah untuk menguji kemampuan sistem Wazuh dalam mendeteksi aktivitas malware melalui integrasi dengan platform *Threat Intelligence Malware Bazaar* pada sistem operasi Linux.

1.4 Manfaat

Adapun manfaat dari penelitian ini sebagai berikut:

1. Menguji efektivitas Wazuh sebagai solusi deteksi malware dengan pendekatan Threat Intelligence.
2. Mengkaji bagaimana automasi Threat Intelligence dapat meningkatkan efektivitas SIEM dalam mendeteksi ancaman.