

BAB II

TINJAUAN PUSTAKA

2.1 *Grand Theory*

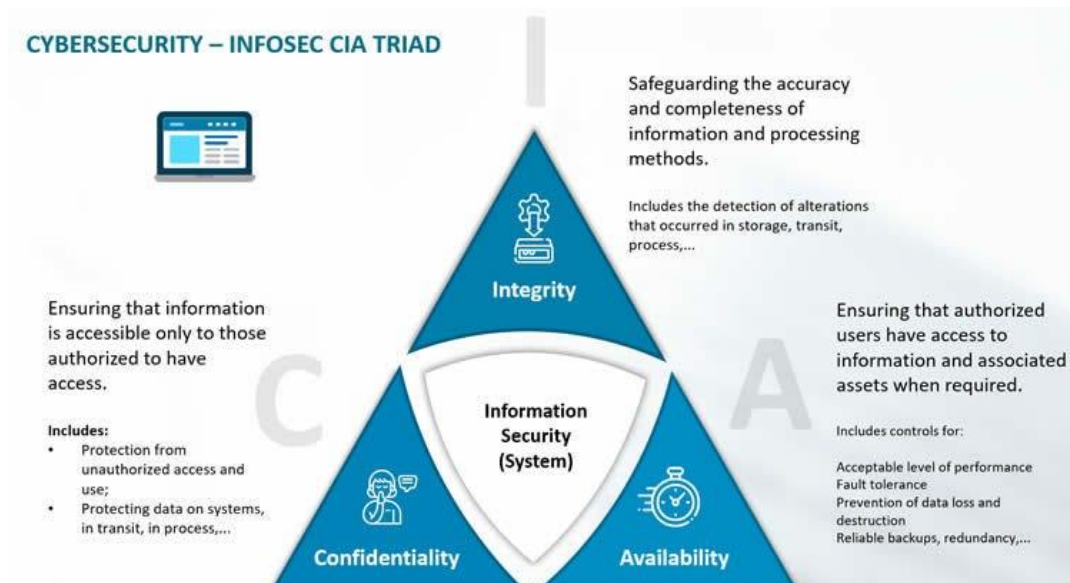
2.1.1 Keamanan Siber (*Cyber Security*)



Gambar 2.1 *Cyber Security Framework*

Sumber : itmtech, 2022

Pentingnya pemahaman masyarakat mengenai keamanan dalam berinternet atau sering disebut dengan istilah *cyber security* sangat diperlukan untuk mengetahui ancaman apa saja yang mungkin ditimbulkan dan bagaimana cara mengatasi ancaman tersebut. Berdasarkan gambar 2.1, dapat dikatakan bahwa *cyber security* adalah kumpulan alat, kebijakan, konsep keamanan, perlindungan keamanan, pedoman, pendekatan manajemen risiko, tindakan, pelatihan, praktik terbaik, jaminan dan teknologi yang dapat digunakan untuk melindungi lingkungan *cyber* dan organisasi dan aset pengguna (Atmojo *et al*, 2021).



Gambar 2.2 CIA Triad Diagram

Sumber : Make Computer Science Great Again, 2023

Berdasarkan gambar 2.2, sistem keamanan informasi (*information security*) memiliki empat tujuan yang sangat mendasar adalah:

- a. Kerahasiaan (*Confidentiality*). Informasi pada sistem komputer terjamin kerahasiaannya, hanya dapat diakses oleh pihak yang diotorisasi, keutuhan serta konsistensi data pada sistem tersebut tetap terjaga. Sehingga upaya orang-orang yang ingin mencuri informasi tersebut akan sia-sia.
- b. Ketersediaan (*Availability*). Menjamin pengguna yang sah untuk selalu dapat mengakses informasi dan sumber daya yang diotorisasi. Untuk memastikan bahwa orang-orang yang memang berhak untuk mengakses informasi yang memang menjadi haknya.
- c. Integritas (*Integrity*) Menjamin konsistensi dan menjamin data tersebut sesuai dengan aslinya, sehingga upaya orang lain yang berusaha merubah data akan segera dapat diketahui.
- d. Penggunaan yang sah (*Legitimate Use*). Menjamin kepastian bahwa sumber daya tidak dapat digunakan oleh orang yang tidak berhak (Atmojo *et al*, 2021).

Indonesia saat ini tengah dalam keadaan mendesak *cyber-security* atau keamanan dunia maya karena melihat kenyataan bahwa tingkat kejahatan di dunia maya atau *cyber crime* di Indonesia sudah mencapai tahap memprihatinkan. Salah satu fakta yang menunjukkan *cyber crime* di Indonesia sudah mengkhawatirkan adalah data CIA yang menyebutkan kerugian yang disebabkan karena tindak kejahatan dengan memanfaatkan maupun di dunia *cyber* di Indonesia telah mencapai 1,20% dari tingkat kerugian akibat *cyber crime* yang terjadi di dunia.

Perkembangan serta kemajuan teknologi dalam dunia *cyber* tidak selalu mampu mengimbangi perkembangan ancaman *cyber* yang ada, dikarenakan kelompok-kelompok kejahatan dapat terus berkembang dan menemukan cara baru untuk mengeksploitasi sistem yang sudah ada. Ancaman siber yang semakin kompleks menunjukkan perlunya inovasi berkelanjutan dalam sistem pertahanan siber untuk melindungi data dan infrastruktur penting (Yao Siang Tiong, 2024). Hal ini juga diperkuat dengan pentingnya pendekatan berbasis intelijen ancaman dan adopsi teknologi canggih seperti *machine learning* untuk mendeteksi pola anomali. Oleh karena itu, pengembangan strategi keamanan siber harus mencakup peningkatan teknologi serta kolaborasi antara penyedia solusi keamanan dan pengguna sistem (CrowdStrike, 2024).

2.1.2 Information Technology Service Management (ITSM)



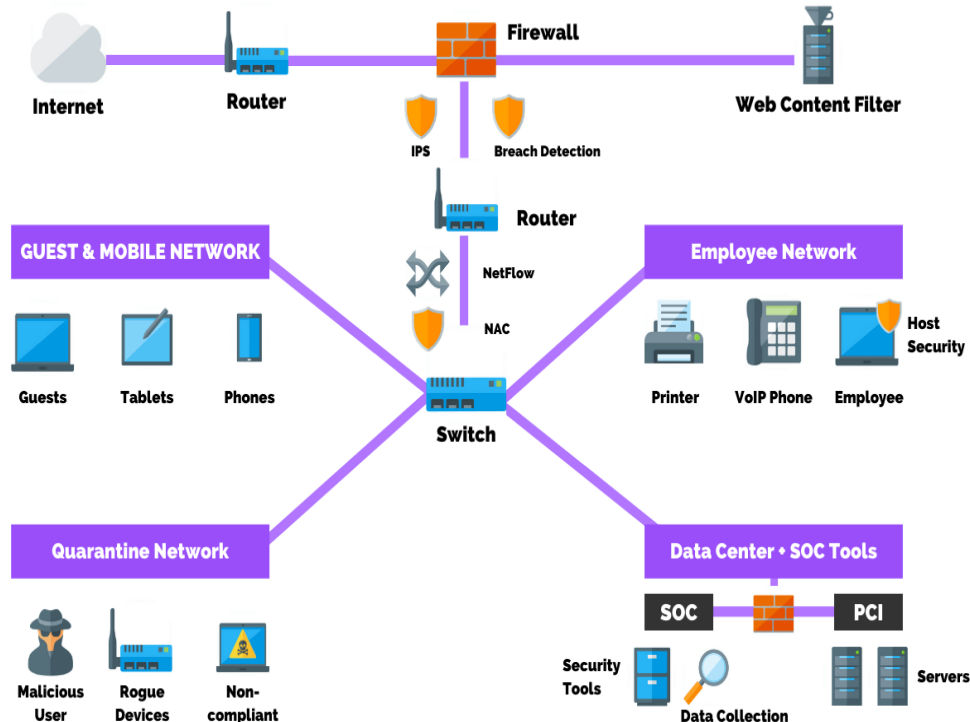
Gambar 2.3 Diagram ITSM

Sumber : itmanagement, 2023

Berdasarkan gambar 2.3 diatas, dapat dikatakan bahwa *Information Technology Service Management* merupakan sebuah cara tim IT untuk mengelola layanan dari IT ke *customer* atau pelanggan. Manajemen layanan teknologi informasi (ITSM) fokus pada manajemen sistem operasional teknologi informasi yang bertujuan untuk memberikan dukungan pada kegiatan bisnis sehari-hari daripada pengembangan teknologi. Misalnya, ITSM tidak terlibat dalam proses produksi perangkat lunak untuk dijual, tetapi lebih pada manajemen sistem TI yang diarahkan untuk membantu memfasilitasi pemasaran atau pengembangan bisnis di perusahaan perangkat lunak. Prinsip yang sama diterapkan di berbagai industri seperti keuangan, ritel, dan pariwisata di mana sistem TI diperlukan untuk sebagian besar operasi internal bisnis meskipun klien tidak memiliki pengetahuan tentang keberadaan sistem tersebut. ITSM mendorong penggunaan teknologi dan memastikan bahwa teknologi tersebut berjalan dengan cara terbaik yang mendukung tujuan bisnis (Stuart *et al*, 2009).

Perspektif layanan kepada konsumen adalah suatu sarana untuk memberikan nilai kepada pelanggan dengan memfasilitasi hasil yang ingin dicapai oleh konsumen dengan cara meningkatkan performa suatu tugas yang berhubungan dengan konsumen dan mengurangi efek kendala kepada konsumen, seperti tanpa risiko dan tanpa kepemilikan biaya. ITSM dapat menguntungkan tim TI pada sebuah organisasi. Prinsip *service management* dapat meningkatkan kinerja seluruh organisasi. ITSM mengarah pada peningkatan efisiensi dan produktivitas. Pendekatan terstruktur untuk *service management* juga menyelaraskan TI dengan tujuan bisnis, menstandarisasi penyampaian *service* berdasarkan anggaran, *resource*, dan hasil. Pada akhirnya, ITSM diharapkan dapat mengurangi biaya dan risiko, dan meningkatkan pengalaman pelanggan (Hermadi *et al*, 2022).

2.1.3 Security Operation Center (SOC)



Gambar 2.4 Arsitektur SOC

Sumber : Jason Firch, 2024

Security operation center (SOC) merupakan sebuah organisasi atau tim yang menjadi sebuah pusat pengawasan keamanan yang bertanggung jawab untuk memantau, menganalisis, dan menanggapi insiden keamanan secara *real-time*. SOC beroperasi selama 24 jam. Berdasarkan gambar 2.4, SOC memiliki beberapa fungsi utama, antara lain:

a. Pendeteksian Ancaman

Melakukan pendeteksian ancaman dengan menggunakan alat pemantauan dan melakukan analisis untuk mendeteksi potensi ancaman siber yang dapat terjadi.

b. Regulasi

Tim SOC memastikan seluruh kegiatan atau *traffic network* yang berkaitan dengan keamanan sesuai dengan regulasi yang telah ditetapkan.

c. Respons Insiden

Bertindak cepat dalam menanggapi insiden keamanan yang terjadi.

d. Monitoring

Melakukan *monitoring* selama 24/7 terhadap aktivitas jaringan untuk mencegah dan menanggapi ancaman.

