JKT Jurnal Komputer Terapan
ISSN : 2443-4159 (Print) ISSN: 2460-5255 (Online)
Politeknik Caltex Riau
Empower You to Global Competition

SISTEM DETEKSI AKTIVITAS BERBAHAYA PADA SERVER MENGGUNAKAN CROWDSEC

Muhammad Arif Fadhly Ridha[1]*, Galih Ihsan Maheswara[1]
Teknik Informatika, Politeknik Caltex Riau, Kota Pekanbaru, 28265, Indonesia[1]
fadhly@pcr.ac.id*, galih20ti@mahasiswa.pcr.ac.id
**Penulis Koresponden*

ABSTRAK

Perkembangan teknologi yang pesat telah mendorong hampir semua sektor bisnis untuk beralih ke dunia digital, namun hal ini juga memicu meningkatnya ancaman cybercrime yang menargetkan sistem dan data. Cyber Threat Intelligence (CTI) adalah pendekatan keamanan siber yang melibatkan pengumpulan, analisis, dan pemahaman data untuk mengidentifikasi motif, target, serta pola serangan pelaku kejahatan siber. Salah satu solusi untuk mengatasi ancaman ini adalah dengan menggunakan perangkat lunak CrowdSec, sebuah proyek sumber terbuka yang dirancang untuk mendeteksi dan mencegah serangan keamanan siber di berbagai lingkungan, termasuk server. Hasil pengujian menunjukkan bahwa CrowdSec efektif dalam mendeteksi serangan SSH brute-force, port scanning, dan SQL injection. Dengan mengenali pola serangan mencurigakan dan memblokir IP penyerang, CrowdSec dapat mengurangi risiko kerusakan pada server. Waktu responnya juga cepat: 23 detik untuk SSH brute-force, 10 detik untuk port scanning, dan 6 detik untuk SQL injection. Keunggulannya dibandingkan Fail2Ban terletak pada fleksibilitas konfigurasi dan kemampuan deteksi yang lebih luas, didukung oleh CrowdSec Hub. Proses instalasi dan konfigurasi yang sederhana menjadikan CrowdSec pilihan ideal untuk meningkatkan keamanan server di berbagai infrastruktur.

Kata kunci: *CrowdSec, CTI, Cyber, Cybercrime*

ABSTRACT

The rapid development of technology has driven almost all business sectors to adopt digital operations, but this shift has also increased the risk of cybercrime, targeting systems and data. Cyber Threat Intelligence (CTI) is a cybersecurity approach that involves collecting, analyzing, and understanding data to identify the motives, targets, and attack patterns of cybercriminals. One solution to address these threats is CrowdSec, an open-source software designed to detect and prevent cyber-attacks in various environments, including servers. Testing results demonstrate that CrowdSec is effective in detecting SSH brute-force, port scanning, and SQL injection attacks. By identifying suspicious attack patterns and blocking attackers' IPs, CrowdSec significantly reduces the risk of server damage. Its response times are fast: 23 seconds for SSH brute-force, 10 seconds for port scanning, and 6 seconds for SQL injection. Compared to Fail2Ban, CrowdSec offers greater configuration flexibility and broader attack detection capabilities, supported by the CrowdSec Hub, which provides a variety of attack scenarios. With its simple installation and configuration process, CrowdSec is an ideal choice for enhancing server security.

Keywords: *CrowdSec, CTI, Cyber, Cybercrime*

Histori Artikel
Diserahkan: 12 Des 2024 Diterima setelah Revisi: 04 Jun 2025 Diterbitkan: 16 Jun 2025

1. PENDAHULUAN

Dalam era digital yang terus berkembang, infrastruktur teknologi informasi dan komunikasi menjadi pusat kehidupan bisnis dan aktivitas harian. Server, baik yang digunakan untuk bisnis, penyedia layanan, atau proyek-proyek pribadi, menyimpan dan mengelola data yang sangat penting. Namun, dengan meningkatnya konektivitas internet, server-server ini semakin rentan terhadap serangan siber yang dapat mengancam integritas dan kerahasiaan data, serta ketersediaan layanan. Serangan siber adalah upaya penjahat dunia maya atau hacker untuk mendapatkan akses ke jaringan atau sistem komputer. Kondisi

saat ini di dunia siber ditandai oleh serangan siber yang semakin kompleks dan sering terjadi. Ancaman seperti serangan brute force, SQL injection, DDoS (Distributed Denial of Service), dan malware terus berkembang. Bahkan dengan langkah-langkah keamanan yang ada, seringkali server dan jaringan masih menjadi sasaran yang rentan. [1]

