

Analisis Kapabilitas Elastic Endpoint Security Berdasarkan Kerangka Cyber Kill Chain untuk Penguatan Pertahanan *Endpoint* Pemerintah

Fatikho Kautsar¹

fatikho.kautsar@bssn.go.id¹

¹Badan Siber dan Sandi Negara

Informasi Artikel

Diterima : 30 Nov 2025

Direvisi : 17 Des 2025

Disetujui : 30 Des 2025

Kata Kunci

Elastic EDR, Cyber Kill Chain, serangan berlapis, endpoint defense, APT

Abstrak

Ancaman siber terhadap sektor pemerintah menunjukkan tren yang semakin agresif dan terstruktur. Laporan Monitoring Keamanan Siber BSSN tahun 2021 mengidentifikasi *web defacement* dan kebocoran data sebagai insiden dominan yang sebagian besar menargetkan instansi pemerintah. Pembaruan lanskap pada tahun 2024 mencatat peningkatan signifikan aktivitas *malicious*, termasuk 330.527.636 anomali trafik serangan yang terdeteksi secara nasional serta dominasi kasus *ransomware*, *illegal access*, dan *data breach* sebagai insiden terbanyak. Temuan ini menegaskan bahwa *endpoint* tetap menjadi titik masuk favorit *adversary* dan memerlukan pendekatan pertahanan yang memahami struktur operasional penyerang. Penelitian ini menganalisis kapabilitas Elastic Endpoint Security sebagai solusi *Endpoint Detection and Response* (EDR) menggunakan kerangka Cyber Kill Chain (CKC) untuk memperkuat pertahanan *endpoint* di sektor pemerintahan. Dua skenario berbasis serangan nyata yang digunakan untuk mengevaluasi efektivitas deteksi pada setiap fase CKC. Hasil menunjukkan bahwa Elastic EDR mampu menginterupsi beberapa tahap krusial, terutama *delivery*, *exploitation*, dan *installation*, serta menghasilkan kontrol proteksi yang relevan dengan kebutuhan pertahanan modern. Studi ini menegaskan potensi EDR open sebagai fondasi strategis pertahanan adaptif bagi instansi pemerintah.

Keywords

Elastic EDR, Cyber Kill Chain, layered attacks, endpoint defense, APT

Abstract

Cyber threats targeting government institutions continue to escalate in sophistication and operational structure. The 2021 BSSN Cybersecurity Monitoring Report identified web defacement and data breaches as the most prevalent incidents across government entities. The 2024 cybersecurity landscape further reinforces this trend, recording 330,527,636 malicious traffic anomalies nationwide and highlighting ransomware, illegal access, and data breaches as the top incident categories. These developments underscore the persistent exploitation of endpoint weaknesses, emphasizing the need for defense strategies grounded in adversarial attack-chain understanding. This study evaluates the detection capabilities of Elastic Endpoint Security as an Endpoint Detection and Response (EDR) solution through the Cyber Kill Chain (CKC) framework to enhance endpoint defense within government environments. Two realistic attack scenarios were executed to assess detection performance across CKC phases. The findings indicate that Elastic EDR effectively disrupts critical stages, particularly delivery, exploitation, and installation, while providing protective responses aligned with modern defense requirements. This study highlights the viability of open EDR solutions as adaptive, cost-effective defensive foundations for public-sector cybersecurity.