Pada tim SOC itu sendiri dibagi menjadi dua, yaitu *blue team* dan *red team* yang dimana masing-masing tim memiliki perannya sendiri, *red team* mengacu kepada bagian keamanan ofensif atau serangan seperti *penetration test* (*pentest*), *vulnerability assessment* (VA), dan *social engineering*, sedangkan *blue team* berfokus kepada hal-hal defensif atau keamanan atau pertahanan seperti *security monitoring*, *incident response*, dan *implementing control* (Riccardo Gracis, 2022).

Selain itu SOC juga memiliki standar operasional yang dimana ditetapkan dalam ISO/IEC-27001 dan ISO27000. ISO/IEC 27001 dan ISO27000 merupakan standar untuk menetapkan persyaratan serta pedoman yang diperlukan untuk mengelola sistem manajemen keamanan

informasi atau *Information Security Management System* (ISMS). Standar ini memberikan kerangka kerja untuk melindungi informasi secara sistematis, memastikan kerahasiaan, integritas, dan ketersediaannya, serta mengelola risiko keamanan informasi dalam suatu organisasi (Riccardo Gracis, 2022).

2.1.4 *Computer Security Incident Response Team* (CSIRT)

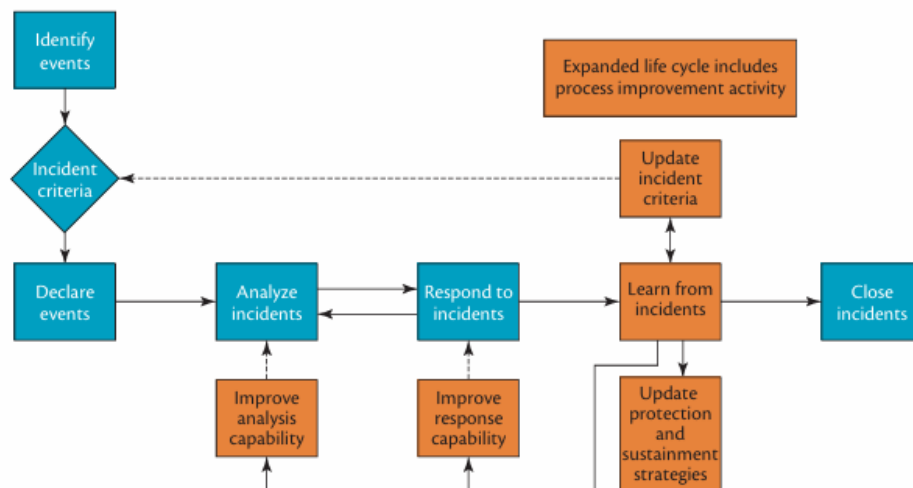


Gambar 2.5 Diagram CSF CSIRT

Sumber : csirt.kemhan, 2024

Berdasarkan gambar 2.5 diatas yang merupakan kerangka berpikir, *Computer Security Incident Response* atau CSIRT merupakan tim yang bertanggung jawab untuk merespons insiden keamanan komputer dalam sebuah organisasi. Tim ini memiliki peran penting dalam keamanan komputer diantaranya mendeteksi, merespon, dan mitigasi terhadap suatu ancaman atau serangan siber. Selain itu CSIRT juga dikenal sebagai *Computer Emergency Response Team* (CERT). CSIRT bekerja sama dengan SOC untuk menangani insiden keamanan dengan efisien. CSIRT awalnya bertujuan untuk merespon mengenai kekurangan keamanan siber dalam arsitektur internet (Lipson, 2002).

Dapat dilihat pada gambar 2.6, bahwa di dalam sebuah organisasi, CSIRT berfokus pada keamanan sistem komputer dan jaringan yang membentuk infrastruktur organisasi tersebut. Jika terdapat beberapa tim keamanan dan CSIRT di dalam organisasi besar, salah satunya mungkin bertugas sebagai koordinator dan titik kontak tunggal bagi pihak eksternal. Tim semacam itu disebut *Coordinating CSIRT*. *Coordinating CSIRT* juga dapat dibentuk sebagai entitas independen yang melayani sekelompok individu dan/atau organisasi tertentu yang dikenal sebagai konstituen. Organisasi yang termasuk dalam konstituen tertentu biasanya memiliki karakteristik yang sama (seperti menjadi bagian dari jaringan penelitian nasional atau berasal dari negara tertentu). *Coordinating CSIRT* bertindak sebagai titik kontak tunggal untuk seluruh kelompok dan berfokus pada aspek keamanan menyeluruh dari organisasi-organisasi tersebut (Kossakowski et al, 2019).



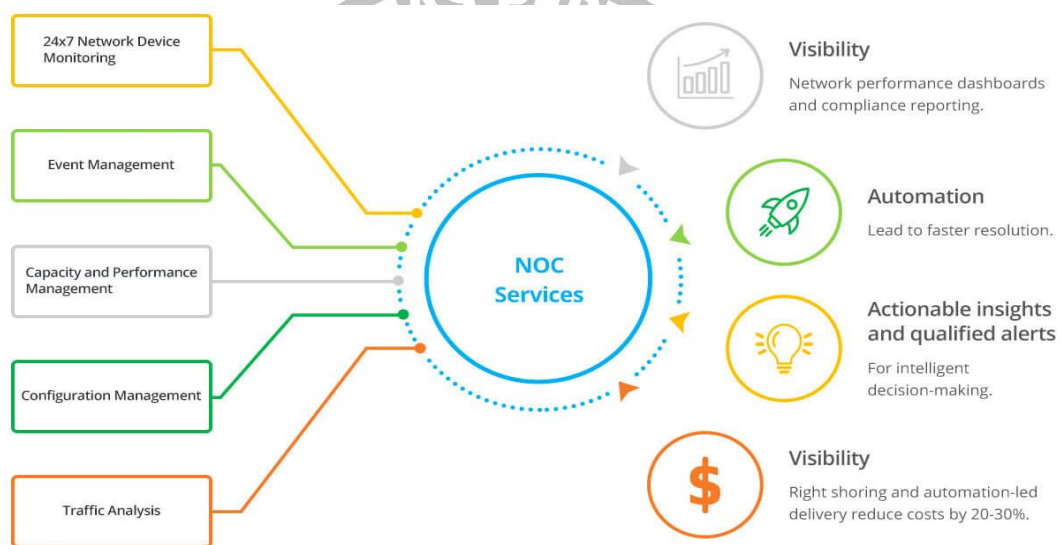
Gambar 2.6 Siklus Penanganan Insiden

Sumber : Ruefle, 2014

Jumlah tim CSIRT dapat bervariasi mulai dari satu orang di organisasi kecil hingga lebih dari 100 orang di organisasi besar yang terdistribusi, tergantung pada tingkat layanan yang ditawarkan, sumber daya yang tersedia, pendanaan, dan ukuran konstituen. Sebagian besar CSIRT menggunakan kombinasi personel penuh waktu dan paruh waktu,

termasuk staf teknis seperti analis insiden, kerentanan, dan *malware*; spesialis forensik; analis jaringan; pakar OS dan aplikasi; serta manajer, penghubung dengan pihak hukum dan penegak hukum, staf hubungan masyarakat, penulis teknis, staf TI dan rekayasa sistem, serta staf administratif (Ruefle *et al*, 2014).

2.1.5 Network Operation Center (NOC)



Gambar 2.7 Diagram NOC Service

Sumber : zones, 2024

Berdasarkan gambar 2.7, *Network Operation Center* (NOC) dapat didefinisikan sebagai kombinasi dari struktur organisasi, staf, proses, produk teknologi dan alat, serta penyedia layanan yang dirancang untuk menyediakan tingkat layanan operasional yang andal bagi pengguna akhir dari jaringan terdistribusi yang heterogen dan multivendor. Banyak organisasi mengintegrasikan NOC mereka ke dalam pusat manajemen perusahaan yang lebih luas. *Network Operations Center* (NOC) memainkan peran sentral dalam jaringan terdistribusi multivendor saat ini dengan membantu para insinyur jaringan memantau kinerja, keandalan, dan stabilitas seluruh jaringan. Dengan meningkatnya pentingnya jaringan dalam keberhasilan bisnis inti, pengelolaan NOC yang efektif menjadi sangat penting (Blum, 2001).

Menjaga jaringan agar tetap berjalan dengan efisien setiap saat, terutama selama periode ekspansi yang cepat, membutuhkan kemampuan untuk membentuk tim profesional jaringan dengan keterampilan teknis yang diperlukan, menetapkan proses dan kebijakan untuk mengontrol aktivitas jaringan, serta memberikan manajemen yang terampil atas seluruh operasi. Para manajer yang bertanggung jawab atas operasi jaringan harus mempertimbangkan berbagai aspek penting untuk memastikan kelancaran operasional diantaranya sebagai berikut :

- a. Tantangan terbesar bagi sebagian besar organisasi adalah merekrut, melatih, dan mempertahankan sekelompok profesional jaringan yang sangat terampil yang dapat memahami berbagai elemen yang kompleks dari jaringan perusahaan modern. Fokus pada tujuan ini mungkin lebih penting untuk kesuksesan daripada teknologi yang baik.
- b. Sumber daya yang mumpuni memungkinkan organisasi untuk mendapatkan keahlian jaringan secara instan guna memaksimalkan kinerja jaringan, serta membantu dengan fungsi-fungsi kritis, seperti keamanan.
- c. Perhatikan dengan seksama proses dan prosedur yang dapat memaksimalkan nilai dari teknologi manajemen jaringan yang tim NOC terapkan. Saat mengembangkan kemampuan NOC (*Network Operation Center*), pastikan untuk mempertimbangkan masa depan, dengan menyadari bahwa akan diperlukan mengintegrasikan teknologi dan layanan baru ke dalam tim NOC (Blum, 2001).

