BAB II TINJAUAN PUSTAKA

A. Penelitian Terkait

Dalam penyusunan penelitian ini, berbagai penelitian terdahulu dijadikan sebagai landasan referensi. Referensi tersebut mencakup jurnal dan karya ilmiah yang memiliki relevansi dengan topik yang dikaji serta kesamaan tujuan dalam pengembangan *Security Operations Center*.

Tabel 1 Penelitian Terkait

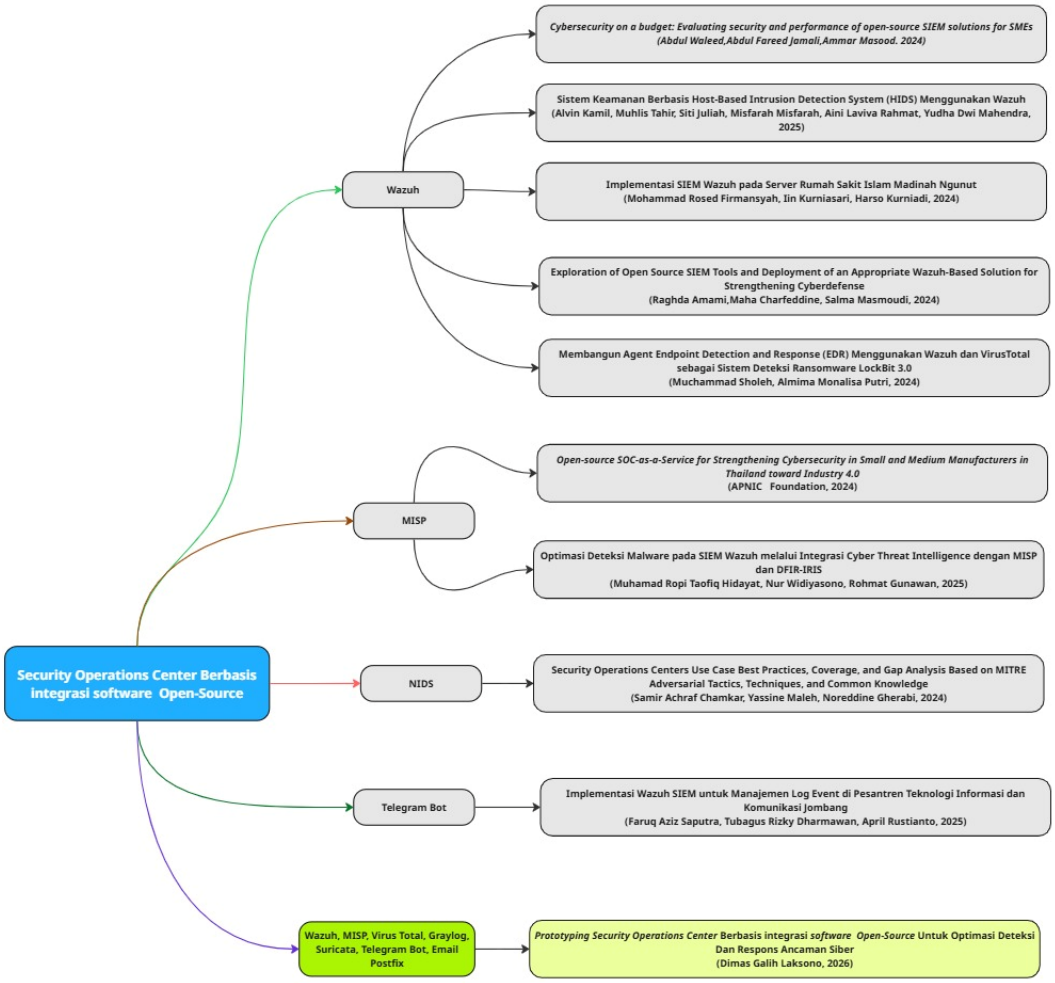
No	Penulis (Tahun)	Keterangan
1	Saputra, F. *et al.* (2023)	**Judul:** Implementasi Wazuh SIEM untuk Manajemen *Log Event* di Pesantren Teknologi Informasi dan Komunikasi Jombang **Hasil:** Sistem berhasil mengirimkan notifikasi *real-time* untuk berbagai insiden keamanan seperti serangan *brute force, Denial of Service (DoS),* dan *SQL Injection*, sehingga meningkatkan respons dan kesadaran keamanan di lingkungan pesantren..
2	Sholeh, M. et al. (2024)	**Judul:** Membangun *Agent Endpoint Detection and Response (EDR)* Menggunakan Wazuh dan VirusTotal sebagai Sistem Deteksi Ransomware LockBit 3.0 **Hasil:** Integrasi Wazuh dengan API VirusTotal berhasil mendeteksi dan menghapus ransomware dalam waktu rata-rata 0,7 detik, menunjukkan efektivitas tinggi dalam deteksi dan respons ancaman berbasis EDR.
3	Manzoor, J. *et al.* (2024)	**Judul:** *Cybersecurity on a budget: Evaluating security and performance of open source SIEM solutions for SMEs* **Hasil:** Evaluasi menunjukkan bahwa Wazuh dan SIEMonster *(Community Edition)* memiliki kapabilitas terbaik dari sisi keamanan dan performa, sehingga dinilai paling sesuai untuk implementasi SIEM dengan anggaran terbatas.
4	APNIC Foundation (2024)	**Judul:** *Open source SOC-as-a-Service for Strengthening Cybersecurity in Small and Medium Manufacturers in Thailand toward Industry 4.0*

