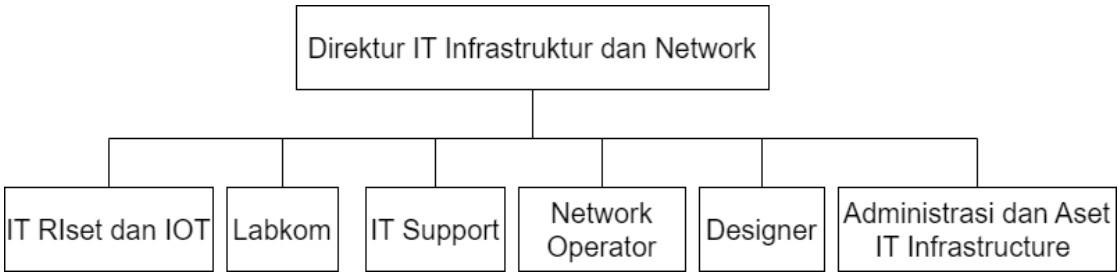
# BAB 2
# TINJAUAN PUSTAKA

## 2.1 Struktur Organisasi

Berikut Gambar 2.1 merupakan diagram struktur organisasi yang berjalan di divisi INFRANET(Infrastruktur dan Network) UNIKOM.




**Gambar 2.1** Struktur Ogranisasi Infranet

Bedasarkan struktur organisasi pada Gambar 2.1, Adapun jobdesk dari masing-masing unit kerja adalah sebagai berikut

1. Unit Kerja IT Riset dan IOT
    a. Melaksanakan fokus kerja dan target kerja sesuai dengan arahan Rektor.
    b. Membangun, melaksanakan, mengawasi dan bertanggung jawab terhadap sistem dan tata kelola yang ada di Direktorat INFRANET.
    c. Sistem yang dibuat harus mudah dioperasikan oleh user di lingkungan UNIKOM.
    d. Melakukan riset yang berkelanjutan terhadap kebutuhan dan pemanfaatan IT Infrastructure and Network dan sesuai dengan pekerjaan yang dilakukan.
    e. Bekerjasama, berkoordinasi dan bersinergi dengan Rektorat/Fakultas/Direktorat/Program Studi/Divisi/UPT/unit kerja lain dalam mereka melakukan pemanfaatan infrastruktur dan jaringan.

f. Mengembangkan program kerja yang bisa meningkatkan efisiensi dan optimalisasi kerja di lingkungan UNIKOM dalam bidang infrastruktur dan jaringan.
g. Mendukung kebutuhan dan kestabilan jaringan pada setiap kegiatan UNIKOM (akreditasi, webinar dan lainnya).
h. Mendokumentasikan dengan baik dan berkala segala pekerjaan di lingkungan Direktorat INFRANET.
i. Bekerja dengan entrepreneurial mindset: kreatif, inovatif, efisien, efektif dan produktif, serta menjadi problem solver, not follower
j. Melakukan budaya organisasi UNIKOM, PIQIE (Profesionalism, Integrity, Quality, Information Technology, Excellence), sebagai landasan kerja di Direktorat INFRANET.
k. Melaksanakan Tri Darma Perguruan Tinggi sesuai Visi, Misi, Tujuan, Motto dan Budaya UNIKOM.

2. Unit Kerja Labkom
   a. Melaksanakan fokus kerja dan target kerja sesuai dengan arahan Rektor.
   b. Membangun, melaksanakan, mengawasi dan bertanggung jawab terhadap sistem dan tata kelola yang ada di Direktorat INFRANET.
   c. Sistem yang dibuat harus mudah dioperasikan oleh user di lingkungan UNIKOM.
   d. Melakukan monitoring, controlling, maintenance dan bertanggung jawab terhadap seluruh infrastruktur Laboratorium Komputer dan semua perangkat komputer (PC, Laptop, Notebook) yang merupakan asset UNIKOM di lingkungan UNIKOM
   e. Bekerjasama, berkoordinasi dan bersinergi dengan Rektorat/Fakultas/Direktorat/Program Studi/Divisi/UPT/unit kerja lain dalam mereka melakukan pemanfaatan infrastruktur dan jaringan.

