Impression: Jurnal Teknologi dan Informasi, Vol. 2 (3) (2023)
Published by: Lembaga Riset Ilmiah – YMMA Sumut

Impression: Jurnal Teknologi dan Informasi

Penerapan Perangkat EvenLog Analyzer pada Digital Forensik Di Lingkungan Fakultas Teknik Universitas Darma Agung

Nelson Hutahean[1], Dewi Sholeha[2], Subur Simanulang [3],
Program Study Teknik Elektro, Universitas Darma Agung, Medan
Email:
alkhansadewi@gmail.com

ARTICLEINFO

Article history:
Received: 10 Oktober 2022
Revised: 10 Oktober 2022
Accepted: 11 November 2022

Keywords:
Log Event,
Database,
Cybercrime

Published by
Impression : Jurnal Teknologi dan Informasi
Copyright © 2023 by the Author(s) |This is an open-access article distributed under the Creative Commons Attribution which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.
https://creativecommons.org/licenses/by/4.0/

ABSTRACT

Mengevaluasi penerapan perangkat EvenLog Analyzer dalam konteks digital forensik di lingkungan Fakultas Teknik Universitas Darma Agung. EvenLog Analyzer digunakan untuk mengumpulkan dan menganalisis log event, yang merupakan data penting dalam mendeteksi aktivitas yang tidak biasa atau mencurigakan pada sistem jaringan. Hasil penelitian menunjukkan bahwa perangkat ini efektif dalam meningkatkan keamanan sistem dengan mendeteksi insiden keamanan secara dini. Ini memungkinkan tim TI untuk merespons ancaman dengan cepat dan efektif, sehingga meningkatkan keseluruhan keamanan digital di lingkungan universitas. Log event ini adalah data penting yang dapat digunakan untuk melacak jejak aktivitas yang tidak biasa, yang kemudian bisa dijadikan dasar dalam investigasi digital forensik. Secara keseluruhan, EvenLog Analyzer dapat dianggap sebagai alat yang efektif dalam meningkatkan keamanan digital, terutama dalam lingkungan pendidikan tinggi yang memerlukan pemantauan dan respon cepat terhadap insiden siber. Namun, efektivitasnya juga sangat bergantung pada bagaimana alat ini diintegrasikan dengan sistem keamanan yang sudah ada dan bagaimana data yang dihasilkan dimanfaatkan oleh tim keamanan.

Corresponding Author:
Author
Department of Engineering, Universitas YMMA Sumut Medan, Indonesia
Jl. Kapten Tandean No.3, Dusun Ampang, Kec. Slipi., Kota Kupang, Nusa Tenggara, Indonesia 20218
Email: author@gmail.com

PENDAHULUAN

Barang bukti dari kasus cybercrime berbeda dengan kejahatan konvensional, dimana penanganan atas bukti elektonik maupun bukti digital yang termuat didalamnya rentan mengalami perubahan atau kontaminasi, sehingga bukti elektronik harus dipacking dan disimpan dengan baik di tempat yang aman (Ivanović, 2018). Dalam mengatasi kondisi tersebut penanganan atas bukti digital diperlakukan khusus dibandingkan dengan bukti fisik pada kejahatan konvensional yang lebih dikenal dengan chain of custody

Meskipun demikian sampai saat ini belum tersedia alat (tools) atau software yang mampu secara komprehensif dan menyeluruh dapat mengimplementasikan konsep dari digital chain of custody (Jain & Kalbande, 2015). Tools yang ada umumnya hanya mampu menangani bagian tertentu dari investigasi bukti digital, tetapi tidak berorientasi pada konsep investigasi forensik digital secara keseluruhan. Sehingga untuk menerapkan konsep digital chain of custody agar diperoleh bukti digital yang potensial

dan kuat serta mampu dipertahankan dalam proses ligitasi, harus dipilih tools yang handal di setiap tahapan dari digital chain of custody (Kao et al., 2018; dan Masvosvere and Venter, 2016).

Disamping metode penanganan bukti digital dengan tools yang telah tersedia berdasarkan konsep digital chain of custody, hal penting lainnya adalah dengan hadirnya lembaga yang menaungi segala aktifitas investigasi criminal dunia maya (cybercrime). Peranan dari lembaga ini adalah menganalisis konsep, proyek terkait investigasi forensik digital, tools dan dukungan hukum di bidang cybercrime dalam rangka merepresentasikan bukti digital yang berintegritas sehingga dapat diterima dalam proses ligitasi (Granja & Rafael, 2015).