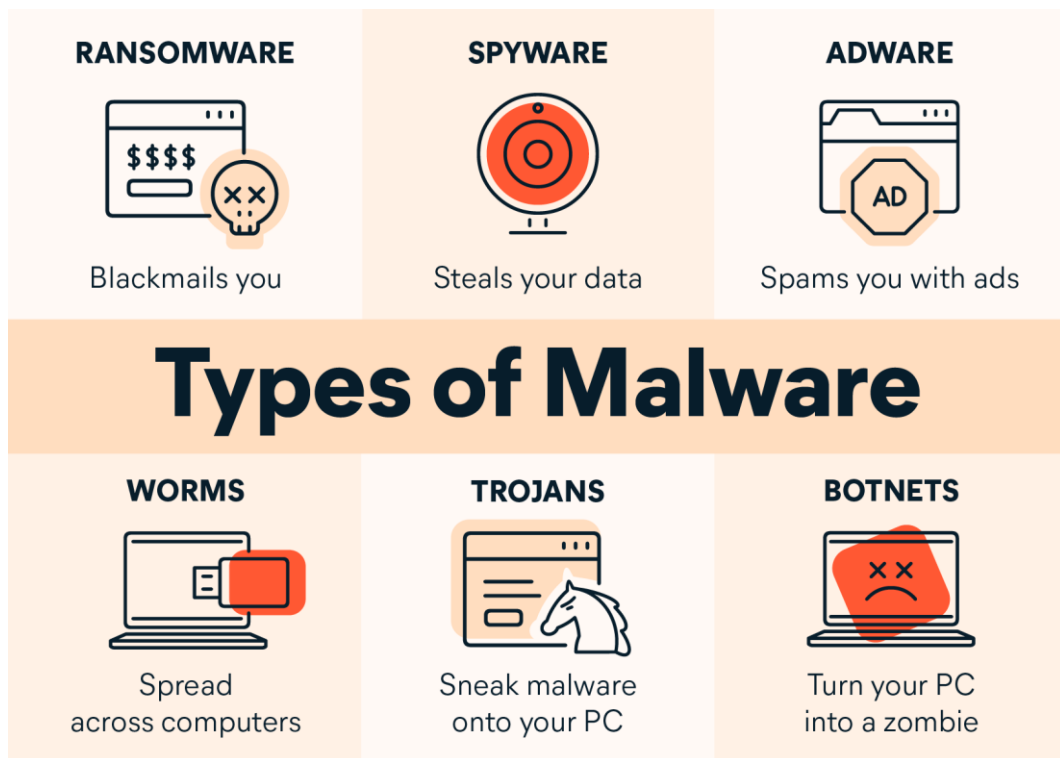
2.2 *Middle Theory*

2.2.1 *Malicious Software (Malware)*

Istilah *malware* merupakan singkatan dari *malicious software*. Seperti namanya, *malware* dirancang untuk merugikan komputer dan pengguna komputer dengan mencuri informasi, merusak *file*, atau melakukan aktivitas nakal yang dapat mengganggu pengguna. *Malware* menyebar secara luas, dan diperkirakan terjadi peningkatan besar dalam insiden keamanan komputer (Adelstein *et al*, 2002; Bergeon *et al*, 2001).

Malware menargetkan aplikasi yang berjalan di atas internet. Karena hampir semua bidang kehidupan menggunakan internet untuk meningkatkan kualitas layanan, ada peningkatan kebutuhan untuk mendeteksi dan menonaktifkan *malware* secepat mungkin agar dampak negatif yang ditimbulkan oleh *malware* ini dapat dihindari. *Malware* yang memiliki kemampuan penyebaran adalah yang paling berbahaya karena tidak ada kontrol pusat, sehingga mempertahankan diri dari ancaman ini bukanlah tugas yang mudah. Studi menunjukkan bahwa *malware* merupakan salah satu ancaman paling signifikan terhadap keamanan komputer (William *et al*, 2008).

Detektor *malware* digunakan untuk mendeteksi *malware* dan pemindai antivirus adalah salah satu cara untuk mendeteksi beberapa di antaranya. Namun, dengan kemajuan teknik pengembangan *malware*, detektor *malware* menggunakan berbagai teknik untuk menghindari dampak buruk dari perangkat lunak ini. Karena keterbatasan teknik deteksi *malware* yang ada, metode *machine learning* dan *data mining* digabungkan dengan metode deteksi yang telah ada untuk meningkatkan efisiensi dalam proses deteksi *malware* (Chumachenko *et al*, 2017).



Gambar 2.8 Jenis Malware

Sumber : Belcic, 2023

Berdasarkan gambar 2.8, *malware* ada dalam berbagai bentuk dan secara luas dikategorikan ke dalam kelas-kelas berikut. Kategori-kategori ini tidak saling eksklusif, meskipun banyak dari *malware* tersebut dapat masuk ke dalam lebih dari satu kategori:

a. **Virus**

Virus menginfeksi komputer dan *file* lainnya dengan cara menggandakan dirinya sendiri. Virus tidak dapat bertahan hidup secara independen, sehingga ia menempel pada *file* lain, terutama *file executable* dan aplikasi. Karena fitur penggandaan ini, virus dapat menyebar di antara *file-file* dan bahkan komputer melalui jaringan. Virus dapat menyebabkan penurunan kinerja sistem dan penolakan layanan (*denial of service*) (Spafford *et al*, 1989).

b. ***Worm***

Worms adalah potongan kode berbahaya yang dapat eksis secara independen. Mereka memiliki fitur untuk menggandakan diri. *Worm* menyebar melalui perangkat penyimpanan dan email, serta mengonsumsi sumber daya jaringan dan komputer, yang berdampak pada penurunan kinerja sistem. Karena mereka dapat membuat banyak salinan diri mereka, pemindai antivirus dapat mengidentifikasi kode-kode ini karena keberadaannya yang berlipat ganda (Li, *et al*, 2014).

c. ***Trojan Horse***

Trojan Horse berperilaku seperti program yang berguna, tetapi memiliki tujuan yang berbahaya. Mereka tidak menggandakan diri, tetapi ditransfer ke komputer melalui interaksi internet, seperti saat mengunduh. Trojan dapat mencuri informasi sensitif, mengamati aktivitas pengguna, dan dapat menghapus, mengubah, atau merusak *file* di sistem tempat mereka berada (Idika *et al*, 2007).

d. ***Ransomware***

Ransomware adalah *malware* yang mengambil alih PC Anda dengan mengenkripsi data, menghentikan beberapa aplikasi, dan tidak memungkinkan Anda menggunakan sistem operasi hingga Anda memenuhi tuntutan. Tuntutan ini biasanya berupa uang. Setelah membayar, tidak ada jaminan bahwa Anda akan mendapatkan kembali kendali atas sistem Anda.

e. ***Rootkit***

Rootkit mengambil alih sistem operasi sehingga dapat menyembunyikan dirinya sendiri atau menciptakan lingkungan yang aman bagi *malware* lain untuk bersembunyi di dalam sistem. Pada dasarnya, ini adalah teknik penyamaran untuk menipu antivirus agar tidak dapat menemukan *malware* dalam sistem dan menganggapnya sebagai aplikasi normal.

f. **Spyware**

Spyware digunakan untuk mencuri informasi pribadi seseorang atau mengawasi aktivitas pengguna. Ini di *instal* tanpa sepengetahuan pemilik sistem dan secara diam-diam mengumpulkan informasi untuk dikirim kembali kepada penciptanya. Bahkan perusahaan besar seperti Google juga menggunakan *spyware* untuk mengumpulkan informasi yang diperlukan tentang pengguna mereka (Yin *et al*, 2007).

g. **Adware**

Adware sering kali sangat mengganggu karena menampilkan iklan di komputer pengguna tanpa izin dan menginterupsi aktivitas yang sedang berlangsung. Tujuan dasar dari *adware* adalah untuk mendapatkan keuntungan finansial.

h. **Cookies**

Cookies adalah bentuk *file* teks yang berisi informasi yang disimpan oleh browser web di komputer pengguna untuk digunakan di masa mendatang. Secara umum, *cookies* tidak berbahaya, tetapi dapat menjadi ancaman ketika digunakan oleh *spyware*.

i. **Sniffers**

Sniffer adalah perangkat lunak yang mengamati dan merekam lalu lintas jaringan. Mereka menganalisis berbagai bidang paket dan mengumpulkan informasi untuk mempersiapkan serangan *malware*.

j. **Botnet**

Bot adalah perangkat lunak yang memungkinkan penyerang mengendalikan komputer yang terinfeksi. Jaringan komputer yang terinfeksi ini dikendalikan oleh peretas untuk melakukan aktivitas jahat tanpa sepengetahuan pemiliknya. Mereka dapat melakukan serangan *denial of service* (dos), mengirim pesan spam, dan mencuri informasi.

k. **Keyloggers**

Keylogger adalah jenis *spyware* yang digunakan untuk merekam penekanan tombol guna mencuri kata sandi, detail kartu kredit, dan informasi penting lainnya. Ini biasanya ditransfer ke komputer ketika perangkat lunak berbahaya lainnya diinstal atau ketika pengguna mengunjungi situs yang terinfeksi.

l. **Spam**

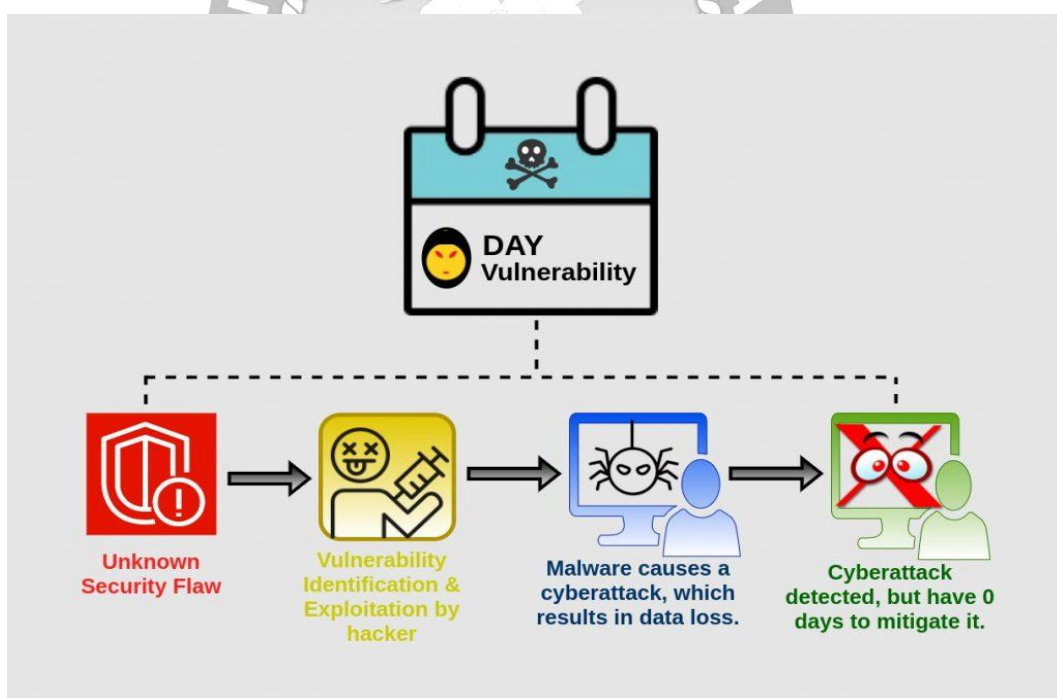
Spam adalah istilah lain untuk email sampah. *Email* yang identik ini dibuat dan dikirim ke banyak penerima sekaligus. Spam mengonsumsi banyak *bandwidth* dan dapat memperlambat sistem.