A. Pendahuluan

Insiden siber pada sektor publik dan privat di Indonesia terus menunjukkan peningkatan dari tahun ke tahun. Berdasarkan Laporan Monitoring Tahunan Badan Siber dan Sandi Negara (BSSN) tahun 2021, serangan seperti web defacement dan kebocoran data masih mendominasi, dengan sektor pemerintah tercatat sebagai pihak yang paling banyak terdampak [1]. Tren serangan yang berfokus pada sektor pemerintah bukanlah fenomena baru. Pusat Operasi Keamanan Siber Nasional (Pusopskamsinas) BSSN pada tahun 2018 mencatat bahwa domain go.id menempati posisi tertinggi sebagai target insiden siber [2]. Situasi ini kembali dipertegas dalam Lanskap Keamanan Siber Indonesia tahun 2022, di mana sektor administrasi pemerintah tercatat menerima aduan siber terbanyak, yakni 110 laporan dalam satu tahun [3]. Data tersebut mencerminkan bahwa instansi pemerintah tetap menjadi target strategis bagi pelaku ancaman, sehingga penguatan keamanan siber di sektor ini merupakan kebutuhan mendesak. Mayoritas serangan modern memanfaatkan titik masuk pada *end-device* [4], [5], yang secara operasional terkoneksi sebagai bagian dari jaringan organisasi dan dikenal sebagai *endpoint* [4]. Salah satu ancaman paling dominan pada *endpoint* adalah *malware*, yang berdasarkan temuan nasional merupakan vektor utama dalam berbagai insiden siber di Indonesia. Fokus pada pertahanan *endpoint* menjadi sangat penting, mengingat sebagian besar serangan siber memanfaatkan titik ini sebagai jalur awal kompromi [4], [5].

Kajian literatur memberikan gambaran bahwa berbagai penelitian sebelumnya telah mengeksplorasi penggunaan Elastic Stack atau ELK Stack untuk mendukung aktivitas deteksi ancaman. Jain (2018) [6] meneliti deteksi lateral movement menggunakan ELK Stack, yaitu fase ketika penyerang telah berhasil menguasai satu sistem dan bergerak ke sistem atau subnet lain. Pendekatan ini berfokus pada deteksi pascainsiden dan identifikasi perpindahan antarhost. Mulyana (2020) [7] mengimplementasikan ELK Stack sebagai *security information and event management* (SIEM) dalam mengidentifikasi tahapan serangan dan memberikan rekomendasi penguatan keamanan di LKPP. Penelitian Admi dan Hakim (2020) [2] merekomendasikan penggunaan Elastic Stack untuk pemantauan jaringan dan *host*, serta menyoroti pentingnya koordinasi keamanan antara pemerintah pusat dan daerah.

Meskipun demikian, penelitian-penelitian terdahulu tersebut cenderung berfokus pada aspek deteksi dan pemantauan, bukan pada proteksi aktif terhadap aset. Sistem *intrusion detection and prevention system* (IDPS) yang umum digunakan masih mengandalkan pemrosesan berbasis log dan bersifat reaktif. Demikian pula, antivirus tradisional hanya efektif mendeteksi *malware* dengan pola yang telah dikenal, sehingga tidak memadai dalam menghadapi serangan *advanced persistent threat* (APT) [8]. APT sendiri merupakan bentuk serangan terstruktur yang dijalankan secara sistematis oleh organisasi lawan dengan tujuan jangka panjang.

Untuk menjawab kebutuhan akan proteksi yang lebih proaktif, penelitian ini mengusulkan penggunaan *Elastic Endpoint Detection and Response* (EDR). EDR memiliki kemampuan monitoring perilaku, deteksi berbasis anomali, respons otomatis, serta integrasi dengan analisis berbasis rantai serangan. Rekomendasi dari NIST SP 1800-24 mengenai keamanan siber sektor kesehatan serta NIST

Cyber Security Framework menegaskan pentingnya penerapan *security continuous monitoring* dan perlindungan *endpoint* guna mencapai tujuan keamanan informasi organisasi [9][10]. Efektivitas Elastic EDR juga didukung oleh studi Karantzas dkk. [5] yang menunjukkan keberhasilan pendeteksian dan pemblokiran DLL attack dan CPL attack, serta ulasan positif dari Gartner Magic Quadrant dan Forrester [11][12] yang menempatkan Elastic sebagai solusi dengan visibilitas dan fleksibilitas tinggi. Selain bersifat open-source dan gratis, Elastic EDR dikategorikan sebagai *Strong Performer* oleh Forrester karena kemampuannya menggabungkan fungsi SIEM dan EDR untuk mempercepat deteksi serta pemulihan insiden. Solusi EDR yang terbuka dan tanpa biaya lisensi memberikan nilai strategis bagi instansi pemerintah yang membutuhkan respons proteksi adaptif namun tetap mempertimbangkan efisiensi biaya [13].