URAIAN TEORI

Forensik digital atau forensik Ilmu komputer menggabungkan keahlian hukum dan keterampilan komputer dalam mengumpulkan dan menganalisis data dari sistem komputer, jaringan, komunikasi nirkabel, dan perangkat penyimpanan. Hal ini bertujuan untuk dapat membawa data tersebut sebagai barang bukti dalam penegakan hukum (Forensik Komputer, n.d.). Forensik digital terus berkembang sebagai bidang baru dalam teknologi informasi. Oleh karena itu, jumlah ahli forensik digital di Indonesia tidak banyak. (Susanto et al., 2023)

Dengan perkembangan teknologi yang pesat, Penyalahgunaan semakin meningkat. Penyalahgunaan ini kerap dibawa ke pengadilan berdasarkan Undang-Undang Nomor 11 Tahun 2008 tentang Transaksi Elektronik. Jika kasus ini dibawa ke pengadilan, bukti digital/elektronik akan sangat penting. Hal ini mengharuskan institusi dan badan hukum untuk memanfaatkan jasa ahli komputer umum dan ahli di bidang tertentu seperti pemrograman, jaringan, keamanan, peretasan, pengembangan web, dan bidang lain yang terkait dengan forensik digital yang ada. Namun, karena pengetahuan khusus, mereka seringkali tidak memahami dasar-dasar yang diperlukan untuk melakukan forensik digital. Forensik digital kini tidak hanya sekedar aspek teknis saja, namun juga langkah-langkah yang perlu dilakukan untuk memverifikasi bukti-bukti yang diperoleh**.**

Log Storage

Tahap log storage menyimpan hasil transformasi agar dapat dilakukan analisis dengan cepat terhadap field dan data hasil normalisasi. Log entry pada tahap log transformation (Chuvakin, Schmidt, dan Phillips, 2013). Strategi dan. media penyimpanan pada. tahap ini bergantung pada format penyimpanan yang. dianut log file (Chuvakin, Schmidt, dan Phillips, 2013) dan. Lokalitas penyimpanan (Daubner, 2018). Lokalitas. Penyimpanan. Log terdiri dari dua tipe, yakni local storage dan centralized storage Menurut Lazar, Gligorijević dan Đukić (2016) menyoroti tantangan big data dalam analisis log, karena semakin banyak data yang diperoleh dari berbagai sumber dan memerlukan solusi terukur untuk penyimpanan dan pemrosesan. Mereka menunjukkan pentingnya arsitektur komputer terdistribusi untuk memproses data dalam jumlah besar. Menurut Sundaresan dan Patel (2017), mereka mempertimbangkan perlunya analisis data waktu nyata dan menyoroti bahwa sistem tradisional seringkali tidak mampu menangani data dari sumber data yang berbeda.

Menurut Kent, Chevalier dan Grance (2006) membahas keragaman protokol untuk perangkat dan aplikasi yang berbeda. Hal ini menyoroti perlunya standar format protokol yang konsisten dan interoperabilitas antar sistem untuk memfasilitasi analisis. Menurut Adams dan Davis (2016), yang menyoroti kesulitan mengintegrasikan protokol dari sumber berbeda dengan format dan struktur berbeda dan menyarankan penggunaan kerangka umum untuk pengumpulan dan analisis protokol.

Keamanan dan Integritas Data

Menurut Rogers dan Seigfried-Spellar (2016) membahas risiko gangguan dan perusakan data log oleh penyerang. Mereka merekomendasikan penggunaan teknik enkripsi untuk memastikan integritas dan keaslian data log.

ISSN: 2963-7333 (Online)

Menurut Carrier dan Spafford (2004) menyarankan penerapan protokol keamanan yang ketat dan terus memantau data log untuk melindunginya dari akses tidak sah.

Menurut Kruegel dan Vigna (2003) membahas tantangan mendeteksi pola serangan yang tersembunyi dalam data log yang sangat besar. Mereka menekankan pentingnya algoritma deteksi anomaly berbasis pembelajaran mesin untuk meningkatkan akurasi dan efisiensi.

Menurut Axelsson (2000), ia mempelajari masalah positif palsu dan negatif palsu dalam deteksi intrusi dan menekankan perlunya kalibrasi berkelanjutan dan penyesuaian model deteksi.

