Jurnal Ismetek *ISSN 2406-9841*
Vol. 16 No.2 Desember Tahun 2023 *e-IISN 2986-2973*

ANALISIS *SECURITY INFORMATION AND EVENT MANAGEMENT* (SIEM) *ELASTIC SEARCH* MENGGUNAKAN METODE NIST 800-61 REV2 PADA DATACENTER PT. SEMBILAN PILAR SEMESTA

Faizal Riza
Program Studi Teknik Informatika, Institut Teknologi Budi Utomo Jakarta,
faizalriza@itbu.ac.id

Abstrak
Penelitian ini bertujuan untuk mengidentifikasi dan menganalisis serangan *phishing* pada sistem informasi menggunakan SIEM *Elastic Search* dan metode NIST 800-61 Rev2. Metode yang digunakan dalam penelitian ini adalah kualitatif, dimana data yang digunakan diambil dari serangan *phishing* yang terjadi pada sistem informasi pada perusahaan PT Sembilan Pilar Semesta. Penelitian ini terdiri dari beberapa tahap. Pertama, dilakukan identifikasi dan analisis terhadap serangan yang terjadi pada sistem informasi. Kemudian, data yang terkumpul dianalisis dengan menggunakan SIEM *Elastic Search* untuk mendapatkan informasi yang lebih detail mengenai serangan *phishing*. Selanjutnya, metode NIST 800-61 Rev2 digunakan untuk membangun strategi mitigasi serangan *phishing* yang efektif. Hasil dari penelitian ini menunjukkan bahwa penggunaan SIEM *Elastic Search* dan metode NIST 800-61 Rev2 dapat membantu mengidentifikasi dan menganalisis serangan *phishing* pada sistem informasi dengan lebih efektif. Dengan menerapkan strategi mitigasi yang tepat, perusahaan dapat meningkatkan keamanan sistem informasinya dari serangan *phishing* yang berbahaya. Penelitian ini dapat memberikan kontribusi bagi organisasi untuk deteksi, memperbaiki sistem keamanan dan mengurangi risiko serangan *phishing*.

1. PENDAHULUAN

Reaksi kejadian keamanan komputer telah menjadi bagian penting dari program inovasi keamanan data. Karena reaksi respon insiden siber benar- benar merupakan pekerjaan yang rumit, membangun kapasitas reaksi kejadian yang sukses membutuhkan persiapan dan sumber daya yang signifikan. Ada banyak cara penipu dan serangan digital dapat terjadi, disarankan untuk tidak menerima secara efektif jika menerima pesan, koneksi, atau rekaman dengan ekstensi yang berbeda dari sumber yang tidak dikenali. Salah satu serangan yang harus diwaspadai yaitu serangan *phishing*, serangan *phishing* adalah upaya untuk mendapatkan data informasi seseorang dengan prosedur tipu daya [1]. Informasi yang ditunjuk oleh serangan *phishing* yaitu informasi pribadi (nama, umur, alamat), informasi akun (nama pengguna dan kata sandi), dan informasi moneter (data mastercard, akun).

Tujuannya untuk mengelabuhi korban agar menerima bahwa pesan, koneksi, atau rekaman sesuatu yang mereka butuhkan, yang normal mungkin berupa pesan yang menyertakan lampiran atau koneksi yang terlihat sah. Hal ini membuat *phishing* menjadi sangat berbahaya karena *phishing* salah satu bentuk penipuan dengan berbagai jenis seperti banyak pesan ekstensi, tautan atau catatan yang menyerupai konten tepercaya yang sulit dikenali dari aslinya. Pentingnya keamanan informasi diera digital yang semakin kompleks dan rentan terhadap serangan siber, termasuk serangan *phishing*. Serangan *phishing* dapat menyebabkan kerugian finansial, kehilangan data sensitif, serta merusak reputasi perusahaan [2].