Dalam penelitian ini, EDR diposisikan sebagai solusi yang dapat diadopsi secara realistis oleh instansi yang tidak memiliki perimeter keamanan *endpoint* dan menghadapi keterbatasan anggaran. Pengujian dilakukan menggunakan kerangka kerja Cyber Kill Chain (CKC) [5], [14] untuk mensimulasikan serangan APT terhadap aset yang telah dipasang EDR. Evaluasi dilakukan dengan membandingkan kondisi sebelum dan sesudah penerapan EDR untuk menilai kapabilitas proteksi secara komprehensif. Penelitian ini juga diselaraskan berdasarkan pembaruan lanskap pada tahun 2024 mencatat peningkatan signifikan aktivitas malicious, termasuk 330.527.636 anomali trafik serangan yang terdeteksi secara nasional serta dominasi kasus *ransomware*, *illegal access*, dan *data breach* sebagai insiden dominan[15].

B. Metode Penelitian

Penelitian ini berfokus pada analisis kapabilitas Elastic Endpoint Security sebagai *Endpoint Detection and Response* (EDR) untuk melindungi aset host pada organisasi XYZ.

Penelitian ini menggunakan pendekatan kualitatif dengan tujuan untuk memahami perilaku dan respons sistem keamanan endpoint dalam menghadapi skenario serangan yang kompleks dan berlapis. Analisis dilakukan dengan menginterpretasikan hasil pengujian, pola alert, serta mekanisme respons Elastic EDR pada setiap fase Cyber Kill Chain. Pendekatan ini dipilih karena fokus penelitian tidak pada pengukuran kinerja kuantitatif, melainkan pada evaluasi efektivitas proteksi dan kemampuan sistem dalam memutus rantai serangan secara kontekstual pada lingkungan instansi pemerintah.

Desain penelitian mengacu pada metodologi ***Design Science Research (DSR)*** [20], yang sesuai untuk pemecahan masalah organisasi dan pengembangan artefak teknologi. DSR digunakan untuk merumuskan permasalahan, mengidentifikasi kebutuhan organisasi, serta merancang solusi yang dapat diuji dan dievaluasi secara sistematis.

Tahapan penelitian meliputi:

1. ***Problem Identification***

Mengidentifikasi hambatan keamanan *endpoint* dan kebutuhan perlindungan aset host.

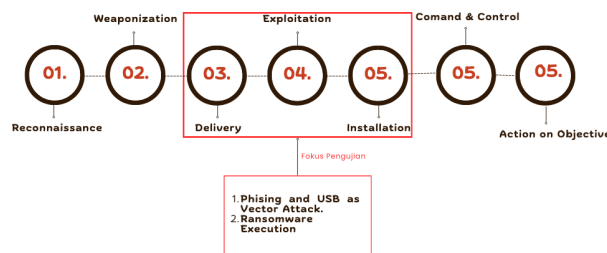
2. ***Literature Review & Requirement Analysis***

Mengkaji penelitian terdahulu, ancaman yang relevan, dan kemampuan solusi yang mungkin diterapkan.

3. **Development**

Membangun sistem EDR menggunakan Elastic Endpoint Security berdasarkan tahapan sebelumnya. Proses pengembangan mengikuti kerangka kerja **SDLC model Waterfall** [21] karena sifatnya yang terstruktur dan berurutan.

4. **Evaluation**



Gambar 1. Skenario Pengujian

Sistem diuji menggunakan skenario serangan APT yang dimodelkan melalui **Cyber Kill Chain (CKC)** [5], [14]. Pengujian dilakukan untuk menganalisis efektivitas deteksi dan proteksi pada setiap fase CKC sebagaimana Gambar 1. Gambar 1 menunjukkan skenario pengujian berbasis Cyber Kill Chain yang digunakan dalam penelitian ini. Setiap fase CKC dimanfaatkan sebagai kerangka untuk mensimulasikan aktivitas penyerang dan mengamati respons Elastic EDR terhadap tahapan serangan tersebut. Pendekatan ini memungkinkan evaluasi sistem keamanan secara terstruktur berdasarkan fase serangan, bukan hanya berdasarkan kejadian individual.

