Jurnal Infortech
Volume 6 No. 1 Juni 2024
E-ISSN: 2715-8160

Penerapan NIST 800-61 REV 2 Untuk Analisa *Ransomware Attack* Pada PT. Sembilan Pilar Semesta Dengan Berbasis SIEM

Julia Ananda Lestari[1], Ghofar Taufik[2*]

[1,2]Universitas Bina Sarana Informatika
e-mail: [1]juliaanandal10@gmail.com, [2]ghofar.gft@bsi.ac.id

Diterima	Direvisi	Disetujui
03-03-2024	05-05-2024	05-06-2024

Abstrak - Di era digital yang semakin maju, keamanan informasi menjadi semakin penting dan harus menjadi prioritas utama bagi organisasi dan perusahaan. Maka dari itu pengetahuan yang baik tentang risiko keamanan informasi yang diperlukan untuk melindungi data penting dan informasi rahasia dari ancaman cyber. Ransomware menjadi salah satu ancaman utama bagi infrastruktur nasional. Penggunaan SIEM atau Security Information and Event Management digunakan untuk mengumpulkan, menganalisis, dan melaporkan aktivitas jaringan yang mencurigakan atau berbahaya. PT Sembilan Pilar Semesta menerapkan Stellar Cyber sebagai sistem manajemen keamanan informasi. Pada penelitian ini akan dibahas tentang penggunaan Stellar Cyber dalam mendeteksi serangan ransomware pada PT Sembilan Pilar Semesta dan menggunakan metode NIST 800-61 Rev 2 untuk analisis dan merespon serangan ransomware. Model NIST 800-61 Rev 2 digunakan untuk membantu organisasi dalam mengidentifikasi serangan ransomware, menangani insiden dengan cepat dan tepat, dan mengurangi dampak dari serangan tersebut. Dengan diterapkannya Stellar Cyber sebagai pendeteksi serangan cyber dan penerapan metode NIST 800-61 rev 2 untuk merspon serangan cyber yang terjadi dapat meminimalisir terjadinya kebocoran data, dan informasi rahasia dari serangan cyber. Hasil dari penelitian ini adalah dapat dilakukan pendeteksian serangan ransomware sekaligus menganalisanya dari mana serangan tersebut muncul. Sekaligus diberikan solusi dalam mengatasi serangan dari ransomware tersebut maupun serangan lainnya (virus, malware dan lainnya)

Kata Kunci: Ransomware, SIEM, Stellar Cyber

Abstract *- In the increasingly advanced digital era, information security is becoming increasingly important and should be a top priority for organizations and companies. Therefore, a good knowledge of information security risks is needed to protect important data and confidential information from cyber threats. Ransomware is one of the main threats to national infrastructure. The use of SIEM or Security Information and Event Management is used to collect, analyze, and report suspicious or malicious network activity. PT Sembilan Pilar Semesta implements Stellar Cyber as an information security management system. This research will discuss the use of Stellar Cyber in detecting ransomware attacks on PT Sembilan Pilar Semesta and using the NIST 800-61 Rev 2 method to analyze and respond to ransomware attacks. The NIST 800-61 Rev 2 model is used to help organizations identify ransomware attacks, handle incidents quickly and appropriately, and reduce the impact of the attack. With the application of Stellar Cyber as a cyber attack detector and the application of the NIST 800-61 rev 2 method to respond to cyber attacks that occur can minimize data leakage, and confidential information from cyber attacks. The result of this research is that it can detect ransomware attacks as well as analyze them from where the attack arises. At the same time, solutions are given in overcoming attacks from ransomware and other attacks (viruses, malware and others).*

Keywords: Ransomware, SIEM, Stellar Cyber

PENDAHULUAN

Perkembangan teknologi informasi yang semakin pesat dan digunakan secara luas dalam berbagai bidang, baik itu dalam bisnis, pemerintahan, maupun kehidupan sehari-hari. Dalam penggunaannya, teknologi informasi memberikan manfaat yang sangat besar, namun pada saat yang sama, juga membawa risiko keamanan yang serius. Di era digital yang semakin maju, keamanan informasi menjadi semakin penting dan harus menjadi prioritas utama bagi organisasi dan perusahaan. Hal ini memerlukan pengetahuan yang baik tentang risiko keamanan informasi dan upaya yang diperlukan untuk melindungi data penting dan informasi rahasia dari ancaman cyber.

"Ransomware Attack merupakan kejadian di mana sebuah organisasi atau perusahaan mengalami serangan malware jenis ransomware yang mengakibatkan data dan sistem komputer mereka

terenkripsi dan diambil alih oleh para pelaku cyber. Ransomware merupakan virus yang menjadi salah satu ancaman utama bagi infrastruktur nasional"(Surya Kusuma et al., 2021). PT Sembilan Pilar Semesta menerapkan Stellar Cyber sebagai sistem manajemen keamanan informasi yang dapat membantu dalam mendeteksi dan mencegah serangan ransomware dengan memantau aktivitas jaringan dan sistem.

"SIEM atau Security Information and Event Management adalah sistem keamanan yang digunakan untuk mengumpulkan, menganalisis, dan melaporkan aktivitas jaringan yang mencurigakan atau berbahaya"(Affandi, 2022) . Metode NIST 800-61 Rev 2 adalah panduan dari National Institute of Standards and Technology (NIST) Amerika Serikat tentang cara mengatasi insiden keamanan informasi. Metode NIST 800-61 Rev 2 dapat menjadi panduan untuk membantu organisasi dalam mengidentifikasi serangan ransomware, menangani insiden dengan cepat dan tepat, dan mengurangi dampak dari serangan tersebut.

Pada penelitian ini menggunakan Stellar Cyber dalam melakukan analisis serangan ransomware pada PT Sembilan Pilar Semesta, dengan menggunakan log yang didapat dari server, aplikasi, firewall dan log tersebut akan diproses dan ditampilkan sebagai peringatan (alert) dan menggunakan metode NIST 800-61 Rev 2 untuk mengambil tindakan yang tepat.

1. *Cybersecurity*

"Cybersecurity adalah serangkaian tindakan yang dilakukan untuk melindungi sistem komputer, informasi, dan jaringan dari cyber attack seperti malware, serangan peretas, dan berbagai jenis tindakan yang mengganggu integritas (integrity), kerahasiaan (confidentiality), serta ketersediaan (availability)" (Prabowo et al., 2021).

2. *Cybercrime*

"Cybercrime adalah tindakan kriminal yang dilakukan secara online melalui komputer atau jaringan internet, seperti pencurian identitas, peretasan sistem, serangan DdoS, penyebaran malware termasuk serangan ransomware"(Rahayu et al., 2021).

3. *Machine Learning*

"Machine Learning adalah salah satu aplikasi Artificial Intelligence (AI) berfokus pada pengembangan algoritma dan teknik untuk membuat program atau sistem komputer yang dapat belajar dan meningkatkan kinerjanya secara otomatis dari pengalaman atau data yang dihadapinya" (Pratama, 2020).

4. *Instrusion Detection System (IDS)*

"Instrusion Detection System (IDS) adalah sistem keamanan komputer menggunakan software atau hardware yang berfungsi untuk mengidentifikasi dan memonitor aktivitas yang mencurigakan atau berpotensi merusak di dalam jaringan atau sistem komputer"(Anis et al., 2022).

5. *Instrusion Prevention System (IPS)*

"Instrusion Prevention System (IPS) adalah sebuah sistem yang dapat mendeteksi yang dirancang untuk mendeteksi, mencegah, dan menghentikan serangan yang mencurigakan atau berbahaya pada jaringan atau sistem komputer" (Wahyudi & Utomo, 2021)

6. *Security Information and Event Management (SIEM)*

"SIEM (Security Information and Event Management) adalah perangkat lunak keamanan yang mengumpulkan log real-time dan melakukan analisis insiden log keamanan dari sumber data perangkat yang berbeda dan beragam tipe log"(Arfanudin et al., 2019).

"SIEM membantu organisasi mengumpulkan dan menganalisis data dari berbagai sumber, termasuk sistem operasi, aplikasi, firewall, dan perangkat jaringan lainnya. Data ini kemudian dianalisis untuk mencari pola atau tanda-tanda yang menunjukkan adanya ancaman keamanan" (Abidian & Andri Setiawan, 2021).