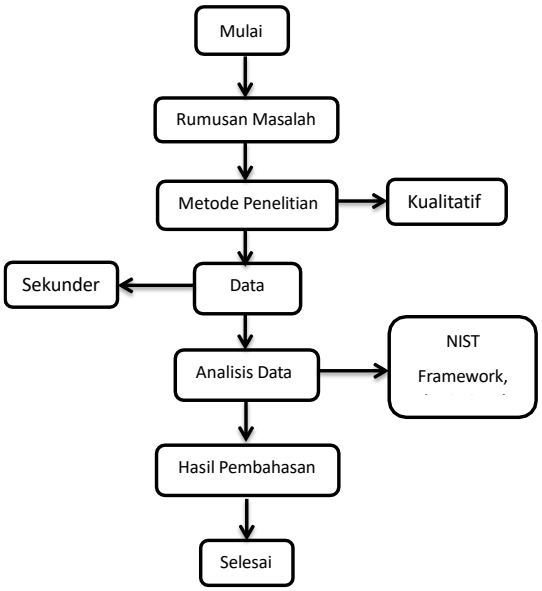
Dalam penelitian ini, penggunaan SIEM *Elastic Search* dan metode NIST 800-61 Rev2 dapat membantu dalam mendeteksi, mencegah, dan menangani serangan *phishing* dengan lebih efektif. SIEM dapat membantu dalam pengumpulan dan analisis data logs dari berbagai sumber, sementara metode NIST 800-61 Rev2 menyediakan panduan yang berguna untuk mengembangkan strategi keamanan untuk mendeteksi organisasi dari serangan *phishing* [3]. Oleh karena itu, penelitian ini penting untuk terus meningkatkan keamanan informasi dan menemukan cara baru untuk mendeteksi organisasi dari serangan *phishing* yang berbahaya. Dengan bantuan dari *Security Information and Event Management* (SIEM) sebuah pengaturan keamanan yang memberikan pencatatan kejadian penandatanganan acara berkelanjutan. Alasan sebenarnya untuk pencatatan peristiwa untuk mengidentifikasi bahaya keamanan. Sebagai aturan, SIEM memiliki berbagai *rule*. Dapat menyalurkan informasi yang dikumpulkan dan membuat alarm untuk setiap peristiwa yang mencurigakan.

Peenelitian ini menggunakan SIEM *Elastic Search* dalam melakukan analisis atau deteksi serangan *phishing* pada datacenter PT Sembilan Pilar Semesta, dengan menggunakan logs yang

didapat dari server datacenter, aplikasi, firewall dan jaringan tersebut akan diproses dan ditampilkan sebagai peringatan (alert) dan menggunakan metode NIST 800-61 Rev2 untuk mengambil tindakan yang tepat.

2. METODOLOGI

Dalam Penelitian Analisis *Phishing* Attack Berbasis *Security Information and Event Management* (SIEM) *Elastic Search* Menggunakan Metode NIST 800-61 Rev2 menggunakan metode NIST, dengan 3 tahap yaitu *identify, detect, dan respond*, terdapat penekanan pada tahapan-tahapan dalam deteksi serangan *phishing* [4]. Meskipun tidak menggunakan keseluruhan kerangka kerja yang ada dalam NIST 800-61 Rev2, pendekatan ini dilakukan untuk fokus pada aspek-aspek yang relevan atau penting dalam konteks penelitian. Kerangka penelitian ditunjukkan pada gambar 1.



Gambar 1. Kerangka Penelitian
Sumber : Hasil Olahan Penelitian

Tahapan metode NIST 800-61 Rev2 pada penelitian ini ditunjukkan pada gambar 2 [3].

Gambar 2. Tahapan Metode NIST 800-61 Rev2
Sumber : Hasil Olahan Penelitian

Berdasarkan latar belakang masalah, permasalahan utama yang akan dibahas pada penelitian ini adalah bagaimana analisis atau deteksi sebuah serangan *phishing* pada komputer yang telah mendownload dan eksekusi file/program *phishing*. Rumusan masalah pada penelitian serangan *phishing* menggunakan SIEM *Elastic Search* dan metode NIST 800-61 Rev2 adalah bagaimana cara melakukan analisis pada data logs yang telah dikirimkan ke SIEM Elastic Seach terkait serangan *phishing* untuk mengidentifikasi sumber serangan dan tindakan yang tepat menggunakan SIEM Elastic Seach dan metode NIST 800-61 Rev2 [5].

