SPIRIT VOL 16 NO 1 (2024) 232 - 245
JURNAL SPIRIT
225/E/KPT/2022

e-ISSN 2721-057X
p-ISSN 2085-3092

TAKSONOMI PERTAHANAN *CYBER SECURITY* MENGGUNAKAN MODEL *CYBER KILL CHAIN*

Slamet[1]
slamet@dinamika.ac.id
Prodi S1 Sistem Informasi [1] (Universitas Dinamika, Surabaya, Indonesia)

Naskah diterima: 2 Mei 2024 ; Direvisi : 25 Mei 2024 ; Disetujui : 25 Mei 2024

Abstrak

Cyber Kill Chain (CKC) telah digunakan secara meluas oleh praktisi keamanan untuk menggambarkan berbagai tahap serangan dan pertahanan *cyber*. Model ini berfokus pada proses penyusupan pada sistem komputer. CKC sering digunakan untuk melindungi jaringan komputer organisasi dengan tahapan-tahapannya adalah: *Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command & Control*, dan *Act on Objectives*. Permasalahannya adalah, evolusi pola serangan dari *intruder* telah berubah, dari cara-cara tradisional menuju cara-cara canggih. Akibatnya pola dari oleh *intruder* makin mudah dilakukan dan makin mudah menerobos pertahanan korban. Untuk itu harus diimbangi dengan pertahanan yang lebih baik, dengan mengkombinasikan antara perangkat analis yang canggih, pemodelan prediktif, dan *cyber kill chain* sebagai model pertahanan *cyber security* organisasi. Hasil dari penelitian ini adalah (a). Persiapan organisasi atau jaringan komputer untuk menghadapi serangan *cyber* dengan menerapkan pendekatan *cyber security* modern di jaringan sendiri. (b). Penerapan kebijakan keamanan di dalam dan di *border* jaringan untuk meningkatkan *cyber security*, dengan solusi mencegah terjadinya kerusakan dan pendeteksian pada serangan yang sedang berlangsung. Dengan demikian, sistem yang diciptakan secara otomatis mendeteksi dan menganalisis perubahan perilaku pengguna dan komputer yang mengindikasikan adanya pelanggaran.

Kata kunci: *Cyber Security, Cyber Kill Chain, Modern Security*

Abstract

The Cyber Kill Chain (CKC) has been widely used by security practitioners to describe the various stages of cyber attacks and defenses. The model focuses on the process of intrusion into a computer system. CKC is used to protect an organization's computer network with its stages being: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command & Control, and Act on Objectives. The problem is, the evolution of attack patterns from intruders has changed, from traditional ways to sophisticated ways. As a result, the attack pattern is easier for intruders to carry out and easier to break through the victim's defense. For this reason, it must be balanced with better defenses, by combining sophisticated analytical tools, predictive modeling, and cyber kill chains as an organizational cyber security defense model. In this research, CKC is used to reveal the status of data breaches. The results of this research are (a). Preparation of organizations or computer networks to face cyber attacks by implementing modern cyber security approaches in their own networks and implementing security policies in border networks. (b). Implementation of security policies to improve cyber security in the network, with solutions to prevent damage and detection of ongoing attacks. Thus, the created system automatically detects and analyzes changes in user and computer behavior that indicate a breach.

Keywords: Cyber Security, Cyber Kill Chain, Modern Security

PENDAHULUAN

Tool-tool pertahanan jaringan konvensional seperti *firewall* [1] dan *antivirus* [2] telah lazim digunakan sebagai model pertahanan dan bahkan telah *embedded* ke dalam sistem operasi sebagai sistem keamanan komputer. *Tools* ini menggunakan pengetahuan statis tentang ancaman dan kerentanan sistem dan dapat mengamati banyaknya serangan yang menimbulkan kebocoran data di dalam komputer.

Di sisi lain, telah terjadi evolusi tujuan [3] dan pemanfaatan *tools* yang canggih dari para *intruder* untuk melakukan serangan *cyber*, sehingga penggunaan *tools* tradisional para praktisi keamanan tidak mampu menandingi kemampuan *tools* dari para *intruder*.

Terjadinya evolusi serangan dari *intruder*, membutuhkan perubahan model pertahanan [4] yang dibangun di atas informasi yang tidak hanya berfokus pada kerentanan, tetapi juga pada ancaman. Mempertahankan elemen-elemen yang lemah dari sebuah sistem, atau mempertahankan sistem sebagai satu kesatuan adalah hal yang penting. Namun yang lebih penting lagi adalah bagaimana mempertahankan diri dari ancaman, dengan cara yang komprehensif tanpa tergantung pada kelemahan sistem.