7. *Stellar Cyber*

"Stellar Cyber adalah platform keamanan siber yang dirancang untuk menggabungkan analisis keamanan, deteksi ancaman, dan tindakan respons keamanan ke dalam satu platform" (Liu, 2021) .

XDR Kill Chain (Extended Detection and Response Kill Chain) adalah model yang digunakan untuk menggambarkan serangkaian tahapan yang diikuti oleh serangan siber dan memandu respons keamanan untuk menghentikan serangan tersebut secepat mungkin. XDR Kill Chain bertujuan untuk membantu organisasi meningkatkan kesiapan keamanan mereka dan mengurangi waktu respons terhadap serangan siber.

Sumber: Modul Stellar Cyber(2021)
Gambar 1 XDR Kill Chain

Tabel 1. 1 Tahapan XDR Kill Chain

XDR Kill Chain Stage	*Icon*	*Summary*	*Associated MITRE | ATT&CK Tactics*	*Associated XDR Tactics*	*Classic Attacks*
Initial Attempts		Penyerang mencoba mengakses jaringan Anda.	*Resource Development* *External Credential Access* *Reconnaissance* *Initial Access*	*XDR SBA External* *XDR NBA External* *XDR UBA*	*Port scanning* *External brute force login attempts* *Phishing* *Probes of known security holes*
Persistent Foothold		Penyerang mencoba mempertahankan akses ke sistem Anda terlepas dari teknik *defensif.*	*Persistence* *Execution* *Defense Evasion* *Command & Control*	*XDR EBA External* *XDR Malware* *XDR Intel*	*External trojans* *Account manipulation*
Exploration		Penyerang sedang memeriksa jaringan Anda, mempelajari lingkungan Anda sebelum mengambil tindakan lebih lanjut.	*Collection* *Discovery*	*Internal XDR NBA*	*Internal port scans* *External SQL dumpfiles* *Suspicious SMB copies*
Propagation		Penyerang mencoba mendapatkan hak istimewa tambahan dan mengakses serta mengontrol sistem tambahan di jaringan Anda.	*Internal Credential Access* *Privilege Escalation* *Lateral Movement*	*Internal XDR UBA* *Internal XDR Malware*	*Internal spyware* *Internal trojans* *Internal brute force*
Exfiltration & Impact		Penyerang mencoba mencuri data, berpotensi membuangnya dengan cara yang menghindari deteksi, dan/atau merusak sistem dan data Anda.	*Exfiltration* *Impact*		*Syn floods* *Ransomware File action anomalies*

Sumber: Stellar Cyber(2021)

8. *Malware*

"Malware (Malicious Software) adalah perangkat lunak yang diciptakan untuk melakukan aktivitas berbahaya atau sebagai perusak software" (Manoppo et al., 2020). "Malware dapat berdampak buruk pada sistem, kerusakan data, penyebaran infeksi, dan banyak kerugian lainnya. Ada beberapa jenis malware yang perlu di ketahui yaitu"(Sinambela et al., 2020).

9. *Ransomware*

"Ransomware adalah salah satu jenis perangkat lunak berbahaya yang bertujuan untuk mengunci data korban dengan mengenkripsi data tersebut dan menuntut tebusan untuk memberikan kunci deskripsi dan memulihkan akses data tersebut. Penyebaran ransomware biasanya melalui email phising ataupun web yang sudah diretas"(Fahriza Cholid Fitra, 2022).

"Ransomware Wannacry adalah serangan dunia maya yang ditemukan pertama kali pada 12 Mei 2017, dan skalanya belum pernah ditemukan sebelumnya, dengan penyebaran yang cepat serangan Ransomware Wannacry menginfeksi lebih dari 200.000 komputer dari lebih 150 negara"(Wahidin et al., 2022).

"Ransomware ryuk adalah serangan yang bekerja dengan cara mengidentifikasi jaringan lalu mengenkripsi jaringan serta menghapus shadow copies sehingga sulit untuk diatasi. Ryuk merupakan perangkat lunak berbahaya yang dapat menimbulkan dampak yang sangat merugikan bagi korbannya seperti, meminta tebusan yang sangat besar" (Fahriza Cholid Fitra, 2022) .

10. *Virustotal*

"Virustotal adalah layanan online yang memiliki database setiap virus yang sebelumnya terdeteksi, kegunaan Virustotal ialah untuk mengecek file, URL, IP ini terindikasi malware atau tidak "(Fahriza Cholid Fitra, 2022).

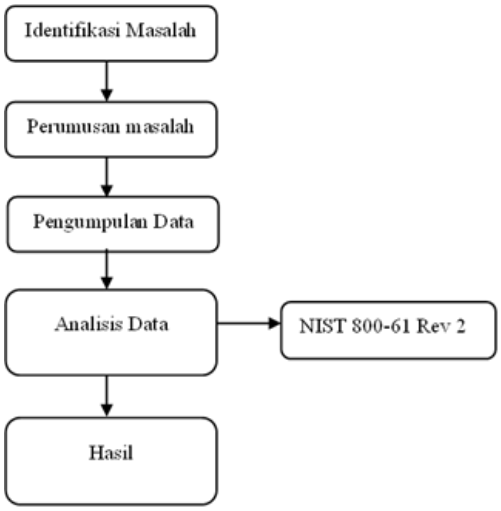
11. *MITRE ATT&CK (Adversary Technique Tactic & Common Knowledge)*

"MITRE ATT&CK (Adversary Technique Tactic & Common Knowledge), yaitu basis pengetahuan yang bisa diakses secara global, dari taktik dan teknik berdasarkan pengamatan dunia nyata. MITRE ATT&CK bertujuan untuk melihat kontras para attacker serta menemukan bagaimana attacker mencari celah keaamanan serta menembus jaringan" (Muhammad Athallariq Rabbani et al., 2020).

METODE PENELITIAN

1. Tahapan Penelitian

Tahapan penelitian mencangkup langkah-langkah pelaksanaan dari awal sampai akhir, adapun langkahnya sebagai berikut :



Sumber: Hasil Penelitian 2023

Gambar 2 Tahapan penelitian

Masing-masing tahapan penelitian diuraikan secara rinci sebagai berikut:

a. Identifikasi Masalah

Pada tahap ini ialah mengidentifikasi masalah yang ada untuk memperoleh pemahaman yang tepat tentang masalah yang dihadapi dan menemukan solusi yang tepat untuk mengatasinya.

b. Perumusan Masalah

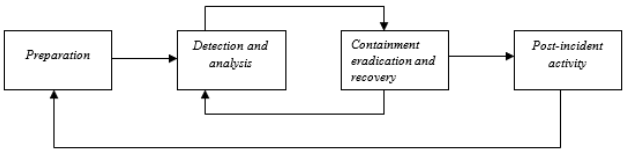
Pada tahap selanjutnya yaitu melakukan perumusan masalah yang berisikan pertanyaan yang jelas dan terstruktur tentang suatu masalah atau topik yang akan diteliti dalam sebuah penelitian untuk memfokuskan penelitian pada masalah yang relevan.

c. Pengumpulan Data

Pada tahap ini peneliti mengumpulkan informasi atau fakta yang relevan. Peneliti melakukan observasi secara langsung di PT. Sembilan Pilar Semesta, lalu melakukan wawancara dengan SOC L2 (Security Operation Center Layer 2) dan Engineer, serta melakukan studi pustaka guna mendapatkan informasi yang diperlukan.

d. Analisis Data

Analisis data dalam penelitian ini menggunakan metode NIST 800-61 Revisi 2 (National Institute of Standards and Technology Special Publication 800-61 Revision 2) yaitu, panduan praktik terbaik yang diterbitkan oleh NIST untuk membentuk suatu organisasi dalam menangani insiden keamanan informasi secara efektif dan efisien.



