JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 10, No. 3, September 2025, Pp. 1914-1924

IMPLEMENTASI DAN PROFILING THREAT INTELLIGENCE DAN THREAT BEHAVIOR PADA OPEN SOURCE SIEM IBM QRADAR

Erlangga Faezal*[1)], Adityas Widjajarto [2)], M. Teguh Kurniawan[3)]
1. Telkom University, Indonesia
2. Telkom University, Indonesia
3. Telkom University, Indonesia

Article Info
Kata Kunci: Fungsi Kontrol Keamanan; IBM QRadar; SIEM; Perilaku Ancaman; Intelijen Ancaman

Keywords: *Security Control Functions*; IBM QRadar; SIEM; Threat Behavior; Threat Intelligence

Article history:
Received 18 July 2024
Revised 12 August 2024
Accepted 30 August 2024
Available online 1 September 2025

DOI :
https://doi.org/10.29100/jipi.v10i3.6293

* Corresponding author.
Erlangga Faezal
E-mail address:
erlanggafaezal@student.telkomuniversity.ac.id

ABSTRAK
Penelitian ini berfokus pada identifikasi dan *profiling* IBM QRadar dalam menunjukkan kemampuan deteksi terhadap berbagai jenis serangan siber. Proses identifikasi dan *profiling* ini menggunakan platform eksperimen yang terdiri dari tiga *server* virtualisasi, yaitu Kali Linux sebagai pengujian penetrasi dan keamanan jaringan, IBM QRadar sebagai SIEM untuk mendeteksi dan menganalisis ancaman keamanan dalam jaringan, serta CentOS sebagai *Target Client*. Kategori teknik serangan yang digunakan adalah *port scanning*, *brute force*, dan DDoS. Hasil pengujian menunjukkan bahwa IBM QRadar mampu mendeteksi aktivitas berbahaya melalui analisis indikator *rules* pada kategori serangan tersebut. Untuk *port scanning*, deteksi mencakup banyaknya permintaan ke berbagai *port*. Pada *brute force*, deteksi mencakup pola permintaan yang tidak biasa. Sementara itu, pada DDoS, deteksi mencakup frekuensi permintaan koneksi. Analisis dilakukan berdasarkan metrik *Response Time* dan metrik Granularitas. Metrik *Response Time* menunjukkan bahwa serangan Hping 3 memiliki waktu respons tercepat yaitu 11 detik, sementara serangan Medusa memiliki waktu respons terlama yaitu 1850 detik. Selain itu, metrik granularitas menunjukkan bahwa serangan Hydra, Brutespray, dan Medusa memiliki skor total tertinggi yaitu 39, sementara serangan LOIC dan Slowloris menempati posisi terakhir dengan skor total 27. Hal ini menunjukkan kemampuan IBM QRadar untuk mencatat dan menganalisis detail setiap serangan dengan sangat baik. Kesimpulan tersebut menunjukkan bahwa IBM QRadar mampu mendeteksi dan merespons berbagai jenis serangan siber berdasarkan *Threat Intelligence* dan monitoring *Threat Behavior*.

ABSTRACT
The research focuses on the identification and profiling of IBM QRadar in demonstrating its detection capabilities against various types of cyber attacks. The identification and profiling process utilizes an experimental platform consisting of three virtualization servers: Kali Linux for penetration testing and network security, IBM QRadar as a SIEM to detect and analyze security threats within the network, and CentOS as the Target Client. The categories of attack techniques used are port scanning, brute force, and DDoS. The test results show that IBM QRadar is capable of detecting malicious activities through the analysis of rule indicators for these categories of attacks. For port scanning, detection includes the number of requests to various ports. For brute force, detection includes unusual request patterns. Meanwhile, for DDoS, detection includes the frequency of connection requests. The analysis is based on Response Time metrics and Granularity metrics. The Response Time metric shows that the Hping 3 attack has the fastest response time at 11 seconds, while the Medusa attack has the longest response time at 1850 seconds. Additionally, the Granularity metric indicates that the Hydra, Brutespray, and Medusa attacks have the highest total score of 39, while the LOIC and Slowloris attacks have the lowest total score of 27. This demonstrates IBM QRadar's capability to accurately record and analyze the details of each attack. These conclusions indicate that IBM QRadar is able to detect and respond to various types of cyber attacks based on Threat Intelligence and monitoring Threat Behavior.

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 10, No. 3, September 2025, Pp. 1914-1924

I. PENDAHULUAN

DALAM era digital yang semakin maju, pengetahuan mengenai ancaman siber menjadi hal yang penting dalam menghadapi kemajuan teknologi. Ancaman siber merupakan serangan yang dapat mengganggu, merusak, atau mencuri data dalam dunia siber, dapat menimbulkan dampak serius pada individu, organisasi, dan masyarakat secara luas. Menyatakan bahwa infrastruktur kritis modern sangat rentan terhadap ancaman siber. Seiring dengan perkembangan teknologi, pusat data dan infrastruktur penting diintegrasikan ke dalam jaringan teknologi global, yang mempermudah akses dan kontrol namun meningkatkan risiko keamanan. Ancaman dari dunia siber mampu menembus sistem keamanan data dan informasi, menyebabkan kegagalan sistem dengan konsekuensi fatal. Kompleksitas dan skala ancaman siber terus berkembang, membuat infrastruktur kritis menjadi target utama bagi pelaku kejahatan siber [1]. Menunjukkan bahwa motivasi serangan siber pada infrastruktur kritis bervariasi, dari tujuan finansial hingga politik. Oleh karena itu, penting bagi organisasi untuk mengantisipasi berbagai ancaman dan mengembangkan strategi keamanan komprehensif untuk melindungi aset penting dan memastikan kontinuitas layanan yang vital bagi masyarakat [2].

Dalam upaya untuk menjaga tingkat keamanan yang optimal, organisasi telah mengimplementasikan berbagai perangkat keamanan, termasuk *Security Information and Event Management* (SIEM). SIEM merupakan sistem yang digunakan untuk mencegah, mendeteksi, dan bereaksi terhadap serangan siber [3]. Pada penelitian ini akan menggunakan salah satu aplikasi SIEM *open source*, yaitu IBM QRadar karena terdapat banyak fitur yang membuat aplikasi ini menjadi sangat *powerful* dan juga dokumentasi yang tersedia pada *website* IBM.