Kelemahan dalam sistem keamanan menjadi penyebab utama pencurian data dan serangan cyber. Sistem keamanan tidak selalu sempurna dan dapat disebabkan oleh berbagai faktor, termasuk kekurangan sumber daya dan ketidaktahuan. Penanganan kejahatan siber menjadi semakin kompleks dan memerlukan sumber daya yang baik. Dalam era digital yang semakin maju, penting bagi perusahaan untuk mengambil tindakan yang serius dalam melindungi server dari ancaman cybercrime dan menciptakan infrastruktur yang lebih aman. Sebagian pemilik server mungkin tidak tahu adanya ancaman, ketidaktahuan ini yang dapat membuat server rentan terhadap serangan. Lemahnya keamanan pada server juga dapat disebabkan karena kekurangan sumber daya, misalnya aplikasi kemanan enterprise yang terlalu mahal atau infrastruktur tidak memiliki cukup spesifikasi untuk memasang alat keamanan ke server.

Kelemahan server untuk mendeteksi dan merespons serangan cyber dengan cepat dan efektif telah menjadi masalah besar dalam lingkungan server saat ini. Dari penelitian Parulian, Pratiwi, & Yustina [2], Menteri Kominfo Jhonny G. Plate, mengungkapkan bahwa sepanjang bulan januari sampai dengan juli 2021 tercatat 741.441.648 ancaman siber yang telah terjadi di Indonesia. Ancaman tersebut dapat dengan mudah dilakukan dengan memanfaatkan jaringan internet dan kemajuan teknologi di era sekarang. Serangan siber yang tidak terdeteksi dapat meningkat menjadi serangan yang berdampak negatif terhadap operasional bisnis dan menyebabkan kerugian yang cukup besar.

CrowdSec adalah program open-source yang dapat digunakan untuk menemukan aktivitas berbahaya di server melalui analisis log untuk menemukan berbagai serangan dan secara otomatis meresponsnya. Kemampuan CrowdSec dalam mendeteksi ancaman dapat ditingkatkan dengan mengumpulkan data CTI (Cyber Threat Inteligence) dari pengguna yang berkontribusi. CrowdSec yang bersifat open source, memungkinkan pengembang dan pengguna untuk menambah, meningkatkan, dan mengubah source code sesuai dengan kebutuhan mereka.

Disisi lain, terdapat sistem keamanan lain yang serupa dengan CrowdSec yaitu Fail2Ban. Menurut Danischevsky dari tulisannya pada Fail2Ban wiki, Fail2Ban adalah software yang mudah diinstal dan dikonfigurasi, efektif dalam mendeteksi serangan brute force, memiliki support komunitas besar dan dokumentasi yang luas karena sudah ada sejak tahun 2004. Namun, kelemahan utamanya adalah fokusnya yang terbatas pada serangan brute force dan kurang efektif untuk jenis serangan lainnya [3]. Tindakan yang diambil oleh Fail2Ban umumnya terbatas pada pemblokiran IP. Berdasarkan penelitian Rendratama, Sukarno, & Wardana [4] dapat disimpulkan bahwa CrowdSec merupakan tools yang sangat efektif di implementasikan sebagai alat deteksi dan respon untuk memblokir serangan secara otomatis sehingga penyerang tidak dapat akses service tujuan. Implementasi sistem deteksi aktivitas berbahaya menggunakan CrowdSec akan membawa banyak keuntungan. Sistem ini tidak hanya dapat meningkatkan keamanan server tetapi juga dapat membantu pemilik server menghadapi ancaman dunia maya yang semakin kompleks. Dengan menggunakan teknologi keamanan seperti CrowdSec, pemilik server dapat mengurangi bahaya serangan siber dan memastikan operasional berkelanjutan.

2. METODE

2.1 PENETRATION TESTING

Penetration Testing (pengujian penetrasi) atau yang sering disebut *pentest*, merupakan kegiatan untuk mengevaluasi keamanan suatu sistem jaringan komputer. Proses ini mensimulasikan serangan siber terhadap sistem komputer untuk mengetahui kerentanan yang dapat dieksploitasi. Tujuan dari simulasi serangan ini adalah untuk menemukan titik lemah dalam pertahanan sebuah sistem yang bisa dimanfaatkan oleh penyerang.