Sumber: (Whitman & Mattord, 2021)

Gambar 3 Metode NIST 800-61 rev 2

1) *Preparation*: Pada tahap ini peneliti mengidentifikasi sumber daya dan personil yang terlibat dalam respons terhadap insiden keamanan informasi, serta penyusunan rencana respons insiden. Peneliti menentukan rencana respon insiden terkait langkah-langkah menghadapi serangan ramsomware.
2) *Detection and Analysis*: tahap ini melibatkan pendeteksian dan pengumpulan informasi tentang insiden keamanan informasi yang terjadi. Peneliti menggunakan Stellar Cyber untuk mendeteksi serangan ransomware dan melakukan analisis serangan ransomware.
3) *Containment, Eradication, and Recovery*: Tahap ini melibatkan penahanan insiden, pemberantasan penyebab insiden, dan pemulihan sistem dan data. Peneliti menentukan mitigasi yang tepat dalam menangani serangan tersebut. Apabila pada tahap ini mitigasi tidak dapat ditemukan atau diterapkan maka kembali lagi ke tahap Detection and Analysis dan masuk lagi ke tahap Containment, Eradication, and Recovery, pada tahap ke-2 dan ke-3 ini akan terus berulang sampai menemukan mitigasi yang dapat diterapkan.
4) *Post-Incident Activity*: Tahap ini melibatkan analisis proses respons insiden dan mengidentifikasi area manapun untuk perbaikan, serta memperbarui rencana respons insiden dan melatih personel. Peneliti membuat laporan mengenai serangan ransomware dan melakukan evaluasi guna menghindari terjadinya perulangan serangan ransomware. Setelah tahap 4 dilakukan kembali ke tahap 1 untuk mempersiapkan serangan yang akan terdeteksi Kembali.

e. Hasil

Pada tahap ini penulis memaparkan hasil dari analisis alert ransomware yang terdeteksi oleh SIEM Stellar Cyber pada PT. Sembilan Pilar Semesta menggunakan Metode NIST 800-61 Rev 2.

2. Metode Pengumpulan Data, Populasi, Sampel Penlitian

a. Metode pengumpulan Data

"Pada penelitian penulis menggunakan data sekunder yaitu data yang diperoleh dari perusahaan dalam bentuk yang sudah jadi" (Hidayati et al., 2019). Data sekunder dalam penelitian ini adalah data Alert yang terdeteksi Oleh Stellar Cyber.

b. Populasi

"Populasi adalah kelompok atau kumpulan individu, objek, atau kejadian yang menjadi subjek keseluruhan dalam penelitian" (Widiasih et al., 2020). Adapun populasi dari penelitian ini yaitu seluruh alert yang terdeteksi oleh Stellar Cyber dari tanggal 1 Febuari 2023 - 25 Mei 2023 dengan total populasi 47 alert pada PT. Sembilan Pilar Semesta.

Tabel III. 1 Populasi Penelitian

Alert Type	**critical**	**High Fidelity**	**Total**	**Stage**	**Tactic**	**Tags**
Possible Phishing Site Visit from Email	740	740	740	*Initial Attempts*	*Initial Access*	*Network Traffic Analysis, Phishing*
Exploited C&C Connection	20	20	20	*Initial Attempts*	*External XDR NBA*	*Network Traffic Analysis*
File Creation Anomaly	4	4	4	*Persistent Foothold*	*XDR EBA*	
Encrypted C&C	2	2	2	*Persistent Foothold*	*Command and Control*	*Network Traffic Analysis*
External User Login Failure Anomaly	0	0	1	*Initial Attempts*	*External Credential Access*	*External*
External Trojan	0	60	60	*Persistent Foothold*	*External XDR Malware*	*External, Malware*
External URL Reconnaissance Anomaly	0	1	2	*Initial Attempts*	*Reconnaissance*	*External, Network Traffic Analysis*
Internal User Agent Anomaly	0	1	1	*Exploration*	*Internal XDR NBA*	*Internal, Network Traffic Analysis*
External Spyware	0	3	3	*Persistent Foothold*	*External XDR Malware*	*External, Malware*
Internal SYN Flood Victim	0	0	1	*Exfiltration & Impact*	*Impact*	*Internal, Network Traffic Analysis*
Internal Non-Standard Port Anomaly	0	3	3	*Exploration*	*Internal XDR NBA*	*Internal, Network Traffic Analysis*
External Handshake Failure	0	0	3	*Persistent Foothold*	*Reconnaissance*	*External, Network Traffic Analysis*
External Ransomware	0	6	6	*Exfiltration & Impact*	*Impact*	*External, Malware, Ransomware*
External IP / Port Scan Anomaly	0	4	6	*Initial Attempts*	*Reconnaissance*	*External, Network Traffic Analysis*
External User Agent Anomaly	0	243	272	*Initial Attempts*	*External XDR NBA*	*External, Network 50Traffic Analysis*
External Scanner Behavior Anomaly	0	5	7	*Initial Attempts*	*Reconnaissance*	*External, Network Traffic Analysis*
External Plain Text Passwords Detected	0	4	4	*Initial Attempts*	*External XDR NBA*	*External, Network Traffic Analysis*
Internal IP / Port Scan Anomaly	0	6	6	*Exploration*	*Discovery*	*Internal, Network Traffic Analysis*
Sensor Status Anomaly	0	93	93	*Initial Attempts*	*XDR SBA*	*Network Traffic Analysis*
Internal Scanner Behavior Anomaly	0	1	2	*Exploration*	*Discovery*	*Internal, Network Traffic Analysis*
Internal User Login Failure Anomaly	0	2	15	*Propagation*	*Internal Credential Access*	*Internal*
Internal Handshake Failure	0	0	4	*Exploration*	*Discovery*	*Internal, Network Traffic Analysis*
External Non-Standard Port Anomaly	0	206	430	*Persistent Foothold*	*Command and Control*	*External, Network Traffic Analysis*

External Other Malware	0	32	32	*Persistent Foothold*	*External XDR Malware*	*External, Malware*
Internal SYN Flood Attacker	0	0	1	*Exfiltration & Impact*	*Impact*	*Internal, Network Traffic Analysis*
Uncommon Application Anomaly	0	20	115	*Initial Attempts*	*External XDR NBA*	*External, Network Traffic Analysis*
Application Usage Anomaly	0	38	38	*Initial Attempts*	*External XDR NBA*	*External, Network Traffic Analysis*
Outbytes Anomaly	0	3	6	*Exfiltration & Impact*	*Exfiltration*	*Network Traffic Analysis*
Data Ingestion Volume Anomaly	0	92	144	*Initial Attempts*	*XDR SBA*	*Network Traffic Analysis*
Outbound Destination Country Anomaly	0	40	45	*Initial Attempts*	*External XDR NBA*	*External, Network Traffic Analysis*
DHCP Server Anomaly	0	4	4	*Exploration*	*Internal XDR NBA*	*Internal*
Bad Destination Reputation Anomaly	0	0	1	*Persistent Foothold*	*XDR Intel*	*Network Traffic Analysis*
Recently Registered Domains	0	56	56	*Initial Attempts*	*External XDR NBA*	*External, Network Traffic Analysis*
Long App Session Anomaly	0	7	42	*Initial Attempts*	*External XDR NBA*	*External, Network Traffic Analysis*
Private to Private Exploit Anomaly	0	0	1	*Propagation*	*Lateral Movement*	*Internal, Network Traffic Analysis*
External Other Malware	0	32	32	*Persistent Foothold*	*External XDR Malware*	*External, Malware*
Internal SYN Flood Attacker	0	0	1	*Exfiltration & Impact*	*Impact*	*Internal, Network Traffic Analysis*
Uncommon Application Anomaly	0	20	115	*Initial Attempts*	*External XDR NBA*	*External, Network Traffic Analysis*
Application Usage Anomaly	0	38	38	*Initial Attempts*	*External XDR NBA*	*External, Network Traffic Analysis*
Outbytes Anomaly	0	3	6	*Exfiltration & Impact*	*Exfiltration*	*Network Traffic Analysis*
Data Ingestion Volume Anomaly	0	92	144	*Initial Attempts*	*XDR SBA*	*Network Traffic Analysis*
Outbound Destination Country Anomaly	0	40	45	*Initial Attempts*	*External XDR NBA*	*External, Network Traffic Analysis*
DHCP Server Anomaly	0	4	4	*Exploration*	*Internal XDR NBA*	*Internal*
Bad Destination Reputation Anomaly	0	0	1	*Persistent Foothold*	*XDR Intel*	*Network Traffic Analysis*
Recently Registered Domains	0	56	56	*Initial Attempts*	*External XDR NBA*	*External, Network Traffic Analysis*
Long App Session Anomaly	0	7	42	*Initial Attempts*	*External XDR NBA*	*External, Network Traffic Analysis*
Private to Private Exploit Anomaly	0	0	1	*Propagation*	*Lateral Movement*	*Internal, Network Traffic Analysis*

Sumber: Stellar Cyber(2021)

c. Sampel Penelitian

"Sampel penelitian adalah bagian dari populasi yang dipilih untuk dianalisis atau diamati dalam penelitian" (Sahir, 2022). Dalam penelitian ini, penulis dapat menentukan sampel yang representatif dari populasi. Pada penelitian ini penulis menggunakan seluruh populasi sebagai sampel penelitian, yaitu seluruh Alert yang terdeteksi oleh Stellar Cyber pada PT. Sembilan Pilar Semesta.