Threat Intelligence dan *Threat Behavior* digunakan untuk meningkatkan deteksi dan respon terhadap ancaman siber dengan menyediakan wawasan tentang teknik dan pola serangan yang terjadi. *Threat Intelligence* mengumpulkan data dari berbagai sumber jaringan tentang ancaman yang terjadi, kemudian diintegrasikan oleh SIEM IBM QRadar untuk membuat aturan deteksi yang sesuai untuk mengidentifikasi pola serangan yang belum dikenal sebelumnya dengan mengkorelasikan data yang relevan dan mendeteksi anomali sesuai dengan karakteristik ancaman [4]. Sementara itu, *Threat Behavior* menganalisis perilaku yang mencurigakan dalam jaringan, seperti aktivitas yang tidak biasa atau anomali dalam lalu lintas, yang dapat menjadi indikasi serangan siber yang sedang berlangsung atau yang akan terjadi [5].

Dalam penggunaannya, terdapat keterbatasan atau tantangan dalam menggunakan SIEM IBM QRadar yaitu kompleksitas dalam konfigurasi dan manajemen sistem, terutama dalam mengatur aturan deteksi yang sesuai untuk berbagai jenis serangan siber. Selain itu, beban kerja yang tinggi dan volume data yang besar dari berbagai sumber jaringan yang berbeda dapat menyebabkan peningkatan waktu respon dan mempengaruhi kinerja sistem. Mengelola dan menganalisis data hasil serangan oleh IBM QRadar membutuhkan upaya untuk menyatukan data agar bisa dianalisis sesuai dengan konfigurasi aturan yang diterapkan. IBM QRadar perlu memiliki kemampuan menyaring peringatan yang tidak relevan, sehingga fokus tetap pada ancaman yang nyata dan penting untuk ditangani dengan cepat dan akurat.

Penelitian ini berfokus pada evaluasi fungsi kontrol SIEM IBM QRadar dalam mendeteksi dan merespons ancaman siber melalui serangan jaringan yaitu *port scanning*, *brute force*, dan DDoS. Penelitian ini secara khusus mengeksplorasi bagaimana IBM QRadar memanfaatkan *Threat Intelligence* dan *Threat Behavior* untuk mengidentifikasi dan menganalisis serangan siber. Dengan menggunakan pendekatan sistem *blackbox*, penelitian ini membatasi analisis pada respons SIEM IBM QRadar tanpa membahas aspek internal *software* yang digunakan. Fokus utama adalah pada efektivitas IBM QRadar dalam memprofile serangan dan mengoptimalkan respons terhadap ancaman yang dilakukan untuk memberikan pemahaman yang lebih dalam tentang kemampuan SIEM IBM QRadar dalam mendeteksi dan merespons ancaman siber.

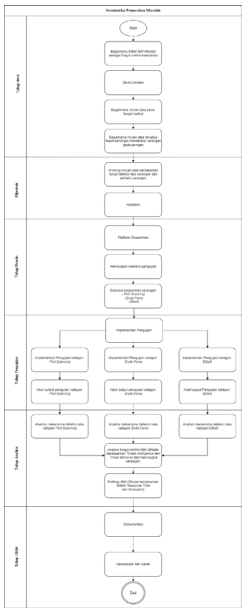
Penelitian ini memberikan kontribusi terhadap bidang keamanan siber dengan pemahaman tentang bagaimana SIEM IBM QRadar dapat mendeteksi dan merespons ancaman siber menggunakan *Threat Intelligence* dan *Threat Behavior*. Dengan serangan *port scanning*, *brute force*, dan DDoS, memberikan pengetahuan cara kerja SIEM IBM QRadar dalam mengenali pola serangan yang belum dikenal. Hasil penelitian ini tidak hanya memperkaya pengetahuan teoritis tentang deteksi ancaman siber, tetapi juga memberikan solusi praktis untuk meningkatkan efektivitas konfigurasi SIEM IBM QRadar, sehingga membantu mengatasi tantangan dalam keamanan siber yang semakin kompleks.

II. METODE PENELITIAN

Sistematika penyelesaian masalah merupakan tahapan terstruktur dalam penelitian, dirancang untuk mengatasi permasalahan yang dirumuskan. Langkah awal hingga akhir penelitian tersusun secara sistematis, memastikan penyelesaian masalah secara terencana. Dengan merumuskan permasalahan awal, penelitian ini mengikuti alur yang terencana, memandu penelitian menuju pemecahan masalah secara efektif. Penyelesaian masalah penelitian

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 10, No. 3, September 2025, Pp. 1914-1924

ini mencangkup 6 tahapan, yaitu: Tahap Awal, Hipotesis, Tahap Perancangan, Tahap Eksperimen, Tahap Analisis, dan Tahap Akhir. Gambaran sistematika penyelesesaian masalah dapat dilihat pada Gambar 1:



Gambar. 1. Sistematika Penelitian

A. Tahap Awal

Tahap Awal dalam penelitian ini yaitu dengan mempelajari fungsi kontrol keamanan SIEM IBM QRadar dengan mengacu pada studi literatur. Studi literatur berguna untuk memperdalam teori mengenai fungsi kontrol keamanan SIEM IBM QRadar melalui jurnal dan buku yang berkaitan dengan fungsi kontrol keamanan. Selanjutnya, analisis mengenai rincian data pada fungsi kontrol yang dihasilkan dari hasil *output* pengujian serta menjadikan sebagai batasan masalah dalam penelitian pada tugas akhir ini. Kemudian, menjelaskan bagaimana data yang dikumpulkan oleh IBM QRadar dapat digunakan untuk mendeteksi berbagai jenis serangan pada jaringan.

B. Tahap Hipotesis

Pada tahap kedua yaitu tahap hipotesis. Pada tahapan ini melakukan hipotesis berupa praduga sementara terhadap *Profiling* rincian data berdasarkan fungsi deteksi tipe serangan dan perilaku serangan.

C. Tahap Desain

Pada tahap ketiga yaitu tahap perancangan pengujian dengan menyiapkan platform eksperimen menggunakan *Virtual Machine*. *Virtual Machine* digunakan dalam penelitian ini karena fleksibilitas dan efisiensi yang ditawarkannya dalam menciptakan lingkungan uji yang terkendali. Penggunaan *Virtual Machine* memungkinkan peneliti untuk mensimulasikan serangan siber tanpa memerlukan perangkat keras fisik yang kompleks, sehingga mempermudah proses pengaturan dan pengulangan eksperimen. Platform ini mencakup pengaturan perangkat keras dan perangkat lunak yang sesuai untuk memastikan bahwa eksperimen dapat berjalan dengan lancar. Selanjutnya melakukan installasi *software* pada *Virtual Machine* dan *Main OS* yang terdiri dari:

1) *Virtual Machine* 1 SIEM IBM QRadar
2) *Virtual Machine* 2 *Client Target*
3) *Virtual Machine* 3 *Attacker*

Setelah itu, dilakukan pembuatan skenario pengujian yang dirancang untuk menguji kemampuan SIEM IBM QRadar dalam mendeteksi berbagai jenis serangan. Skenario pengujian ini mencakup tiga kategori serangan utama, yaitu:

1) *Port Scanning*
2) *Brute Force*
3) DDoS

Skenario pengujian yang melibatkan serangan *port scanning*, *brute force*, dan DDoS dipilih karena ketiganya merupakan jenis serangan siber yang secara terus-menerus berusaha merusak dan mengganggu jaringan. Kriteria pemilihan serangan ini didasarkan pada relevansi kemampuannya untuk mengeksploitasi kelemahan jaringan secara sistematis. Dengan serangan tersebut pengujian ini memberikan gambaran yang komprehensif tentang kemampuan deteksi dan respons IBM QRadar terhadap ancaman yang bersifat terus-menerus dan merusak.