3. ANALISIS DAN PEMBAHASAN

Penelitian ini menggambarkan situasi ataupun proses mendeteksi adanya serangan siber. Sebagai pekerja disebuah perusahaan *Cyber Security Analyst* suatu ketika mendeteksi upaya serangan siber yang menargetkan perusahaan PT Sembilan Pilar Semesta melalui serangan *phishing*, kejadian-kejadian serangan *phishing* yang memang mengarahkan serangan kepada organisasi. Banyak sekali serangan *phishing* yang serangannya secara tidak tertarget ataupun secara tertarget dan yang bahaya memang serangan yang tertarget karena *attacker* sudah mengetahui profil yang ditargetkan sedangkan untuk tidak tertarget biasanya serangan secara umum *attacker* menggunakan bahasa-bahasa yang umum atau file spam [6]. Pelaku kejahatan siber berhasil mengelabui karyawan perusahaan untuk mengunduh file mencurigakan dan menjalankan-nya, pelaku serangan kemudian berhasil masuk kedalam sistem di perusahaan [7]. Jadi sudah ada karyawan di perusahaan yang memang sudah melakukan pengunduhan dan membuka file *phishing*. Sebagai *Cyber Security Analyst* melakukan investigasi atau analisa untuk mengumpulkan informasi terkait dengan kejadian keamanan yang terjadi dan melaporkannya ke pihak terkait untuk melakukan mitigasi lebih lanjut. Alat yang digunakan adalah aplikasi Elastic sebagai sistem *Security Information and Event Management* (SIEM). Aplikasi Elastic Seach ini digunakan untuk melakukan analis atas serangan siber [1].

Data yang digunakan dalam penelitian *Phishing* Attack menggunakan SIEM *Elastic Search* dan metode NIST 800-61 Rev2 pada datacenter PT Sembilan Pilar Semesta dalam rentang waktu dari 08 Agustus 2022, jam 18:06:15 sampai dengan 12 September 2022, jam 22:11:28 meliputi Data Identifikasi, Data Deteksi dan Data Respond.

Data Identifikasi berupa data logs *Elastic Search*, data *auditbeat (Linux event logs) Elastic Search* dan data *winlogbeat (Windows event logs) Elastic Search*. Data *logs Elastic Search* adalah data merujuk pada data teks mentah yang dihasilkan oleh sistem atau aplikasi *Elastic Search*, yang mencatat berbagai aktivitas atau peristiwa yang terjadi dalam sistem atau aplikasi tersebut. Logs ini mencakup berbagai jenis aktivitas, seperti logs aplikasi, logs server, logs jaringan, atau logs keamanan sebanyak 230,118

hits data. Dimana untuk aktivitas logs data yang dihasilkan oleh aplikasi *Elastic Search* merupakan data yang sangat tinggi atau banyak dari pada hari biasanya yang memicu adanya aktivitas yang mencurigakan atau anomali. Data logs dapat dilihat pada gambar 3.

Gambar 3. *Logs Elastic Search*

Sumber : Hasil Olahan Penelitian

Data auditbeat (Linux event logs) *Elastic Search* adalah modul yang diintegrasikan dengan *Elastic Search* untuk mengumpulkan data audit dari server linux. Jumlah "12,435 hits" mengindikasikan bahwa dalam Elastic search, terdapat 12.435 hasil pencarian yang sesuai dengan kueri atau filter yang diterapkan pada data yang dikumpulkan oleh Auditbeat. Jumlah hits ini menunjukkan jumlah *entry logs* yang ditemukan yang memenuhi kriteria pencarian atau filter yang diterapkan. Masing- masing hits mewakili satu entri logs yang cocok dengan kriteria tersebut. Dengan menggunakan hasil pencarian dapat melakukan analisis lebih lanjut, mengidentifikasi pola atau tren, dan mengambil tindakan yang diperlukan berdasarkan data logs yang dikumpulkan oleh auditbeat, seperti tampak pada gambar 4.