3. Metode Analisis Data

Metode analisis data yang digunakan dalam penelitian ini adalah sebagai berikut:

a. Mengidentifikasi Indikator Alert

Langkah pertama yang dilakukan adalah mengidentifikasi alert. Indikator alert dapat berupa IP sumber, IP target, port, URL, nama file, tingkat keparahan serangan, dan traffic jaringan yang mencurigakan. Dalam hal ini peneliti dapat menerapkan metode NIST 800-61 rev 2 guna memudahkan peneliti dalam mengindentifikasi indikator alert.

b. Menganalisis Alert

Setelah identifikasi indikator alert, peneliti melakukan analisis dari indikator alert yang terkumpul. Peneliti menganalisis tentang penyebab timbulnya alert external ransomware dan menentukan mitigasi yang tepat untuk menangani serangan tersebut. Untuk memudahkan analisis alert tersebut peneliti menggunakan panduan NIST 800-61 rev 2.

c. Menentukan Tindakan Yang Tepat

Setelah analisis alert dilakukan, peneliti menentukan tindakan yang tepat untuk menangani serangan external ransomware yang terjadi. Tindakan ini didapatkan dari hasil analisis mitigasi.

d. Pemulihan dan Melakukan Report

Setelah penanganan alert tersebut berhasil, langkah selanjutnya adalah pemulihan sistem guna meminimalisir terjadi penyerangan kembali. Lalu peneliti melakukan report guna menjadi catatan untuk objek penelitian.

HASIL DAN PEMBAHASAN

1. Preparation

Pada tahap preparation penulis melakukan persiapan dengan mempersiapkan beberapa daftar sumber daya sebelum terjadinya serangan ransomware seperti:

a. Servers

Server digunakan untuk menghasilkan log dan catatan kejadian yang dapat memberikan petunjuk tentang aktivitas yang mencurigakan atau ancaman yang mungkin terjadi. Stellar Cyber dan server saling terhubung untuk memastikan bahwa data yang relevan dapat diakses, dianalisis, dan diolah dengan baik.

b. End points

End points yang digunakan dalam penlitian ini adalah desktop-1v2lorn, dengan processor 11th Gen Intel(R) Core(TM) i3-1115G4 @ 3.00GHz 3.00 GHz, dan RAM 8,00 GB (7,73 GB usable).

c. Network

Dalam penelitian ini network digunkan sebagai jalur komunikasi perangkat seperti komputer, server, dan perangkat lainnya untuk berinteraksi dan berbagi data.

d. Employess

Anggota tim SOC (Security Operation Center) terdari 13 angota sebagai SOC layer 1, 4 anggota sebagai SOC layer 2, dan 1 anggota sebagai SOC layer 3. Jadi jumlah keseluruhan adalah 18 anggota.

e. Security Products

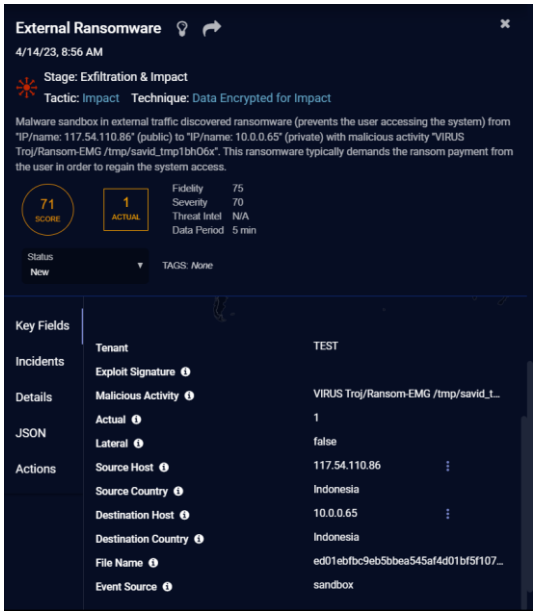
Security products yang digunakan dalam penelitian ini adalah firewall, IDS/IPS, dan Stellar Cyber.

2. Detection and Analysis

a. Indikator Alert

Sebagai mana yang dijelaskan sebelum nya bahwa indikator *alert* meliputi *IP* sumber, *IP* target, *port*, *URL*, nama *file*, tingkat keparahan serangan, dan *traffic* jaringan yang mencurigakan.

1) Alert External Ransomware (Wannacry)



Sumber: *SIEM Stellar Cyber*

Gambar 4 *More Info Stellar Cyber* 1

Dari gambar diatas maka didapati indikator alert sebagai berikut:

Tabel 3 Indikator Alert External Ransomware Wannacry

Nama Event:	External Ransomware
Waktu Deteksi :	14 April 2023, 8:56
Score :	71 (*High*)
IP Sumber :	117.54.110.86 (Indonesia)
IP Target :	10.0.0.65 (Indonesia)
Lateral :	False
File Name :	ed01ebfbc9eb5bbea545af4d01bf5f10716618404804 39c6e5babe8e080e41aa
Md5 :	84c82835a5d21bbcf75a61706d8ab549
Keterangan:	*SIEM Stellar Cyber* mendeteksi adanya *ransomware* dari *IP* 117.54.110.86 menuju *IP* 10.0.0.65 dengan aktivitas berbahaya *VIRUS Troj/Ransom-EMG /tmp/savid_tmp1bhO6x*. Ransomware ini biasanya menuntut pembayaran tebusan dari pengguna untuk mendapatkan kembali akses sistem

Sumber: Hasil Penelitian 2023

2) Alert External Ransomware (Ryuk)

Sumber: SIEM Stellar Cyber

Gambar 5 More Info Stellar Cyber 2

Dari gambar diatas maka didapati indikator alert sebagai berikut:

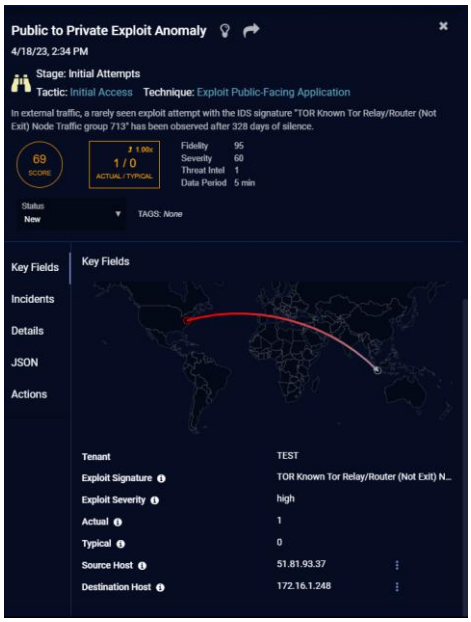
Tabel 3 Indikator Alert External Ransomware Ryuk

Nama Event:	External Ransomware
Waktu Deteksi :	13 April 2023, 12:16
Score :	71 (*High*)
IP Sumber :	117.54.110.86 (Indonesia)
IP Target :	10.0.0.65 (Indonesia)
Lateral :	False
File Name :	23f8aa94ffb3c08a62735fe7fee5799880a8f322ce1d55ec49a13a3f85312db2
Md5 :	5ac0f050f93f86e69026faea1fbb4450
Keterangan:	*SIEM Stellar Cyber* mendeteksi adanya *ransomware* dari *IP* 117.54.110.86 menuju *IP* 10.0.0.65 dengan aktivitas berbahaya *VIRUS Troj/Ransom-FAB*. *Ransomware* ini biasanya menuntut pembayaran tebusan dari pengguna untuk mendapatkan kembali akses sistem.