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 10, No. 3, September 2025, Pp. 1914-1924

Implementasi pengujian akan dilakukan pada tahap pengujian selajutnya, di mana setiap skenario serangan akan dijalankan dan dilakukan *monitoring* untuk mengevaluasi efektivitas SIEM IBM QRadar dalam mendeteksi dan merespons ancaman tersebut.

D. Tahap Pengujian

Pada tahap keempat dilakukan implementasi skenario eksperimen serangan berdasarkan tiga kategori utama untuk menguji kemampuan SIEM IBM QRadar dalam mendeteksi dan merespons ancaman. Berikut adalah rincian dari tahap pengujian ini:

1) Implementasi Pengujian kategori *Port Scanning*
2) Implementasi Pengujian kategori *Brute Force*
3) Implementasi Pengujian kategori DDoS

Setelah implementasi pengujian, hasil *output* dari setiap kategori serangan akan dianalisis untuk mengevaluasi kemampuan deteksi dan respon dari SIEM IBM QRadar.

E. Tahap Analisis

Pada tahap kelima yaitu melakukan analisis. Setelah implementasi pengujian, hasil *output* dari setiap kategori serangan akan dianalisis untuk mengevaluasi kemampuan deteksi dan respon dari SIEM IBM QRadar. Berikut adalah langkah-langkah dalam tahap analisis:

1) Analisis mekanisme deteksi rules kategori *Port Scanning*
2) Analisis mekanisme deteksi rules kategori *Brute Force*
3) Analisis mekanisme deteksi rules kategori DDoS

Selanjutnya, hasil analisis yang telah didapatkan akan digunakan sebagai dasar untuk analisis fungsi kontrol IBM QRadar berdasarkan *Threat Intelligence* dan *Threat Behavior* dari hasil output serangan. Berikut merupakan aspek pada analisi fungsi kontrol meliputi:

1) *Identification* mengukur kemampuan sistem dalam mengenali entitas yang mencoba mengakses jaringan, termasuk pencatatan informasi seperti alamat IP dan nama pengguna.
2) *Authentication* menilai efisiensi sistem dalam memverifikasi identitas entitas melalui proses validasi kredensial, seperti *username* dan *password*.
3) *Authorization* menentukan hak akses entitas yang telah diidentifikasi dan diautentikasi, dengan memberikan atau menolak akses ke sumber daya sesuai dengan kebijakan keamanan.
4) *Accounting* mengevaluasi kemampuan sistem dalam mencatat aktivitas entitas yang telah diidentifikasi, diautentikasi, dan diberi otorisasi, dengan fokus pada pencatatan *log* yang rinci untuk keperluan audit dan keamanan.

hasil analisis ini juga akan digunakan untuk melakukan *profiling* IBM QRadar berdasarkan metrik waktu respon dan granularitas data pada aplikasi IBM QRadar. *Profiling* ini bertujuan untuk memahami performa SIEM IBM QRadar dalam mendeteksi dan merespons ancaman.

F. Tahap Akhir

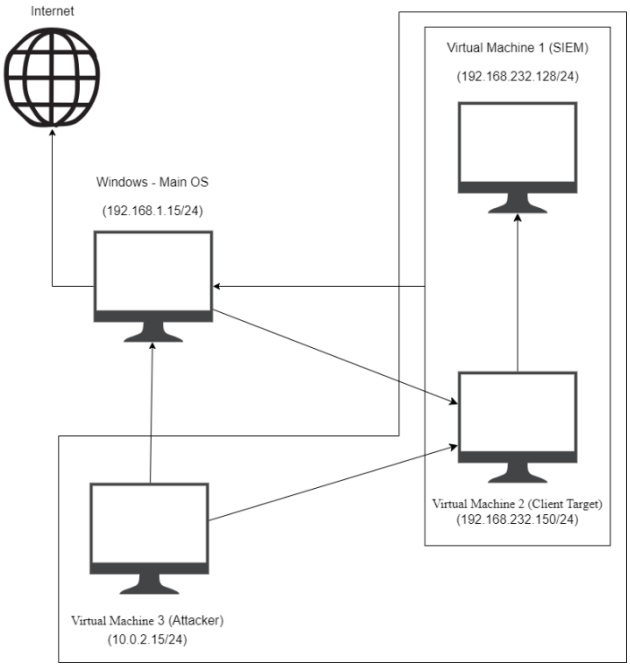
Pada tahap akhir ini, berupa penyusunan kesimpulan berdasarkan hasil fungsi kontrol *output* serangan dan nilai tertinggi metrik waktu respons dan granularitas, saran yang diperoleh berdasarkan fungsi kontrol pada SIEM IBM QRadar.

III. HASIL DAN PEMBAHASAN

A. Platform Eksperimen

Platform eksperimen yang digunakan dalam penelitian ini terdiri dari beberapa komponen utama: *Main OS* (Laptop) sebagai host untuk menjalankan semua *Virtual Machine*, *Virtual Machine* 1 (SIEM) IBM QRadar digunakan untuk mengumpulkan, menampilkan, dan menghubungkan data jaringan untuk memberikan gambaran keseluruhan tentang jaringan dan peristiwa keamanan [6]. *Virtual Machine* 2 (*Client Target*) yang menjadi *target* serangan untuk merusak, mencuri, atau mengakses informasi secara tidak sah [7]. *Virtual Machine* 3 (*Attacker*) untuk mengeksploitasi kelemahan atau celah dalam sistem keamanan [8]. Pada Gambar 2 merupakan Platform Eksperimen yang digunakan.