Saat ini, lebih dari 80% serangan dimulai dengan mencari calon korban [5] secara acak menggunakan *tools* yang banyak tersedia secara gratis di internet. Serangan dengan model acak dapat dilakukan dalam skala kecil dan besar. Serangan tidak selalu dilakukan oleh *intruder* melalui proses pengintaian terlebih dulu. Namun *intruder* seringkali mencoba membobol keamanan secara langsung, dengan mengandalkan kesalahan yang telah dilakukan oleh calon korban (misalnya konfigurasi mesin yang salah, kurangnya *update* aplikasi keamanan atau karena faktor kelalaian manusia).

Serangan-serangan ini biasanya dimulai dengan *phishing* secara massal ke media sosial, internet, email atau *platform* lain [6]. *Intruder* tidak selalu melakukan persiapan yang komprehensif untuk melakukan serangan. *Intruder* bisa meminta korbannya untuk menginstall *malware*, berharap calon korban terpancing dan menginstall aplikasi *malware* ke komputernya [7].

Untuk mengurangi probabilitas setiap percobaan serangan secara signifikan, terdapat teknik pertahanan yang lebih baik dari cara konvensional, yaitu teknik pertahanan jaringan yang menggunakan pengetahuan tentang lawan, pemodelan ancaman, dan skenario-skenario serangan [8].

Untuk itu dalam paper ini digunakan model *cyber kill chain* [9] untuk memahami tujuan dan metode serangan sehingga para para praktisi kemanan, seperti *Computer Security Incident Respons Team* (CSIRT) [10] lebih mudah mengidentifikasi jenis serangan dan menentukan metode pertahanan *cyber* yang tepat bagi organisasi.

Untuk memahami bagaimana serangan komputer dilakukan dan bagaimana bereaksi secara tepat terhadap setiap serangan, maka proses serangan perlu dianalisis pada tahapan-tahapan keberadaannya. Tiap tahap dari serangan komputer adalah sebuah rantai sebab akibat, yang disebut sebagai *cyber kill chain*.

Di dalam *cyber kill chain*, serangan yang efektif (yang bisa mengakibatkan pencurian data) merupakan sebuah rangkaian peristiwa: dari fase identifikasi awal, yang bertujuan untuk mengenal korban dengan cara meretas aliran data dalam jaringan komputer, penggunaan kerentanan, dan infeksi pengendalian sistem. Analisis dilakukan di setiap peristiwa untuk mendapatkan pengetahuan dan menggunakan pengetahuan ini untuk memutus rantai serangan sedini mungkin[11].

Semakin komprehensif dalam menganalisis kejadian-kejadian ini, semakin banyak hal yang dapat dipelajari dari *intruder*. Deteksi serangan yang tepat menjadi kunci pertahanan terbaik.

METODE

Untuk mencapai tujuan penelitian, beberapa tahapan yang dilakukan adalah (a). Mempersiapkan sistem pertahanan organisasi, (b). Mendeteksi terjadinya insiden dan mencegah terjadi serangan *cyber*, dan (c). Menentukan implementasi model pertahanan terbaik, setelah mendapatkan hasil analisis dari tahap a dan b.

3.1. Persiapan Sistem Pertahanan

Pada tahap ini dilakukan pemahaman terhadap sistem keamanan dan bagaimana serangan komputer dapat dipahami oleh tim keamanan (CSIRT) [10] organisasi. Hal pertama yang dilakukan adalah merencanakan arsitektur keamanan yang dapat mendeteksi serangan dan mengidentifikasi tempat yang akan menjadi target serangan[12].

Perencanaan ini digunakan untuk memudahkan pemilihan tindakan dan pertahanan seperti pemilihan cara dan *tools* yang digunakan. Tujuan utamanya adalah untuk memutus rantai serangan pada setiap tahap *kill chain*.

3.2. Mendeteksi Insiden dan Mencegah Serangan

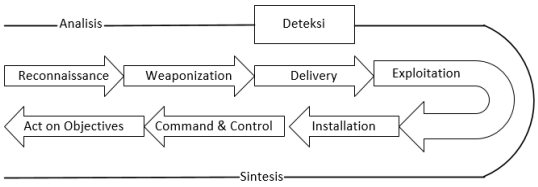
Setelah disiapkan model pertahanannya, tahap kedua adalah mendeteksi adanya insiden keamanan yang dapat mencegah terjadinya serangan lebih parah.

Langkah-langkah yang diambil bergantung pada insiden yang terjadi. Model serangan komputer yang dilakukan menggunakan skenario serangan umum, seperti serangan DDOS [21], *phising* [17][22][23], *Man In The Middle Attack* [24] dan serangan *malware* [25].

Pada tahap ini, dilakukan deteksi terjadinya insiden, kemudian dilakukan analisis keamanan berdasarkan informasi dari sistem pertahanan. Dengan demikian dapat ditentukan lokasi dari fase insiden itu terdeteksi.