No	Penulis (Tahun)	Keterangan
		Hasil: Integrasi Wazuh dengan MISP memungkinkan ekstraksi *Indicators of Compromise (IoC)* secara otomatis. Pengujian menunjukkan peningkatan kesadaran keamanan serta penurunan risiko kerentanan pada lingkungan UKM manufaktur.
5	Chamkar, S. *et al.* (2024)	**Judul:** *Security Operations Centers Use Case Best Practices, Coverage, and Gap Analysis Based on MITRE Adversarial Tactics, Techniques, and Common Knowledge* **Hasil:** *Playbook* respons insiden berbasis MITRE ATT&CK dapat diimplementasikan secara efektif pada SOC yang menggunakan SIEM/SOAR *open source*, sehingga meningkatkan kesiapan dan konsistensi respons terhadap serangan siber.
6	Amami, R. et al. (2024)	**Judul:** *Exploration of Open Source SIEM Tools and Deployment of an Appropriate Wazuh-Based Solution for Strengthening Cyberdefense* **Hasil:** Penelitian menunjukkan bahwa penggunaan Wazuh sebagai solusi SIEM berbasis *open source* efektif dalam meningkatkan kemampuan pertahanan siber melalui pemantauan *log*, deteksi ancaman, serta analisis keamanan secara terpusat.
7	Owolafe, O. & Alabi, A. J. (2024)	**Judul:** *Comparative Analysis of Wazuh, Graylog, and ELK Stack for Cyber Threat Detection and Response* **Hasil:** Hasil perbandingan menunjukkan bahwa Wazuh, Graylog, dan ELK Stack masing-masing memiliki keunggulan dalam deteksi dan respons ancaman, dengan Wazuh unggul dalam integrasi keamanan, sedangkan ELK Stack dan Graylog lebih fleksibel dalam pengolahan dan visualisasi *log*.
8	Firmansyah, M. R. et al. (2024)	**Judul:** Implementasi SIEM Wazuh pada Server Rumah Sakit Islam Madinah Ngunut **Hasil:** Integrasi Wazuh dengan sistem notifikasi (Telegram Bot) mampu meningkatkan monitoring keamanan secara real-time serta mempercepat respons terhadap insiden keamanan
9	Hidayat, M. R. T. *et al.* (2025)	**Judul:** Optimasi Deteksi *Malware* Pada SIEM Wazuh Melalui Integrasi *Cyber Threat Intelligence* Dengan MISP Dan DFIR-IRIS

No	Penulis (Tahun)	Keterangan
		Hasil: Integrasi Wazuh dengan MISP dan DFIR-IRIS terbukti meningkatkan efektivitas deteksi *malware*, mempercepat respons insiden, serta memperbaiki manajemen informasi ancaman secara keseluruhan.
10	Ang, S. et al. (2025)	**Judul:** *Utilizing IDS and IPS to Improve Cybersecurity Monitoring Process* **Hasil:** Implementasi IDS dan IPS mampu meningkatkan efektivitas proses pemantauan keamanan dengan mendeteksi aktivitas mencurigakan secara lebih cepat serta memberikan perlindungan berlapis terhadap ancaman siber.
11	Kamil, A. T. *et al.* (2025)	**Judul:** Sistem Keamanan Berbasis *Host-Based Intrusion Detection System (HIDS)* Menggunakan Wazuh **Hasil:** Wazuh berhasil digunakan untuk memantau perubahan file dan aktivitas mencurigakan pada *host*, sehingga meningkatkan keamanan server dan mendukung konsep SOC berbasis *open source* tanpa biaya lisensi.