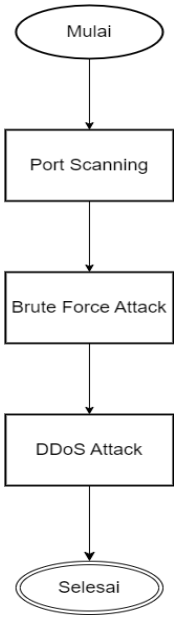
JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 10, No. 3, September 2025, Pp. 1914-1924



Gambar. 2. Platform Eksperimen

Spesifikasi perangkat keras yang digunakan adalah laptop dengan prosesor Intel Core i7, 16GB RAM, dan 1TB SSD. Perangkat lunak yang digunakan termasuk VMware Workstation Pro untuk virtualisasi, CentOS sebagai sistem operasi untuk VM SIEM dan *target*, serta Kali Linux untuk VM *attacker*. IBM QRadar versi *Community Edition* digunakan sebagai SIEM utama untuk eksperimen ini. spesifikasi perangkat keras dan perangkat lunak dapat mempengaruhi hasil eksperimen, terutama dalam hal kecepatan respon dan akurasi deteksi serangan. Misalnya, prosesor yang lebih cepat atau RAM yang lebih besar dapat mempercepat proses analisis dan mengurangi kemungkinan *bottleneck*, sementara versi perangkat lunak yang berbeda dapat memberikan performa yang bervariasi dalam mendeteksi ancaman.

B. Skenario Eksperimen Penyerangan



Gambar. 3. Skenario Eksperimen Penyerangan

Skenario pengujian melibatkan tiga teknik serangan utama:

1) Port Scanning

Port scanning adalah sebuah teknik yang dirancang untuk mengidentifikasi *port-port* yang terbuka dan layanan-layanan yang tersedia pada suatu *host* di dalam jaringan [9]. Dengan menggunakan Nmap - Zenmap GUI dengan berbagai *profile* seperti *Intense Scan*, *Intense Scan plus UDP*, dan *Intense Scan All TCP Ports* untuk mendeteksi *port* terbuka dan layanan yang berjalan di sistem *target*.

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 10, No. 3, September 2025, Pp. 1914-1924

2) Brute Force

Brute Force digunakan untuk menyerang *server*, dengan tujuan memperoleh akses tanpa izin. Metode ini melibatkan percobaan setiap kombinasi yang mungkin dari nama pengguna dan kata sandi administrator hingga menemukan yang benar [10]. Dengan menggunakan Hydra, Brutespray, dan Medusa untuk mencoba berbagai kombinasi *username* dan *password* pada berbagai protokol seperti HTTP, FTP, dan SSH.

3) DDoS

Distributed Denial of Service (DDoS) adalah bentuk serangan siber yang bertujuan untuk mengganggu dan menghambat layanan jaringan dengan membanjiri *server target* dengan lalu lintas internet yang sangat besar, sehingga menyebabkan layanan tidak dapat diakses oleh pengguna yang sah [11]. Dengan menggunakan Hping 3, LOIC, dan Slowloris untuk mengirimkan sejumlah besar permintaan ke *target* sehingga menyebabkan gangguan layanan.

C. Analisis Indikator Rules

proses identifikasi keberadaan objek atau aktivitas tertentu dalam jaringan komputer atau sistem informasi. Ini melibatkan penggunaan algoritma yang mempelajari pola dari data jaringan atau *log* aktivitas untuk mengklasifikasikan dan mendeteksi aktivitas yang mencurigakan atau tidak sah[12]. Digunakan Analisis indikator *rules* untuk berbagai jenis serangan menunjukkan bahwa IBM QRadar mampu mendeteksi aktivitas berbahaya dengan akurasi tinggi. Indikator *rules* untuk kategori serangan sebagai berikut:

1) Serangan *port scanning* dianalisis dengan indikator
   a. Deteksi banyaknya permintaan ke berbagai *port*.
   b. Frekuensi permintaan koneksi.
   c. Variasi *port* yang akan dilakukan *scanning*.
   d. Pola permintaan yang tidak biasa.

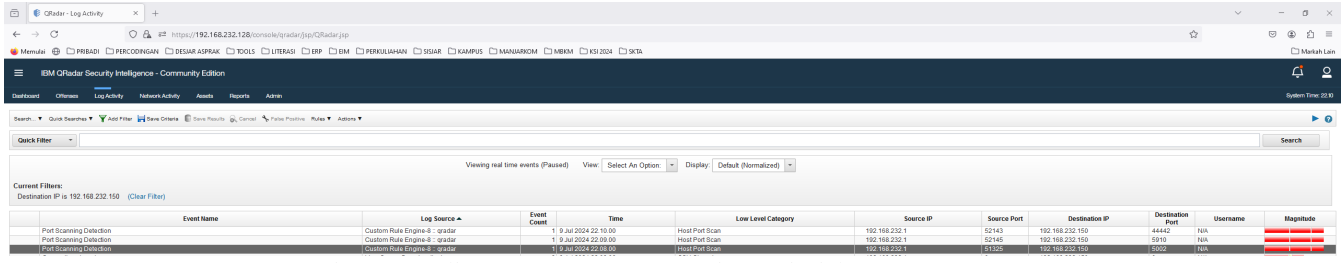
2) Serangan *brute force* dianalisis dengan indikator
   a. Jumlah percobaan *login* yang gagal.
   b. Kecepatan percobaan.
   c. Pola akses yang tidak biasa.

3) Serangan DDoS dianalisis dengan indikator
   a. Jumlah permintaan yang dikirim.
   b. Volume lalu lintas.
   c. Durasi serangan.

Berikut merupakan hasil indikator berdasarkan kategori serangan yang dilakukan:

1) Port Scanning

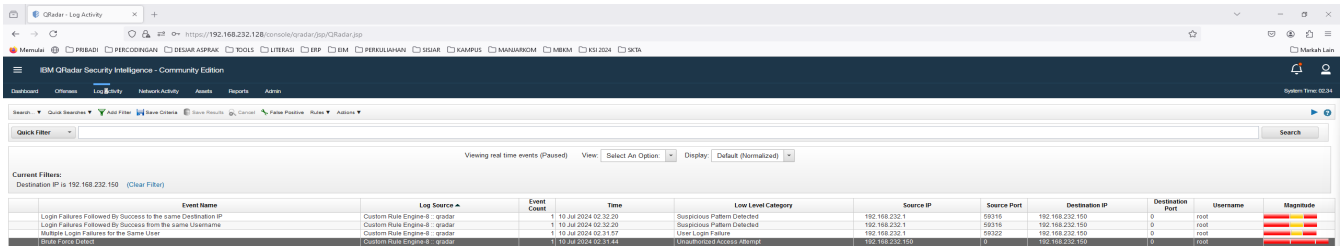
Hasil indikator berdasarkan kategori serangan *port scanning* berhasil mendeteksi adanya aktivitas *port scanning*. Pada Gambar 4 menunjukkan tampilan *log monitoring* dari IBM QRadar mendeteksi serangan *port scanning*.