Pada Pengujian ini dilakukan penetrasi ke server yang sudah di install Crowdsec Security Engine, sehingga bouncer akan mendeteksi Alert(peringatan). Berikut Teknik pengujian penetrasi yang akan dilakukan pada pengujian proyek akhir ini :

i) Secure Shell Brute Force
Untuk teknik ini dilakukan menggunakan software bernama hydra dengan menargetkan IP Address server yang sudah di scan.
ii) Port Scanning
Untuk Teknik ini dilakukan dengan software yang populer digunakan untuk port scaning yaitu nmap.
iii) SQL Injection
Untuk Teknik ini dilakukan dengan menggunakan tools SQLMap yang dirancang khusus untuk mengekploitasi kerentanan SQL Injection.

Setelah dilakukan serangan ke server, Bouncer akan mendeteksi alert maka bouncer akan memproses dan merespon serangan tersebut. Bagian ini mencakup langkah-langkah yang diambil peneliti untuk menjawab pertanyaan penelitian atau menguji hipotesis, serta teknik, alat, atau pendekatan yang digunakan dalam proses tersebut.

2.2 SKENARIO PENGUJIAN

SSH Brute Force adalah percobaan berbagai kombinasi username dan password, dalam upaya untuk mendapatkan akses ke sistem melalui layanan SSH (Secure Shell). Berikut Skenario Pengujian SSH Brute Force:

i) Scan IP
Diasumsikan penyerang sudah mendapatkan IP Network dari server. Selanjutnya scan ip network menggunakan Nmap pada port 22 untuk mengetahui ip dari device yang sedang menggunakan ssh.Scan IP Public.
ii) Wordlist
Sebelum lanjut ke penyerangan, wordlistnya harus dipersiapkan terlebih dahulu untuk digunakan sebagai trial and error dari username dan passwordnya. Untuk wordlist yang digunakan adalah wordlist yang sudah disiapkan di kali linux yaitu rockyou.txt.
iii) Menggunakan Hydra
Pada pengujian ini menggunakan Dictionary Attack dengan hydra. Dictionary Attack ini adalah serangan yang menggunakan beberapa daftar nama pengguna dan dan password yang diberikan kepada hydra untuk melakukan brute forcing. Untuk pengujian ssh-bf menggunakan wordlist dari kali linux rockyou.txt. perintah yang digunakan untuk simulasi serangan ini adalah “hydra -L path/wordlist -P path/wordlist IP_Address ssh”, maka hydra akan melakukan serangan brute force secara otomatis.
iv) Respon
Jika serangan terdeteksi, crowdsec dapat melakukan tindakan, seperti memblokir IP client atau menampilkan IP sumber dan geolokasi dari ip tersebut serta Teknik serangan yang digunakan.

Port Scanning adalah kegiatan pemindaian atau pencarian yang dilakukan pada beberapa port di sistem komputer atau jaringan untuk identifikasi kerentanan atau titik masuk exploitasi. Berikut skenario pengujian untuk port scanning:

i) Ping Domain Website
Pertama yang dilakukan adalah ping domain website di cmd, ketika domain tersebut sudah di ping akan terlihat ip public dari website yang kita ping domainnya.yang dilakukan adalah mencari kelemahan dan kerentanan pada website ctf.slashroot.id menggunakan sqlmap.
ii) Scan IP Public
Setelah kita mendapatkan ip public dari domain website yang kita ping, selanjutnya scan menggunakan NMAP ip tersebut. NMAP akan memberikan informasi seputar ip yang di ping seperti host status, port status, ip range dan traceroute.
iii) Deteksi Serangan
CrowdSec menggunakan scenario untuk mendeteksi pola serangan. Skenario ini biasanya mencakup konfigurasi TCP Scan dari pola aktifitas port yang tidak biasa..
iv) Respon
Jika serangan terdeteksi, crowdsec dapat bekerja sama dengan firewall untuk keputusan yang diambil kemudian merespon dengan memblokir alamat IP, menampilkan lokasi IP penyerang,

berapa lama IP diblokir dan serangan yang digunakan.