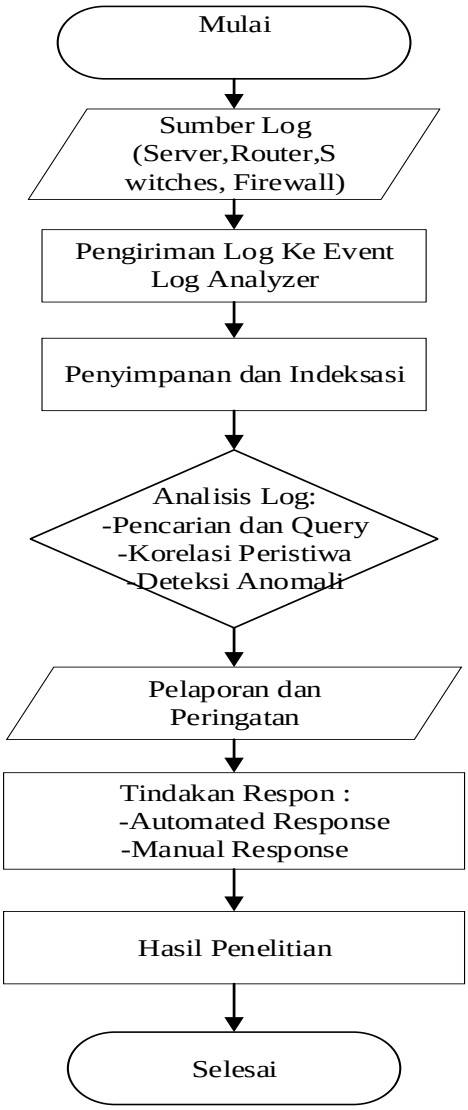
Dengan berkembangnya teknologi informasi, pelaku kejahatan memanfaatkan berbagai ruang siber untuk meningkatkan kejahatan. Risiko dan serangan dunia maya telah menjadi masalah utama. Serangan dunia maya meningkat secara signifikan, mengakibatkan banyak gangguan pada proses penting perbankan dan menyebabkan kerugian finansial yang besar pada sistem. Untuk menekan kejahatan siber dan ancaman siber, industri keuangan ingin memanfaatkan kecerdasan buatan dan langkah-langkah keamanan siber lainnya untuk meningkatkan pengalaman nasabah dan efisiensi proses perbankan. Oleh karena itu, tujuan dari penelitian ini adalah untuk mengungkap reaksi sistem keamanan siber terhadap serangan siber, bagaimana serangan siber menguntungkan sistem internal bank, dan motivasi untuk memperkuat langkah-langkah pencegahan untuk menyelamatkan basis data dan server bank.(Hapsah et al., 2024)

Untuk mengevaluasi dan mempelajarinya pengalaman bank-bank Indonesia melawan serangan siber dengan menyelidiki apakah untuk menegakkan pelanggaran. Penelitian ini menggunakan kuesioner sebagai alat utama untuk mengumpulkan data responden tentang bagaimana mereka pernah mengalami serangan siber setidaknya dua tahun lalu.(Sari, 2023).

Internet of Things memiliki kemampuan untuk menghubungkan objek-objek cerdas dan memungkinkannya berinteraksi dengan lingkungan dan perangkat komputasi cerdas lainnya melalui jaringan Internet. Namun, baru-baru ini, keamanan Internet of Things terancam oleh serangan siber yang menggunakan berbagai serangan penolakan layanan untuk menyusup ke perangkat Internet of Things yang ditargetkan. Penelitian ini bertujuan untuk mendeteksi dan mencegah serangan denial of service berupa synchronous Flooding dan ping Flooding pada jaringan Internet of Things dengan menggunakan pendekatan finite state automation. (Boltenhagen et al., 2021)Dengan hasil pengujian menunjukkan bahwa pendekatan finite state automaton berhasil mendeteksi serangan synchronous Flooding dan ping Flooding pada jaringan Internet of Things, namun mencegah serangan dengan biaya yang signifikan pada penggunaan prosesor dan memori.(Antony & Gustriansyah, 2021)

E-commerce adalah aktivitas perdagangan yang dilakukan secara online dengan menggunakan internet untuk tujuan bisnis. Seiring kemajuan teknologi dan meningkatnya penggunaan perdagangan elektronik, kejahatan yang merugikan dapat terjadi. Penggunaan data pribadi dalam e-commerce rentan terhadap serangan siber. Artikel ini berfokus pada penyelidikan bagaimana langkah-langkah keamanan, risiko, dan strategi yang dijelaskan berdampak pada keamanan informasi pribadi pengguna e-commerce. (Kehista et al., 2023)