Gambar. 4. Tampilan *Log Monitoring* IBM QRadar Mendeteksi Serangan *Port Scanning*

2) Brute Force

Hasil indikator berdasarkan kategori serangan brute force berhasil mendeteksi adanya aktivitas *brute force*. Pada Gambar 5 menunjukkan tampilan *log monitoring* dari IBM QRadar mendeteksi serangan *brute force*.

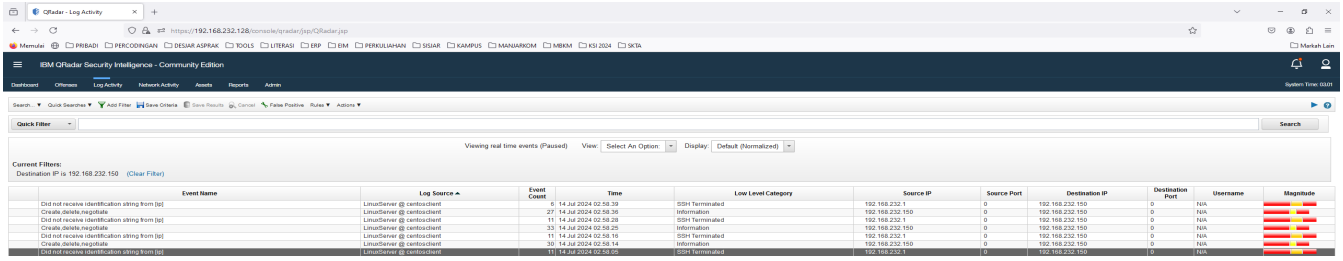


Gambar. 5. Tampilan *Log Monitoring* IBM QRadar Mendeteksi Serangan *Brute Force*

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 10, No. 3, September 2025, Pp. 1914-1924

3) DDoS

Hasil indikator berdasarkan kategori serangan DDoS tidak berhasil mendeteksi secara langsung adanya serangan DDoS. Namun, IBM QRadar memberikan informasi yang merujuk pada kemungkinan serangan DDoS. Diperlukan tambahan indikator *rules* untuk dapat mendeteksi dan merespons serangan DDoS dengan lebih baik. Pada Gambar 6 menunjukkan tampilan *log monitoring* dari IBM QRadar mendeteksi serangan DDoS.



Gambar. 6. Tampilan *Log Monitoring* IBM QRadar Mendeteksi Serangan DDoS

D. Analisis Fungsi Kontrol

Fungsi kontrol adalah mekanisme dan strategi yang diterapkan untuk mengendalikan dan mengelola operasi serta interaksi antara komponen fisik dan dalam suatu sistem [13]. Analisis fungsi kontrol pada IBM QRadar dilakukan untuk mengevaluasi efektivitas sistem dalam mendeteksi dan merespons berbagai jenis serangan siber. Fungsi kontrol utama yang dianalisis mencakup aspek *Identification*, *Authentication*, *Authorization*, dan *Accounting*.

1) Identification

a. Deteksi Aktivitas Mencurigakan: IBM QRadar memiliki kemampuan untuk mendeteksi aktivitas mencurigakan yang dapat mengindikasikan serangan siber. Misalnya, untuk serangan *port scanning*, QRadar mendeteksi banyaknya permintaan ke berbagai *port* yang menunjukkan upaya untuk menemukan celah keamanan di jaringan.
b. Pelacakan Sumber Serangan: QRadar mampu melacak alamat IP sumber serangan, memungkinkan administrator untuk mengidentifikasi dan mengambil tindakan terhadap perangkat atau pengguna yang mencurigakan.

2) Authentication

a. Verifikasi Identitas Pengguna: Dalam serangan *brute force*, IBM QRadar menganalisis upaya *login* yang gagal berulang kali sebagai indikator upaya akses tidak sah. QRadar mencatat setiap upaya *login*, termasuk waktu dan asal permintaan, yang membantu dalam verifikasi dan penanganan percobaan akses yang tidak sah.
b. Deteksi Pola Akses yang Tidak Biasa: QRadar mendeteksi dan mengidentifikasi pola akses yang tidak biasa, seperti upaya akses dengan kecepatan tinggi atau dari lokasi yang tidak biasa, yang dapat mengindikasikan upaya serangan *brute force*.

3) Authorization

a. Izin Akses ke Sumber Daya: QRadar memastikan bahwa hanya pengguna yang berwenang yang dapat mengakses sumber daya tertentu. Dalam kasus serangan, QRadar mencatat setiap upaya akses yang tidak sah ke sumber daya yang dilindungi.
b. Pencegahan Akses Tidak Sah: Dengan mencatat dan memantau upaya akses, QRadar membantu dalam mencegah akses tidak sah ke sumber daya kritis, memastikan bahwa hanya pengguna yang telah diotorisasi yang dapat mengakses informasi sensitif.

4) Accounting

a. Pencatatan Aktivitas Serangan: QRadar mencatat semua aktivitas yang terkait dengan serangan siber, termasuk jenis serangan, waktu kejadian, alamat IP sumber, dan respon yang diberikan oleh sistem. Pencatatan ini penting untuk analisis lebih lanjut dan untuk mengambil tindakan pencegahan di masa mendatang.
b. Penyimpanan *Log* untuk Analisis: *Log* yang disimpan oleh QRadar mencakup semua detail terkait serangan dan aktivitas mencurigakan, memungkinkan analisis forensik yang mendalam untuk memahami pola serangan dan meningkatkan strategi pertahanan.
c. Audit dan Pelaporan: QRadar menyediakan kemampuan untuk melakukan audit dan pelaporan aktivitas jaringan, memberikan gambaran lengkap tentang status keamanan dan aktivitas yang terjadi di jaringan.

Hasil analisis fungsi kontrol ini menunjukkan bahwa IBM QRadar efektif dalam mendeteksi, menganalisis, dan merespons berbagai jenis serangan siber. Kemampuan dalam mencatat dan melacak aktivitas serangan serta menyediakan data yang diperlukan untuk analisis forensik dan audit membantu organisasi dalam meningkatkan keamanan jaringan mereka dan merespons ancaman siber dengan lebih efisien.