Penelitian ini memiliki perbedaan yang signifikan dibandingkan dengan studi-studi sebelumnya karena berfokus pada pengembangan model *Security Operations Center (SOC)* berbasis integrasi *software open source* yang bersifat komprehensif dan terukur. Model yang diusulkan mengintegrasikan komponen Wazuh, Graylog, dan MISP, serta memanfaatkan mekanisme *enrichment* intelijen ancaman dan notifikasi *real-time* untuk mendukung deteksi, *triase*, dan respons insiden secara efisien.

Selain itu, penelitian ini juga menekankan pada aspek evaluasi kinerja dan efektivitas operasional SOC secara sistematis. Pengujian dilakukan dengan menggunakan skenario serangan simulatif yang mencakup berbagai vektor ancaman, termasuk *malware*, *intrusion attempts*, dan serangan berbasis jaringan. Hasil pengujian menunjukkan bahwa integrasi antara Wazuh, Graylog, dan MISP tidak hanya meningkatkan kemampuan deteksi dini, tetapi juga mempercepat proses *triase* insiden melalui otomatisasi korelasi *log* dan *enrichment* intelijen ancaman.



Gambar 1 *Mind Map* Penelitian Sebelumnya

B. Landasan Teori

1. Security Operations Center (SOC)

Security Operations Center adalah lokasi tempat *security professional* bertanggung jawab untuk memantau, mendeteksi, menganalisis, dan merespons ancaman keamanan siber secara berkelanjutan. SOC berfungsi sebagai benteng utama dalam mempertahankan keamanan informasi melalui pengawasan lalu lintas jaringan dan aktivitas sistem secara *real-time*, serta pengelolaan insiden keamanan dari tahap awal hingga mitigasi, dengan tujuan menjaga integritas, ketersediaan, dan kerahasiaan aset digital organisasi[7], [8].

Gambar 2 CIA triad

Dalam kerangka operasionalnya, SOC menggabungkan tiga komponen utama, yaitu *people*, *process*, dan *technology* yang didukung oleh tata kelola dan kepatuhan terhadap standar *governance* dan *compliance* untuk meningkatkan postur keamanan organisasi secara keseluruhan[7], [9], [10].

Gambar 3 Three Pillars of Cyber Security

2. Prototipe

Prototipe adalah pendekatan dalam pengembangan sistem atau perangkat lunak dengan membuat model awal dari sistem yang diusulkan untuk diuji dan dievaluasi sebelum pengembangan penuh dilakukan. Prototipe berfungsi sebagai representasi sementara dari produk akhir yang membantu pengembang dan pemangku kepentingan memahami kebutuhan, fungsi, dan interaksi sistem secara lebih jelas serta memperoleh umpan balik untuk penyempurnaan[11]. Proses ini bersifat iteratif, di mana prototipe dibuat, diuji, dan direvisi berulang kali hingga sesuai dengan kebutuhan

pengguna, sehingga dapat mengurangi risiko kesalahan desain dan mempercepat validasi sebelum implementasi akhir.

3. *Software Open Source*

   Software open source adalah perangkat lunak yang kode sumbernya tersedia secara bebas untuk umum sehingga dapat dilihat, dipelajari, dimodifikasi, dan didistribusikan kembali oleh siapapun sesuai dengan lisensi *open source* yang berlaku[12]. Pendekatan ini mendorong transparansi, kolaborasi, dan inovasi dari berbagai latar belakang pengembang untuk berkontribusi dalam pengembangan dan perbaikan perangkat lunak[13].