f. Mengembangkan program kerja yang bisa meningkatkan efisiensi dan optimalisasi kerja di lingkungan UNIKOM dalam bidang infrastruktur dan jaringan.
g. Mendukung kebutuhan dan kestabilan jaringan pada setiap kegiatan UNIKOM (akreditasi, webinar dan lainnya).
h. Mendokumentasikan dengan baik dan berkala segala pekerjaan di lingkungan Direktorat INFRANET.
i. Bekerja dengan entrepreneurial mindset: kreatif, inovatif, efisien, efektif dan produktif, serta menjadi problem solver, not follower
j. Melakukan budaya organisasi UNIKOM, PIQIE (Profesionalism, Integrity, Quality, Information Technology, Excellence), sebagai landasan kerja di Direktorat INFRANET.
k. Melaksanakan Tri Darma Perguruan Tinggi sesuai Visi, Misi, Tujuan, Motto dan Budaya UNIKOM.

3. Unit Kerja IT support
   a. Melaksanakan fokus kerja dan target kerja sesuai dengan arahan Rektor.
   b. Membangun, melaksanakan, mengawasi dan bertanggung jawab terhadap sistem dan tata kelola yang ada di Direktorat INFRANET.
   c. Sistem yang dibuat harus mudah dioperasikan oleh user di lingkungan UNIKOM.
   d. Secara berkala melakukan maintenance dan peningkatan infrastruktur teknologi informasi yang dimiliki oleh UNIKOM dengan tetap memperhatikan efisiensi dan optimalisasi.
   e. Melakukan monitoring, controlling, maintenance dan bertanggung jawab terhadap seluruh infrastruktur Laboratorium Komputer dan semua perangkat komputer (PC, Laptop, Notebook) yang merupakan asset UNIKOM di lingkungan UNIKOM
   f. Melakukan riset yang berkelanjutan terhadap kebutuhan dan pemanfaatan IT Infrastructure and Network dan sesuai dengan pekerjaan yang dilakukan.

g. Bertanggung jawab untuk melakukan pencegahan dan menangani segala bentuk hack/cybercrime terhadap infrastuktur, jaringan, dan sosial media resmi di lingkungan UNIKOM.
h. Bekerjasama, berkoordinasi dan bersinergi dengan Rektorat/Fakultas/Direktorat/Program Studi/Divisi/UPT/unit kerja lain dalam mereka melakukan pemanfaatan infrastruktur dan jaringan.
i. Mengembangkan program kerja yang bisa meningkatkan efisiensi dan optimalisasi kerja di lingkungan UNIKOM dalam bidang infrastruktur dan jaringan.
j. Membuat/menyempurnakan/mensosialisasikan buku panduan atau prosedur, aturan dan kebijakan terkait penggunaan jaringan dan infrastruktur teknologi informasi milik UNIKOM.
k. Mendukung kebutuhan dan kestabilan jaringan pada setiap kegiatan UNIKOM (akreditasi, webinar dan lainnya).
l. Mendokumentasikan dengan baik dan berkala segala pekerjaan di lingkungan Direktorat INFRANET.
m. Membuat sistem yang mampu terjaga keamanannya, tidak dapat di hack atau dicuri datanya oleh pihak luar.
n. Bekerja dengan entrepreneurial mindset: kreatif, inovatif, efisien, efektif dan produktif, serta menjadi problem solver, not follower
o. Melakukan budaya organisasi UNIKOM, PIQIE (Profesionalism, Integrity, Quality, Information Technology, Excellence), sebagai landasan kerja di Direktorat INFRANET.
p. Melaksanakan Tri Darma Perguruan Tinggi sesuai Visi, Misi, Tujuan, Motto dan Budaya UNIKOM.
q. Melakukan pendataan asset infokus/projector dan menyelesaikan trouble infokus/projector yang ada di lingkungan civitas UNIKOM.
r. Melakukan pendataan asset printer dan menyelesaikan trouble printer yang ada di lingkungan civitas UNIKOM.

s. Melakukan pendataan asset AC dan mendata trouble AC yang ada di lingkungan civitas UNIKOM.