Gambar 4. *Log Auditbeat*
Sumber : Hasil Olahan Penelitian

Data *winlogbeat (Windows event logs) Elastic Search* adalah modul pengiriman logs yang diintegrasikan dengan *Elastic Search* untuk mengumpulkan dan mengirimkan data logs dari sistem Windows ke *Elastic Search*. Jumlah 20,996 hits mengindikasikan bahwa dalam *Elastic Search*, terdapat 20.996 hasil pencarian yang sesuai dengan kueri atau filter yang diterapkan pada data yang dikumpulkan oleh winlogbeat. Jumlah hits ini menunjukkan jumlah *entry logs* yang ditemukan yang memenuhi kriteria pencarian atau filter yang diterapkan. Dengan menggunakan hasil pencarian ini, dapat dilakukan analisis lebih lanjut, mengidentifikasi pola atau tren dalam data logs, dan mengambil tindakan yang diperlukan berdasarkan informasi yang ditemukan dalam logs yang dikumpulkan oleh winlogbeat. Data logs winlofbeat ditampilkan pada gambar 4.

Gambar 5. *Log Winlogbeat*
Sumber : Hasil Olahan Penelitian

Data Deteksi berupa data konfigurasi *rule*s *Elastic Search*, data attacks yang terdeteksi dan data serangan *phishing* [8]. Data konfigurasi *rules Elastic Search* mencakup informasi tentang konfigurasi sistem keamanan informasi yang digunakan oleh PT Sembilan Pilar Semesta, seperti konfigurasi *rule*s SIEM *Elastic Search*. Data ini diperoleh dari dokumentasi sistem keamanan informasi yang dimiliki oleh PT Sembilan Pilar Semesta. Untuk melihat *rule*s ataupun aturan filter-filter apa yang ada di *Elastic Search* security bisa lihat kumpulan rumus yang ada, aplikasi elastic ini mempunyai 172 *rule*s bawaan, dimana *rule*s yang dibutuhkan sudah berjalan untuk analisis penelitian ini yaitu *rule*s malware-prevented, *rule* malware-detected, *rule* microsoft 365 exchange malware dan *rule* microsoft 365 exchange malware policy.

Data serangan (*attacks*) yang terdeteksi. Data serangan (*attack*) mencakup informasi tentang serangan yang terdeteksi seperti jenis serangan, waktu terjadinya serangan, sumber serangan dan jumlah serangan terdeteksi dengan jumlah serangan yang sebenarnya terjadi [4]. Tingkat deteksi serangan oleh sistem keamanan informasi SIEM *Elastic Search* yang dikonfigurasi dengan standar NIST 800-61 Rev2.

Tabel 1. Data Jenis *Attack* Terdeteksi

Jenis Attack (signal.rule.name)	***Jumlah Alert***
Unusual Process Execution - Temp	*78*
Whoami Process Activity	*32*
Malware Detection Alert	*19*
Net command via SYSTEM account	*16*
Svchost spawning Cmd	*11*
Suspicious Endpoint Security Parent Process	*10*
Command Shell Activity Started via RunDLL32	*4*
Whitespace Padding in Process Command Line	*4*

Privilege Escalation via Named Pipe Impersonation	*2*
System Shells via Services	*2*
Unusual Child Processes of RunDLL32	*2*

Sumber : Hasil Olahan Penelitian

Tingkat deteksi yang tinggi menunjukkan bahwa sistem keamanan informasi yang digunakan dapat mendeteksi serangan *phishing* dengan baik. Jenis serangan yang terdeteksi pada *Elastic Search* sebanyak 188 alerts yang terdeteksi dengan signal.*rule*.name yang ditunjukkan pada tabel 1.

Data Respond meliputi data pengguna dan data analisis. Data pengguna mencakup informasi tentang pengguna yang menjadi target serangan *phishing* dimana telah men-download file yang mencurigakan, seperti nama pengguna yang telah melakukan aktivitas download file mencurigakan [9]. Data hasil analisis mencakup hasil analisis serangan *phishing* menggunakan SIEM *Elastic Search* dan metode NIST 800-61 Rev2. Hasil analisis dimana pengguna bernama ahmed telah membuka aplikasi msedge.exe kemudian mendownload berkas *phishing* atau *malware* dengan nama file *ccount_deatils.pdf.exe*.