Sumber: Hasil Penelitian 2023

3) Alert Public to Private Exploit Attempt Anomalies (TOR)

Konsep dasar dari TOR (The Onion Router) adalah menggunakan teknik enkripsi dan pengalihan lalu lintas data melalui beberapa simpul relay agar sulit dilacak. TOR memungkinkan pengguna untuk menyembunyikan identitas dan lokasi mereka dengan mengarahkan lalu lintas internet melalui serangkaian simpul relay yang tersebar di seluruh dunia.



Sumber: SIEM Stellar Cyber

Gambar 6 More Info Stellar Cyber 2

Dari gambar diatas maka didapati indikator alert sebagai berikut:

Tabel 3 Indikator Alert External 1) Alert Public to Private Exploit Attempt Anomalies (TOR)

Nama Event:	Public to Private Exploit Attempt Anomalies
Waktu Deteksi :	18 April 2023, 14:34
Score :	69 (*High*)
IP Sumber :	51.81.93.37 (United States)
IP Target :	172.16.1.248 (Indonesia)
Signature :	*TOR Known Tor Relay/Router (Not Exit) Node Traffic group 713*
Keterangan:	*SIEM Stellar Cyber* mendeteksi adanya *ransomware* dari *IP* 117.54.110.86 menuju *IP* 10.0.0.65 dengan aktivitas berbahaya *VIRUS Troj/Ransom-EMG /tmp/savid_tmp1bhO6x*. Ransomware ini biasanya menuntut pembayaran tebusan dari pengguna untuk mendapatkan kembali akses sistem

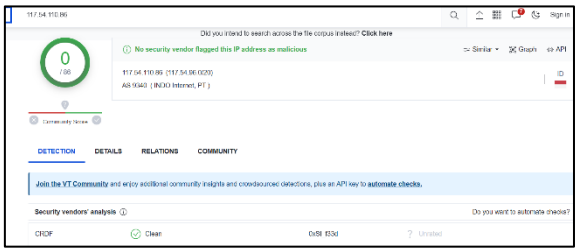
Sumber: Hasil Penelitian 2023

b. Analisis Alert

1) Analisis alert external ransomware (wannacry)

a) Virustotal

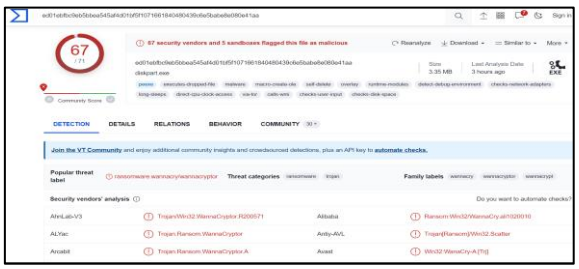
Pemeriksaan Source IP (117.54.110.86), dari hasil pemeriksaan Source IP pada Virustotal, source IP dinyatakan memiliki reputasi yang bagus.



Sumber: Hasil Penelitian 2023

Gambar 7 Hasil Source IP Pada Virustotal

Pemeriksaan Md5 dari hasil pemeriksaan Md5 pada virustotal Md5 dinyatakan memiliki reputasi yang buruk dan terdeteksi sebagai ransomware wannacry. (84c82835a5d21bbcf75a61706d8ab549)

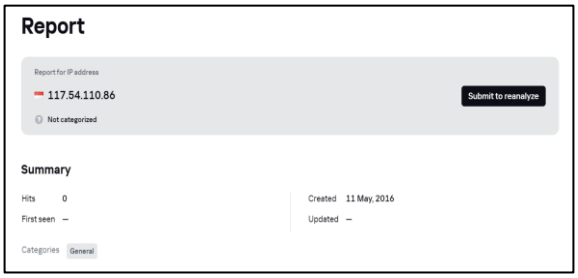


Sumber: Hasil Penelitian 2023

Gambar 8 Hasil Md5 pada Virustotal

b) Kaspersky

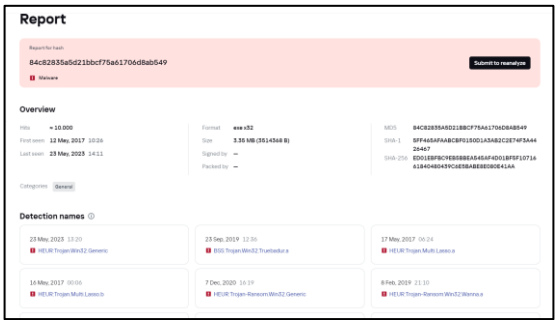
Pemeriksaan Source IP (117.54.110.86), dari hasil pemeriksaan Source IP pada Kaspersky, Source IP dinyatakan memiliki reputasi yang bagus.



Sumber: Hasil Penelitian 2023

Gambar 9 Hasil Kaspersky

Pemeriksaan Md5 dari hasil pemeriksaan Md5 pada Kaspersky Md5 dinyatakan memiliki reputasi yang buruk dan terdeteksi mengandung malware. (84c82835a5d21bbcf75a61706d8ab549)



Sumber: Hasil Penelitian 2023

Gambar 10 Hasil Kaspersky

2) Analisis alert external ransomware (Ryuk)

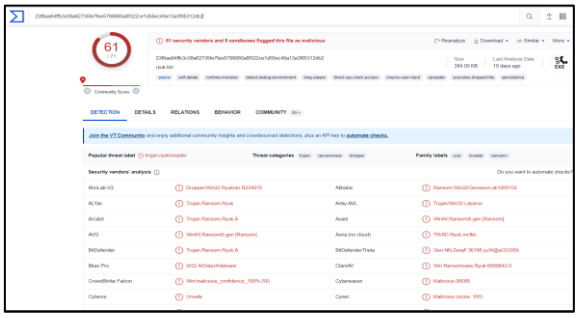
a. Virustotal

Pemeriksaan source IP (117.54.110.86), dari hasil pemeriksaan source ip pada virustotal, source ip dinyatakan memiliki reputasi yang bagus.

Sumber: Hasil Penelitian 2023

Gambar 11 Hasil Virustotal

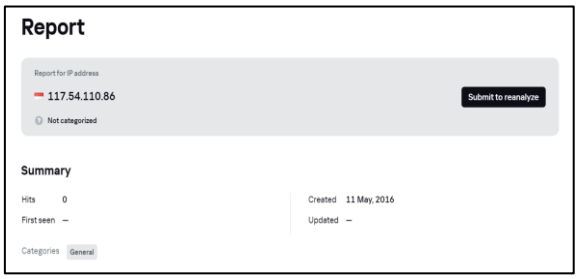
Setelah dilakukan pemeriksaan file, dari hasil pemeriksaan Md5 pada virustotal Md5 dinyatakan memiliki reputasi yang buruk dan terdeteksi sebagai ransomware Ryuk. (23f8aa94ffb3c08a62735fe7fee5799880a8f322ce1d55ec49a13a3f85312db2)



Sumber: Hasil Penelitian 2023

Gambar 12 Hasil Virustotal

b. Kaspersky
Pemeriksaan Source IP (117.54.110.86), dari hasil pemeriksaan Source IP pada Kaspersky, Source IP dinyatakan memiliki reputasi yang bagus.



Sumber: Hasil penelitian 2023
Gambar 13 Hasil Kaspersky

Setelah dilakukan pemeriksaan file, dari hasil pemeriksaan Md5 pada Kaspersky Md5 dinyatakan memiliki reputasi yang buruk dan terdeteksi sebagai ransomware Ryuk. (23f8aa94ffb3c08a62735fe7fee5799880a8f322ce1d55ec49a13a3f85312db2)

Sumber: Hasil Penelitian 2023
Gambar 14 Hasil Kaspersky

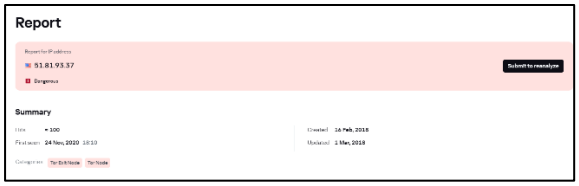
1) Analisis Alert Public to Private Exploit Attempt Anomalies (TOR)

a) Virustotal
Pemeriksaan source IP (51.81.93.37) dari hasil pemeriksaan source ip pada virustotal, source IP dinyatakan memiliki reputasi malware.