METODE PENELITIAN

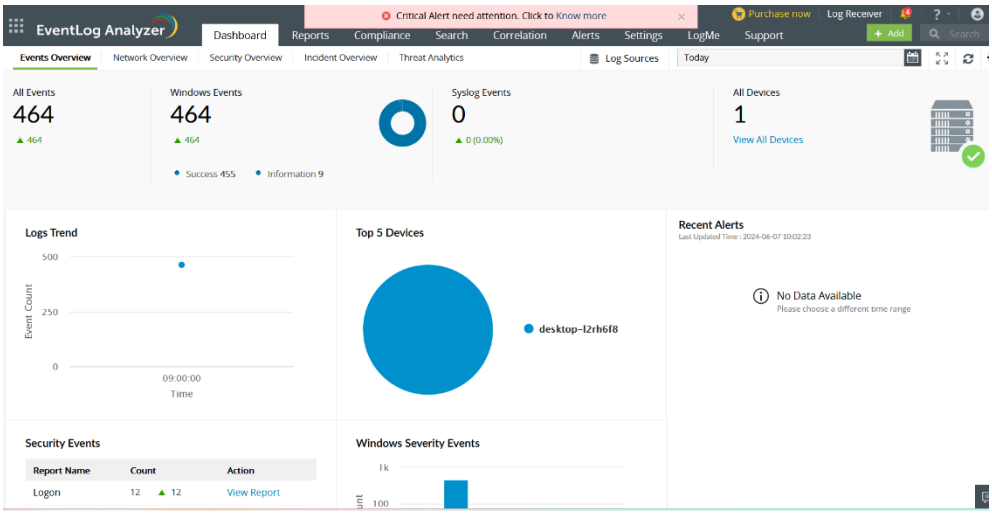


1. Perangkat Lunak (Software) Manage Engine EventLog Analyzer
2. Perangkat keras (Hardware)

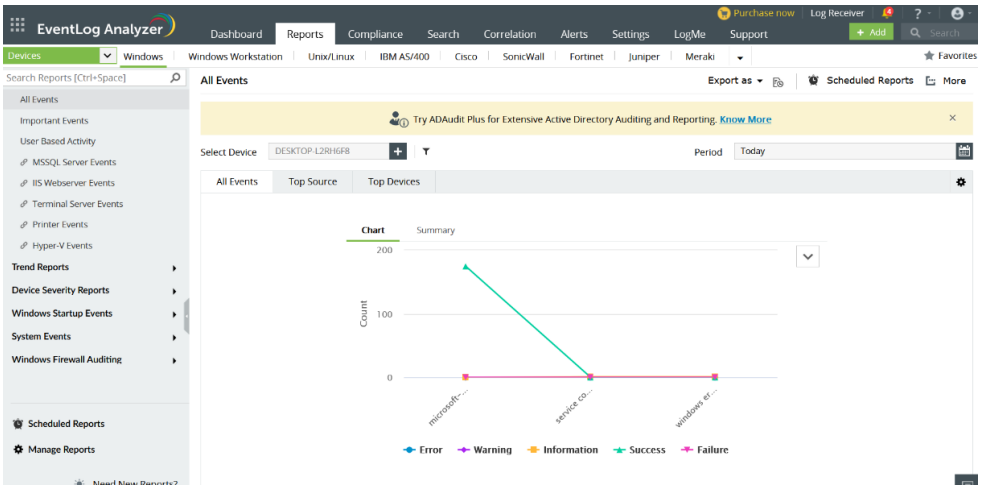
   a. Server : Prosesor multi-core, RAM 32 GB
   b. Storage Arrays : Penyimpanan tambahan
   c. Network Devices : Router, Switch dan Firewall

ISSN: 2963-7333 (Online)

HASIL PENELITIAN



Gambar 1. Tampilan Dashboard hasil pengumpulan data otomatis perangkat Eventlog Analyzer dari windows 11

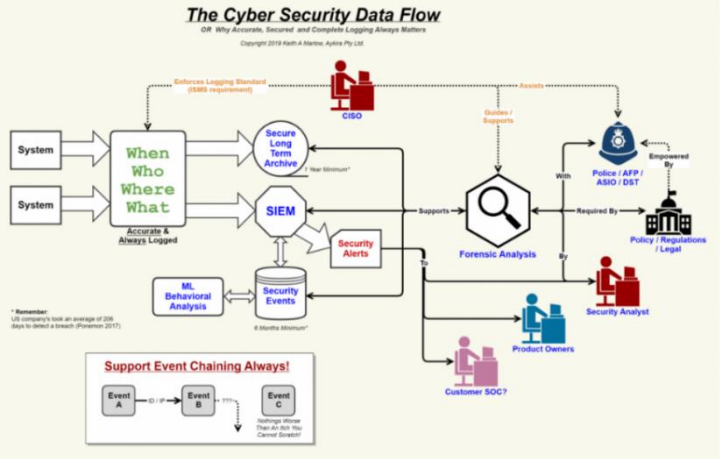


Gambar 2. Grafik dari Kumpulan data keamanan pada jaringan yang terdeteksi cybercrime