Percobaan penelitian dilakukan sebanyak dua kali dimana proses deteksi dan pencegahan serangan adalah representasi terjadi di fase awal dan representasi terjadi di fase akhir dari tahapan *cyber kill chain*.

Dalam percobaan pertama, proses deteksi dan pencegahan serangan dilakukan pada fase *delivery* dari tahapan *cyber kill chain*, sebagaimana terlihat pada gambar 2.

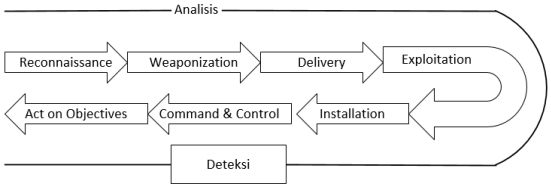


Gambar 2. Deteksi Serangan pada fase *Delivery* dalam *Cyber Kill Chain*

Apabila serangan terdeteksi pada tahap awal, misalnya terjadi pada fase *delivery*, maka analisis dan sintesis yang terjadi dilakukan pada tahap *delivery* sampai dengan *action on objective*. Analisis dan sintesis digunakan untuk mengetahui langkah dan metode yang akan digunakan oleh *intruder* dalam meretas dan menginstal sistem kerusakan kepada korban. Sintesis didapatkan setelah membangun pengetahuan tentang taktik dan *tool* yang digunakan oleh *intruder*.

Analisis dan sintesis dilakukan dengan mengumpulkan informasi sebanyak-banyaknya tentang *intruder*, sehingga dapat ditentukan vektor serangan berisi kerentanan-kerentanan yang dapat merusak infrastruktur.

Pada percobaan kedua, proses deteksi dan interupsi serangan dilakukan pada fase *Command and Control*.



Gambar 3. Deteksi Serangan pada fase *Command and Control*

Sebagaimana terlihat pada gambar 3, jika fase serangan terjadi di fase akhir pada *Command and Control*, maka langkah-langkah prosedur penanganan insiden (seperti menghentikan serangan, membatasi ancaman dan memulihkan

insiden) dilakukan dengan menganalisis seberapa jauh serangan telah terjadi di tahapan *Reconnaissance* sampai *Command and Control*.

Analisis yang dilakukan menjawab pertanyaan-pertanyaan: (a). Mengapa penyerang bisa mencapai tempat yang begitu jauh, (b). Perangkat dan prosedur apa saja dari infrastruktur yang ikut serta dalam serangan tersebut, dan (c). Elemen mana yang seharusnya bekerja dan melindungi organisasi dalam serangan ini.

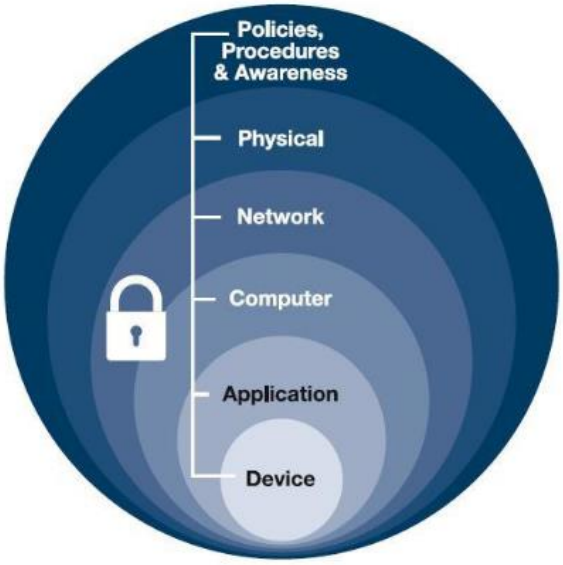
3.3. Implementasi Pertahanan Terbaik

Pada tahap terakhir ditentukan model pertahanan terbaik, berdasarkan apa yang sudah dilakukan pada tahap (a). persiapan pertahanan dan tahap (b). pendeteksian dan pencegahan serangan.

Tujuan dari tahap ini adalah mendapatkan *tool-tool* dengan kinerja dan ketersediaan yang tinggi serta perangkat kebijakan yang dapat menangani tugas dalam mendeteksi dan mencegah terjadinya serangan.

4. Hasil dan Pembahasan

Untuk dapat mengganggu atau menghambat serangan secara signifikan, pertama disiapkan desain infrastruktur yang memperhitungkan kebutuhan keamanan organisasi. Metode yang digunakan untuk mendesain sistem keamanan adalah *Defense in Depth* [26].



Gambar 4. ***Defense in Depth*** **(DiD)**
(Sumber www.networkaccess.com)

Defense in Depth (DiD) adalah strategi yang memanfaatkan berbagai langkah keamanan untuk melindungi aset organisasi secara holistik, mulai dari *device*, aplikasi, komputer, dan jaringan yang digunakan. Selain itu juga penyiapan fisk organisasi dan berbagai kebijakan, prosedur dan *awareness* organisasi. Konsepnya adalah bahwa jika satu garis pertahanan dikompromikan, lapisan tambahan ada sebagai cadangan untuk memastikan bahwa ancaman dihentikan di sepanjang jalan.