5. **Conclusion & Artifact Delivery**

Menyusun kesimpulan dan rekomendasi penguatan keamanan.

C. Hasil dan Pembahasan

Untuk memposisikan penelitian ini dalam konteks penelitian terdahulu, dilakukan telaah terhadap sejumlah studi yang relevan terkait keamanan endpoint dan deteksi serangan siber. Ringkasan penelitian-penelitian tersebut disajikan pada Tabel 1, termasuk pendekatan yang digunakan serta keterbatasan masing-masing studi.

Tabel 1. Ringkasan Penelitian Terdahulu terkait Keamanan Endpoint

Penelitian	Pendekatan	Fokus Utama	Keterbatasan
Jain (2018)	ELK Stack	Deteksi lateral movement	Fokus pascainsiden, tanpa proteksi
Mulyana	ELK Stack	Identifikasi	Tidak

(2020)	(SIEM)	tahapan serangan	mengevaluasi respons endpoint
Admi & Hakim (2020)	Elastic Stack	<i>Monitoring host & jaringan</i>	Tidak membahas proteksi aktif
Penelitian ini	Elastic EDR + CKC	<i>Evaluasi proteksi endpoint berbasis attack-chain</i>	Terbatas pada dua skenario serangan.

Berdasarkan Tabel 1, terlihat bahwa sebagian besar penelitian sebelumnya berfokus pada aspek deteksi dan pemantauan, khususnya menggunakan ELK Stack sebagai SIEM. Berbeda dengan penelitian terdahulu, penelitian ini menitikberatkan pada evaluasi proteksi endpoint secara proaktif dengan memanfaatkan Elastic EDR dan kerangka Cyber Kill Chain sebagai pendekatan evaluatif.

Pengujian kapabilitas Elastic Endpoint Security sebagai EDR dilakukan menggunakan skenario serangan berbasis kerangka Cyber Kill Chain (CKC). Seluruh rangkaian uji dilaksanakan pada lingkungan terisolasi yang mereplikasi kondisi jaringan internal organisasi XYZ, yaitu network 192.168.40.0/24. Pengujian dilakukan pada fase pra dan pasca implementasi untuk menilai efektivitas fungsi proteksi, deteksi, dan respons pada aset *endpoint*.

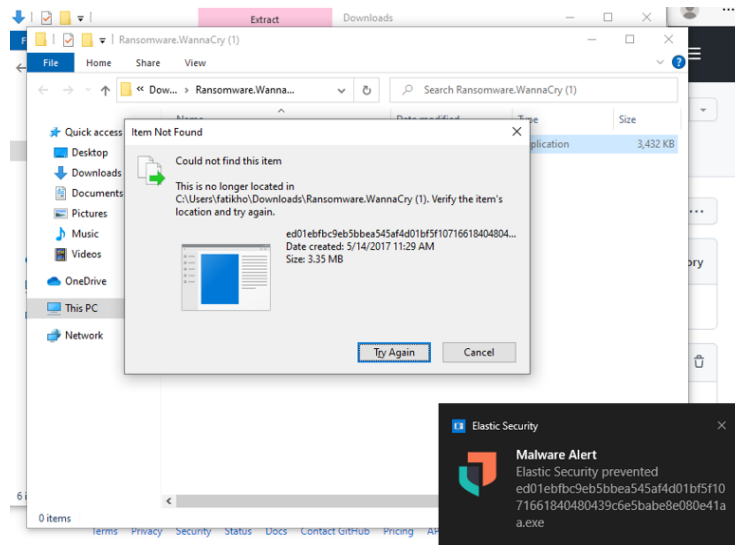
Pemilihan CKC sebagai kerangka evaluasi mengacu pada teori bahwa serangan berbasis APT terdiri dari tahapan berurutan mulai dari reconnaissance hingga action on objective [14]. Pendekatan ini memungkinkan peneliti mengidentifikasi di fase mana EDR mampu menginterupsi serangan, sejalan dengan konsep pemecahan rantai serangan yang juga dikemukakan pada penelitian Jain [6] dan Karantzas dkk. [5]. Selain itu, karena sebagian besar serangan modern memanfaatkan *malware* sebagai vektor utama [16], [17], maka pendekatan pengujian berfokus pada simulasi serangan berbasis *malware* dan *backdoor*, yang relevan dengan karakteristik ancaman *endpoint* pada instansi pemerintah.