PEMBAHASAN

Sleuth Kit mendukung banyak sistem file dan memastikan kompatibilitas dengan berbagai platform. Komunitas dan Peluang Penelitian bersifat open source, ini merupakan lahan subur bagi para peneliti dan mendapat dukungan kuat dari komunitas. Integrasi dengan Autopsy: Dapat digunakan dengan Autopsy untuk memberikan pengalaman GUI untuk meningkatkan kegunaan. Cellebrite UFED

Spesialisasi sebagai perangkat lunak forensic seluler, X-Way Forensik, X-Way adalah Alat Analisis Serbaguna dari analisis struktur file hingga pemulihan data, alat ini menawarkan spektrum kemampuan yang luas. Volatilitas berspesialisasi dalam menganalisis dump RAM. Dan terakhir Aksioma Magnet dirancang dengan antarmuka yang intuitif, ini mengakomodasi penyelidik berpengalaman dan pendatang baru.



Gambar 3. The Cyber Security Data Flow

Monitoring server proses pemantauan sumber daya sistem server seperti memantau kinerja server juga membantu mengidentifikasi masalah terkait kinerja lainnya seperti pemanfaatan sumber daya, waktu henti aplikasi, dan waktu respon terhadap suatu service. File Integrity Monitoring (FIM) merupakan aktifitas memonitor integritas sebuah file untuk men(2016)jaga keutuhan suatu file dari perubahan yang tidak terotorisasi, dengan memanfaatkan Wazuh sebagai salah satu aplikasi open source untuk melakukan monitoring memiliki berbagai macam fitur untuk melakukan monitoring.

PENUTUP

Perangkat EvenLog Analyzer terbukti efektif dalam mengumpulkan dan menganalisis log event di lingkungan Fakultas Teknik. Ini membantu dalam mengidentifikasi dan merekonstruksi kejadian yang berpotensi mencurigakan atau menunjukkan adanya aktivitas yang tidak biasa pada sistem jaringan.
Implementasi EvenLog Analyzer dapat meningkatkan keamanan sistem secara signifikan dengan memberikan kemampuan deteksi dini terhadap insiden keamanan. Hal ini memungkinkan tim IT untuk merespons dengan cepat terhadap ancaman yang terdeteksi.

REFERENSI

Antony, F., & Gustriansyah, R. (2021). Deteksi Serangan Denial of Service pada Internet of Things Menggunakan Finite-State Automata. *MATRIK : Jurnal Manajemen, Teknik Informatika Dan Rekayasa Komputer*, *21*(1). https://doi.org/10.30812/matrik.v21i1.1078

Boltenhagen, M., Chatain, T., & Carmona, J. (2021). Model-based trace variant analysis of event logs. *Information Systems*, *102*. https://doi.org/10.1016/j.is.2020.101675

Forensik Komputer. (n.d.).

☼ ISSN: 2963-7333 (Online)

Hapsah, Z. F., Irwan, M., & Nasution, P. (2024). Analisis Tingkat Keamanan Data Perusahaan yang Rentan Terhadap Serangan Cyber dalam Sistem Informasi Manajemen. *WANARGI : Jurnal Manajemen Dan Akuntansi*, *1*(2).

Jeklin, A., Bustamante Farías, Ó., Saludables, P., Para, E., Menores, P. D. E., Violencia, V. D. E., Desde, I., Enfoque, E. L., En, C., Que, T., Obtener, P., Maestra, G. D. E., & Desarrollo, E. N. (2016). Implementasi Security Information and Event Management (Siem) Untuk Deteksi Dan Analisa Insiden Keamanan Pada Web Server. *Correspondencias & Análisis*, *15018*.

Kehista, A. P., Fauzi, A., Tamara, A., Putri, I., Fauziah, N. A., Klarissa, S., & Damayanti, V. B. (2023). Analisis Keamanan Data Pribadi pada Pengguna E-Commerce: Ancaman, Risiko, Strategi Kemanan (Literature Review). *Jurnal Ilmu Manajemen Terapan*, *4*(5).

Sari, I. (2023). Keamanan Komputer dan Ancaman Cyber di Era Digital. *Jurnal Teknologi Terkini*, *3*(4).

Susanto, E., Antira, Lady, Kevin, K., Stanzah, E., & Majid, A. A. (2023). Manajemen Keamanan Cyber di Era Digital. *Journal of Business And Entrepreneurship*, *11*(1). https://doi.org/10.46273/jobe.v11i1.365