DiD membahas kerentanan keamanan pada perangkat keras, perangkat lunak dan pada manusia, karena kelalaian atau kesalahan manusia sering kali menjadi penyebab pelanggaran keamanan.

Dengan strategi DiD, dipersiapkan infrastruktur yang dapat melawan serangan di dalam organisasi. Infrastruktur pertahanan digunakan untuk menetapkan sasaran kinerja peralatan, prosedur, kebijakan dan kinerja pelaku (orang), untuk tugas-tugas seperti:

(a). Mendeteksi serangan dan mendiagnosis skenario dengan benar untuk mengambil langkah menetralisir serangan dari sistem keamanan untuk tujuan pertahanan. Proses mendeteksi dan mendiagnosis serangan menggunakan *Host Intrusion Detection System* (HIDS), *Network Intrusion Detection System* (NIDS), *firewall, antivirus*, penganalisis *log*, penganalisis trafik jaringan, *Security Information and Event Management* (SIEM), kontrol integritas *file*, dan sistem komputer pengguna yang sudah kuat keamanannya.

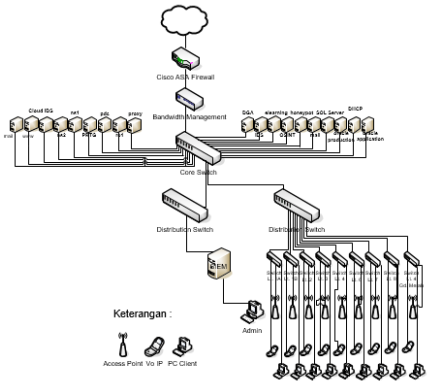
(b). Pencegahan untuk menangkal serangan, menggunakan *Intrusion Prevention System*, *scan lock*, *firewall*, *Access Control List* (ACL), uji penetrasi, penyamaran *code*, konfigurasi khusus, *update* kerentanan dan ketersediaan, dan penerapan kebijakan keamanan informasi yang baik.

(c). Mengacaukan serangan, dengan menggunakan solusi teknis yang bisa menghalangi serangan computer. Metode yang digunakan adalah *hardening* sistem, menggunakan komputer sebagai perangkap jaringan (*honeypot, honeynet*), dan menentukan batasan kesesuaian koneksi (berdasarkan *protocol, port, IP address*) atau basis data tertentu.

(d). Melemahkan serangan, dengan penolakan serangan terhadap akses DDoS, http, FTP. Teknik yang digunakan untuk menyelesaikan tugas ini adalah perubahan konfigurasi untuk mempersingkat *time session* (*waiting time* yang singkat), kebijakan yang menghalangi masuknya layanan (batasan waktu, batasan untuk pengguna yang berbeda).

(e). Menghalangi serangan dengan menipu *intruder*. Caranya adalah dengan mengelabui *intruder* atau memaksa asumsi yang salah tentang sistem, sehingga menghasilkan pemilihan vektor serangan yang tidak efektif. Alat-alat yang digunakan mengelabui seperti *honeypot*, pengaburan *code* dari aplikasi, restorasi informasi aplikasi *server*, atau membuat konfigurasi yang salah.

Sedangkan bentuk (contoh) infrastruktur jaringan yang dapat digunakan, seperti terlihat pada gambar 5.



Gambar 5. Infrastruktur Jaringan yang diimplementasikan dengan Konsep Pertahanan DiD

Sedangkan solusi-solusi teknis lainnya pada tahapan *cyber kill chain* dapat dilihat pada tabel 1 sampai dengan tabel 7.

Deteksi Serangan	Cegah Serangan	Ganggu Serangan	Pelemahan Serangan	Kelabui Serangan
• IDS • Honeypot • *Web Analytics*	• IPS • Port *scanning* • Firewall • Access Control List	• HoneNet • *Connec* • *tions Limit* • *Data limit* • IPS	• *Timeout*	• Honeypot • *Version obfuscating*

Tabel 1. Solusi teknis untuk pertahanan pada tahap *Reconnaissance*

Deteksi Serangan	Cegah Serangan	Ganggu Serangan	Pelemahan Serangan	Kelabui Serangan
• *Threat information sharing* • *Vulnerability intelligence* • NIDS	• *Threat information sharing* • *Penetration Testing* • *Application obfuscation* • *System and application patching* • *Version hidden* • NIPS	• *Hardening* • *Version obfuscation*	• *Application obfuscation* • *Unused service disabling*	