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 10, No. 3, September 2025, Pp. 1914-1924

E. Metrik Response Time

Metrik *Response time* adalah waktu yang dibutuhkan oleh suatu sistem untuk menanggapi permintaan deteksi. *Response Time* dipengaruhi oleh beberapa faktor seperti pola beban kerja, tingkat layanan, dan distribusi beban yang tidak merata [14]. Metrik *Response Time* yang dilakukan berdasarkan berapa lama proses deteksi IBM QRadar terhadap serangan yang dilakukan sesuai dengan langkah-langkah yang telah ditentukan. Pengukuran waktu respon dilakukan dalam nilai detik (s). Pengukuran waktu respon dicatat menjadi dua aspek yaitu: Waktu Serangan dan Waktu Deteksi. Pada penelitian ini, akan dilakukan perhitungan untuk mendapatkan hasil waktu respon detik (s) dari setiap jenis serangan berdasarkan kedua aspek tersebut.

$$T_r = T_d - T_a$$

Dengan:
T_r = *Response time* (detik)
T_d = *Detection time*
T_a = *Attack time*

Setelah perhitungan terhadap pengukuran waktu respon dilakukan, langkah selanjutnya adalah melakukan identifikasi terhadap pengukuran waktu respon dari setiap serangan yang dilakukan. Hasil dari pengukuran waktu respon akan diperingkatkan berdasarkan waktu respon yang paling cepat dari keseluruhan serangan yang dilakukan. Perangkingan ini disusun berdasarkan tahapan yang telah ditentukan, yaitu pada Tabel 1:

TABEL 1
HASIL PERBANDINGAN METRIK *RESPONSE TIME*

Jenis Serangan	Waktu Serangan	Waktu Deteksi	Time Metrik (s)
Hping 3	02:57:54	02:58:05	11
Brutespray	10:46:24	10:47:00	36
Slowloris	03:32:10	03:32:56	46
LOIC	03:13:32	03:15:10	98
Nmap - Zenmap GUI Profile Intense Scan	22:07:00	22:08:00	60
Nmap - Zenmap GUI Profile Intense Scan, All TCP Ports	01:23:00	01:25:00	120
Hydra	02:23:15	02:31:44	509
Nmap - Zenmap GUI Profile Intense Scan plus UDP	16:31:00	16:51:00	1200
Medusa	01:27:53	01:58:43	1850

Perangkingan pada Tabel 1 menyimpulkan bahwa pengujian serangan Hping 3 memiliki waktu yang paling sedikit yaitu sebesar 11 detik, sehingga dalam perangkingan ditempatkan pada posisi pertama. Sedangkan pengujian serangan Medusa menempati posisi paling terakhir dengan catatan waktu 1850 detik.

F. Metrik Granularity

Metrik *Granularity* adalah tingkat detail yang digunakan dalam pengukuran dan analisis data. Dalam konteks pembelajaran metrik, hal ini merujuk pada kemampuan untuk menangkap kesamaan visual pada berbagai tingkat detail [15]. Metrik *Granularity* dilakukan dengan mempertimbangkan empat aspek utama, yaitu *magnitude*, *relevance*, *severity*, dan *credibility*. Pada penelitian ini, akan dilakukan perhitungan untuk mendapatkan skor total dari setiap jenis serangan berdasarkan keempat aspek tersebut. Pengukuran granularitas dilakukan sesuai dengan langkah-langkah yang telah ditentukan. Aspek-aspek ini diambil berdasarkan referensi dari panduan dan dokumentasi IBM QRadar, yang menjelaskan pentingnya masing-masing aspek dalam menilai dan mendeteksi serangan siber. Pada penelitian ini, akan dilakukan perhitungan untuk mendapatkan skor total dari setiap jenis serangan berdasarkan keempat aspek tersebut.

$$Skor\ Total = M + R + S + C$$

Dengan:
M = *Magnitude*
R = *Relevance*
S = *Severity*
C = *Credibility*

Berikut merupakan perangkingan hasil dari pengukuran pengukuran granulasi pada pengujian deteksi IBM QRadar terhadap serangan yang dilakukan. Perangkingan disusun berdasarkan skor total yang paling besar dari keseluruhan serangan yang dilakukan berdasarkan tahapan yang telah ditentukan, yaitu pada Tabel 2:

JIPI (Jurnal Ilmiah Penelitian dan Pembelajaran Informatika)
Journal homepage: https://jurnal.stkippgritulungagung.ac.id/index.php/jipi
ISSN: 2540-8984
Vol. 10, No. 3, September 2025, Pp. 1914-1924

TABEL 2
HASIL PERBANDINGAN METRIK *GRANULARITY*

Jenis Serangan	*Magnitude*	*Relevance*	*Severity*	*Credibility*	Skor Total
Hydra	10	10	9	10	39
Brutespray	10	10	9	10	39
Medusa	10	10	9	10	39
Nmap - Zenmap GUI Profile Intense Scan	9	10	8	10	37
Nmap - Zenmap GUI Profile Intense Scan plus UDP	9	10	8	10	37
Nmap - Zenmap GUI Profile Intense Scan, All TCP Ports	9	10	8	10	37
Hping 3	8	10	4	10	32
LOIC	6	10	1	10	27
Slowloris	6	10	1	10	27

Perangkingan pada Tabel di atas menyimpulkan bahwa jenis serangan Hydra, Brutespray, dan Medusa memiliki skor total tertinggi yaitu sebesar 39, sehingga menempati posisi pertama. Sedangkan jenis serangan LOIC dan Slowloris menempati posisi terakhir dengan skor total 27.

G. Perbandingan Metrik Response Time dan Granularity

Perbandingan antara metrik *response time* dan *granularity* pada IBM QRadar memberikan gambaran yang jelas tentang efektivitas sistem dalam mendeteksi dan menganalisis serangan siber. Response *time* mengukur kecepatan deteksi, sedangkan *granularity* menilai kedalaman informasi yang dihasilkan. Serangan Hping 3 memiliki waktu respon tercepat yaitu 11 detik, akan tetapi mendapatkan skor granularitasnya yang relatif rendah dengan nilai total 32. Sebaliknya, serangan Hydra membutuhkan waktu respon yaitu 509 detik, namun memiliki skor granularitas yang lebih tinggi dengan nilai total 39. Sementara itu, serangan Medusa memiliki waktu respon paling lambat yaitu1850 detik, tetapi juga memiliki skor granularitas yang tinggi dengan nilai total 39. Hal ini menunjukkan bahwa serangan dengan waktu respon cepat seperti Hping 3, tidak selalu disertai dengan skor granularitas yang tinggi. Sebaliknya, serangan yang lebih kompleks seperti Hydra dan Medusa cenderung memiliki skor granularitas yang lebih tinggi meskipun membutuhkan waktu deteksi yang lebih lama.