1. Hasil Pengujian Fase *Delivery*

Pada tahap *delivery*, Elastic EDR berhasil memberikan *prevention malware alert* pada aset host yang telah terpasang elastic-agent. Peringatan tersebut tampil secara otomatis ketika payload berbahaya dikirimkan ke *endpoint*, menandakan bahwa EDR dapat mengenali pola serangan dan menghentikan aktivitas tidak sah sebelum mencapai tahap eksploitasi. Sesuai teori pada studi *malware*, payload yang dikirimkan pada tahap ini umumnya mengandung komponen berbahaya yang dikemas secara *obfuscated* [18]. Meskipun teknik *obfuscation* sering digunakan untuk menghindari deteksi, Elastic mampu mengidentifikasi artefak perilaku mencurigakan karena mekanisme deteksinya berbasis perilaku (*behaviour-based detection*), bukan sekadar signature.

Hasil dashboard Elastic pada port 5601 menunjukkan enam alert yang tercatat pada rentang waktu pengujian, dengan empat alert berkategori *high severity*. Alert tersebut sesuai dengan dua *malicious objective* yang dijalankan saat simulasi serangan. Informasi detail mengenai aktivitas *malware*, perubahan sistem, proses yang dijalankan, serta file yang dimusnahkan menunjukkan bahwa Elastic tidak hanya mendeteksi ancaman tetapi juga mampu mengeksekusi tindakan proteksi secara otomatis, sejalan dengan tujuan EDR untuk memberikan respons *real-time* [8].

2. Deteksi dan Respons pada Tahap Exploitation–Installation



Gambar 2. Elastic Security Alert on Endpoint Interface

Hasil pengujian sebagaimana Gambar 2 menunjukkan bahwa Elastic EDR mampu memutus rantai serangan pada fase *exploitation* dan *installation*, ketika payload mencoba mengeksekusi kode berbahaya dan memperoleh persistensi di sistem korban. Temuan ini konsisten dengan penelitian Karantzas dkk. [5], yang membuktikan efektivitas Elastic dalam mendeteksi serangan berbasis DLL dan CPL injection. Pada penelitian ini, Elastic mampu:

- mencegah eksekusi file berbahaya,
- menghentikan proses *malware*,
- mendeteksi percobaan modifikasi registry atau *persistence key*,
- serta melakukan *file quarantine* terhadap artefak serangan.

Keberhasilan ini memperkuat pernyataan bahwa mekanisme proteksi Elastic berada pada level *multi-layer*, sebagaimana dijelaskan dalam teori EDR yang mencakup pencegahan, deteksi, dan respons dalam satu siklus keamanan [8].

3. Tahap Command and Control (C2) dan Action on Objective

Pada skenario *remote access* berbasis backdoor, Elastic mendeteksi aktivitas komunikasi jaringan tidak lazim yang berpotensi menjadi saluran C2. Alert yang muncul menunjukkan adanya proses yang mencoba membangun koneksi outbound yang tidak dikenal. Hal ini memperlihatkan kemampuan EDR dalam mengidentifikasi pola komunikasi berbahaya, meskipun tahap C2 lebih sulit dideteksi tanpa *rule customization*. Observasi ini sejalan dengan temuan Mulyana [7], bahwa deteksi berbasis log membutuhkan dukungan perilaku untuk memperoleh visibilitas lebih baik terhadap aktivitas jaringan.