Industri internet berkembang dengan cepat, pengguna dan organisasi membutuhkan aktivitas yang aman dan terjamin melalui internet. *Malware* adalah ancaman terbesar bagi dunia elektronik saat ini karena mereka berbahaya bagi pengguna dengan mencuri informasi mereka, merusak data dan melumpuhkan jaringan dan sistem dengan serangan jahat. Makalah ini menyajikan dan mengulas jenis-jenis *malware* yang selalu menjadi bahaya bagi dunia komputer. Dari hari ke hari, para penulis *malware* meningkatkan dan mengembangkan teknik kamuflase dari virus yang terenkripsi sederhana hingga virus polimorfik dan metamorfik yang sangat kompleks dan sulit dideteksi (Tahir, 2018).

2.2.2 **Zero day exploit**

Zero-day sering kali dikaitkan dengan istilah kerentanan, eksploitasi, dan serangan. Penting untuk mengetahui perbedaan antara istilah-istilah tersebut (Kaspersky, 2018; Azam *et al*, 2023; Ali, 2022). *Zero day exploit* biasanya menyerang perusahaan-perusahaan besar, organisasi pemerintah, perangkat keras, *firmware*, *Internet of Things* (IoT), dan pengguna yang memiliki akses ke informasi sensitif perusahaan, di antara target-target lainnya (GeeksforGeeks, 2020; Singh *et al*, 2024).

Seperti yang dijelaskan gambar 2.9, bahwa *Zero day exploit* merupakan ketika kerentanan yang dimanfaatkan penyerang untuk mengambil keuntungan dari celah keamanan tersebut dan celah tersebut menjadi kerentanan yang dikenal luas ketika ditemukan dan diserang untuk pertama kalinya. Karena kerentanan ini ditemukan untuk pertama kalinya, tidak ada solusi untuk itu, sehingga dapat dieksploitasi hingga kerentanan tersebut diperbaiki. Untuk deteksi awal kerentanan, organisasi menggunakan beberapa teknik seperti virtual LAN, *Intrusion Detection System* (IDS), *Intrusion Protection System* (IPS), dan akses *Wi-Fi* yang dilindungi, terutama WPA2 menggunakan teknik enkripsi yang kuat dan kunci yang dienkripsi 4096 kali (Kumar, 2014).



Gambar 2.9 Diagram Alur *Malware*

Sumber : Dehran, 2023

Zero-day exploit juga sering kali menjadi bagian dari ancaman siber lanjutan seperti *Advanced Persistent Threats* (APT), di mana serangan dilakukan secara terencana dan terarah terhadap target dengan tujuan mencuri data atau mengganggu operasi penting. Serangan ini memanfaatkan kerentanan sebagai awal, sebelum meluncurkan tahap

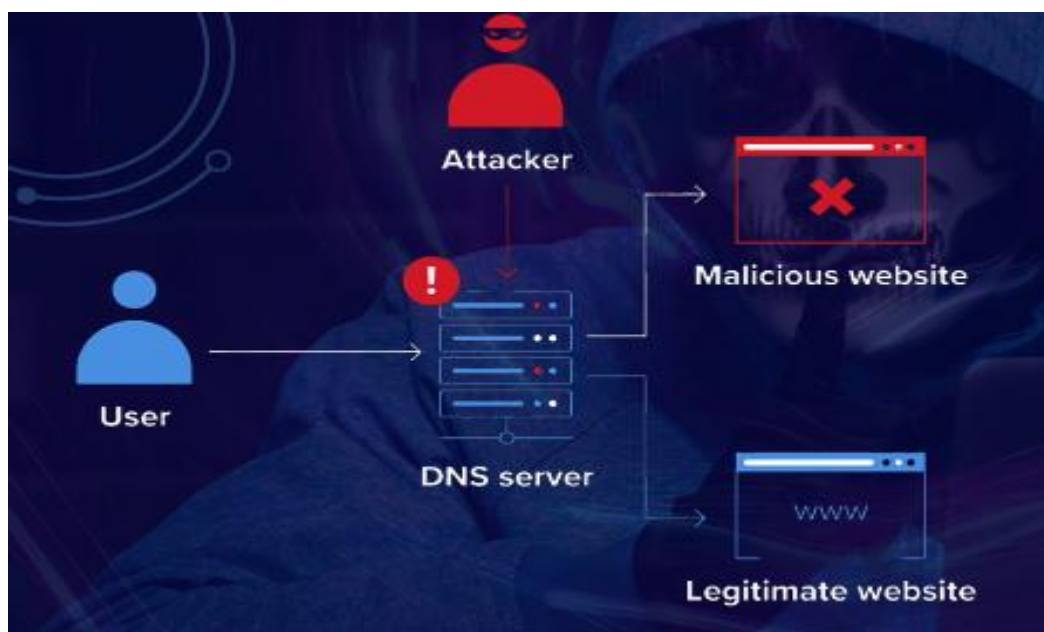
serangan berikutnya yang lebih kompleks. APT menggunakan teknik canggih, seperti kombinasi *exploit* dengan rekayasa sosial atau *spear-phishing*, untuk memastikan serangan tidak terdeteksi oleh sistem keamanan tradisional (Gupta *et al*, 2023; Li *et al*, 2023). Oleh karena itu, pendekatan keamanan siber berbasis prediksi seperti *Threat Intelligence* dan *machine learning* menjadi semakin penting dalam mendeteksi pola anomali yang dapat mengindikasikan serangan (Chen *et al.*, 2024).

Sebagai contoh sebuah *worm* komputer yang sangat cerdas yang dikenal sebagai *Stuxnet* memanfaatkan empat celah perangkat lunak zero-day yang berbeda dalam sistem operasi Microsoft Windows (Hurst and Shone, 2024; Gouda *et al.*, 2022). Selain itu fasilitas nuklir Iran menjadi target beberapa serangan pada tahun 2010 menggunakan *Stuxnet*. Setelah menyusup ke jaringan komputer dari sebuah fasilitas pembangkit listrik nuklir, worm ini mengirimkan perintah berbahaya ke *centrifuge* yang digunakan untuk memperkaya uranium. Instruksi ini memutar *centrifuge* dengan sangat cepat sehingga menyebabkan kerusakan, dan secara keseluruhan, *Stuxnet* merusak 1.000 *centrifuge* (Waheed *et al*, 2024).

2.2.3 Domain Name Server Spoofing (DNS Spoofing)

Domain Name System (DNS) adalah salah satu protokol penting untuk kelancaran aplikasi internet. DNS menyediakan cara untuk mencocokkan nama domain dengan alamat IP yang sesuai, sehingga mengurangi kebutuhan untuk mengingat alamat IP dari sebuah server web. DNS juga disebut sebagai basis data catatan sumber karena tidak hanya mempertahankan pemetaan nama *host* ke alamat IP, tetapi juga catatan lainnya seperti nama server, *mail exchanger*, dan sebagainya. Namun, protokol ini rentan terhadap serangan seperti *DNS cache poisoning*, *DNS amplification attacks*, dan *DNS query flood* (Kaminsky, 2008; MacFarland *et al*, 2017; Zargar *et al*, 2013).

Berdasarkan gambar 2.10 berikut bahwa serangan-serangan ini dapat membahayakan kerahasiaan dan integritas pengguna akhir dengan mengubah lalu lintas mereka atau menyebabkan *Denial-of-Service* (DoS) dengan menargetkan ketersediaan sumber daya. Berbagai alat dan teknik tersedia di luar sana untuk meluncurkan serangan semacam itu (Tripathi *et al*, 2017).



Gambar 2.10 Cara Kerja *DNS Spoofing*

Sumber : Farhan, 2024

DNS rentan terhadap tiga jenis serangan populer. Dalam subseksi ini, kami akan menjelaskan secara singkat masing-masing serangan tersebut.

a. *Kaminsky DNS Cache Poisoning*

Dan Kaminsky mengusulkan pendekatan untuk menyerang catatan *nameserver authority* dengan terlebih dahulu memaksa *nameserver* korban untuk memicu kueri resolusi DNS untuk domain target, kemudian mengirimkan respons DNS yang dipalsukan sehingga *nameserver* korban menerima respons tersebut seolah-olah bahwa itu dikirim oleh *nameserver authority* untuk domain target. Namun, untuk meluncurkan serangan ini,

penyerang perlu memiliki pengetahuan sebelumnya tentang nomor *port* dan nilai identifikasi kueri yang saat ini digunakan oleh *nameserver*. Oleh karena itu, jika kedua nilai nomor *port* 16 bit dan nilai identifikasi kueri 16 bit diacak, akan sangat sulit bagi penyerang untuk menebak kombinasi yang benar sebelum *nameserver* korban mencapai *nameserver authority* yang sebenarnya (Kaminsky, 2008).

b. **DNS Amplification Attack**

Amplifikasi DNS biasanya merupakan serangan DDoS (*distributed denial of service*) di mana penyerang memanfaatkan beberapa *zombie* untuk menghasilkan kueri DNS kecil dengan alamat IP sumber yang dipalsukan. Kueri ini dimaksudkan untuk menghasilkan volume lalu lintas jaringan yang besar karena pesan respons DNS jauh lebih besar dibandingkan dengan pesan kueri DNS. Volume lalu lintas jaringan yang besar ini diarahkan ke korban untuk menghabiskan sumber dayanya. Serangan ini memanfaatkan *resolver* DNS terbuka untuk memantulkan dan memperbesar lalu lintas jaringan. Karena serangan ini menghasilkan sejumlah besar lalu lintas respons DNS di *host* korban, berbagai teknik berbasis *cloud* dapat mendeteksi dan mengurangi serangan ini segera setelah lalu lintas DNS melampaui ambang batas yang telah ditentukan (MacFarland *et al*, 2017; Cisa, 2013).

