BAB 1
PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi yang semakin pesat telah diiringi dengan meningkatnya ancaman siber, baik dalam bentuk malware, phishing, ransowmare, maupun serangan berbasis jaringan lainnya. Ancaman tersebut tidak hanya menargetkan individu, tetapi juga organisasi, institusi pemerintah, dan sektor bisnis. Oleh Karena itu, diperlukan mekanisme yang mampu mendeteksi, menganalisis, serta merespons ancaman siber secara terstruktur.

Salah satu pendekatan yang digunakan dalam keamanan siber modern adalah Threat Intelligence, yaitu proses pengumpulan, analisis, dan distribusi informasi terkait indikator ancaman *Indicator of Compromise* (IoC) seperti alamat Ip, domain, hash malware, URL. Informasi ini sangat penting untuk membantu tim keamanan dalam mengidentifikasi potensi serangan sejak dini dan meningkatkan kesiapan dalam menghadapi insiden.

Dalam operasional kemanan siber, salah satu tantangan adalah tidak terintegrasinya informasi ancaman yang berasal dari berbagai sumber seperti server dan jaringan, sehingga membutuhkan proses pengumpulan dan analisis yang kompleks. Sistem seperti SIEM dirancang untuk mengkorelasikan data dari berbagai sumber, namun tanpa korelasi yang optimal, proses deteksi dan respon tidak berjalan secara optimal. Selain itu, SIEM sering menghasilkan alert dalam jumlah besar yang dapat mengalami kelelahan dalam menangani peringatan (alert fatigue) dan memperlambat respon insiden (Ramadhani et al., 2025).

MISP berperan sebagai pusat pengelolaan Threat Intelligence yang tidak hanya berfungsi sebagai repositori IoC, tetapi juga sebagai sarana kolaborasi antar organisasi dalam menghadapi ancaman siber (Hidayat et al., 2025). Dengan adanya mekanisme berbagi informasi yang terstruktur, MISP dapat meningkatkan efektivitas deteksi ancaman serta mempercepat proses mitigasi insiden keamanan. Informasi yang tersimpan dalam MISP dapat dimanfaatkan oleh berbagai sistem kemanan lain untuk mendukung pengambilan keputusan yang lebih akurat dan berbasis data.

Namun, keberadaan Threat Intelligence saja belum cukup untuk menjamin keamanan sistem. Informasi IoC yang diperoleh dari MISP perlu dianalisis lebih lanjut, dikorelasikan dengan data lain, serta diintegrasikan ke dalam proses penanganan insiden. Oleh karena itu, MISP nantinya akan diintegrasikan dengan platform lain seperti TheHive dan Cortex.

Dengan mengintegrasikan MISP, TheHive, dan Cortex, terbentuk sebuah ekosistem keamanan siber yang terpusat untuk pengumpulan, analisis, pemantauan dan respon ancaman. Pendekatan ini sejalan dengan konsep *Security Operations Center* (SOC) modern yang menekankan kolaborasi sistem, otomatisasi analisis, dalam penanganan insiden keamanan.

Penelitian ini bertujuan untuk mengimplementasikan dan mengintegrasikan MISP, TheHive, Cortex sebagai sistem Threat Intelligence untuk mendukung pengelolaan informasi ancaman siber. Pada penelitian ini, MISP berfungsi sebagai platform yang berfungsi sebagai platform yang mengumpulkan, mengelola, menyimpan, dan mendistribusikan IoC dalam bentuk *Event* atau *Attribute*. *Event* yang telah dipublikasikan kemudian diteruskan ke TheHive sebagai *Alert* untuk dianalisis lebih lanjut menggunakan Cortex. Integrasi ketiga platform tersebut diharapkan mampu membangun sistem Threat Intelligence yang bersifat terstruktur dan kolaboratif.

1.2 Perumusan Masalah

Berdasarkan latar belakang di atas, rumusan masalah dalam penelitian ini adalah:

1. Bagaimana cara mengimplementasikan dan mengintegrasikan *Malware Information Sharing Platform* (MISP) dengan TheHive dan Cortex.
2. Bagaimana alur pertukaran data ancaman *Indicator of Compromise* (IOC) dapat dilakukan secara terintegrasi antara MISP, TheHive dan Cortex.
3. Bagaimana proses analisis indikator ancaman melalui Cortex dalam mendukung investigasi insiden.
4. Bagaimana Peran MISP sebagai pusat *Threat Intelligence* dalam mendukung proses manajemen insiden pada *Security Operation Center.*
5. Bagaimana integrasi MISP, TheHive dan Cortex dalam membentuk sistem *Threat Intelligence* yang terstruktur dan terdokumentasi.

1.3 Batasan Masalah

Agar ruang lingkup penelitian tidak terlalu luas, batasan masalah yang diterapkan adalah sebagai berikut:

6. Penelitian ini hanya mencakup integrasi tiga komponen, MISP, TheHive dan Cortex.
7. Lingkungan Implementasi dibangun dalam jaringan laboratorium (Lab Environment) menggunakan sistem virtualisasi.
8. Penelitian tidak membahas teknik mitigasi malware secara mendalap seperti patching sistem atau reverse engineering.
9. Penelitian tidak membahas aspek keamanan tingkat lanjut seperti konfigurasi firewall.
10. IoC yang digunakan dalam penelitian bersifat simulasi, tidak berasal dari insiden nyata.

1.4 Tujuan dan Manfaat

1.4.1 Tujuan

Penelitian ini bertujuan untuk mengimplementasikan integrasi antara misp, thehive dan cortex membentuk sebuah sistem SOC berbasis Open-Source, merancang arsitektur sistem Threat intelligence yang dapat mengumpulkan, mengelola dan mendistribusikan ancaman secara terstruktur, serta membangun mekanisme pertukaran *Indicator Of Compromise* (IoC) sehingga dapat memudahkan proses manajemen insiden.

1.4.2 Manfaat

Hasil dari penelitian ini diharapkan dapat memberikan manfaat sebagai berikut:

1. Mendukung penerapan konsep pertukaran informasi ancaman siber.
2. Meningkatkan penerapan alur kerja terintegrasi dalam proses deteksi dan manajemen insiden.
3. Mendukung peningkatan manajemen informais ancaman secara terpusat dan terdokumentasi.
4. Meningkatkan kolaborasi antar analisis keamanan dalam proses identifikasi dan analisis ancaman.