Pada tahap *action on objective*, upaya selanjutnya seperti pengumpulan data, enkripsi file, atau modifikasi sistem berhasil diblokir. Hal ini menunjukkan bahwa Elastic EDR mampu mencegah eskalasi serangan sebelum masuk fase kerusakan atau pencurian data yang menjadi ciri APT [8], [14].

4. Interpretasi Hasil terhadap Teori dan Kebutuhan Organisasi

Berdasarkan penelitian yang telah dilakukan dihasilkan tabel pemetaan hasil kapabilitas Elastic EDR yang efektif memotong rantai serangan CKC sebagaimana Tabel 2.

Tabel 2. Pemetaan Cyber Kill Chain (CKC) vs Kapabilitas Elastic EDR

Fase CKC	Attack Vector	Kapabilitas Proteksi Elastic	Outcome
Delivery	Phising Email, USB Drive Insertion	File Reputation Check & Static Analysis saat file ditulis ke disk.	Detected
		Memory Threat Protection (Shellcode injection block) & Behavioral Analysis.	Prevented
Exploitation	Mengunduh Malware	Malware Prevention	Blocked
Installation	Menjalankan program	Rule & Ransomware Protection (Canary files).	
		Network Intrusion Detection (Event network_flow).	Alert
C2	Komunikasi outbound ke server penyerang.		

Dengan demikian, peneliti mengonfirmasi beberapa temuan penting dari telaah pustaka:

- **EDR sebagai solusi proteksi aktif:**
Berbeda dengan pendekatan berbasis SIEM saja [6], [7], Elastic EDR menyediakan proteksi berlapis yang efektif menghadapi serangan *real-time*.
- **Kelemahan antivirus tradisional:**
Antivirus konvensional hanya mampu mendeteksi pola yang dikenal [8], sedangkan Elastic berhasil menangani payload berbahaya yang menggunakan teknik *evasion* dan *obfuscation*.
- **Relevansi CKC untuk menganalisis APT:**
CKC terbukti membantu mengidentifikasi fase kritis yang dapat diputus. Elastic berhasil menginterupsi serangan pada fase *delivery*, *exploitation*, dan *installation*, menandakan bahwa solusi ini efektif untuk mencegah aksi berbahaya sebelum mencapai tujuan akhir serangan.
- **Kesesuaian dengan rekomendasi NIST SP 1800-24 dan NIST CSF:**
Temuan mendukung pentingnya *continuous monitoring* dan proteksi *endpoint* sebagaimana diusulkan NIST [9][10].

5. Analisis Temuan Berdasarkan Cyber Kill Chain

Hasil pengujian menunjukkan bahwa Elastic EDR memiliki efektivitas paling signifikan pada fase *delivery*, *exploitation*, dan *installation*. Pada fase *delivery*, sistem mampu mendeteksi dan mencegah pengiriman payload berbahaya sebelum

berhasil dieksekusi. Pada fase *exploitation* dan *installation*, Elastic EDR berhasil memblokir eksekusi *malware* serta mencegah terbentuknya mekanisme persistensi pada *endpoint*.

Temuan ini mengindikasikan bahwa mekanisme deteksi berbasis perilaku yang diterapkan Elastic EDR lebih adaptif dibanding pendekatan berbasis signature atau log semata, khususnya dalam menghadapi serangan yang menggunakan teknik *evasion*. Dengan memutus serangan pada fase-fase awal, dampak lanjutan pada fase *command and control* dan *action on objective* dapat dicegah secara efektif.

Namun demikian, hasil juga menunjukkan bahwa fase *reconnaissance* dan sebagian aktivitas *command and control* memerlukan penyesuaian aturan deteksi (*rule customization*) agar visibilitas ancaman dapat ditingkatkan. Hal ini menunjukkan bahwa meskipun Elastic EDR menyediakan proteksi dasar yang kuat, optimalisasi kebijakan keamanan tetap diperlukan agar sistem dapat menghadapi variasi teknik serangan yang lebih luas.

Dengan demikian, penelitian ini tidak hanya mengevaluasi kinerja Elastic EDR, tetapi juga menunjukkan bagaimana Cyber Kill Chain dapat digunakan sebagai kerangka evaluasi pertahanan *endpoint* yang relevan untuk menghadapi ancaman siber modern di sektor pemerintahan.