4. Unit Kerja Network Operator

a. Melaksanakan fokus kerja dan target kerja sesuai dengan arahan Rektor.
b. Membangun, melaksanakan, mengawasi dan bertanggung jawab terhadap sistem dan tata kelola yang ada di Direktorat INFRANET.
c. Sistem yang dibuat harus mudah dioperasikan oleh user di lingkungan UNIKOM.
d. Secara berkala melakukan maintenance dan peningkatan infrastruktur teknologi informasi yang dimiliki oleh UNIKOM dengan tetap memperhatikan efisiensi dan optimalisasi.
e. Melakukan monitoring dan controlling jaringan lokal maupun internet di lingkungan UNIKOM.
f. Bekerjasama dengan Civitas Akademik UNIKOM, Wakil Rektor, Dekan, Direktur, Ketua Program Studi, Ketua Divisi dan UPT di lingkungan UNIKOM dalam domain jaringan dan infrastruktur teknologi informasi.
g. Melakukan riset yang berkelanjutan terhadap kebutuhan dan pemanfaatan IT Infrastructure and Network dan sesuai dengan pekerjaan yang dilakukan.
h. Bertanggung jawab untuk melakukan pencegahan dan menangani segala bentuk hack/cybercrime terhadap infrastuktur, jaringan, dan sosial media resmi di lingkungan UNIKOM.
i. Bekerjasama, berkoordinasi dan bersinergi dengan Rektorat/Fakultas/Direktorat/Program Studi/Divisi/UPT/unit kerja lain dalam mereka melakukan pemanfaatan infrastruktur dan jaringan.
j. Mengembangkan program kerja yang bisa meningkatkan efisiensi dan optimalisasi kerja di lingkungan UNIKOM dalam bidang infrastruktur dan jaringan.

k. Memastikan seluruh sistem informasi ter-backup dengan baik di infrastruktur milik UNIKOM.
l. Membuat/menyempurnakan/mensosialisasikan buku panduan atau prosedur, aturan dan kebijakan terkait penggunaan jaringan dan infrastruktur teknologi informasi milik UNIKOM.
m. Mendukung kebutuhan dan kestabilan jaringan pada setiap kegiatan UNIKOM (akreditasi, webinar dan lainnya).
n. Membuat laporan tertulis traffic jaringan secara berkala kepada Rektor.
o. Mendokumentasikan dengan baik dan berkala segala pekerjaan di lingkungan Direktorat INFRANET.
p. Membuat sistem yang mampu terjaga keamanannya, tidak dapat di hack atau dicuri datanya oleh pihak luar.
q. Bekerja dengan entrepreneurial mindset: kreatif, inovatif, efisien, efektif dan produktif, serta menjadi problem solver, not follower
r. Melakukan budaya organisasi UNIKOM, PIQIE (Profesionalism, Integrity, Quality, Information Technology, Excellence), sebagai landasan kerja di Direktorat INFRANET.
s. Melaksanakan Tri Darma Perguruan Tinggi sesuai Visi, Misi, Tujuan, Motto dan Budaya UNIKOM.

5. Unit Kerja Designer
   a. Melaksanakan fokus kerja dan target kerja sesuai dengan arahan Rektor.
   b. Membangun, melaksanakan, mengawasi dan bertanggung jawab terhadap sistem dan tata kelola yang ada di Direktorat INFRANET.
   c. Sistem yang dibuat harus mudah dioperasikan oleh user di lingkungan UNIKOM.
   d. Bekerjasama, berkoordinasi dan bersinergi dengan Rektorat/Fakultas/Direktorat/Program Studi/Divisi/UPT/unit kerja lain dalam mereka melakukan pemanfaatan infrastruktur dan jaringan.

e. Mengembangkan program kerja yang bisa meningkatkan efisiensi dan optimalisasi kerja di lingkungan UNIKOM dalam bidang infrastruktur dan jaringan.
f. Membuat desain dan tugas lain yang diperlukan oleh Rektor UNIKOM.
g. Mendukung kebutuhan dan kestabilan jaringan pada setiap kegiatan UNIKOM (akreditasi, webinar dan lainnya).
h. Mendokumentasikan dengan baik dan berkala segala pekerjaan di lingkungan Direktorat INFRANET.
i. Bekerja dengan entrepreneurial mindset: kreatif, inovatif, efisien, efektif dan produktif, serta menjadi problem solver, not follower
j. Melakukan budaya organisasi UNIKOM, PIQIE (Profesionalism, Integrity, Quality, Information Technology, Excellence), sebagai landasan kerja di Direktorat INFRANET.
k. Melaksanakan Tri Darma Perguruan Tinggi sesuai Visi, Misi, Tujuan, Motto dan Budaya UNIKOM.