Berdasarkan hasil analisis metrik yang telah dilakukan, efektivitas deteksi IBM QRadar bervariasi tergantung pada jenis serangan yang dihadapi. IBM QRadar menunjukkan efektivitas yang lebih tinggi dalam mendeteksi serangan sederhana seperti Hping 3 yang terdeteksi dengan waktu respon tercepat 11 detik. Namun, untuk serangan yang lebih rumit seperti Medusa, waktu responnya jauh lebih lambat 1850 detik. Namun demikian, Serangan seperti Hydra dan Medusa menunjukkan skor granularitas yang lebih tinggi, masing-masing dengan nilai total 39. Hal ini menandakan bahwa meskipun Hydra membutuhkan waktu respon 509 detik dan Medusa membutuhkan waktu respon 1850 detik, IBM QRadar mampu memberikan informasi yang lebih rinci mengenai serangan tersebut. Kelemahan yang teridentifikasi adalah bahwa IBM QRadar cenderung lebih lambat dalam mendeteksi serangan yang lebih kompleks, seperti Medusa, yang membutuhkan waktu deteksi hingga 1850 detik, yang dapat mengurangi responsivitas terhadap ancaman yang memerlukan tindakan cepat.

H. Tinjauan Pustaka dan Perbandingan Hasil Penelitian

Tabel 3 menyajikan ringkasan dari beberapa penelitian sebelumnya yang relevan, yang mencakup Judul, penelitian, tahun, tujuan, metode, dan perbedaan. Dengan membandingkan hasil penelitian ini dengan studi-studi sebelumnya, dapat diidentifikasi keunikan dari pendekatan yang diambil dan bagaimana penelitian ini memperkaya literatur yang ada dalam bidang *Security Information and Event Management* (SIEM).

TABEL 3
TINJAUAN PUSTAKA DAN PERBANDINGAN HASIL PENELITIAN

No	Judul	Penelitian	Tahun	Tujuan	Perbedaan	Referensi
1	Analisis Serangan Router dengan *Security Information and Event Management* dan Implikasinya pada Indeks Keamanan Informasi	Citra Arfanudin, Bambang Sugiantoro, Yudi Prayudi	2019	Penelitian ini bertujuan untuk mengimplementasikan *Security Information and Event Management* (SIEM) di lembaga pemerintah dengan fokus pada pemantauan waktu nyata dan deteksi ancaman di lingkungan *cloud* untuk meningkatkan keamanan informasi.	Penelitian ini bertujuan pada serangan terhadap router dan dampaknya terhadap Indeks Keamanan Informasi, sedangkan perbedaan penelitian ini yang berfokus pada analisis efektivitas SIEM IBM QRadar dalam mendeteksi berbagai jenis serangan siber dengan menggunakan metrik *response time* dan *granularity*.	[16]
2	*Facing Cyber-Physical Security Threats by* PSIM-SIEM *Integration*	Flavio Frattini, Ugo Giordano, Vincenzo Conti	2019	Penelitian ini bertujuan untuk mengintegrasikan sistem PSIM dan SIEM guna mendeteksi ancaman keamanan siber-fisik yang mungkin mengancam infrastruktur kritis. Integrasi ini memungkinkan pemantauan baik	Penelitian ini bertujuan pada integrasi sistem PSIM dan SIEM untuk mendeteksi ancaman keamanan siber-fisik, sedangkan perbedaan penelitian ini lebih mengedepankan analisis metrik respon time dan granularitas	[17]

No	Judul	Penelitian	Tahun	Tujuan	Perbedaan	Referensi
				pada aspek fisik maupun logis dari sistem keamanan, serta mengelola ancaman yang teridentifikasi dari kedua aspek tersebut.	dalam konteks mendeteksi berbagai jenis serangan siber.	
3	*Proposed Framework for Network Lateral Movement Detection Based On User Risk Scoring in SIEM*	Airull Azizi Awang Lah, Marwan Hadri Bin Azmi, Rudzidatul Akmam Dziyayuddin	2018	Mengusulkan kerangka kerja untuk deteksi pergerakan antar sistem jaringan berdasarkan penilaian risiko pengguna di SIEM, dengan tujuan meningkatkan deteksi serangan gerakan lateral dalam jaringan	Penelitian ini fokus pada pengembangan kerangka kerja untuk mendeteksi pergerakan antar sistem dalam jaringan menggunakan penilaian risiko pengguna SIEM, sedangkan perbedaan penelitian ini berfokus deteksi dan respon serangan menggunakan metrik *response time* dan metrik *granularity*.	[18]
4	*SIEM selection criteria for an efficient contextual security*	Nabil Moukafih, Ghizlane Orhanou, Soukaina Sabir	2017	Memfasilitasi proses pengambilan keputusan dalam memilih solusi *Security Operations Center* (SOC) yang terbaik, serta untuk meningkatkan daftar kriteria pemilihan sehingga pengguna dapat memaksimalkan manfaat dan fitur dari solusi SIEM untuk menciptakan lingkungan yang lebih aman	Penelitian ini lebih berfokus pada proses seleksi dan kriteria untuk memilih solusi SIEM yang tepat bagi SOC, sedangkan perbedaan penelitian ini lebih spesifik pada implementasi atau penggunaan teknis SIEM dalam mendeteksi serangan pada jaringan.	[19]
5	*Effective Security Monitoring Using Efficient SIEM Architecture*	Muhammad Sheeraz, Muhammad Arsalan Paracha, Mansoor Ul Haque, Muhammad Hanif Durad, Syed Muhammad Mohsin, Shahab S. Band, Amir Mosavi	2023	Menyajikan dan menganalisis sistem SIEM terbaru yang ada, baik yang *opensource* maupun milik perusahaan, serta untuk mengusulkan sebuah arsitektur SIEM yang komprehensif dan modular. Arsitektur ini akan membantu organisasi dalam pengembangan atau penerapan sistem SIEM yang lebih efisien dan sesuai dengan kebutuhan mereka.	Penelitian ini fokus pada analisis dan pengembangan arsitektur SIEM yang komprehensif dan terstruktur sedangkan perbedaan penelitian ini berfokus pada aspek implementasi kinerja SIEM dalam mendeteksi dan merespons ancaman serangan pada jaringan.	[20]

IV. KESIMPULAN

Penelitian ini menunjukkan bahwa IBM QRadar memiliki kemampuan deteksi yang tinggi terhadap berbagai jenis serangan siber, terutama dalam aspek *Identification* dan *Accounting*. Eksperimen dengan teknik serangan seperti *port scanning*, *brute force*, dan DDoS menunjukkan bahwa IBM QRadar mampu mendeteksi aktivitas berbahaya dengan akurasi tinggi melalui analisis indikator *rules port scanning*, *brute force*, dan DDoS. Fungsi kontrol yang dianalisis mencakup *Identification*, *Authentication*, *Authorization*, dan *Accounting*, dengan IBM QRadar menunjukkan performa yang baik dalam mendeteksi dan melacak sumber serangan serta mencatat aktivitas untuk analisis lebih lanjut. Metrik *Response Time* menunjukkan bahwa serangan Hping 3 memiliki waktu respon tercepat dengan 11 detik, sementara Medusa memiliki waktu respon terlama dengan 1850 detik. Metrik *Granularity* menunjukkan bahwa serangan Hydra, Brutespray, dan Medusa memiliki skor granularitas tertinggi, mengindikasikan kemampuan IBM QRadar dalam mencatat detail setiap serangan dengan akurat. Keseluruhan hasil IBM QRadar dalam mendeteksi dan merespons berbagai jenis serangan siber, mendukung fungsi *Threat Intelligence* dan *Monitoring Threat Behavior*.