Tabel 2. Solusi teknis untuk pertahanan pada tahap *Weaponization*

Deteksi Serangan	Cegah Serangan	Ganggu Serangan	Pelemahan Serangan	Kelabui Serangan
• IDS • Firewall • *Network analysis users*	• Network IPS • Firewall • Port *Knocking* • ACL mengubah setting pabrik • *Network traffic disable* • Proxy	• *Hardening* • *In-line* AV	• *Mandatory* • *Integrity*	• Honeypot

Tabel 3. Solusi teknis untuk pertahanan pada tahap *Delivery*

Deteksi Serangan	Cegah Serangan	Ganggu Serangan	Pelemahan Serangan	Kelabui Serangan
• HIDS	• Local sandbox • *System and application update*	• *Hardening* • DEP	• *Configuration auto rollback*	• Honeypot

Tabel 4. Solusi teknis untuk pertahanan pada tahap *Exploitation*

Deteksi Serangan	Cegah Serangan	Ganggu Serangan	Pelemahan Serangan	Kelabui Serangan
• HIDS • IP Sonar • *Integrity check* • *Configuration check*	• *App whitelisting* • Host IPS • Jail (chroot)	• *Hardening* • AV	• *Configuration auto rollback* • Tarpit	• Honeypot • DNS *redirect*

Tabel 5. Solusi teknis untuk pertahanan pada tahap *Installation*

Deteksi Serangan	Cegah Serangan	Ganggu Serangan	Pelemahan Serangan	Kelabui Serangan
• NIDS • SIEM • TI *Feed*	• *Whitelisting* FW • ACL	•NIPS	• QoS	• Honeypot

Tabel 6. Solusi teknis untuk pertahanan pada tahap *Command and Control*

Deteksi Serangan	Cegah Serangan	Ganggu Serangan	Pelemahan Serangan	Kelabui Serangan
Log Analysis				

Tabel 7. Solusi teknis untuk pertahanan pada tahap *Act on Objectives*

4.2 Hasil Deteksi insiden dan Interupsi Serangan

Yang pertama, apabila serangan terdeteksi pada fase *delivery* (tahap awal), maka analisis dilakukan di awal, selanjutnya dilakukan sintesis pada fase berikutnya dari tahapan *kill chain*. Sintesis dilakukan untuk mengetahui langkah yang dilakukan dan metode yang ingin digunakan oleh *intruder* untuk meretas dan menginstal sistem selanjutnya.

Hasil dari sintesis adalah membangun pengetahuan tentang taktik dan *tools* yang digunakan *intruder*. Pengetahuan ini memberikan perlindungan keamanan untuk mempertahankan dari serangan.

Dengan melakukan analisis dan sintesis, ditemukan vektor serangan, kerentanan yang merusak infrastruktur, dan dikumpulkan informasi sebanyak-banyaknya tentang *intruder*. Informasi ini digunakan untuk menentukan indikator kompromi (*indicator of compromise*/IoC), yang dapat meningkatkan garis pertahanan *cyber*.

Yang kedua, apabila deteksi dan analisis insiden dilakukan di tahap akhir (*command and control*), maka didapatkan efektivitas dalam menilai pertahanan *cyber*, seperti bagaimana *malware* melewati garis pertahanan, dimana terdapat informasi tentang kelemahan sistem.

Pada percobaan ini digunakan aplikasi *Open Source* Zenarmor untuk mendeteksi dan mendapatkan perlindungan yang efektif terhadap serangan, baik itu di fase "*Delivery*" atau "*Command and Control*". Zenarmor kompatibel dengan *firewall* berbasis BSD seperti OPNsense dan pfSense.

Zenarmor menggunakan pertahanan intelijen berbasis *Cloud Artificial Intelligence* dalam menghentikan *malware zero-day* dan serangan *phishing* secara *real time*. Zenarmor dapat mendeteksi dan memblokir *botnet* baru, memeriksa konten lebih mendalam untuk mencegah ancaman dan tidak melakukan *bypass* penyaringan berbasis IP, port, dan DNS.

Langkah-langkah yang dicontohkan pada gambar 6 adalah deteksi yang dilakukan pada fase "*Command and Control*". Sedangkan apabila memilih fase *Delivery*, dapat dilakukan dengan mengganti pilihan: *Block* Opsi *Botnet Delivery* dalam *Advanced Security*. *Login* Zenconsole, Pilih *Zenconsole* > *My Firewalls*. Kemudian pilih *Policies* > *Default* > *Security*. *Block* Opsi *Botnet Command and Control* dalam *Advanced Security*. Lakukan *Synchronize the Policy*.

Gambar 6 adalah mendeteksi dan mencegah serangan *Command and Control* pada Zenarmon. Sedangkan *rule (policy)* untuk mendeteksi dapat dilihat pada

Gambar 6. Mendeteksi dan Mencegah Serangan pada fase *Command and Control*

gambar 7. Untuk hasil pendeteksian dan pencegahan dapat dilihat pada gambar 8.