c. **DNS Query Flooding**

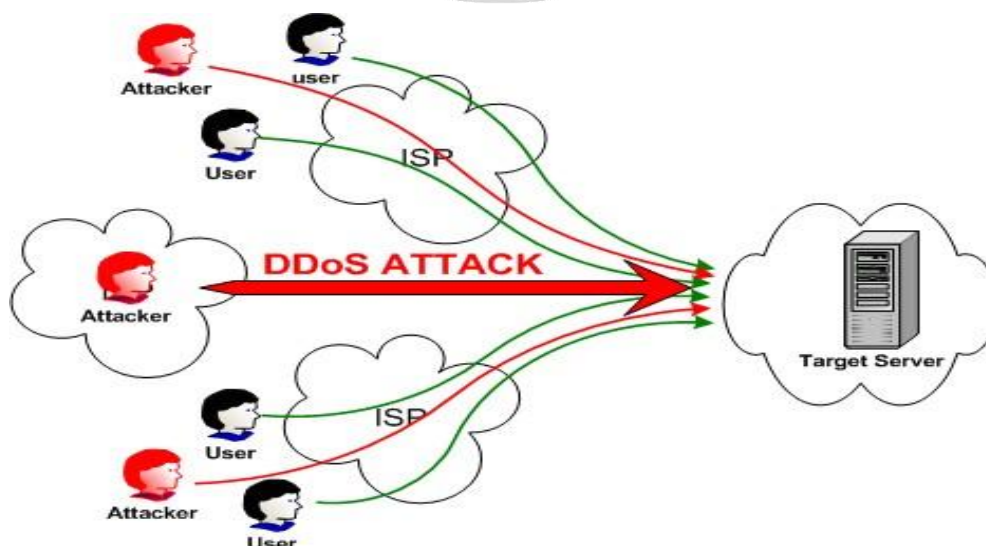
Serangan ini mirip dengan serangan amplifikasi DNS karena juga merupakan jenis serangan DDoS. Namun, untuk meluncurkan serangan ini, penyerang membanjiri *nameserver* korban dengan sejumlah besar kueri DNS sehingga tidak dapat menyelesaikan kueri DNS dari klien yang sah. Karena serangan ini juga menghasilkan volume lalu lintas DNS yang besar, serangan ini dapat dengan mudah terdeteksi jika lalu lintas DNS

melampaui ambang batas yang telah ditentukan (Zargar *et al*, 2013; Taylor, 2024).

Untuk meningkatkan keamanan DNS, beberapa mekanisme telah diperkenalkan, seperti *DNS Security Extensions* (DNSSEC), yang memungkinkan validasi integritas data dan otentikasi asal data dengan menggunakan kriptografis. DNSSEC dirancang untuk mencegah serangan seperti *DNS cache poisoning* dengan memastikan bahwa respon DNS tidak dimanipulasi oleh pihak yang tidak sah. Selain itu, pengadopsian praktik terbaik seperti *rate limiting*, pengawasan *query*, dan enkripsi *query* melalui protokol DNS juga menjadi hal penting dalam melindungi infrastruktur DNS dari berbagai jenis serangan (Schomp *et al*, 2019; Atkins *et al*, 2018).

2.2.4 Distributed Denial of Service (Ddos)

Serangan *distributed denial-of-service* (DDoS) telah menjadi ancaman nyata bagi jaringan, digital, dan infrastruktur siber (Geng *et al*, 2000), serangan ini mampu menyebabkan gangguan besar-besaran pada infrastruktur teknologi komunikasi informasi (TIK). Ada banyak alasan untuk meluncurkan serangan DDoS ini termasuk keuntungan finansial, keuntungan politik, dan gangguan (Ottis, 2008; Neslen, 2012; Musil, 2014).



Gambar 2.11 Diagram Ddos

Sumber : Terabit Komputer In Teknologi, 2024

Berdasarkan gambar 2.11, bahwa serangan DDoS dapat melumpuhkan jaringan dan layanan dengan membanjiri server, sambungan jaringan, dan perangkat jaringan (*router*, *switch*, dan lain-lain) dengan *traffic* yang tidak sah. Serangan ini dapat menyebabkan degradasi layanan atau penolakan layanan secara total yang mengakibatkan kerugian besar.

Meningkatnya ketergantungan pada Internet dan pusat data telah memperparah masalah ini. Meningkatnya ketergantungan infrastruktur penting suatu negara pada TIK telah memunculkan kebutuhan akan solusi yang efisien untuk perlindungan terhadap serangan *DDoS*. Sebagai contoh, pusat data yang menjalankan layanan penting, seperti *smart grid*, perlu dilindungi agar dapat terus memberikan layanan yang sangat andal (Paroutis *et al*, 2014; Bawany *et al*, 2015).

Untuk mengatasi ancaman serangan DDoS, berbagai teknik mitigasi telah dikembangkan, termasuk sistem *Intrusion Prevention System* (IPS), *firewall* tingkat aplikasi, dan layanan mitigasi berbasis *cloud*. Salah satu pendekatan yang populer adalah menggunakan *Distributed Denial-of-Service Mitigation (DDoS Mitigation)*, yang mengandalkan pemfilteran lalu lintas secara *real-time* untuk membedakan antara lalu lintas sah dan tidak sah, sehingga hanya *traffic valid* yang dapat mencapai server. Selain itu, penggunaan teknik *rate limiting* dan *blackholing* dapat membantu mengurangi dampak serangan dengan membuang *traffic* yang mencurigakan sebelum mencapai target. Strategi ini sering dipadukan dengan pengawasan berbasis *machine learning*, yang memungkinkan identifikasi pola serangan secara dinamis untuk mencegah ancaman yang lebih canggih (Kalkan & Gür, 2018; Kumar *et al.*, 2020).

2.2.5 Phishing

Phishing adalah teknik serangan *cyber* di mana penyerang memanipulasi korban untuk berbagi informasi sensitif, seperti *credential login*, detail kartu kredit, atau data pribadi lainnya. Serangan ini sering kali berbentuk email yang menipu, situs web palsu, atau pesan

palsu yang tampaknya berasal dari organisasi terpercaya. Penyerang mengeksploitasi pemicu psikologis seperti urgensi, ketakutan, atau otoritas untuk memikat korban untuk mengklik tautan berbahaya atau mengunduh *malware*. Efektivitas dan sifat *phishing* yang tersebar luas menjadikannya salah satu ancaman paling umum keamanan siber secara global (Musil *et al*, 2020; Arshad *et al*, 2021; Ayeni *et al*, 2024).

Konsekuensi dari *phishing* adalah signifikan, mencakup pencurian keuangan, penipuan identitas, dan reputasi kerusakan pada individu dan organisasi. *Spear phishing*, sebuah bentuk *phishing* yang ditargetkan *phishing*, memanfaatkan detail pribadi untuk meningkatkan kredibilitas, sementara bisnis sedangkan penipuan kompromi email (BEC) mengeksploitasi hubungan profesional. Munculnya *smishing* (*phishing* SMS) dan *vishing* (*phishing* suara) mencerminkan penyerang beradaptasi dengan saluran komunikasi baru. Studi menunjukkan bahwa serangan *phishing* bertanggung jawab atas lebih dari 80% pelanggaran data, dengan kecanggihannya meningkat setiap tahunnya (Musil *et al*, 2020; Arshad *et al*, 2021).

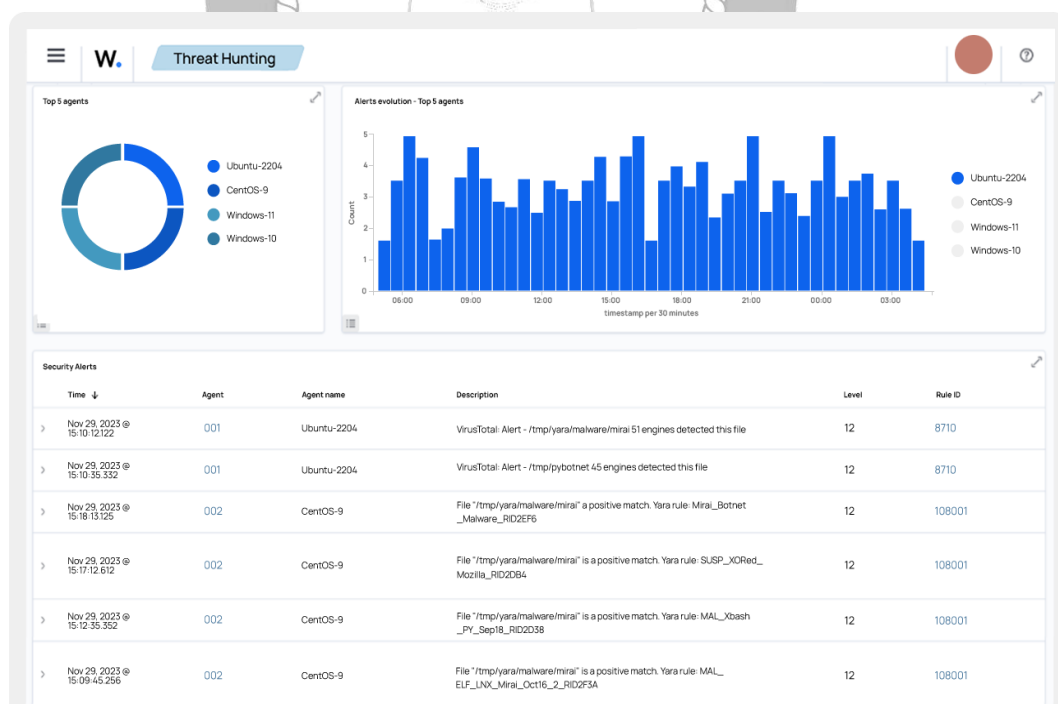


Gambar 2.12 Cara Mitigasi *Phising*

Sumber : padangsambian.denpasarkota, 2024

Berdasarkan gambar 2.12, cara *memitigasi phishing* membutuhkan kombinasi solusi teknologi dan edukasi pengguna. Sistem penyaringan email yang canggih dan algoritme pembelajaran mesin kini mampu mendeteksi pola *phishing* dan memblokir ancaman secara *real-time*. Kampanye kesadaran menekankan pada pengenalan tanda-tanda *phishing*, seperti URL yang mencurigakan atau lampiran yang tidak diminta. Otentikasi multi-faktor (MFA) semakin memperkuat keamanan akun dengan menambahkan lapisan verifikasi ekstra. Penelitian terus mengeksplorasi solusi *anti-phishing* berbasis AI untuk mengatasi lanskap ancaman dunia maya yang terus berkembang (Musil *et al*, 2020; Ayeni *et al*, 2024).