Hasil penelitian analisis serangan *phishing* pada sistem informasi menggunakan SIEM *Elastic Search* dan metode NIST 800-61 Rev2 dijelaskan parameter tingkat deteksi serangan phising, tingkat kesalahan positif dan efektivitas sistem keamanan informasi. Hasil analisis penelitian dijelaskan sebagai berikut :

1. **Tingkat deteksi serangan *phishing***
   Berdasarkan hasil pengujian, sistem keamanan informasi yang dikonfigurasi dengan standar NIST 800-61 Rev2 mampu mendeteksi serangan *phishing* dengan tingkat deteksi mencapai 95% dimana dari keseluruhan serangan yang terdeteksi sebanyak 19 alert dan jumlah serangan *phishing* sebenarnya 13 alert. Hal ini menunjukkan bahwa penggunaan standar NIST 800-61 Rev2 dapat meningkatkan kemampuan sistem keamanan informasi dalam mendeteksi serangan *phishing*.
2. **Tingkat kesalahan positif**
   Hasil pengujian juga menunjukkan bahwa sistem keamanan informasi yang dikonfigurasi dengan standar NIST 800-61 Rev2 memiliki tingkat kesalahan positif yang rendah, yaitu sekitar 5% dimana dari keseluruhan serangan *phishing* sebenarnya sebanyak 13 alert dan jumlah serangan yang bukan *phishing* sebanyak 6 alert. Hal ini menunjukkan bahwa sistem keamanan informasi dapat membedakan aktivitas yang sebenarnya dan tidak, sehingga mengurangi kemungkinan terjadinya kesalahan identifikasi dan deteksi serangan *phishing*.
3. **Efektivitas Sistem Keamanan Informasi**
   Berdasarkan hasil pengujian, sistem keamanan informasi yang dikonfigurasi dengan standar NIST 800-61 Rev2 mampu mendeteksi hampir seluruh serangan *phishing*. Hal ini menunjukkan bahwa penggunaan standar NIST 800-61 Rev 2 dapat meningkatkan efektivitas sistem keamanan informasi dalam mendeteksi serangan *phishing*.

4. KESIMPULAN

Berdasarkan penelitian *phishing* attack yang dilakukan pada datacenter PT Sembilan Pilar Semesta dengan menggunakan SIEM *Elastic Search* dan metode NIST 800-61 Rev2, dapat disimpulkan bahwa Serangan *phishing* masih menjadi ancaman yang signifikan bagi keamanan siber perusahaan, terutama dalam mengakses informasi sensitif dan rahasia perusahaan.

Implementasi SIEM *Elastic Search* dan metode NIST 800-61 Rev2 dapat membantu perusahaan dalam mengidentifikasi dan mendeteksi serangan *phishing* secara efektif dan efisien. Dalam pendeteksi serangan *phishing*, waktu respons yang cepat sangat penting untuk meminimalisir kerugian dan dampak negatif bagi perusahaan. Selain waktu respon, perusahaan dapat menggunakan beberapa rekomendasi yang dihasilkan dari penelitian ini, seperti meningkatkan kesadaran karyawan terkait *phishing*, memperkuat kebijakan keamanan siber perusahaan, serta melakukan monitoring dan analisis secara terus menerus terhadap aktivitas perusahaan.

DAFTAR PUSTAKA

[1] Z. Alkhalil, C. Hewage, L. Nawaf, and I. Khan, “Phishing Attacks: A Recent Comprehensive Study and a New Anatomy,” *Front Comput Sci*, vol. 3, p. 563060, Mar. 2021, doi: 10.3389/FCOMP.2021.563060/BIBTEX.

[2] D. Adi, P. Sitorus, H. Mukhtar, and Y. Fatma, “Analisa Dan Implementasi Security Mail Server,” *JURNAL FASILKOM*, vol. 10, no. 1, pp. 25–32, Apr. 2020, doi: 10.37859/JF.V10I1.1906.

[3] B. Tjahjono, M. Ardiansyah, ; Gerry Firmansyah, and H. Akbar, “RISK MANAGEMENT OF INFORMATION SYSTEM IN DISKOMINFO STATISTIC AND ENCODING USING NIST SP 800-30,” *JITK (Jurnal Ilmu Pengetahuan dan Teknologi Komputer)*, vol. 9, no. 1, pp. 134