D. Simpulan

Penelitian ini menunjukkan bahwa Elastic Endpoint Security memiliki kapabilitas proteksi yang signifikan dalam memutus rantai serangan berbasis Cyber Kill Chain (CKC). Pengujian yang dilakukan pada lingkungan terisolasi yang merepresentasikan aset organisasi XYZ membuktikan bahwa Elastic EDR mampu menginterupsi serangan pada fase *delivery*, *exploitation*, dan *installation* melalui mekanisme deteksi berbasis perilaku dan respons otomatis. Hasil ini mengonfirmasi keterbatasan solusi tradisional seperti IDPS dan antivirus yang hanya mengandalkan analisis signature dan pemrosesan berbasis log.

Integrasi fungsi SIEM dan EDR dalam Elastic menyediakan visibilitas yang lebih komprehensif terhadap aktivitas *endpoint*, memungkinkan organisasi mendeteksi anomali, memblokir *payload* berbahaya, serta mengurangi waktu respons insiden. Temuan penelitian ini sejalan dengan rekomendasi NIST SP 1800-24 dan NIST Cyber Security Framework yang menekankan pentingnya *continuous monitoring* dan perlindungan *endpoint* sebagai fondasi keamanan siber.

Selanjutnya, mempertimbangkan perkembangan teknologi kecerdasan buatan (AI) juga mendorong munculnya bentuk serangan baru seperti *AI-driven phishing*, otomatisasi eksploitasi kerentanan, hingga *generative malware* yang mampu memodifikasi diri untuk menghindari deteksi. Tren ini menunjukkan bahwa pendekatan pertahanan berbasis perilaku dan attack-chain menjadi semakin relevan. Penelitian lanjutan dapat mengevaluasi kapabilitas Elastic EDR dalam menghadapi serangan yang memanfaatkan AI, atau mengintegrasikan sumber *threat intelligence* berbasis AI sebagai bagian dari mekanisme proteksi adaptif.

Dalam konteks instansi pemerintah yang apabila memiliki keterbatasan anggaran dan kompetensi SDM keamanan TI, Elastic EDR terbukti sebagai solusi yang layak untuk diterapkan. Secara keseluruhan, Elastic EDR dapat menjadi unsur

strategis dalam meningkatkan ketahanan siber sektor pemerintahan dan mendukung upaya penguatan pengelolaan aset kritikal.

