

BAB I

PENDAHULUAN

1.1 Latar Belakang

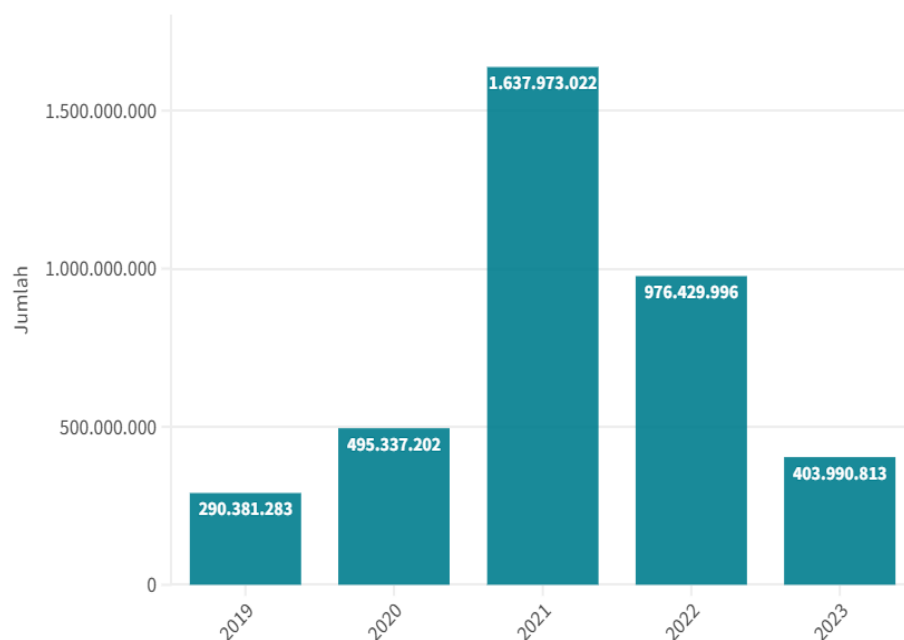
Perkembangan teknologi di dunia semakin dinamis dan tak terduga dalam hal keamanan komputer. Karena ancaman siber semakin sering terjadi, canggih, dan merusak, alat keamanan lama tidak lagi memadai. Solusi titik dan pertahanan yang terisolasi meninggalkan celah yang memungkinkan penyerang menembus jaringan 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 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.

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas rumusan masalah dari penelitian ini adalah sebagai berikut :

- a. Bagaimana *malware* dapat dideteksi dengan implementasi XDR?
- b. Bagaimana respon XDR terhadap serangan domain server?
- c. Apa saja tantangan teknis yang dihadapi tim SOC dan CSIRT dalam mengimplementasikan XDR?

1.3 Batasan Masalah

Dari rumusan masalah yang ditetapkan dalam penelitian ini, maka dirasa perlu untuk dilakukan pembatasan masalah agar penelitian lebih terfokus dan tidak meluas dari pembahasan yang dimaksudkan. Penelitian ini menitikberatkan kepada pengembangan Tim SOC dan CSIRT dengan implementasi XDR dengan poin sebagai berikut :

a. Fokus penelitian

Penelitian ini difokuskan pada implementasi XDR tanpa membahas secara dalam aspek manajerial atau kebijakan organisasi.

b. Metodologi

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

c. 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.

d. Keterbatasan deteksi

Deteksi pada pengetesan atau uji ini dilakukan untuk mendeteksi *malware* dan serangan atau penetrasi terhadap domain server.

e. Pengujian

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*.

1.4 Tujuan

Penelitian bertujuan untuk menerapkan dan membandingkan ilmu yang telah dipelajari di perkuliahan secara teoritis dengan keadaan asli pada suatu organisasi, sehingga dapat diidentifikasi masalah yang ada di lapangan. Tujuan dari penelitian ini meliputi, yaitu:

- a. Menganalisis dan mengevaluasi kinerja XDR berdasarkan kecepatan dalam mendeteksi *malware* dan respon terhadap ancaman.

- b. Mengidentifikasi jenis serangan utama pada domain server dan faktor penyebabnya.
- c. Merumuskan strategi peningkatan efisiensi kerja tim SOC dan CSIRT melalui implementasi XDR.

1.5 Manfaat

Penelitian ini diharapkan dapat memberikan manfaat bagi penulis, pembaca, penyelenggara pendidikan, akademisi, *stakeholder* dan instansi tempat penelitian berlangsung. Manfaat kegiatan ini dibagi menjadi teoritis dan praktis sebagai berikut:

1.5.1 Manfaat Teoritis

a. Pengembangan teori

Adapun penelitian ini dapat membantu mengembangkan teori XDR dan *cyber security* yang sudah ada dengan memberikan data ataupun perspektif yang baru guna memperkaya pemahaman mengenai sebuah fenomena baru khususnya dalam bidang *cybersecurity*.

b. Referensi bagi penelitian lain

Penelitian ini dapat dijadikan sebagai acuan ataupun dasar bagi penelitian-penelitian selanjutnya yang dapat menciptakan hal baru bagi eksplorasi ilmiah terutama dalam bidang *cyber security*.

c. Pemahaman konseptual

Penelitian ini dapat membantu pemahaman serta memperjelas konsep-konsep yang ada ataupun fenomena tertentu agar lebih mudah dipahami.

d. Validasi teori

Penelitian ini dapat digunakan untuk menguji ataupun memvalidasi sebuah teori-teori mengenai XDR dan *cyber security* yang sudah ada.

1.5.2 Manfaat Praktis

a. Bagi penyelenggara pendidikan (Unhan dan Kemhan).

Memberikan sebuah rekomendasi pertahanan yang dapat diadopsi untuk meningkatkan pertahanan siber di lingkungan Universitas pertahanan maupun Kementerian Pertahanan.

b. Bagi Instansi Pemerintahan.

Memberikan sebuah gambaran serta rekomendasi pertahanan terhadap infrastruktur teknologi informasi yang kemudian dapat di implementasikan bagi instansi pemerintahan seperti TNI, POLRI dan Kementerian.