4. Optimasi

   Optimasi didefinisikan sebagai suatu pendekatan sistematis yang bertujuan untuk mencapai hasil yang paling optimal pada suatu sistem, melalui pemanfaatan sumber daya yang tersedia secara tepat. Dalam ranah ilmu komputer, matematika, maupun manajemen, optimasi diarahkan untuk memaksimalkan kinerja, kualitas, atau keuntungan, sekaligus meminimalkan biaya, waktu, dan penggunaan sumber daya, dengan memperhatikan berbagai kendala yang berlaku[14].

5. Deteksi ancaman siber

   Deteksi ancaman siber adalah proses mengidentifikasi, memantau, dan menganalisis aktivitas mencurigakan atau berbahaya pada sistem, jaringan, maupun aplikasi yang berpotensi mengancam keamanan informasi. Proses ini bertujuan untuk menemukan indikasi serangan seperti *malware*, *intrusion*, kebocoran data, atau penyalahgunaan akses sedini mungkin dengan menggunakan teknologi dan metode seperti IDS/IPS, SIEM, EDR, analisis *log*, serta *threat intelligence* sehingga organisasi dapat mengambil tindakan pencegahan dan respons yang tepat untuk meminimalkan dampak serangan[15], [16].

6. Respons ancaman siber

   Respons ancaman siber adalah serangkaian tindakan terstruktur yang dilakukan untuk menangani, mengendalikan, dan memulihkan sistem setelah adanya indikasi ancaman atau insiden keamanan siber. Proses ini mencakup identifikasi dan analisis insiden, penahanan *(containment)* untuk mencegah penyebaran dampak, penghapusan ancaman *(eradication)*, serta pemulihan sistem agar dapat beroperasi normal kembali[16], [17]. Respons ancaman siber juga melibatkan dokumentasi, evaluasi, dan perbaikan berkelanjutan guna meningkatkan kesiapan keamanan di masa depan serta meminimalkan dampak kerugian terhadap organisasi.

7. Efektivitas

   Efektivitas merupakan ukuran kemampuan suatu sistem atau proses dalam mencapai tujuan yang telah ditetapkan. Dalam keamanan siber, efektivitas merujuk pada kemampuan solusi keamanan dalam mendeteksi, mencegah, dan menanggapi ancaman secara tepat sesuai kebutuhan organisasi. Tingkat efektivitas ini tercermin dari kecepatan dan ketepatan dalam mendeteksi serta menangani insiden keamanan, yang umumnya diukur melalui indikator seperti *Mean Time to Detect (MTTD), Mean Time to Respond (MTTR),* dan tingkat akurasi deteksi[18].

8. Wazuh

   Wazuh adalah platform *open source Security Information and Event Management (SIEM)* yang berfungsi untuk memantau, mendeteksi, dan menganalisis ancaman siber melalui pengelolaan *log* secara terpusat serta pemantauan aktivitas sistem secara *real-time,* sehingga meningkatkan visibilitas dan kemampuan respons terhadap insiden keamanan pada lingkungan TI[19].

9. Malware Information Sharing Platform (MISP)

   MISP adalah platform intelijen ancaman *open source* yang dirancang untuk mengumpulkan, menyimpan, berbagi, dan mengaitkan *Indicator of Compromise (IoC)* serta informasi ancaman siber secara terstruktur. Platform ini membantu organisasi meningkatkan kemampuan deteksi, respons, dan kolaborasi terhadap ancaman[15]. MISP juga mendukung pertukaran intelijen ancaman secara otomatis dan terstandarisasi, serta dapat diintegrasikan dengan sistem lain seperti SIEM atau IDS untuk memperkuat keamanan siber secara menyeluruh[20].