6. Unit Kerja Administrasi dan Aset It Infrastructure
   a. Melaksanakan fokus kerja dan target kerja sesuai dengan arahan Rektor.
   b. Membangun, melaksanakan, mengawasi dan bertanggung jawab terhadap sistem dan tata kelola yang ada di Direktorat INFRANET.
   c. Sistem yang dibuat harus mudah dioperasikan oleh user di lingkungan UNIKOM.
   d. Bekerjasama, berkoordinasi dan bersinergi dengan Rektorat/Fakultas/Direktorat/Program Studi/Divisi/UPT/unit kerja lain dalam mereka melakukan pemanfaatan infrastruktur dan jaringan.
   e. Mengembangkan program kerja yang bisa meningkatkan efisiensi dan optimalisasi kerja di lingkungan UNIKOM dalam bidang infrastruktur dan jaringan.

f. Membuat/menyempurnakan/mensosialisasikan buku panduan atau prosedur, aturan dan kebijakan terkait penggunaan jaringan dan infrastruktur teknologi informasi milik UNIKOM.
g. Mendukung kebutuhan dan kestabilan jaringan pada setiap kegiatan UNIKOM (akreditasi, webinar dan lainnya).
h. Mendokumentasikan dengan baik dan berkala segala pekerjaan di lingkungan Direktorat INFRANET.
i. Bekerja dengan entrepreneurial mindset: kreatif, inovatif, efisien, efektif dan produktif, serta menjadi problem solver, not follower
j. Melakukan budaya organisasi UNIKOM, PIQIE (Profesionalism, Integrity, Quality, Information Technology, Excellence), sebagai landasan kerja di Direktorat INFRANET.
k. Melaksanakan Tri Darma Perguruan Tinggi sesuai Visi, Misi, Tujuan, Motto dan Budaya UNIKOM.
l. Melakukan pendataan asset infokus/projector dan menyelesaikan trouble infokus/projector yang ada di lingkungan civitas UNIKOM.
m. Melakukan pendataan asset printer dan menyelesaikan trouble printer yang ada di lingkungan civitas UNIKOM.
n. Melakukan pendataan asset AC dan mendata trouble AC yang ada di lingkungan civitas UNIKOM.

## 2.2 Landasan Teori

Landasan Teori beriksikan teori-teori pendukung yang diguankan dalam proses analisis dan implementasi pada masalah yang diangkat.

### 2.2.1 Cybercrime

Bedasarkan The Council of Europe pada tahun 2001 di Convention on Cybercrime, menyatakan bahwa cybercrime adalah “(1)Pelanggaran terhadap confidentiality, integrity, dan availability dari data atau sistem komputer. (2) Pelanggaran yang berkaitan dengan computer. (3) Pelanggaran yang berkaitan dengan konten. (4) Pelanggaran yang berkaitan hak cipta dan hak terkait”.

Pelanggaran yang berkaitan dengan konten seperti pelanggaran hak cipta mungkin umumnya tidak dianggap sebagai cybercrime. Pada kenyatanya dibeberapa negara, pelanggaran hak cipta tidak dianggap sebagai pelanggaran pidana. Pelanggaran hak cipta sering kali ditegakan melalui upaya hukum perdata dikarenakan banyaknya masalah yang cukup rumit. Selain dari ke 4 defini yang disampaikan oleh The Council of Europe pada tahun 2001, cybercrime juga dapat bermakna sebagai upaya penyerangan secara besar-besaran dan terkoordinasi terhadap infrastuktur informasi yang penting organisasi[11]. Bedasarakan pengertian tersebut, *Cyberattack* merupakah salah satu dari cybercrime.

#### 2.2.1.1 Cyberattack

*Cyberattack* pada dasarnya merupakan kampanye asimetris. *Cyberattack* melibatkan penggunaan kecerdasan secara licik (hacking) untuk mengalahkan sistem yang besar dan kuat dengan mendeteksi kelemahan kritisnya dan mengeksploitasi kelemahan tersebut melalui pemikiran asimetris. Kunci utama dari keberhasilan *Cyberattack* adalah kecepatan dan akurasi.