E. Referensi

- [1] N. Adi, "Laporan Tahunan Monitoring Keamanan Siber 2021," Report Direktorat Keamanan Siber dan Sandi, Badan Siber dan Sandi Negara, DKI Jakarta, 2021.
- [2] A. Admi dan A. Hakim, "Penerapan Elastic Stack sebagai Tools Alternatif Pemantauan Traffic Jaringan dan Host pada Instansi Pemerintah untuk Memperkuat Keamanan dan Ketahanan Siber Indonesia," JUSTINDO (Jurnal Sistem & Teknologi Informasi Indonesia), vol. 5, no. 2, hlm. 69–77, Feb 2020.
- [3] N Taufik, N Nur, M Hendri, dan A Claudia, "Lanskap Keamanan Siber Indonesia 2022," Badan Siber dan Sandi Negara, DKI Jakarta, hlm. 1–96, 2022.
- [4] S. Slate, "Endpoint Security: An Overview and a Look into the Future," Journal, 2018. Diakses: 5 Desember 2022. [Daring]. Tersedia pada: <https://www.cs.tufts.edu/comp/116/archive/spring2018/sslate.pdf>
- [5] G. Karantzas dan C. Patsakis, "An Empirical Assessment of Endpoint Security Systems Against Advanced Persistent Threats Attack Vectors," Journal of Cybersecurity and Privacy, vol. 1, no. 3, hlm. 387–421, Agu 2021, doi: 10.3390/jcp1030021.
- [6] U. Jain, "Lateral movement detection using ELK stack," M.S Thesis, University of Houston, Houston, 2018.
- [7] M. Nana, "Identifikasi tahapan serangan berdasarkan model Cyber Kill Chain menggunakan elastic stack: studi kasus Lembaga Kebijakan Pengadaan Barang/Jasa Pemerintah," Tesis, Universitas Indonesia, Depok, 2020.
- [8] H. Kim, H. J. Kwon, dan K. K. Kim, "Modified cyber kill chain model for multimedia service environments," Multimed Tools Appl, vol. 78, no. 3, hlm. 3153–3170, Feb 2019, doi: 10.1007/s11042-018-5897-5.
- [9] J. Cawthra dkk., "Securing Picture Archiving and Communication System (PACS) Cybersecurity for the Healthcare Sector," Gaithersburg, MD, Des 2020. doi: 10.6028/NIST.SP.1800-24.
- [10] Liebster Josh, "The NIST CyberSecurity Framework: Detect | 11:11 Innovation Blog," 27 Oktober 2022. <https://1111systems.com/blog/the-nist-cybersecurity-framework-detect/> (diakses 2 Desember 2022).
- [11] Foresster Wave, "Forrester Endpoint Detection and Response Wave | Elastic," Forrester Wave™: Endpoint Detection and Response Providers, Q2 2022, 2022. <https://www.elastic.co/explore/security-without-limits/forrester-edr-wave-2022> (diakses 7 Oktober 2022).
- [12] J. Malleo, "Elastic Recognized in the 2021 Gartner Magic Quadrant for Security Information and Event Management | Elastic," 7 Juli 2021. <https://www.elastic.co/about/press/elastic-recognized-in-the-2021->

gartner-magic-quadrant-for-security-information-and-event-management (diakses 17 Desember 2022).

- [13] S. H. Park dkk., "Performance Evaluation of Open-Source Endpoint Detection and Response Combining Google Rapid Response and Osquery for Threat Detection," *IEEE Access*, vol. 10, hlm. 20259–20269, 2022, doi: 10.1109/ACCESS.2022.3152574.
- [14] P. N. Bahrami, A. Dehghantanha, T. Dargahi, R. M. Parizi, K. K. R. Choo, dan H. H. S. Javadi, "Cyber kill chain-based taxonomy of advanced persistent threat actors: Analogy of tactics, techniques, and procedures," *Journal of Information Processing Systems*, vol. 15, no. 4, hlm. 865–889, 2019, doi: 10.3745/JIPS.03.0126.
- [15] Badan Siber dan Sandi Negara, *Lanskap Keamanan Siber Indonesia 2024*. Jakarta: BSSN, 2024.
- [16] A. Selamat, A. Abdelrahman, dan M. A. Abuagoub, "A Survey on Malwares and Malware Detection Systems A Survey on Malware and Malware Detection Systems," *Int J Comput Appl*, vol. 67, no. 16, hlm. 975–8887, 2013.
- [17] Y. Ilhamdi dan Y. N. Kunang, "Analisis Malware Pada Sistem Operasi Windows Menggunakan Teknik Forensik," dalam *Bina Darma Conference on Computer Science*, 2022.
- [18] Zafar-uz-Zaman, Muhammad, dan Islamabad Section, "Static and Dynamic Malware Analysis Using Machine Learning," dalam *16th International Bhurban Conference on Applied Sciences & Technology (IBCAST)*, Jan 2019.
- [19] S. K. Hobradsch, "A Holistic Methodology for Profiling Ransomware Through A Holistic Methodology for Profiling Ransomware Through Endpoint Detection Endpoint Detection," Ph.D. dissertation, Dakota State University, Washington, 2018. [Daring]. Tersedia pada: <https://scholar.dsu.edu/theses/325>
- [20] A. Dresch, · Daniel, P. Lacerda, J. Antônio, dan V. Antunes, *Design Science Research A Method for Science and Technology Advancement*. Porto Alegre Brazil: Springer International, 2015. doi: 10.1007/978-3-319-07374-3.
- [21] T Scott, *System Analysis And Design*, 12th Edition. Boston, United States of America: Cengage Learning, 2020.