4.3 Realisasi Implementasi Pertahanan Terbaik

Berdasarkan hasil deteksi insiden dan langkah-langkah sebelumnya, ditemukan dan ditentukan model pertahanan terbaik, berupa implementasi kebijakan dan teknis terbaik.

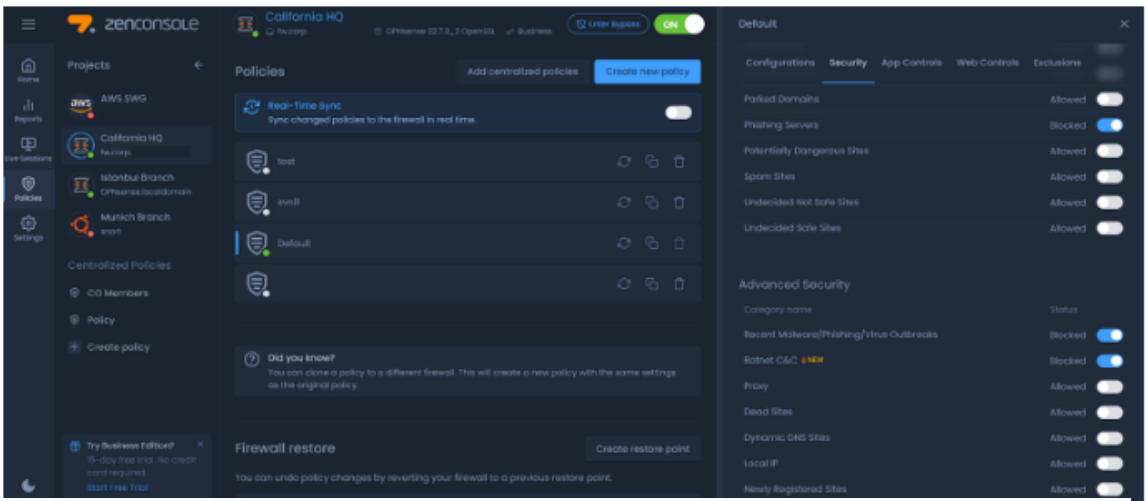
4.3.1 Implementasi kebijakan pada tahapan-tahapan "*cyber kill chain*" adalah:

1. *Reconnaissance*

a. Memeriksa trafik jaringan untuk mendeteksi dan mencegah *port scanning*.
b. Menyaring URL untuk mendeteksi pengalihan ke situs berbahaya.

2. *Weaponization*

3. *Delivery*



Gambar 7. Pengaturan Trafik *Rule* Deteksi Serangan pada fase *Command and Control*

Gambar 8. Dashboard Deteksi Serangan pada fase *Command and Control*

Memeriksa trafik jaringan (termasuk SSL) dan memblokir aplikasi yang dianggap berisiko.

a. Melindungi semua *end point* termasuk infrastruktur *Virtual Private Network* (VPN).
b. Memblokir komunikasi terhadap URL yang mencurigakan dan berisiko.
c. Memblokir kemampuan untuk mengirim *malware* yang diketahui, menggunakan mekanisme perlindungan seperti *Intrusion Prevention System*, *antimalware*, pemantauan lalu lintas DNS dan pemblokiran file.
d. Memblokir ancaman melalui analisis *online* menggunakan *WildFire*.

4. *Exploitation*

a. Memblokir ancaman, melalui analisis *online* menggunakan *WildFire*.
b. Mengendalikan aplikasi yang dapat mengakses aplikasi lain atau alat yang tidak dikenal.

5. *Installation*

a. Melindungi eskalasi izin lokal pada perangkat *endpoint* yang terhubung ke *firewall* pusat.
b. Melindungi pencurian data sensitif seperti *password* dan data-data pribadi.
c. Mengimplementasikan model *Zero-Trust* untuk menciptakan zona aman dengan hak akses yang dikendalikan secara ketat dan memantau lalu lintas antar/inter zona.
d. Mengontrol aplikasi untuk mengakses aplikasi dan alat yang tidak dikenal.

6. *Command & Control*

a. Memblokir komunikasi pengiriman ke *server Command and Control*.
b. Memblokir komunikasi terhadap URL yang mencurigakan dan berisiko.
c. Memblokir teknik serangan baru, dengan mendeteksi jenis aplikasi secara independen dari port.
d. Mengimplementasikan *honeypot* untuk mengarahkan trafik jaringan yang mencurigakan ke perangkap lokal dan analisis malware.
e. Mengendalikan permintaan DNS dengan membangun basis data terkait alamat dan *domain* berbahaya untuk melindungi perangkat lain.