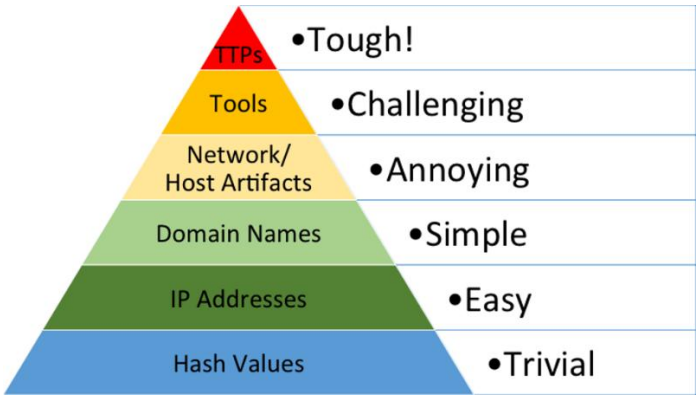
10. Graylog

    Graylog adalah platform *open source* untuk menerima, mengelola, menganalisis, dan memvisualisasikan *log* dari berbagai sumber dalam infrastruktur TI secara *real-time*[21]. Platform ini membantu tim keamanan mendeteksi ancaman, menyelidiki insiden, dan memantau aktivitas sistem dengan lebih efektif[22]. Graylog menawarkan fitur pencarian *real-time*, pembuatan *dashboard*, pemberian peringatan *(alerting),* serta kemampuan integrasi dengan berbagai sumber *log* untuk mendukung operasi keamanan dan kepatuhan.

11. Indicator of Compromise (IoC)

    Indicator of Compromise (IoC) merupakan bukti teknis yang mengindikasikan adanya potensi atau indikasi pelanggaran keamanan pada sistem, jaringan, maupun *endpoint*. IoC dimanfaatkan oleh tim SOC sebagai acuan dalam mendeteksi aktivitas berbahaya, melakukan analisis insiden, serta mengenali pola serangan yang telah atau sedang terjadi. IoC berperan

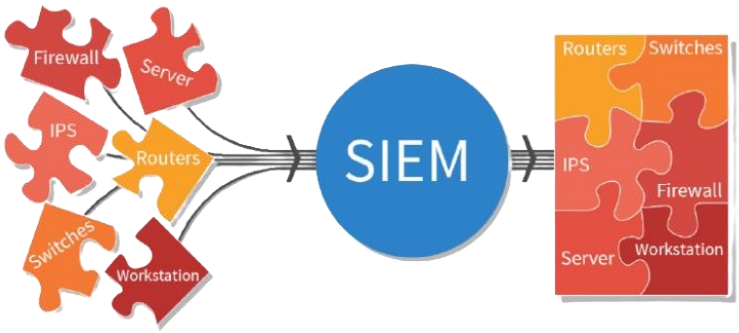
penting dalam proses deteksi dan penanganan insiden karena memungkinkan SOC untuk mengintegrasikan dan mengkorelasikan data dari berbagai sumber keamanan, seperti SIEM, EDR, IDS/NIDS, serta *Threat Intelligence Platform*. Dengan mengkorelasikan IoC terhadap *log* dan *event* yang dikumpulkan, analis SOC dapat mempercepat proses *triage*, menentukan tingkat keparahan insiden, serta mengambil tindakan mitigasi yang tepat. Selain itu, pemanfaatan IoC berkontribusi dalam menurunkan nilai *Mean Time to Detect (MTTD)* dan *Mean Time to Respond (MTTR)* dengan menyediakan indikator yang telah tervalidasi untuk mendukung deteksi ancaman yang lebih cepat dan presisi[7], [23], [24].



Gambar 4 Indicator of Compromise Pyramid

12. Security Information and Event Management (SIEM)

Security Information and Event Management (SIEM) adalah solusi keamanan siber yang berfungsi mengumpulkan, menganalisis, dan mengkorelasikan *log* serta *event* keamanan dari berbagai sumber dalam infrastruktur TI, seperti server, perangkat jaringan, aplikasi, dan sistem keamanan. SIEM membantu organisasi mendeteksi ancaman dan insiden keamanan secara *real-time*, menyediakan visibilitas terpusat, mendukung investigasi insiden, serta membantu pemenuhan kepatuhan dan pelaporan keamanan [5], [25], [26], [27].



Gambar 5 Security Information and Event Management

13. Endpoint Detection and Response (EDR)

Endpoint Detection and Response adalah solusi keamanan siber yang memantau, mendeteksi, menganalisis, dan merespons aktivitas berbahaya pada *endpoint* seperti komputer dan server secara *real-time*[28]. Pada konteks *Security Operations Center*, EDR berperan penting dalam mengumpulkan data aktivitas *endpoint* untuk mengidentifikasi perilaku mencurigakan, memungkinkan investigasi insiden secara mendalam, serta menyediakan kemampuan respons seperti isolasi perangkat, penghentian proses berbahaya, dan remediasi guna mencegah penyebaran ancaman di dalam jaringan[7], [28].