Sumber: Hasil penelitian 2023

Gambar 15 Hasil Virus Total

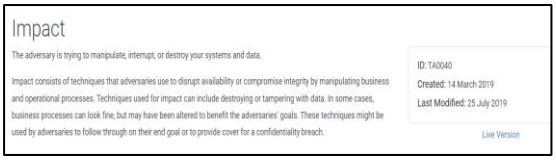
b) Kaspersky
Pemeriksaan Source IP (51.81.93.37), dari hasil pemeriksaan Source IP pada Kaspersky, Source IP dinyatakan memiliki reputasi berbahaya dengan kategori Tor Exit Node dan Tor Node.



Sumber: Hasil Penelitian 2023

Gambar 16 Hasil Kaspersky

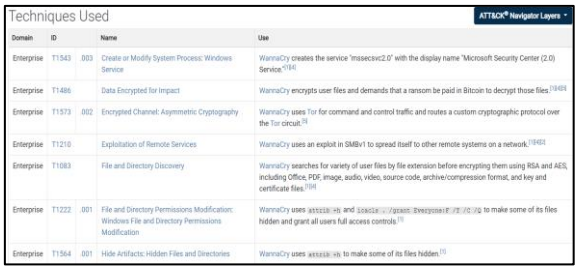
c. TTP (Tactic, Techniques, and Procedure)
1) TTP alert external ransomware (wannacry dan ryuk)
a) Tactic
Taktik yang digunakan pada event external ransomware ini adalah taktik Impact, yaitu attacker berupaya memanipulasi, menyela, atau menghancurkan sistem dan data.



Sumber: Hasil Penelitian 2023

Gambar 17 Taktik External Ransomware

b) Techniques
1. Techniques Wannacry



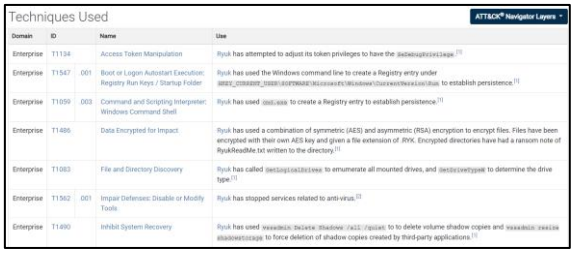
Sumber: Hasil Penelitian 2023

Gambar 18 Teknik Wannacry

Teknik yang digunakan adalah sebagai berikut:

a. WannaCry membuat layanan "mssecsvc2.0" dengan nama tampilan "Microsoft Security Center (2.0) Service.
b. WannaCry mengenkripsi file pengguna dan meminta uang tebusan dibayarkan dalam Bitcoin untuk mendekripsi file tersebut.
c. WannaCry menggunakan TOR untuk perintah dan kontrol lalu lintas dan merutekan protokol kriptografi khusus melalui sirkuit TOR.
d. WannaCry mencari berbagai file pengguna dengan ekstensi file sebelum mengenkripsinya menggunakan RSA dan AES, termasuk Office, PDF, gambar, audio, video, kode sumber, format arsip/kompresi, dan file kunci dan sertifikat.
e. WannaCry menggunakan attrib +hdan icacls . /grant Everyone:F /T /C/Q untuk membuat beberapa filenya disembunyikan dan memberikan kontrol akses penuh kepada semua pengguna.
f. WannaCry menggunakan attrib +h untuk menyembunyikan beberapa file-nya.

2. Techniques Wannacry



Sumber: Hasil Penelitian 2023

Gambar 19 Teknik Ryuk

Teknik yang digunakan adalah sebagai berikut:

a. *Ryuk* telah mencoba menyesuaikan hak istimewa tokennya untuk memiliki *SeDebugPrivilege*.
b. *Ryuk* telah menggunakan baris perintah *Windows* untuk membuat *entri Registry* dibawah *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run* untuk membangun persistensi.
c. *Ryuk* telah digunakan *cmd.exe* untuk membuat *entri Registry* untuk menetapkan persistensi.
d. *Ryuk* telah menggunakan kombinasi enkripsi simetris *(AES)* dan asimetris *(RSA)* untuk mengenkripsi *file*. *File* telah dienkripsi dengan kunci *AES* mereka sendiri dan diberi ekstensi *file* .*RYK*. Direktori terenkripsi memiliki catatan tebusan *RyukReadMe.txt* yang ditulis ke direktori.
e. *Ryuk* telah memanggil *GetLogicalDrives* untuk menghitung semua *drive* yang terpasang, dan *GetDriveTypeW* untuk menentukan jenis *drive*.
f. *Ryuk* telah menghentikan layanan yang terkait dengan *anti-virus*.
g. *Ryuk* telah terbiasa *vssadmin Delete Shadows /all /quiet* menghapus salinan bayangan *volume* dan *vssadmin resize shadowstorage* memaksa penghapusan salinan bayangan yang dibuat oleh aplikasi pihak ketiga.

c) Procedure

1. Procedure Wannacry

Wannacry mengenkripsi file pengguna dan meminta uang tebusan dibayarkan dalam Bitcoin untuk mendekripsi file tersebut

2. Procedure Wannacry

Ryuk telah menggunakan kombinasi enkripsi simetris (AES) dan asimetris (RSA) untuk mengenkripsi file. File telah dienkripsi dengan kunci AES mereka sendiri dan diberi ekstensi file .RYK. Direktori terenkripsi memiliki catatan tebusan RyukReadMe.txt yang ditulis ke direktori tersebut

2) TTP Alert Public to Private Exploit Attempt Anomalies

a. Tactic

Berikut taktik yang digunakan dalam alert Public to Private Exploit Attempt Anomalies

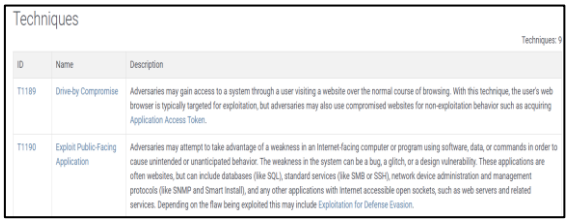
Sumber: Hasil Penelitian 2023

Gambar 20 Taktik Public to Private Exploit Attempt Anomalies

Taktik yang digunakan pada event external ransomware ini adalah taktik Initial Access, yaitu attacker berupaya untuk mendapatkan pijakan termasuk spearphishing yang ditargetkan dan mengeksploitasi kelemahan pada server web publik. Pijakan yang diperoleh melalui akses awal memungkinkan akses lanjutan, seperti akun yang valid dan penggunaan layanan jarak jauh eksternal, atau mungkin penggunaan terbatas karena perubahan kata sandi.

b. Techniques

Berikut Techniques yang digunakan dalam alert Public to Private Exploit Attempt Anomalies



Sumber: Hasil Penelitian 2023

Gambar 21 Teknik Public To Private Exploit Attempt Anomalies

Teknik yang digunakan adalah sebagai berikut:

1. Musuh dapat memperoleh akses ke sistem melalui pengguna yang mengunjungi situs web selama penjelajahan normal. Dengan teknik ini, *browser web* pengguna biasanya ditargetkan untuk dieksploitasi, tetapi musuh juga dapat menggunakan situs web yang disusupi untuk perilaku *non*-eksploitasi seperti memperoleh Token Akses Aplikasi.
2. Musuh mungkin mencoba memanfaatkan kelemahan dalam komputer atau program yang terhubung ke Internet menggunakan perangkat lunak, data, atau perintah untuk menyebabkan perilaku yang tidak diinginkan atau tidak diantisipasi. Kelemahan dalam sistem bisa berupa *bug*, *glitch*, atau kerentanan desain. Aplikasi ini sering berupa situs web, tetapi dapat menyertakan *database* (seperti *SQL*), layanan standar (seperti *SMB* atau *SSH*), administrasi perangkat jaringan dan protokol manajemen (seperti *SNMP* dan *Smart Install*), dan aplikasi lain dengan soket terbuka yang dapat diakses Internet, seperti *server web* dan layanan terkait. Tergantung pada cacat yang dieksploitasi, ini mungkin termasuk *Eksploitasi* untuk Penghindaran Pertahanan .

c. Procedure

Berikut Procedure yang digunakan dalam alert Public to Private Exploit Attempt Anomalies

Sumber: Hasil Penelitian 2023

Gambar 22 Procedure Public to Private Exploit Attempt Anomalies

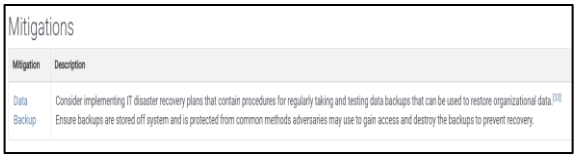
Contoh Prosedur:

1) Telah melakukan serangan injeksi *SQL* terhadap situs web eksternal organisasi.
2) Telah mengeksploitasi *CVE-2019-19781* untuk *Citrix*, *CVE-2019-11510* untuk *VPN Aman Pulse*, *CVE-2018-13379* untuk *VPN FortiGate*, dan *CVE-2019-9670* dalam perangkat lunak *Zimbra* untuk mendapatkan akses.
3) Telah menggunakan injeksi *SQL* untuk kompromi awal.
4) Mengeksploitasi *CVE-2020-10189* melawan *Zoho ManageEngine Desktop Central, dan CVE-2019-19781* untuk mengkompromikan *Citrix Application Delivery Controllers (ADC)* dan perangkat *gateway*
5) telah diamati menggunakan injeksi *SQL* untuk mendapatkan akses ke sistem.