2.2.6 Wazuh



Gambar 2.13 GUI Wazuh

Sumber : Wazuh, 2025

Wazuh merupakan sebuah platform *open-source* dan gratis untuk deteksi ancaman dan pemantauan keamanan sesuai dengan aturan keamanan yang telah ditetapkan. Platform ini dapat digunakan untuk memantau *endpoint* seperti desktop, laptop, server, atau perangkat jaringan

seperti *firewall* dan *router*, dan untuk mengumpulkan dan menganalisis data secara *real-time*. Wazuh dapat melakukan hal-hal sebagai berikut:

a. Analisis keamanan

Pengumpulan, agregasi, pengindeksan dan pemrosesan data keamanan, membantu organisasi mendeteksi intrusi, ancaman, dan anomali perilaku.

b. Deteksi Intrusi

Wazuh akan memindai sistem yang dipantau untuk mencari ancaman seperti *malware*, *rootkit*, dan anomali yang mencurigakan. Mereka dapat mendeteksi *file* tersembunyi.

c. Analisis Data Log

Wazuh dapat membaca operasi log sistem dan aplikasi, dan meneruskannya dengan aman ke user untuk dilakukan analisis berbasis *rules* atau aturan yang ditetapkan.

d. Pemantauan Integritas File

Wazuh memonitor *file* sistem, mengidentifikasi perubahan dalam konten, izin, kepemilikan, dan atribut *file* yang perlu diperhatikan.

e. Pendeteksi Kerentanan

Wazuh dapat membaca perangkat lunak serta data dan mengirimkan informasi ini ke server yang di mana informasi ini dikorelasikan dengan CVE (Common Vulnerability and Exposure) atau tinjauan kemampuan Wazuh untuk mendeteksi serangan berdasarkan analisis log kerentanan dan paparan basis data, untuk mengidentifikasi perangkat lunak yang rentan terhadap serangan.

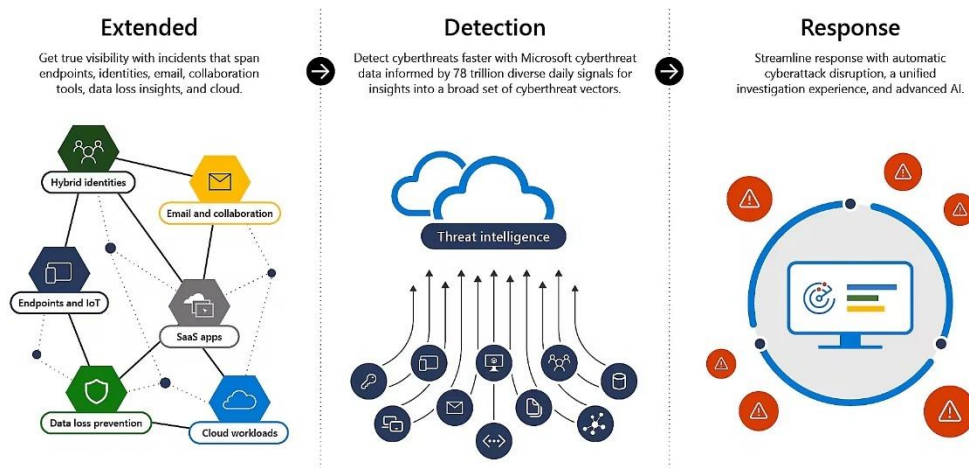
f. Penilaian Konfigurasi

Wazuh memonitor sistem sistem dan pengaturan konfigurasi aplikasi untuk memastikannya sesuai dengan kebijakan dan standar keamanan. Agen melakukan pemindaian berkala untuk mendeteksi aplikasi yang diketahui diketahui rentan, belum ditambah, atau dikonfigurasi secara tidak aman.

Maka dengan ini dapat dikatakan bahwa Wazuh merupakan Salah satu solusi yang dapat membantu meningkatkan keamanan sistem informasi. Wazuh dapat menjadi alat yang ampuh dalam *monitoring* dan deteksi ancaman karena dapat menampilkan semua serangan yang terdeteksi dengan sangat detail dan secara *real-time* seperti pada gambar 2.13. Selain itu, Wazuh dapat ditanamkan di berbagai infrastruktur teknologi informasi.

2.3 Applied Theory

2.3.1 Konsep Extended *Detection* and Response (XDR)



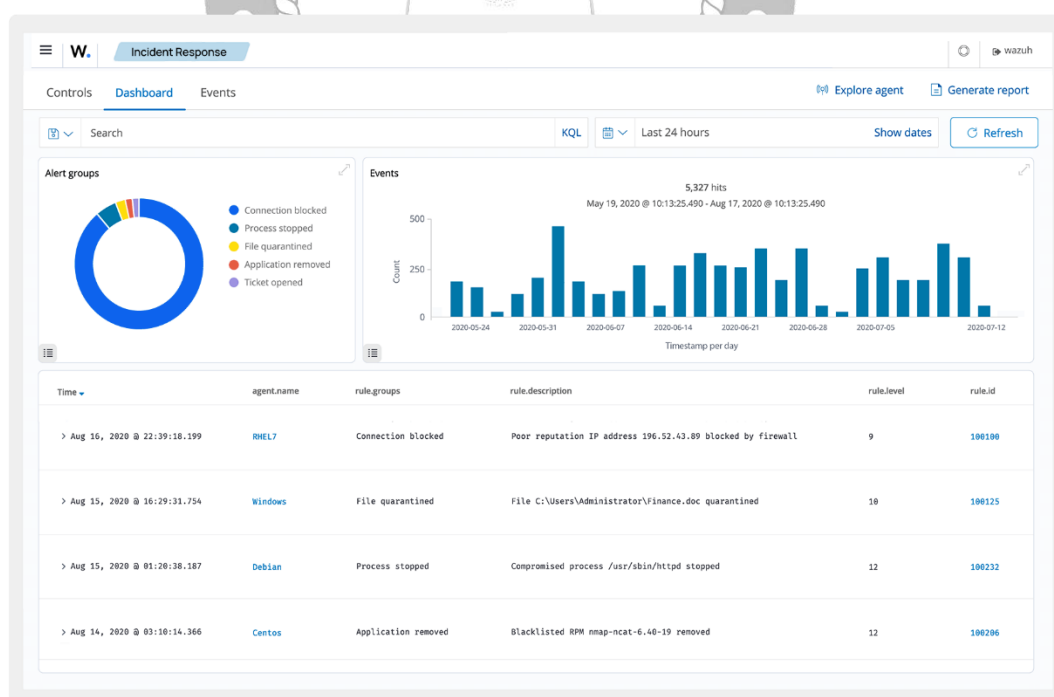
Gambar 2.14 Diagram XDR

Sumber : microsoft, 2024

Seperti pada gambar 2.13, dapat dikatakan bahwa XDR merupakan pendekatan untuk *threat detection and response*, hal ini memberikan pandangan yang luas serta lugas dari seluruh cakupan teknologi. Dengan demikian, XDR memungkinkan visibilitas data di seluruh jaringan, *cloud*, *endpoint*, dan aplikasi, menerapkan analitik dan otomatisasi untuk mendeteksi, menganalisis, memburu, dan mitigasi ancaman (Cisco, 2021). Titik pembeda utama dari XDR adalah bahwa ia mengumpulkan dan menghubungkan data dari seluruh infrastruktur, termasuk email, titik akhir, server, beban kerja cloud, dan jaringan, sehingga memungkinkan visibilitas

global dan konteks ancaman tingkat lanjut. Oleh karena itu, ancaman dapat dianalisis, diprioritaskan, dikejar, dan diperbaiki untuk mencegah kehilangan data dan pelanggaran keamanan.

Seiring dengan meningkatnya visibilitas, begitu juga dengan konteks ancaman, peristiwa yang tidak akan sebelumnya tidak akan ditangani sebelumnya dapat dikorelasikan secara keseluruhan, memungkinkan tim keamanan untuk mengidentifikasi dan menghilangkan atau mengurangi tingkat keparahan dan cakupan serangan. XDR mengkonsolidasikan beberapa produk menjadi deteksi insiden keamanan yang kohesif dan terpadu dan platform respons yang terpadu, deteksi titik akhir yang terus berkembang deteksi titik akhir yang berkembang dan solusi respons (Mcafee, 2021).



Gambar 2.15 GUI XDR Wazuh

Sumber : Wazuh, 2024

Secara umum, ia menyediakan fitur-fitur seperti deteksi dan respons terhadap serangan yang ditargetkan (seperti ditampilkan pada gambar 2.15), dukungan untuk analisis perilaku pengguna dan perangkat,

ancaman intelijen, memungkinkan pengurangan kebutuhan untuk menganalisis peristiwa positif palsu dengan mengkorelasikan dan mengkonfirmasi peringatan ini secara otomatis, itu membuat triase insiden yang lebih akurat, memungkinkan memprioritaskan aktivitas, dan komprehensif analisis infrastruktur. Dengan demikian, tim keamanan akan memiliki lebih banyak informasi tentang hal-hal berikut ini:

a) **Detection**

Ancaman kritis dan peristiwa keamanan yang terkumpul peristiwa keamanan yang dikumpulkan dianalisis lebih lanjut pada platform yang kompleks.

b) **Investigate**

Memungkinkan korelasi dari semua informasi peristiwa yang dikumpulkan yang relevan dan memberikan dukungan dalam mengidentifikasi akar penyebab masalah.

c) **Recommendation**

Memberikan saran untuk memperdalam investigasi melalui pertanyaan lebih lanjut pertanyaan lebih lanjut dan memungkinkan tindakan yang harus diambil untuk mengatasi atau memperbaiki risiko atau ancaman yang terdeteksi risiko atau ancaman yang terdeteksi.

d) **Hunt**

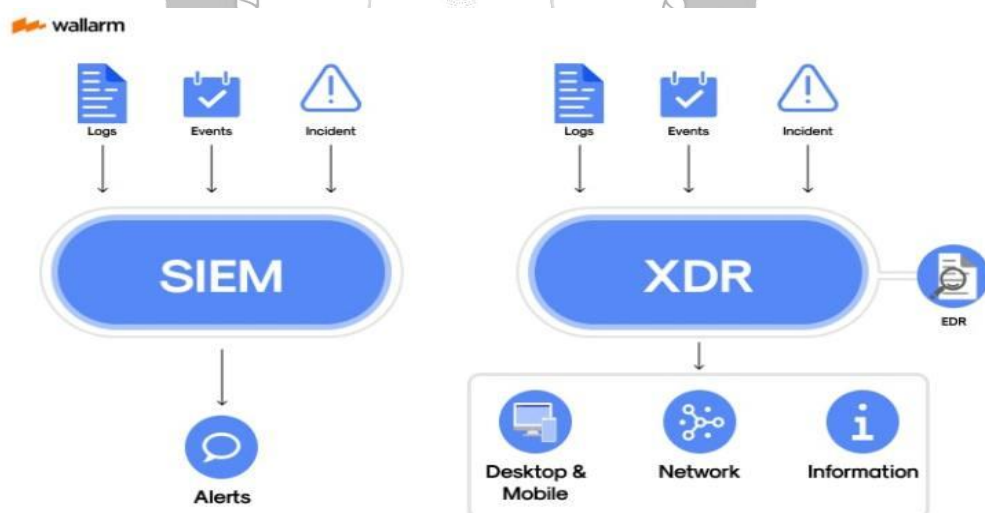
Hal ini akan memungkinkan permintaan data repositori data dari berbagai vendor untuk mendeteksi perilaku dan ancaman yang mencurigakan perilaku dan ancaman yang mencurigakan, dan dengan demikian mengambil tindakan resolusi.

e) **Response**

Memungkinkan untuk memblokir serangan yang diketahui dan tidak diketahui berbasis intelijen dengan memanfaatkan analitik buatan dan perlindungan ancaman perilaku untuk menghentikan *malware*, eksploitasi, dan serangan tanpa *file* (Brandao *et al*, 2021).