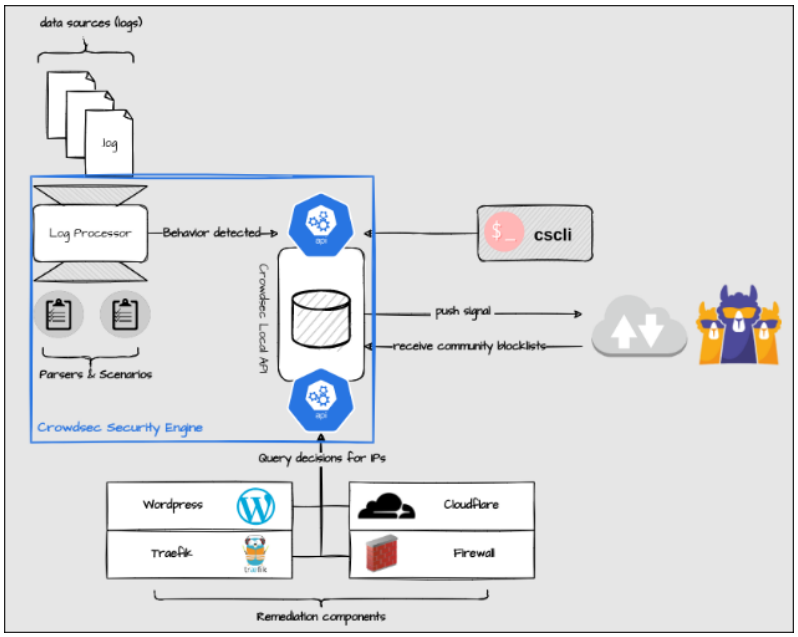
Sql Injection adalah cara untuk menyisipkan atau memanipulasi perintah SQL, yang memanfaatkan celah dalam pengolahan input. Tujuannya untuk mendapatkan akses atau mengubah data dalam database. Berikut skenario pengujian untuk SQL Injection:

i) Vulnerability Assesment
Pertama yang dilakukan adalah mencari kelemahan dan kerentanan pada website ctf.slashroot.id menggunakan sqlmap.
ii) Menjalankan SQLmap
Setelah kita mendapatkan kelemahan dan kerentanan, selanjutnya gunakan sqlmap untuk memulai serangan ke website.
iii) Table Database
Setelah serangan dilakukan, tampilkan table database dengan perintah –table untuk menampilkan table. Setelah table tampil, untuk mengetahui isi dari table tersebut, gunakan perintah –T <nama table> untuk menampilkan isi dari table. Jika yang ditampilkan table user maka akan tertera username dan password untuk masuk ke website tersebut.
iv) Respon
Jika serangan terdeteksi, Crowdsec akan memblokir alamat IP penyerang, mengirimkan lokasi IP penyerang dan tipe serangan yang digunakan.

3. HASIL DAN PEMBAHASAN

3.1 CROWDSEC

CrowdSec merupakan software open-source dan ringan yang digunakan untuk menganalisis perilaku pengguna saat mengakses server, sehingga sistem kemudian akan secara otomatis memblokir alamat IP pengguna jika terdeteksi ancaman, yang disimpan sebagai daftar blokir di database (gambar 1).



Gambar 1. Crowdsec Workflow

CrowdSec dirancang untuk melindungi suatu sistem dari berbagai macam serangan. Crowdsec mendeteksi perilaku secara lokal dan mengelola pola ancaman berdasarkan log pada sistem yang nantinya akan disesuaikan dengan scenario yang ada. Scenario adalah file YAML berisikan aturan aturan tertentu yang memicu terjadinya banning IP jika terjadi ancaman pada sistem.

CrowdSec memiliki 2 komponen penting yaitu security engine yang akan melakukan analisis log dan mendeteksi ancaman. Remediation component sebagai pengambil tindakan berdasarkan keputusan dari security engine.

Ada 2 cara atau metode instalasi crowdsec, menggunakan paket manager dari sistem operasi liux atau menggunakan docker container. Pada penelitian ini akan menggunakan paket manager dari linux sebagai

metode instalasi crowdsec. Untuk bisa menjalankan crowdsec pada server dengan optimal dibutuhkan setidaknya minimal 2 core CPU, 2 GB RAM, dan penyimpanan minimal 5 GB.