14. Intrusion Detection System (IDS)

Intrusion Detection System (IDS) adalah sistem keamanan yang berfungsi untuk memantau lalu lintas jaringan atau aktivitas sistem guna mendeteksi adanya upaya penyusupan, serangan, atau aktivitas mencurigakan secara *real-time*. IDS bekerja dengan menganalisis pola lalu lintas dan perilaku sistem, lalu memberikan peringatan *(alert)* kepada administrator ketika terdeteksi ancaman, sehingga memungkinkan tindakan lanjutan sebelum serangan menyebabkan dampak yang lebih besar[29], [30], [31], [32].

15. Intrusion Prevention System (IPS)

Intrusion Prevention System (IPS) adalah sistem keamanan yang berfungsi untuk memantau lalu lintas jaringan secara *real-time* serta mendeteksi dan mencegah upaya penyusupan atau serangan siber, berbeda dengan IDS yang hanya memberikan peringatan, IPS dapat secara otomatis mengambil tindakan seperti memblokir *trafik* berbahaya, memutus koneksi, atau menghentikan serangan, sehingga membantu melindungi jaringan dari ancaman sebelum menimbulkan dampak yang lebih serius [32], [33].

16. Network-based Intrusion Detection System (NIDS)

Network-based Intrusion Detection System (NIDS) adalah sistem keamanan yang berfungsi untuk memantau dan menganalisis lalu lintas jaringan guna mendeteksi aktivitas mencurigakan, serangan, atau upaya penyusupan. NIDS ditempatkan pada titik strategis dalam jaringan untuk menginspeksi paket data yang melintas dan akan memberikan peringatan kepada administrator ketika terdeteksi pola serangan, sehingga membantu organisasi mengidentifikasi ancaman terhadap keamanan jaringan secara dini[30], [34], [35], [36].

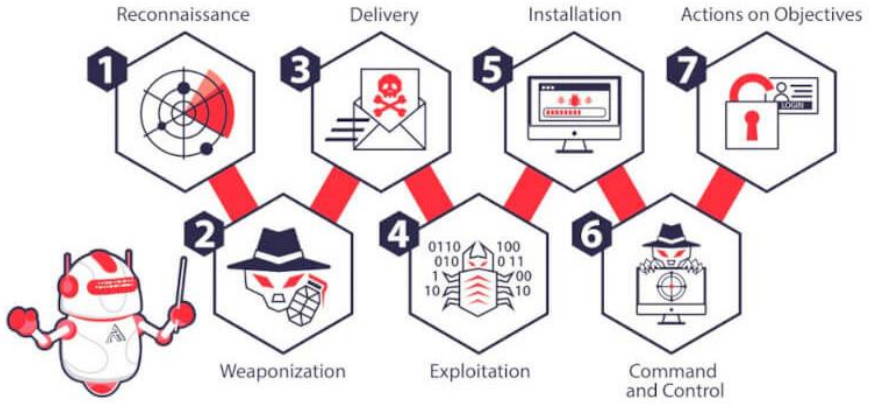
17. Extended Detection and Response (XDR)

Extended Detection and Response adalah pendekatan keamanan siber terpadu yang menggabungkan deteksi dan respons ancaman dari berbagai *domain* ke dalam satu platform terpusat. Tidak seperti EDR yang hanya

fokus pada *endpoint*, XDR mengumpulkan dan mengkorelasikan data dari berbagai sumber seperti *endpoint*, jaringan, *email*, *cloud*, dan aplikasi untuk memberikan visibilitas ancaman yang lebih luas. Pendekatan ini membantu tim SOC dalam mengidentifikasi serta menangani serangan yang kompleks yang melibatkan banyak vektor serangan sekaligus, sehingga mempercepat proses deteksi dan respons[37], [38], [39].

18. MITRE ATT&CK

MITRE ATT&CK *(Adversarial Tactics, Techniques, and Common Knowledge)* adalah kerangka kerja berbasis pengetahuan yang memetakan perilaku pelaku ancaman siber dalam bentuk taktik, teknik, dan prosedur (TTP) yang disusun berdasarkan observasi terhadap serangan dunia nyata. Kerangka ini menggambarkan tahapan lengkap siklus serangan, mulai dari akses awal hingga tujuan akhir penyerang, sehingga menyediakan taksonomi serangan yang terstruktur untuk memahami pola ancaman secara komprehensif[4], [40].



Gambar 6 Cyber Kill Chain