XDR tidak hanya meningkatkan visibilitas dan respons terhadap ancaman, tetapi juga memfasilitasi kolaborasi yang lebih baik di antara tim keamanan. Dengan mengintegrasikan data dari berbagai sumber, XDR mengurangi silo informasi dan memungkinkan berbagi intelijen ancaman secara *real-time*. Kemampuan analitik canggihnya membantu tim menganalisis pola serangan, sehingga dapat mengantisipasi dan memitigasi ancaman sebelum menjadi insiden serius. Dengan demikian, XDR berfungsi sebagai alat deteksi dan respons, sekaligus mendukung strategi keamanan yang lebih proaktif dan kolaboratif (Cisco 2024; McNutt *et al*, 2024).

2.3.2 Pembeda Antara SIEM, XDR dan SOAR



Gambar 2.16 Perbedaan XDR dengan SIEM

Sumber : Novikov, 2024

XDR dianggap sebagai penerus SIEM. Kemampuan utama SIEM adalah mengumpulkan dan menganalisis volume besar peristiwa log dan data lainnya. Ini terutama merupakan alat penelitian, yang membutuhkan tim keamanan untuk melakukan banyak analisis untuk menyimpulkan. Berdasarkan gambar 2.14, XDR berfokus pada deteksi ancaman dan tanggapan. Ini membedakan dengan secara otomatis merespons ancaman

secara otomatis atau, jika itu tidak memungkinkan, itu mempercepat penyelidikan dan analisis, meningkatkan waktu respons. Fitur pembeda XDR adalah bahwa ia memberikan visibilitas ke seluruh siklus hidup serangan dalam kaitannya dengan seluruh lingkungan, dari infiltrasi ke gerakan lateral, pembersihan, atau mitigasi. Mengadopsi EDR, SIEM, dan solusi lainnya secara mandiri tidak memberikan konteks strategis strategis dan korelasi yang diperlukan untuk menilai ancaman saat ini lingkungan saat ini secara bermakna. Solusi XDR dapat membantu mengisi celah ini (Brandao *et al*, 2021).

Tabel 2.1 Perbedaan Antara XDR dengan SIEM

Fitur	XDR	SIEM	SOAR
Cakupan	XDR, mencakup <i>endpoint</i> , jaringan, <i>cloud</i> , dan identitas	SIEM, dengan fokus pada pengumpulan dan analisis log	Mengelola dan mengotomatiskan respons keamanan secara holistik
Deteksi Ancaman	Deteksi ancaman secara <i>real-time</i> termasuk <i>threat hunting</i> tingkat lanjut dan respons insiden	Deteksi ancaman berbasis log, dengan mengandalkan analisis dan korelasi berbasis <i>rule</i>	Mengintegrasikan deteksi ancaman dari berbagai sumber dan memberikan respons otomatis
Pengumpulan Data	Pengumpulan data berbasis agen dan tanpa agen, termasuk data <i>endpoint</i> , jaringan, dan <i>cloud</i>	Pengumpulan data berbasis log, mengandalkan pengumpulan log berbasis agen dan tanpa agen	Mengumpulkan data dari berbagai sumber dan sistem keamanan
Analisis Data	Analisis tingkat lanjut, termasuk <i>machine learning</i> , analisis perilaku kebiasaan, dan deteksi anomali	Analisis berbasis <i>rule</i> , korelasi, dan pemfilteran data log	Analisis dan prioritas insiden dengan konteks, sering kali menggunakan machine learning

Fitur	XDR	SIEM	SOAR
Respon Insiden	Respons insiden secara <i>real-time</i> , termasuk penahanan, perbaikan, dan analisis pasca-insiden	Respons insiden berbasis log, mengandalkan analisis dan respons manual	Respons otomatis dan orkestrasi untuk insiden dengan playbook yang telah ditentukan
Dukungan Cloud	Dukungan asli untuk lingkungan cloud, termasuk AWS, Azure, dan Google Cloud	Dukungan terbatas untuk lingkungan cloud, membutuhkan integrasi tambahan	Dukungan untuk cloud dengan otomatisasi respons di lingkungan cloud
Manajemen Identitas dan Akses	Integrasi dengan sistem manajemen identitas dan akses, termasuk autentikasi dan otorisasi	Dukungan terbatas untuk manajemen identitas dan akses, dengan fokus pada pengumpulan dan analisis log	Integrasi dengan sistem manajemen identitas dan akses untuk respons yang lebih baik
Analisis Lalu Lintas Jaringan	Analisis lalu lintas jaringan secara <i>real-time</i> , termasuk analisis flow dan <i>packet capture</i>	Dukungan terbatas untuk analisis lalu lintas jaringan, dengan mengandalkan analisis berbasis log	Analisis lalu lintas jaringan dengan reaksi otomatis terhadap ancaman
Perlindungan Beban Kerja Cloud	Dukungan asli untuk perlindungan beban kerja cloud, termasuk pemantauan fungsi kontainer dan tanpa server	Dukungan terbatas untuk perlindungan beban kerja cloud, membutuhkan integrasi tambahan	Perlindungan dan respons otomatis untuk beban kerja cloud

Fitur	XDR	SIEM	SOAR
Biaya	Biasanya lebih mahal daripada solusi SIEM, karena analitik tingkat lanjut dan respons insiden waktu nyata	Biasanya lebih murah daripada solusi XDR, karena analisis dan korelasi berbasis log	Biaya bervariasi, tergantung pada solusi dan integrasi yang digunakan
Kompleksitas	Lebih kompleks untuk diimplementasikan dan dikelola, karena analitik tingkat lanjut dan respons insiden secara real-time	Tidak terlalu rumit untuk diimplementasikan dan dikelola, karena analisis dan korelasi berbasis log	Kompleksitas tinggi, memerlukan pengaturan playbook dan integrasi
Integrasi	Membutuhkan integrasi dengan alat dan sistem keamanan yang ada, termasuk titik akhir, jaringan, dan manajemen identitas	Biasanya membutuhkan integrasi dengan alat dan sistem keamanan yang ada, termasuk titik akhir, jaringan, dan manajemen identitas	Memerlukan integrasi dengan berbagai alat dan sistem keamanan untuk orkestrasi
Pelaporan dan Visualisasi	Kemampuan pelaporan dan visualisasi tingkat lanjut, termasuk dasbor dan peringatan	Kemampuan pelaporan dan visualisasi yang terbatas, bergantung pada analisis dan korelasi berbasis log	Pelaporan dan visualisasi insiden dengan analisis konteks
Orkestrasi Keamanan	Dukungan asli untuk orkestrasi keamanan, termasuk respons dan remediasi insiden otomatis	Dukungan terbatas untuk orkestrasi keamanan, membutuhkan integrasi tambahan	Fokus utama pada orkestrasi keamanan, dengan kemampuan untuk mengotomatiskan respons

Sumber : sentinelone, 2024

Pada dasarnya SIEM dan XDR adalah dua solusi keamanan yang berbeda yang melayani tujuan berbeda dalam bidang deteksi dan respons ancaman. Sementara SIEM adalah solusi keamanan komprehensif yang mengumpulkan, memantau, dan menganalisis data terkait keamanan dari berbagai sumber, XDR adalah solusi yang lebih khusus yang berfokus secara khusus untuk mendeteksi dan merespons ancaman tingkat lanjut, seperti APT (*Advanced Persistent threats*) dan serangan *zero-day* (SentinelOne, 2024).

2.4 Hasil Penelitian Terdahulu

Berdasarkan hasil literasi mengenai penelitian terdahulu yang sudah ada, parameter mengenai metode dan hasil, persamaan dan perbedaan akan disajikan dalam bentuk tabel sebagai berikut.

Tabel 2.2 Hasil Penelitian Terdahulu

No .	Peneliti, Tahun, Judul	Metode dan Hasil	Persamaan	Perbedaan
1	Brandao <i>et al</i> , 2021 – <i>Extended Detection and Response</i>	XDR digunakan untuk alat dan sebuah pendekatan dalam keamanan siber. XDR dapat meningkatkan efektivitas operasi keamanan berdasarkan parameter waktu.	XDR sebagai <i>tools</i> atau alat guna meningkatkan keamanan siber.	Fokus pada konteks mendeteksi ancaman dalam keamanan siber.
2	George <i>et al</i> , 2021 - XDR: <i>The Evolution of Endpoint Security Solutions - Superior Extensibility and Analytics to Satisfy the Organizational Needs of the Future</i>	XDR digunakan untuk alat serta pendekatan dalam keamanan siber. XDR dapat meningkatkan visibilitas dan respon.	XDR sebagai alat untuk meningkatkan visibilitas yang luas dan dapat mendeteksi ancaman serta meresponnya.	Berfokus pada evolusi perubahan serta perbedaan dari EDR.

No	Peneliti, Tahun, Judul	Meotde dan Hasil	Persamaan	Perbedaan
3	George <i>et al</i> , 2023 - <i>Extending Detection and Response: How MXDR Evolves Cybersecurity</i>	XDR digunakan untuk mengoleksi data diantaranya <i>network traffic, cloud workloads</i> , dan <i>identity events</i> yang di kombinasikan dengan pendekatan MDR. XDR dapat mengoptimalkan operasi keamanan dan mengurangi risiko terhadap kemanan siber.	XDR digunakan untuk mengintegrasikan data yang terdapat pada sistem keamanan siber.	Berfokus terhadap pengintegrasian XDR dengan pendekatan MDR.
4	Kaur <i>et al.</i> , 2024 - <i>Evolution of Endpoint Detection and Response (EDR) in Cyber Security: A Comprehensive Review</i>	XDR digunakan sebagai pendekatan guna mengintegrasikan data yang terdapat di semua lapisan keamanan siber. XDR meningkatkan efektivitas terhadap merespon ancaman.	XDR digunakan untuk mengintegrasikan data dari seluruh <i>layer</i> atau lapisan keamanan yang terdapat dalam sistem keamanan siber.	Berfokus pada progress atau perkembangan EDR yang mendekati XDR.
5	Bassey <i>et al</i> , 2024 - <i>Enhancing DDoS Attack Prevention And Detection Using IDS And XDR</i>	XDR digunakan sebagai pendeteksi ancaman terutama Ddos. XDR yang di integrasikan dengan IDS dapat melakukan pendeteksian dan mitigasi teradap Ddos. XDR efektif dalam menghadapi ancaman Ddos.	XDR digunakan untuk mendeteksi ancaman serta merespon ancaman terhadap keamanan siber.	Befokus kepada pendeteksian hanya dalam bentuk ancaman Ddos.