Bagi *attack*er, kecepatan sangatlah penting dalam melakukan *Cyberattack*. Hal tersebut dikarenakan *attack*er berusaha menghindari deteksi. Dalam *Cyberattack*, usaha menghindari deteksi lebih kemasalah waktu dibandingkan masalah kecanggihan sebuah umpan (decoy). Faktanya, strategi pencegahan yang paling efisien adalah memperlambat *attack*er, bukan mengalahkannya. Selain kecepatan, akurasi juga menjaadi salah satu penentu keberhasilan dari *Cyberattack*. Semakin kurang akurat suatu operasi pada tahap *reconnaissance*, maka akan banyak meninggalkan *traces* dan *footprint* dari proses ekplorasinya[12].

#### 2.2.1.2 Kategori Cyberattack

Secara umum, *cyberattack* dibaagi menjadi dua kategori, yaitu *Active attack* dan passive *attack*. *Active attack* merupakan serangan yang dilakukan dengan cara meng-*intercept* koneksi dan mengubah informasi(data) atau mengambil alih fungsi dari sistem. *Active attack* dapat membahayakan tiga aspek security yaitu *availability*, *integrity*, *authenticity*. Sedangan passive *attack*

merupakan serangan yang dilakukan dengan cara meng-*intercept* informasi tanpa adanya perubahan yang dilakukan terhadap informasi tersebut. Passive *attack* membahayakan aspek *confidentiality*[13].

**2.2.1.3 Jenis Cyber*attack***

Ada berbagai jenis *cyberattack* yang berhasil diidentifikai, beberapa diantaranya cukup popular, yaitu:

1. *Denial of Service* (DoS) dan *Distributed Denial of Service* (DDoS).

   Denial of Service (DoS) merupakan sebuah serangan yang membebani sumber daya sistem, sehingga sistem tidak dapat memberikan respon terhadap permintaan layanan. Serangan Distributed Denial of Service (DDoS) juga serangan terhadap sumber daya sistem. Pada DDoS, serangan diluncurkan dari sejumlah besar mesin host lain yang telah terinfeksi oleh malware attacker sehingga dapat dikendalikan oleh attacker.

   Ada berbagai jenis serangan DoS dan DDoS, yang paling umum adalah TCP SYN flood attack, teardrop attack, Smurf attack, Ping of Deat attack dan botnets.

2. *Password attack*

   Password merupakan mekanisme yang sering digunakan untuk mengautentikasi user ke sistem informasi. Oleh karena itu, serangan terhadap password merupakan salah satu pendekatan yang paling efektif untuk menyerang sebuaah sistem. Ada berbagai macam cara untuk mendapatkan password seseorang, seperti social engineering, bruteforce, dan dictionary attack.

3. *Malware attack*

   Malware attack merupakan sebuah serangan yang menggunakan malicious software (malware). Malware sendiri merupakan program yang menginfeksi komputer dan menggagu kinerja komputer. Umumnya malware dibangun untuk tujuan yang merugikan. Ada berbagai macam malware, diantaranya:

   a. Virus

Virus merupakan program yang dapat menulari program lain dengan cara menempelkan dirinya pada program tersebut. Program yang ditempelkan akan berkerja sebagai virus juga yang nantinya akan menginfeksi program lainnya.

b. Worm

Worm merupakan program yang dapat menggandakan dirinya tanpa harus menginfeksi program lain. Worm dapat menyebar sendiri melalui network.

c. Wabbit

Wabbit merupakan program yang dapat menggandakan dirinya tanpa harus menginfeksi program lain tetapi hanya sebatas komputer lokal saja.

d. Trojan

Trojan merupakan program yang tampak seperti program jinak yang dibuat untuk keperluan baik-baik, padahal dibalik layar melakukan serangan terhadap komputer yang terinstall trojan seperti membuat komputer menjadi lambat, mencuri data, dan serangan lainnya.

e. Adware dan Spyware

Adware adalah program yang dibuat untuk memenuhi komputer dengan berbagai iklan yang menggangu. Sedangkan spyware merupkana program yang dibuat untuk mencuri informasi dari komputer target dan informasi tersebut akan dikirimkan ke orang lain yang tidak berhak.

f. Rootkit

Rootkit merupakan program yang terdiri dari berbagai macam malware menjadi satu[14].