Security engine hanya mesin pendeteksi, tidak akan memblokir serangan yang masuk. Perlu komponen remediasi untuk eksekusi respon, komponen remediasi juga disebut sebagai *"Bouncer". Crowdsec* menyediakan banyak komponen remediasi untuk berbagai service seperti *nginx*, *aws*, *firewall*, *cloudflare*,dll menyesuaikan pada kebutuhan *server*. Pada penelitian ini menggunakan komponen remediasi *"crowdsec-firewall-bouncer"* yang di dukung dengan *firewall iptables*. Bouncer menggunakan fungsi dari iptables untuk memblokir IP yang dianggap berbahaya dan secara otomatis memperbarui aturan firewall berdasarkan keputusan CrowdSec.

Name	IP Addr	Valid	Last API Pull	Type	Version	Auth Type
cs-firewall-bouncer-1721781586	127.0.0.1	✓	2024-07-24T00:50:11Z	crowdsec-firewall-bouncer	v0.0.28-debian-pragmatic-	api-key

Gambar 2. Crowdsec Bouncer

Collection dalam crowdsec adalah kumpulan dari beberapa komponen yang saling berhubungan untuk mendeteksi dan merespon ancama tertentu. Komponen yang dimaksud adalah parser dan scenario. Tahapan ini merupakan cara untuk menyederhanakan proses implementasi dan konfigurasi crowdsec. Dengan menggunakan collection, dapat memudahkan dalam instalasi dan konfigurasi scenario untuk jenis ancaman tertentu. Collection ini dapat dibagikan ke sesama pengguna crowdsec lewat CrowdSec Hub sehingga pengguna lain dapat menerapkan konfigurasi yang sudah dipastikan bisa memblokir serangan.

COLLECTIONS

Name	Status	Version	Local Path
crowdsecurity/apache2	✓ enabled	0.1	/etc/crowdsec/collections/apache2.yaml
crowdsecurity/base-http-scenarios	✓ enabled	1.0	/etc/crowdsec/collections/base-http-scenarios.yaml
crowdsecurity/http-cve	✓ enabled	2.6	/etc/crowdsec/collections/http-cve.yaml
crowdsecurity/iptables	✓ enabled	0.2	/etc/crowdsec/collections/iptables.yaml
crowdsecurity/linux	✓ enabled	0.2	/etc/crowdsec/collections/linux.yaml
crowdsecurity/mysql	✓ enabled	0.1	/etc/crowdsec/collections/mysql.yaml
crowdsecurity/sshd	✓ enabled	0.3	/etc/crowdsec/collections/sshd.yaml

Gambar 3. Crowdsec Collection

3.2 KEMAMPUAN DETEKSI DAN RESPON

Pengujian dilakukan dengan metode *White Box* dan *Penetration Testing*, terdapat tiga skenario penyerangan dengan *tools* hydra untuk ssh-bf, nmap untuk *port scanning* dan sqlmap untuk *sql injection.* Berikut kemampuan Crowdsec dalam mendeteksi dan merespon:

i) Pada pengujian SSH-bf, penujian yang dilakukan adalah menggunakan tools dari kali linux yaitu hydra, dengan memanfaatkan kumpulan wordlist dari kali linux untuk kombinasi username dan passwordnya. Berdasarkan hasil pengujian ssh brute-force, crowdsec berhasil mendeteksi dan memblokir ip dari penyerang yang berusaha mendapatkan akses masuk ke server. Keberhasilan dalam mendeteksi dan memblokir serangan SSH brute force menunjukkan bahwa CrowdSec memiliki kemampuan deteksi yang bagus untuk mengidentifikasi pola serangan dan melakukan tindakan pencegahan yang cepat. Hydra mencatat waktu mulai serangan adalah 02:39:35 dan waktu crowdsec berhasil memberikan alert dan merespon serangan adalah 19:39:58. Karena crowdsec memberikan alert dengan zona waktu UTC maka harus dikakukan konversi dari UTC ke GMT+7. 19:39:58 dikonversikan ke GMT+7 hasilnya adalah 02:39:58. Dari waktu mulai serangan ke waktu crowdsec berhasil merespon serangan adalah 23 Detik.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-07-28 02:39:35

Gambar 4. Waktu Mulai Serangan

472 | Ip:103.190.46.245 | crowdsecurity/ssh-bf | ID | 9341 PT INDONESIA COMNETS PLUS | ban:1 | 2024-07-27 19:39:58.02427026 +0000 UTC