3. Containment Eradication and Recovery

a. Mitigasi Alert External Ransomware

Berikut mitigasi yang dapat di terapkan pada alert external ransomware

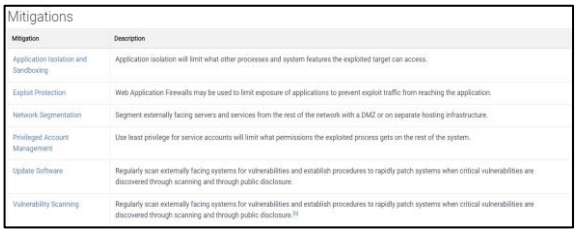


Sumber: Hasil Penelitian 2023

Gambar 23 Mitigasi External Ransomware

Pertimbangkan untuk menerapkan rencana pemulihan bencana TI yang berisi prosedur pengambilan dan pengujian cadangan data secara teratur yang dapat digunakan untuk memulihkan data organisasi. Pastikan cadangan disimpan dari sistem dan dilindungi dari metode umum yang mungkin digunakan musuh untuk mendapatkan akses dan menghancurkan cadangan untuk mencegah pemulihan.

b. Mitigasi Alert Public to Private Exploit Attempt Anomalies



Sumber: Hasil Penelitian 2023

Gambar 24 Mitigasi Public to Private Exploit Attempt Anomalies

Prosedur :

1) Isolasi aplikasi akan membatasi proses dan fitur sistem apa yang dapat diakses oleh target yang dieksploitasi.
2) *Firewall Aplikasi Web* dapat digunakan untuk membatasi pemaparan aplikasi untuk mencegah lalu lintas eksploitasi mencapai aplikasi.
3) Gunakan hak istimewa paling sedikit untuk akun layanan akan membatasi izin apa yang

didapat proses yang dieksploitasi di seluruh sistem.

4) Secara teratur memindai sistem yang menghadap ke luar untuk mencari kerentanan dan menetapkan prosedur untuk menambal sistem dengan cepat ketika kerentanan kritis ditemukan melalui pemindaian dan melalui pengungkapan publik.
5) Secara teratur memindai sistem yang menghadap ke luar untuk mencari kerentanan dan menetapkan prosedur untuk menambal sistem dengan cepat ketika kerentanan kritis ditemukan melalui pemindaian dan melalui pengungkapan publik.

4. *Post-incident activity*

Post-incident activity merupakan serangkain tindakan yang dilakukan setelah terjadi insiden keamanan komputer. Tujuan dari post-incident activity adalah untuk memastikan bahwa insiden telah diatasi dengan benar, mengidentifikasi penyebab insiden, dan mengambil langkah-langkah untuk mencegah terjadinya insiden serupa di masa depan. Berikut beberapa komponen yang digunakan penulis pada tahap Post-incident activity.

a. Lessons Learned

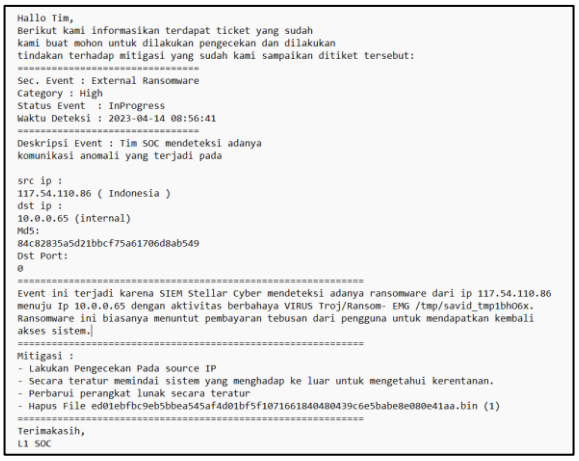
Pada komponen ini penulis melakukan evaluasi insiden guna mengidentifikasi pelajaran yang dapat dipetik:

1) Pentingnya menjaga sistem dan perangkat lunak tetap diperbarui dengan menginstal *patch* keamanan terbaru.
2) Pentingnya memperkuat keamanan jaringan dengan menggunakan *firewall*, deteksi intrusi, *filter email*, dan solusi keamanan jaringan lainnya.
3) Pentingnya memiliki rencana pemulihan bencana yang komprehensif.

b. Membuat Laporan Tindak Lanjut

Laporan digunakan untuk memberitahukan kepada pihak terkait bahwa terjadi event external ransomware dan disimpan sebagai arsip. Berikut laporannya:

1) Laporan Alert External Ransomware (Wannacry)
Berikut adalah contoh report alert external ransomware yang akan dieskalasikan ke layer selanjutnya guna dilakukan pemeriksaan lebih lanjut.

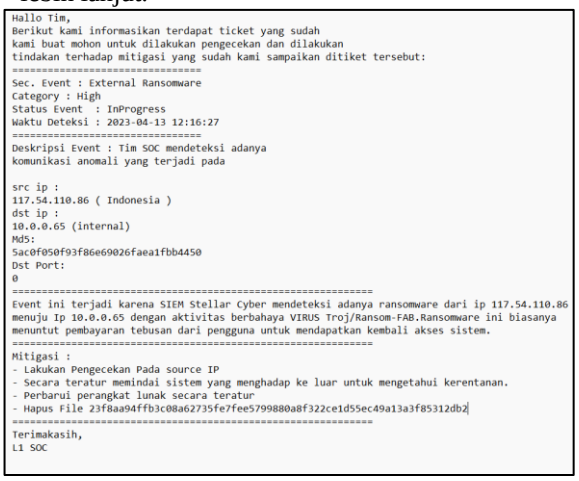


Sumber: Hasil Penelitian 2023

Gambar 25. Laporan 1

Laporan tersebut berisikan beberapa point mengenail alert external ransomware (wannacry) seperti, nama event, waktu deteksi, status event, kategori, IP sumber, IP target, Md5, port target, informasi penyebab munculnya alert external ransomware dan mitigasi yang dapat diterapkan.

2) Laporan Alert External Ransomware (Ryuk)
Berikut adalah contoh report alert external ransomware (ryuk) yang akan dieskalasikan ke layer selanjutnya guna dilakukan pemeriksaan lebih lanjut.



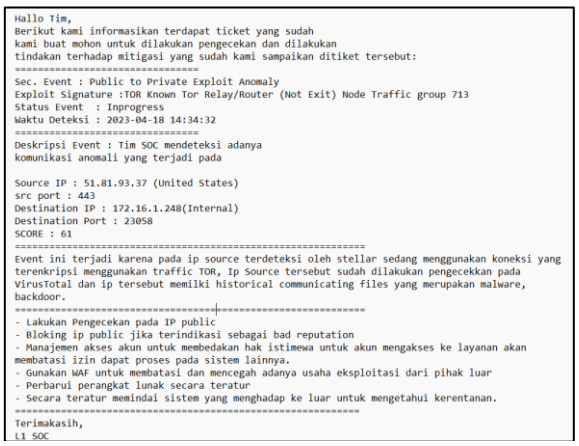
Sumber: Hasil Penelitian 2023

Gambar 26. Laporan 2

Laporan tersebut berisikan beberapa point mengenail alert external ransomware (ryuk) seperti, nama event, waktu deteksi, status event, kategori, IP sumber, IP target, Md5, port target, informasi penyebab munculnya alert external ransomware dan mitigasi yang dapat diterapkan.