7. *Act on Objectives*

a. Memblokir komunikasi pengiriman ke *server Comand and Control*.
b. Kebijakan mengurangi kebocoran data dengan mendeteksi arah transmisi yang tidak biasa.
c. Memblokir komunikasi terhadap URL yang mencurigakan dan berisiko.
d. Mendefinisikan kebijakan dan hak untuk mentransfer file ke saluran yang dikenal dan terkontrol, misalnya penghapusan upaya untuk mentransfer data secara diam-diam.

4.3.2 Implementasi teknis pada infrastruktur *cyber security* adalah:

Implementasi teknis dilakukan dengan menerapkan mekanisme perlindungan terhadap ancaman yang terdeteksi dan tidak terdeteksi, menggunakan *application* firewall dengan kemampuan:

a. Sistem *Intrusion Prevention System* (IPS)
b. Sekaligus sebagai anti-virus
c. Mengendalikan paket dalam 7 lapisan yang disebut *Deep Package Inspection*
d. Menganalisis lalu lintas terenkripsi (SSL)
e. Melindungi jaringan secara total dengan memusatkan koneksi *workstation*.

PENUTUP

a. Proses pertahanan konvensional yang berfokus pada kerentanan saja tidak cukup, maka pemahaman tentang ancaman, kemampuan dari ancaman, doktrin terkait ancaman, dan pola

operasi ancaman juga diperlukan untuk membangun ketahanan. Untuk itu digunakan sistem intelijen dalam pertahanan *cyber security* untuk menjaga model ancaman canggih yang terus berkembang.

b. Pertahanan terhadap serangan harus disiapkan dengan matang dan sistem perlindungan *cyber security* harus diterapkan guna mendapatkan system pertahanan terbaik. Pertahanan ini didapat dengan solusi teknis dan non teknis di dalam model *cyber kill chain* yang menggunakan semua pengetahuan, alat, dan solusi organisasi yang tersedia ketika mendesain solusi.
c. Pertahanan dengan persiapan yang matang dalam *cyber kill chain* dengan menyediakan struktur pertahanan yang dapat menganalisis ancaman, mengekstrak indikator ancaman, dan dapat mendorong tindakan defensif. Model ini juga memprioritaskan investasi untuk mengisi kesenjangan kemampuan, dan berfungsi sebagai model untuk mengukur efektivitas tindakan dari *Computer Security Incident Respons Team* (CSIRT).
d. *Cyber security* bukanlah suatu keadaan statis, namun merupakan suatu proses, sehingga agar implementasinya efektif, maka harus dilakukan pendekatan pembangunan *cyber security* sebagai sebuah proses yang berkesinambungan.

DAFTAR PUSTAKA

[1] P. Yadav, R.S., Likhar, *Firewall: A Vital Constituent of Network Security*. Springer Singapore, 2024.

[2] S. Deshpande and H. Wang, "Design of Quantum Computer Antivirus."

[3] J. Zhang and D. Tenney, "The Evolution of Integrated Advance Persistent Threat and Its Defense Solutions: A Literature Review," *Open Journal of Business and Management*, vol. 12, no. 01, pp. 293–338, 2024, doi: 10.4236/ojbm.2024.121021.

[4] K. O. Chee and C. Science, "Security Modelling and Analysis of Internet of Things against Evolving Attacks," 2024.

[5] O. Gulyas and G. Kiss, "Impact of cyber-Attacks on the financial institutions," *Procedia Computer Science*, vol. 219, pp. 84–90, 2023, doi: 10.1016/j.procs.2023.01.267.

[6] A. Wijoyo, A. Saputra, M. R. A. Pratama, and R. Rahman, "Analisis Serangan Phising dan Strategi Deteksinya," *JRIIN: Jurnal Riset Informatika dan Inovasi*, vol. 1, no. 4, pp. 1–6, 2023.

[7] J. Beerman, D. Berent, Z. Falter, and S. Bhunia, "A Review of Colonial Pipeline Ransomware Attack," *Proceedings - 23rd IEEE/ACM International Symposium on Cluster, Cloud and Internet Computing Workshops, CCGridW 2023*, pp. 8–15, 2023, doi: 10.1109/CCGridW59191.2023.00017.

[8] A. Shehu, M. Umar, and A. Aliyu, "Cyber Kill Chain Analysis Using Artificial Intelligence," *Asian Journal of Research in Computer Science*, vol. 16, no. 3, pp. 210–219, 2023, doi: 10.9734/ajrcos/2023/v16i3357.

[9] G. Matto, "The Cyber Kill Chain Model and Its Applicability on The Protection of Students Academic Information Systems (SAIS) in Tanzanian HEIs," vol. 6, no. 1, pp. 548–560, 2024, doi: 10.51519/journalisi.v6i1.676.

[10] S. R. B. Mohd Kassim, S. Li, and B. Arief, "Understanding How National CSIRTs Evaluate Cyber Incident Response Tools and Data: Findings from Focus Group Discussions," *Digital Threats: Research and Practice*, vol. 4, no. 3, 2023, doi: 10.1145/3609230.