Gambar 5. Waktu Respon Serangan

ii) Pada pengujian *port scaning*, pengujian dilakukan dengan menggunakan *tools nmap* untuk melakukan *scanning* terhadap *port-port* pada *server.* Berdasarkan hasil pada pengujian *port scanning*, *crowdsec* mampu mendeteksi *scanning* yang mencurigakan seperti perilaku scan cepat dan terus menerus dari IP yang sama CrowdSec juga dapat menyamarkan atau tidak memperlihatkan service yang berjalan pada port yang aktif, dengan itu penyerang tidak

mengetahui service apa saja yang terdapat pada server sehingga penyerang tidak bisa melakukan serangan lanjutan seperti menyerang website atau DDoS.

```
NSE: Script Post-scanning.
Initiating NSE at 03:59
Completed NSE at 03:59, 0.00s elapsed
Initiating NSE at 03:59
Completed NSE at 03:59, 0.00s elapsed
Initiating NSE at 03:59
Completed NSE at 03:59, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 184.48 seconds
           Raw packets sent: 2072 (95.800KB) | Rcvd: 60 (2.664KB)
Waktu mulai: 2024-07-28 03:56:21
```

Gambar 6. Waktu Mulai Serangan

```
474 | Ip:103.190.46.245 | crowdsecurity/iptables-scan-multi_ports | ID | 9341 PT INDONESIA
COMNETS PLUS | ban:1 | 2024-07-27 20:56:31.280779253 +0000 UTC
```

Gambar 7. Waktu Respon Serangan

Nmap mencatat waktu mulai serangan adalah 03:56:21 dan waktu crowdsec berhasil memberikan alert dan merespon serangan adalah 20:56:31. Karena crowdsec memberikan alert dengan zona waktu UTC maka harus dikakukan konversi dari UTC ke GMT+7. 19:39:58 dikonversikan ke GMT+7 hasilnya adalah 03:56:31. Dari waktu mulai serangan ke waktu crowdsec berhasil merespon serangan adalah 10 Detik.

iii) Pada pengujian *sql injection*, pengujian dilakukan dengan menggunakan tools *sqlmap* untuk memindai dan mengeksploitasi kelemahan *website* terhadap serangan *sql injection. Sqlmap* digunakan untuk mengirimkan *payload* berbahaya untuk mendapatkan akses ke database. Berdasarkan hasil pengujian sql injection, crowdsec berhasil menahan penyerang sebelum mendapatkan informasi struktur database dari sqlmap. Crowdsec berhasil mendeteksi pola mencurigakan dalam request HTTP yang menunjukkan adanya serangan SQL injection dan merespon dengan memblokir ip dari penyerang.Respon CrowdSec terhadap serangan *sql injection* menunjukkan kemampuan CrowdSec dalam melindungi *website* dari upaya manipulasi database. Kecepatan deteksi dan respon dalam waktu 6 detik menunjukkan kemampuan CrowdSec dalam merespon serangan dan mencegah kebocoran data dan kerusakan sistem.

```
[*] starting @ 14:05:58 /2024-07-28/
```

Gambar 8. Waktu Mulai Serangan

```
484 | Ip:103.190.46.245 | crowdsecurity/http-sqli-probbing-detection | ID | 9341 PT INDONESIA
COMNETS PLUS | ban:1 | 2024-07-28 07:06:04.584961214 +0000 UTC
```

Gambar 9. Waktu Respon Serangan

4. KESIMPULAN

Berdasarkan hasil penelitian dan pembahasan yang telah dilakukan, dapat disimpulkan bahwa CrowdSec memberikan hasil yang efektif dalam mendeteksi dan merespons serangan seperti SSH brute-force, port scanning, dan SQL injection. CrowdSec mampu mengenali pola-pola serangan mencurigakan dan secara otomatis memblokir IP penyerang, sehingga secara signifikan mengurangi potensi kerusakan pada server akibat serangan siber.

Hal ini menunjukkan kehandalan CrowdSec dalam melindungi sistem dari berbagai ancaman. Selain itu, waktu respons CrowdSec terhadap berbagai jenis serangan tergolong cepat, yaitu 23 detik untuk SSH brute-force, 10 detik untuk port scanning, dan 6 detik untuk SQL injection. Respons yang cepat ini sangat penting untuk meminimalkan risiko kerusakan, sehingga server menjadi lebih aman dari potensi serangan. Keunggulan lain yang ditunjukkan oleh CrowdSec adalah fleksibilitas konfigurasi dan kemampuan deteksi yang lebih luas dibandingkan Fail2Ban.