3) Laporan Alert Public To Private Exploit Attempt Anomalies

Berikut adalah contoh Alert Public To Private Exploit Attempt Anomalies (TOR) yang akan dieskalasikan ke layer selanjutnya guna dilakukan pemeriksaan lebih lanjut



```
Hallo Tim,
Berikut kami informasikan terdapat ticket yang sudah
kami buat mohon untuk dilakukan pengecekan dan dilakukan
tindakan terhadap mitigasi yang sudah kami sampaikan ditiket tersebut:
================================
Sec. Event : Public to Private Exploit Anomaly
Exploit Signature :TOR Known Tor Relay/Router (Not Exit) Node Traffic group 713
Status Event  : Inprogress
Waktu Deteksi : 2023-04-18 14:34:32
================================
Deskripsi Event : Tim SOC mendeteksi adanya
komunikasi anomali yang terjadi pada

Source IP : 51.81.93.37 (United States)
src port : 443
Destination IP : 172.16.1.248(Internal)
Destination Port : 23058
SCORE : 61
================================================================
Event ini terjadi karena pada ip source terdeteksi oleh stellar sedang menggunakan koneksi yang
terenkripsi menggunakan traffic TOR, Ip Source tersebut sudah dilakukan pengecekkan pada
VirusTotal dan ip tersebut memiliki historical communicating files yang merupakan malware,
backdoor.
========================================+=======================
- Lakukan Pengecekan pada IP public
- Bloking ip public jika terindikasi sebagai bad reputation
- Manajemen akses akun untuk membedakan hak istimewa untuk akun mengakses ke layanan akan
membatasi izin dapat proses pada sistem lainnya.
- Gunakan WAF untuk membatasi dan mencegah adanya usaha eksploitasi dari pihak luar
- Perbarui perangkat lunak secara teratur
- Secara teratur memindai sistem yang menghadap ke luar untuk mengetahui kerentanan.
================================================================
Terimakasih,
L1 SOC
```

Sumber: Hasil Penelitian 2023

Gambar 27. Laporan 3

Laporan tersebut berisikan beberapa point mengenai Alert Public To Private Exploit Attempt Anomalies (TOR) seperti, nama event, waktu deteksi, status event, kategori, IP sumber, IP target, Signature, port target, port sumber informasi penyebab munculnya alert external ransomware dan mitigasi yang dapat diterapkan.

5. Hasil

Hasil yang diperoleh penelitian diatas adalah sebagai berikut:

a. Stellar Cyber tidak hanya mendeteksi serangan ransomware, tetapi dapat mendeteksi serangan lainnya, salah satu contohnya ialah Public To Private Exploit Attempt Anomalies.
b. Serangan ransomware memiliki beberapa kategori namun dengan tujuan yang sama yaitu meminta tebusan kepada target yang terinfeksi serangan ransomware.
c. Layanan online seperti virustotal dan kaspersky dapat digunakan dalam pemeriksaan reputasi sebuah IP, URL, dan file.
d. MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) dapat digunakan dalam menentukan taktik, teknik, dan prosedur (TTP), serta mitigasi penyerangan.
e. Metode NIST 80061-rev 2 dapat diterapkan dalam merespon dan menganalisis serangan ransomware, serta mengurangi dampak yang ditimbulkan dari serangan tersebut.

KESIMPULAN

Dengan menggunakan NIST 800-61 Rev 2 dan *Stellar Cyber*, serangan ransomware dapat dideteksi serta dapat melakukan analisis serangan ransomware yang terjadi sangat cepat melalui kerentanan jaringan atau melalui tautan yang mencurigakan. Sekaligus memberikan solusi penanganan serangan dengan memperkuat keamanan jaringan menggunakan firewall, deteksi intrusi, filter email, dan solusi keamanan jaringan lainnya, serta melakukan backup data sangat penting dilakukan untuk meminimalisir dampak yang ditimbulkan oleh ransomware. Metode NIST 80061-rev 2 memudahkan suatu organisasi dalam merespon insiden keamanan komputer dengan cara yang efisien, efektif dan terkoordinasi. Sehingga memberikan rekomendasi bagi perusahaan mengenai langkah-langkah apa saja yang harus diterapkan dalam menangani dan mengantisipasi serangan *ransomeware* yang sedang berlangsung atau dimasa yang akan datang. Untuk penelitian selanjutnya, menggunakan NIST 800-61 Rev 2 dan *Stellar Cyber* dapat digunakan untuk menedeteksi serangan selain *ransomware* seperti *malware*, *virus* dan lain sebagainya. Atau dengan menggunakan metode dan model selain NIST 800-61 Rev 2 dan *Stellar Cyber* untuk melakukan pendeteksian serangan *ransomware*.

REFERENSI

Abidian, W., & Andri Setiawan, M. (2021). *Implementasi Splunk dalam Membangun Security Information and Event Management Berdasarkan Log Firewall (studi kasus: Jaringan UII)*.

Affandi, M. (2022). *Analisa Security Information and Event Management (Siem) Menggunakan Elastic Stack Siem Dan Splunk Skripsi*. 1–134.

Anis, M., Hilmi, A., & Khujaemah, E. (2022). NETWORK SECURITY MONITORING WITH INTRUSION DETECTION SYSTEM. *Jurnal Teknik Informatika (JUTIF)*, *3*(2), 249–253. https://doi.org/10.20884/1.jutif.2022.3.2.117

Arfanudin, C., Sugiantoro, B., & Prayudi, Y. (2019). *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* (Vol. 2, Issue 1).

Fahriza Cholid Fitra. (2022). *15523095*.

Liu, C. (2021). *Introduction to Stellar Cyber*.

Muhammad Athallariq Rabbani, Avon Budiyono, & Adityas Widjajarto. (2020). Implementasi dan

Analisis Security Auditing Menggunakan Open Source Software Dengan Framework Mitre ATT&CK. *E-Proceeding of Engineering*, *7*(2), 7080–7087.

Prabowo, A., Kaestria, R., Windiarti, I. S., & Sulistyowati, S. (2021). Kerangka Kerja Pelatihan Cybersecurity Untuk Siswa Sekolah Menengah Pertama dan Atas (SMP-SMA). *Jurnal Sains Komputer Dan Teknologi Informasi*, *4*(1), 72–80. https://doi.org/10.33084/jsakti.v4i1.3071

Pratama, R. R. (2020). Analisis Model Machine Learning Terhadap Pengenalan Aktifitas Manusia. *MATRIK : Jurnal Manajemen, Teknik Informatika Dan Rekayasa Komputer*, *19*(2), 302–311. https://doi.org/10.30812/matrik.v19i2.688

Rahayu, S. K., Ruqoyah, S., Berliana, S., Pratiwi, S. B., & Saputra, H. (2021). Cybercrime dan dampaknya pada teknologi e-commerce. *Journal of Information System, Applied, Management, Accounting and Research*, *5*(3), 632. https://doi.org/10.52362/jisamar.v5i3.478

Sinambela, S., Pangestu, A. R., Feriyanto, R., & Komputer, F. I. (2020). *Analisis Aplikasi Malware pada Android dengan Metode Statik*. 2621–4970.

Surya Kusuma, R., Umar, R., & Riadi, I. (2021). Network Forensics Against Ryuk Ransomware Using Trigger, Acquire, Analysis, Report, and Action (TAARA) Method. *Kinetik: Game Technology, Information System, Computer Network, Computing, Electronics, and Control*, *4*. https://doi.org/10.22219/kinetik.v6i2.1225

Wahidin, G. W., Syaifuddin, S., & Sari, Z. (2022). Analisis Ransomware Wannacry Menggunakan Aplikasi Cuckoo Sandbox. *Jurnal Repositor*, *4*(1), 83–94. https://doi.org/10.22219/repositor.v4i1.1373

Wahyudi, F., & Utomo, L. T. (2021). *Edumatic: Jurnal Pendidikan Informatika Perancangan Security Network Intrusion Prevention System Pada PDTI Universitas Islam Raden Rahmat Malang*. *5*(1). https://doi.org/10.29408/edumatic.v5i1.3278

Whitman, M. E., & Mattord, H. J. T. A.-T. T.-. (2021). *Principles of incident response and disaster recovery* (Third edit). Cengage Learning. https://doi.org/LK - https://worldcat.org/title/1241558097