[11] Y. Ahmed, A. T. Asyhari, and M. A. Rahman, "A Cyber Kill Chain Approach for Detecting Advanced Persistent Threats," *Computers, Materials and Continua*, vol. 67, no. 2, pp. 2497–2513, 2021, doi: 10.32604/cmc.2021.014223.

[12] M. Aamir, S. S. H. Rizvi, M. A. Hashmani, M. Zubair, and J. A. . Usman, "Machine Learning Classification of Port Scanning and DDoS Attacks: A Comparative Analysis," *Mehran University Research Journal of Engineering and Technology*, vol. 40, no. 1, pp. 215–229, 2021, doi: 10.22581/muet1982.2101.19.

[13] Y. Li, J. Hua, H. Wang, C. Chen, and Y. Liu, "DeepPayload: Black-box backdoor attack on deep learning models through neural payload injection," *Proceedings - International Conference on Software Engineering*, pp. 263–274, 2021, doi: 10.1109/ICSE43902.2021.00035.

[14] C. Guo, Z. Song, Y. Ping, G. Shen, Y. Cui, and C. Jiang, "Pratd: A phased remote access trojan detection method with double-sided features," *Electronics (Switzerland)*, vol. 9, no. 11, pp. 1–19, 2020, doi: 10.3390/electronics9111894.

[15] V. Valeros and S. Garcia, "Growth and Commoditization of Remote Access Trojans," *Proceedings - 5th IEEE European Symposium on Security and Privacy Workshops, Euro S and PW 2020*, pp. 454–462, 2020, doi: 10.1109/EuroSPW51379.2020.00067.

[16] M. Nasereddin, A. ALKhamaiseh, M. Qasaimeh, and R. Al-Qassas, "A systematic review of detection and prevention techniques of SQL injection attacks," *Information Security Journal*, vol. 32, no. 4, pp. 252–265, 2023, doi: 10.1080/19393555.2021.1995537.

[17] R. Alabdan, "Phishing attacks survey: Types, vectors, and technical approaches," *Future Internet*, vol. 12, no. 10, pp. 1–39, 2020, doi: 10.3390/fi12100168.

[18] R. Casolare, C. De Dominicis, G. Iadarola, F. Martinelli, F. Mercaldo, and A. Santone, "Dynamic mobile malware detection through system call-based image representation," *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 12, no. 1, pp. 44–63, 2021, doi: 10.22667/JOWUA.2021.03.31.044.

[19] M. A. Hakim and N. A. Abdullah, "A Dropper Remover Tool," vol. 4, no. 1, pp. 79–91, 2023.

[20] T. Neubert and C. Vielhauer, "Kill chain attack modelling for hidden channel attack scenarios in industrial control systems," *IFAC-PapersOnLine*, vol. 53, no. 2, pp. 11074–11080, 2020, doi: 10.1016/j.ifacol.2020.12.246.

[21] L. F. Eliyan and R. Di Pietro, "DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges," *Future Generation Computer Systems*, vol. 122, pp. 149–

171, 2021, doi: 10.1016/j.future.2021.03.011.

[22] S. Slamet, "Pertahanan Pencegahan Serangan Social Engineering Menggunakan Two Factor Authentication (2Fa) Berbasis Sms (Short Message System)," *Spirit*, vol. 14, no. 2, pp. 23–29, 2023, doi: 10.53567/spirit.v14i2.260.

[23] S. Slamet, "Desain Arsitektur Aplikasi Qr Code Sebagai Anti Phishing Serangan Qr Code," *Spirit*, vol. 15, no. 1, pp. 42–48, 2023, doi: 10.53567/spirit.v15i1.280.

[24] M. A. Al-shareeda, M. Anbar, S. Manickam, and I. H. Hasbullah, "Review of Prevention Schemes for Man-In-The-Middle (MITM) Attack in Vehicular Ad hoc Networks," *International Journal of Engineering and Management Research*, vol. 10, no. 3, pp. 153–158, 2020, doi: 10.31033/ijemr.10.3.23.

[25] S. G. Selvaganapathy, S. Sadasivam, and V. Ravi, "A Review on Android Malware: Attacks, Countermeasures and Challenges Ahead," *Journal of Cyber Security and Mobility*, vol. 10, no. 1, pp. 177–230, 2021, doi: 10.13052/jcsm2245-1439.1017.

[26] A. Mosteiro-Sanchez, M. Barcelo, J. Astorga, and A. Urbieta, "Securing IIoT using Defence-in-Depth: Towards an End-to-End secure Industry 4.0," *Journal of Manufacturing Systems*, vol. 57, pp. 367–378, 2020, doi: 10.1016/j.jmsy.2020.10.011.