DAFTAR PUSTAKA

[1] K. L. G. Snider, R. Shandler, S. Zandani, and D. Canetti, “Cyberattacks, cyber threats, and attitudes toward cybersecurity policies,” *J Cybersecur*, vol. 7, no. 1, 2021, doi: 10.1093/cybsec/tyab019.
[2] A. Alqudhaibi, M. Albarrak, A. Aloseel, S. Jagtap, and K. Salonitis, “Predicting Cybersecurity Threats in Critical Infrastructure for Industry 4.0: A Proactive Approach Based on Attacker Motivations,” *Sensors*, vol. 23, no. 9, May 2023, doi: 10.3390/s23094539.
[3] G. González-Granadillo, S. González-Zarzosa, and R. Diaz, “Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures,” *Sensors*, vol. 21, no. 14, Jul. 2021, doi: 10.3390/s21144759.
[4] K. Kandasamy. S Sandeep Sekharan, *Proceedings of the 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET) : 22-24 March 2017, Chennai, India*. 2017.
[5] E. Ukwandu *et al.*, “Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends,” Mar. 01, 2022, *MDPI*. doi: 10.3390/info13030146.
[6] S. Gupta, B. S. Chaudhari, and B. Chakrabarty, “Vulnerable network analysis using war driving and security intelligence,” in *Lecture Notes in Networks and Systems*, vol. 7, Springer, 2018, pp. 465–471. doi: 10.1007/978-981-10-3812-9_49.
[7] C. H. A. Kuran *et al.*, “Vulnerability and vulnerable groups from an intersectionality perspective,” *International Journal of Disaster Risk Reduction*, vol. 50, Nov. 2020, doi: 10.1016/j.ijdrr.2020.101826.
[8] M. , L. H. K. , & T. M. Al-Shabi, “Gated-Dilated Networks for Lung Nodule Classification in CT scans,” *IEEE Access*, 2019.
[9] E. V Ananin, A. V Nikishova, and I. S. Kozhevnikova, “Port Scanning Detection Based on Anomalies,” 2017.

[10] R. P. Aji, Y. Prayudi, and A. Luthfi, "ANALYSIS OF BRUTE FORCE ATTACK LOGS TOWARD NGINX WEB SERVER ON DASHBOARD IMPROVED LOG LOGGING SYSTEM USING FORENSIC INVESTIGATION METHOD," vol. 4, no. 1, pp. 39–48, 2023, doi: 10.20884/1.jutif.2023.4.1.644.

[11] S. Balasubramaniam *et al.*, "Optimization Enabled Deep Learning-Based DDoS Attack Detection in Cloud Computing," *International Journal of Intelligent Systems*, vol. 2023, 2023, doi: 10.1155/2023/2039217.

[12] Y. Amit, P. Felzenszwalb, and R. Girshick, "Object Detection," in *Computer Vision*, Springer International Publishing, 2020, pp. 1–9. doi: 10.1007/978-3-030-03243-2_660-1.

[13] D. G. Rosado *et al.*, "Managing cybersecurity risks of cyber-physical systems: The MARISMA-CPS pattern," *Comput Ind*, vol. 142, Nov. 2022, doi: 10.1016/j.compind.2022.103715.

[14] W. Cheng, F. Ren, W. Jiang, and T. Zhang, "Optimizing the Response Time of Memcached Systems via Model and Quantitative Analysis," *IEEE Transactions on Computers*, vol. 70, no. 9, pp. 1458–1471, Sep. 2021, doi: 10.1109/TC.2020.3011619.

[15] D. Manandhar, M. Bastan, and K. H. Yap, "Semantic granularity metric learning for visual search," *J Vis Commun Image Represent*, vol. 72, Oct. 2020, doi: 10.1016/j.jvcir.2020.102871.

[16] S. Kasus, D. Komunikasi, I. Kota, T. Citra Arfanudin, B. Sugiantoro, and Y. Prayudi, "ANALISIS SERANGAN ROUTER DENGAN SECURITY INFORMATION AND EVENT MANAGEMENT DAN IMPLIKASINYA PADA INDEKS KEAMANAN INFORMASI ANALYSIS OF ROUTER ATTACK WITH SECURITY INFORMATION AND EVENT MANAGEMENT AND IMPLICATIONS IN INFORMATION SECURITY INDEX," 2019.

[17] F. Frattini, U. Giordano, and V. Conti, "Facing cyber-physical security threats by PSIM-SIEM integration," in *Proceedings - 2019 15th European Dependable Computing Conference, EDCC 2019*, Institute of Electrical and Electronics Engineers Inc., Sep. 2019, pp. 83–88. doi: 10.1109/EDCC.2019.00026.

[18] A. A. A. Lah, R. A. Dziyauddin, and M. H. Azmi, "Proposed Framework for Network Lateral Movement Detection Based on User Risk Scoring in SIEM," in *2018 2nd International Conference on Telematics and Future Generation Networks, TAFGEN 2018*, Institute of Electrical and Electronics Engineers Inc., Dec. 2018, pp. 149–154. doi: 10.1109/TAFGEN.2018.8580484.

[19] M. Nabil, S. Soukainat, A. Lakbabi, and O. Ghizlane, "SIEM selection criteria for an efficient contextual security," in *2017 International Symposium on Networks, Computers and Communications, ISNCC 2017*, Institute of Electrical and Electronics Engineers Inc., Oct. 2017. doi: 10.1109/ISNCC.2017.8072035.

[20] M. Sheeraz *et al.*, "Effective Security Monitoring Using Efficient SIEM Architecture," *Human-centric Computing and Information Sciences*, vol. 13, p. 17, 2023, doi: 10.22967/HCIS.2023.13.017.