Sumber : diolah oleh peneliti, 2024

Tabel 2.2 memberikan ringkasan mengenai penelitian terdahulu yang relevan dengan implementasi XDR pada tim SOC dan CSIRT dalam penignkatan sistem keamanan informasi. Penelitian (Brandao *et al*, 2021 –

Extended Detection and Response) membahas penggunaan XDR sebagai alat dan pendekatan dalam keamanan siber. XDR diidentifikasi sebagai solusi yang dapat meningkatkan efektivitas operasi keamanan dengan memberikan kemampuan deteksi dan respons yang lebih baik terhadap ancaman. Fokus utama dari penelitian ini adalah pada konteks deteksi ancaman dalam keamanan siber, menekankan pentingnya integrasi berbagai sumber data untuk meningkatkan respons terhadap insiden keamanan.

Penelitian (George *et al*, 2021 - *XDR: The Evolution of Endpoint Security Solutions*) dalam studi ini, XDR juga diposisikan sebagai alat dan pendekatan dalam keamanan siber, dengan penekanan pada peningkatan visibilitas dan respons terhadap ancaman. Penelitian ini menyoroti bagaimana XDR dapat memberikan visibilitas yang lebih luas dan kemampuan untuk mendeteksi serta merespons ancaman secara efektif. Berbeda dengan penelitian sebelumnya, fokus penelitiannya adalah pada evolusi dan perubahan yang terjadi dari EDR ke XDR, serta bagaimana XDR memenuhi kebutuhan organisasi di masa depan.

Penelitian (George *et al*, 2023 - *Extending Detection and Response: How MXDR Evolves Cybersecurity*) penelitian ini mengeksplorasi penggunaan XDR dalam mengumpulkan data dari berbagai sumber, termasuk lalu lintas jaringan, beban kerja *cloud*, dan peristiwa identitas, yang kemudian digabungkan dengan pendekatan *Managed Detection and Response* (MDR). Hasilnya menunjukkan bahwa XDR dapat mengoptimalkan operasi keamanan dan mengurangi risiko terhadap keamanan siber. Fokus utama dari penelitian ini adalah pada integrasi XDR dengan pendekatan MDR, yang memberikan perspektif baru dalam pengelolaan keamanan.

Penelitian (Kaur *et al*, 2024 - *Evolution of Endpoint Detection and Response (EDR) in Cyber Security: A Comprehensive Review*) membahas XDR sebagai pendekatan untuk mengintegrasikan data di semua lapisan keamanan siber. Penelitian ini menekankan bahwa XDR meningkatkan efektivitas respons terhadap ancaman dengan mengumpulkan dan menganalisis data dari seluruh lapisan sistem keamanan. Fokus dari penelitian ini adalah pada perkembangan EDR menuju XDR, menunjukkan bagaimana XDR dapat menjadi solusi yang lebih komprehensif dalam menghadapi tantangan keamanan siber.

Penelitian (Basseyy *et al*, 2024 - *Enhancing DDoS Attack Prevention And Detection Using IDS And XDR*) dalam penelitian ini, XDR digunakan sebagai alat untuk mendeteksi ancaman, khususnya serangan DDoS. Penelitian menunjukkan bahwa integrasi XDR dengan *Intrusion Detection Systems* (IDS) dapat meningkatkan kemampuan pendeteksian dan mitigasi terhadap serangan DDoS. Fokus utama dari penelitian ini adalah pada pendeteksian ancaman dalam konteks serangan DDoS, menyoroti efektivitas XDR dalam menghadapi jenis ancaman ini.

2.5 Kerangka Berpikir

Judul

Implementasi Extended *Detection* and Response Pada Security Operation Center dan Cyber Security Incident Response Team Dalam Peningkatan Sistem Keamanan Informasi Guna Meningkatkan Sistem Pertahanan Informasi

Masalah

- **Masalah Umum:** Perkembangan ancaman siber yang semakin kompleks dan berbahaya bagi infrastruktur teknologi informasi
- **Masalah Penelitian:** Maraknya serangan siber terhadap infrastruktur teknologi informasi seperti *malware*, *domain attack* dan eksploitasi.

Teori Penyelesaian Masalah

Implementasi XDR pada tim SOC dan CSIRT untuk peningkatan sistem keamanan informasi mengacu pada beberapa teori serta penelitian terdahulu yang relevan dengan topik diatas :

- **Extended Detection and Response (XDR):** Penelitian oleh Brandao *et al.* (2021) menjabarkan XDR serta menunjukkan bahwa XDR dapat meningkatkan efektivitas operasi keamanan siber yang dapat meningkatkan keamanan informasi teknologi di dalam infrastruktur teknologi informasi.
- **XDR untuk optimalisasi keamanan siber:** Penelitian oleh George *et al.* (2023) menjelaskan mengenai XDR yang dapat melakukan pengkoleksian data, analisis dan respon terhadap anomali atau insiden yang dikombinasikan dengan pendekatan MDR yang dapat mengoptimalkan operasi keamanan siber.
- **Efisiensi serta efektivitas XDR terhadap keamanan siber:** Penelitian oleh Kaur *et al.* (2024) menjabarkan bahwasanya XDR mengintegrasikan data dari seluruh *layer* atau lapisan keamanan yang terdapat di infrastruktur teknologi informasi yang kemudian meningkatkan efektivitas terhadap merespon ancaman dan efisien secara waktu.

Solusi dari Masalah Berdasarkan Teori Pendukung

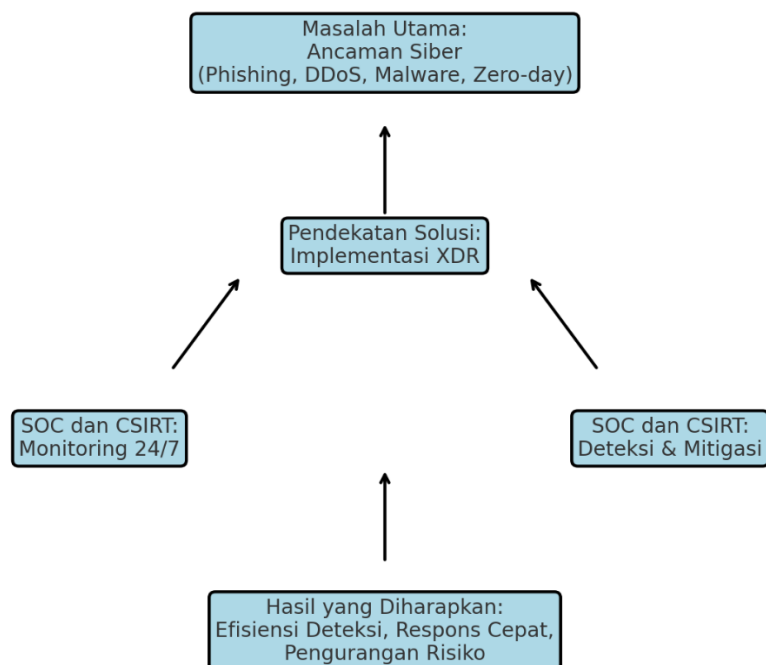
Berdasarkan teori dan penelitian yang sudah ada, Brando *et al.*, (2021) XDR digunakan sebagai alat dan pendekatan guna meningkatkan keamanan informasi dengan operasi keamanan *Detection, Investigate, Recommendation, Hunt*, dan *Response*. Pada penelitian yang dilakukan oleh George *et al.*, (2023); Kaur *et al.*, (2024); dan Bassey *et al.*, (2024), para peneliti mengatakan bahwa XDR dapat membantu meningkatkan efektivitas terhadap respon ancaman, deteksi ancaman, mitigasi dan mengurangi risiko terhadap ancaman keamanan infrastruktur teknologi informasi.

XDR diintegrasikan dengan seluruh lapisan keamanan dan XDR akan mengumpulkan, menganalisis dan merespon berdasarkan data dari seluruh lapisan keamanan yang ada pada infrastruktur.

Hasil Dari Penelitian

Penelitian ini diharapkan dapat membantu meningkatkan keamanan informasi pada tim SOC dan CSIRT dengan menggunakan XDR yang diintegrasikan dengan seluruh lapisan keamanan pada infrastruktur keamanan informasi serta dapat meningkatkan efisiensi kerja tim SOC dan CSIRT dalam mengidentifikasi masalah.

Kesimpulan : XDR akan menjadi alat serta pendekatan atas peningkatan dan pengembangan sistem keamanan informasi dengan mengintegrasikannya dengan seluruh lapisan keamanan yang ada pada infrastruktur keamanan. Dengan adanya penelitian ini diharapkan akan menjadi solusi atas tantangan yang dihadapi oleh tim SOC dan CSIRT.



Gambar 2.17 Kerangka Berpikir

Sumber : Diolah oleh penulis, 2024

Berdasarkan gambar 2.15 diatas, dapat dikatakan bahwa kerangka berpikir penelitian ini dimulai dengan mengidentifikasi masalah utama, yaitu meningkatnya ancaman siber kompleks terhadap infrastruktur teknologi informasi, misalnya *phishing*, serangan *Distributed Denial of Service* (DDoS), *malware*, dan *zero-day exploits*. Ancaman ini memerlukan pendekatan yang lebih komprehensif dikarenakan sistem keamanan tradisional seringkali tidak mampu mendeteksi dan merespons serangan

secara efektif. Dalam penelitian ini, implementasi *Extended Detection and Response* (XDR) disarankan menjadi solusi untuk mengatasi tantangan ini. XDR memiliki kemampuan integrasi data berdasarkan berbagai instrumen teknologi informasi seperti *endpoint*, jaringan, *cloud*, dan email untuk meningkatkan visibilitas dan analisis ancaman.

Selanjutnya, XDR diintegrasikan di kelola oleh *Security Operations Center* (SOC) dan *Computer Security Incident Response Team* (CSIRT) untuk memperkuat kemampuan *monitoring*, deteksi, dan mitigasi ancaman. Dalam hal *monitoring*, SOC memanfaatkan visibilitas menyeluruh dari data yang di koleksi dan di integrasikan oleh XDR untuk mengawasi jaringan secara *real-time*, sedangkan dalam hal pendeteksian dan mitigasi dilakukan menggunakan dukungan analisis berbasis kecerdasan buatan (AI). Hal ini memungkinkan respons yang lebih cepat terhadap insiden maupun ancaman keamanan dan mengurangi risiko peningkatan ancaman.

Pada akhirnya, *output* yang diperlukan berdasarkan implementasi XDR merupakan peningkatan efisiensi pada deteksi dan respons ancaman, mitigasi, dan pengurangan risiko kerugian dari ancaman siber. Dengan pendekatan yang terintegrasi ini, sistem keamanan infrastruktur teknologi informasi dan diharapkan sanggup menghadapi tantangan ancaman siber yang terus berkembang.