Dengan adanya CrowdSec Hub, yang menyediakan berbagai skenario serangan, CrowdSec mampu memberikan perlindungan yang lebih lengkap. Proses instalasi dan konfigurasi yang sederhana juga menunjukkan bahwa CrowdSec dapat diimplementasikan dengan mudah, menjadikannya solusi yang

cocok untuk berbagai jenis infrastruktur server. Penilitian selanjutnya dapat melakukan kombinasi CrowdSec dengan Security Information and Event Management (SIEM) atau Security Orchestration (SOAR).

DAFTAR PUSTAKA

[1] K. Baker, "Types Of Cyber Attack," *CrowdStrike*, 9 November 2023. [Online]. Available: https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/

[2] S. Parulian, D. A. Pratiwi, and M. C. Yustina, "Ancaman dan Solusi Serangan Siber di Indonesia," *Telecommunications, Networks, Electronics, and Computer Technologies*, p. 86, 2021.

[3] S. Danischevsky, "Fail2Ban," 1 Juni 2023. [Online]. Available: https://github.com/fail2ban/fail2ban/wiki

[4] M. T. S. Rendratama, P. Sukarno, and A. A. Wardana, "Perancangan dan Analisis Crowdsec Sebagai Intrusion Prevention System pada Infrastruktur Server," *e-Proceeding of Engineering*, vol. 10, no. 2, pp. 1888–1893, 2023.

[5] U. Airlangga, "Knowledge Base Apa Itu CISRT," 2024. [Online]. Available: https://kb.dsi.unair.ac.id/?kb=cisrt-apa-itu

[6] H. E. Ardiyanto and T. I. Bayu, "Perancangan Security Information and Event Management (SIEM) Menggunakan Open Source SIEM (OSSIM)," *Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana*, pp. 2–5, 2018.

[7] CrowdSec, "Docs CrowdSec," 2023. [Online]. Available: https://doc.crowdsec.net/

[8] M. H. Dar and S. Z. Harahap, "Implementasi SNORT INTRUSION DETECTION SYSTEM (IDS) Pada Sistem Jaringan Komputer," *Informatika: Fakultas Sains dan Teknologi*, pp. 15–18, 2018.

[9] R. Kurniawan and B. Rahardjo, "Studi Model Organisasi CSIRTs (Computer Security Incident Response Teams) pada Perusahaan Berskala Besar," in *Seminar Nasional Aplikasi Teknologi Informasi (SNATI)*, 2007.

[10] S. Lund, A. Madgavkar, J. Manyika, S. Smit, K. Ellingrud, and O. Robinson, "The Future of Work after COVID-19," *McKinsey & Company*, 18 Februari 2021. [Online]. Available: https://www.mckinsey.com/featured-insights/future-of-work/the-future-of-work-after-covid-19

[11] Y. R. Mulyadi, "Linux Ubuntu Server," 2023. [Online]. Available: https://www.idn.id/linux-ubuntu-server/

[12] M. D. Pratama, F. Nova, and D. Prayama, "Wazuh sebagai Log Event Management dan Deteksi Celah Keamanan pada Server dari Serangan DoS," *Jurnal Ilmiah Teknologi Sistem Informasi (JITSI)*, 2022.

[13] H. R. P. Sailellah, "Pengertian Firewall dalam Jaringan Komputer dan Jenis-Jenisnya," 28 April 2023. [Online]. Available: https://it.telkomuniversity.ac.id/pengertian-firewall-dalam-jaringan-komputer-dan-jenis-jenisnya/

[14] Dewaweb Team, "Mengenal Linux: Sistem Operasi Open Source dan Gratis," 7 Februari 2023. [Online]. Available: https://www.dewaweb.com/blog/sistem-operasi-linux/

[15] Y. Yuliana, H. A. Mooduto, and R. Hadi, "Deteksi Ancaman Keamanan Pada Server dan Jaringan Menggunakan OSSEC," *Jurnal Ilmiah Teknologi Sistem Informasi (JITSI)*, 2022.