4. Cross-site scripting (XSS) attack

XSS attack merupakan sebuah serangan yang menyerang database suatu website dengan menggunakan sumber daya pihak ketiga untuk menjalankan script di web browser atau scriptable application korban. Dampak yang paling berbahaya dari XSS adalah ketika XSS digunakan untuk mengkeploitasi vulnerability tambahan yang menyebabkan attacker tidak hanya dapat mencuri cookies saja, tetapi attacker juga dapat mengambil informasi dari network,

mengakses dan mengontrol mesin korban secara remote, dan mendapatkan data dari input keyboard korban (log key).

5. Phishing dan Spear Phishing Attack

Phishing attack merupakan sebuah serangan cyber dengan cara mengirimkan email yang terlihat seperti email dari source yang terpecaya dengan tujuan untuk mendapatkan informasi personal atau mempengaruhi target untuk melakukan sesuatu. Phising attack merupakan kombinasi dari social engineering dan tipu daya teknis.Phising attack dapat berupa sebuah attachment pada email yang akan menyebarkan malware pada komputer target, Dapat juga berupa link ke website palsu yang menipu target sehingga target mendownload malware atau menyerahkan informasi personal kepada penyerang.

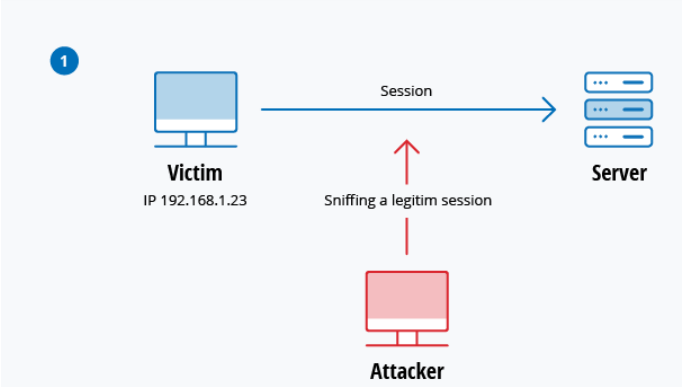
Salah satu jenis serangan phishing adalah sper phishing. Spear Phishing merupakan serangan phishing yang menargetkan suatu individua atau organisasi. Penyerang spear phishing melakukan riset terlebih dahulu terhadapt target dan membuat pesan yang sangat personal dan relevan terhadap target. Oleh sebab itulah spear phising sangat susah untuk di deteksi dan lebih susah lagi untuk melakukan defend terhadap serangan spear phishing.

6. Man-in-the-Middle (MitM) Attack

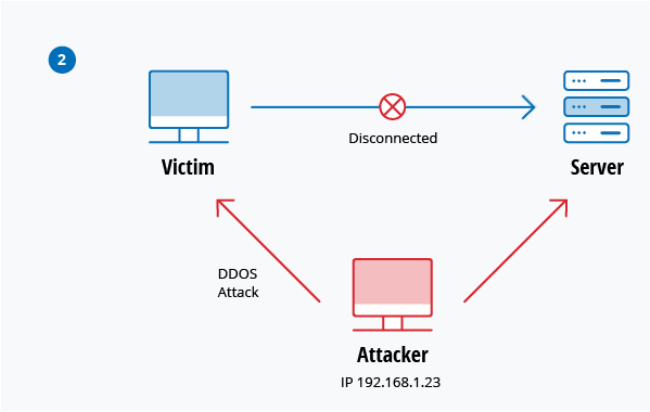
Merupakan sebuah attack yang terjadi ketika hacker menempatkan dirinya ditengah-tengah komunikasi antara client dan server. Berikut beberapa jenis MitM attack:

a. Session Hijacking

Pada jenis MitM ini, attacker membajak session antara trusted klien dengan server network. Komputer attacker akan mengganti IP addressnya sesuai dengan IP trusted klien saat server melanjutkan sessionnya, yang dimana bahwa server percaya bahwa saat itu server sedang berkomunikasi dengan trusted klien.




**Gambar 2.2** Ilustrasi 1 Session Hijacking




**Gambar 2.3** Ilustrasi 2 Session Hijacking

b. Ip Spoofing

Ip Spoofing merupakan sebuah serangan yang digunakan oleh attacker untuk meyakinkan sebuah sistem bahwa sistem tersebut sedang berkomunikasi dengan entitass yang dikenali dan dipercaya sistem sehingga attacker dapat memperoleh akses ke sistem. Attacker akan mengirimkan paket menggunakan IP address dari host yang dikenali dan dipercaya daripada menggunakan IP addressnyaa sendiri ke target host.

c. Replay

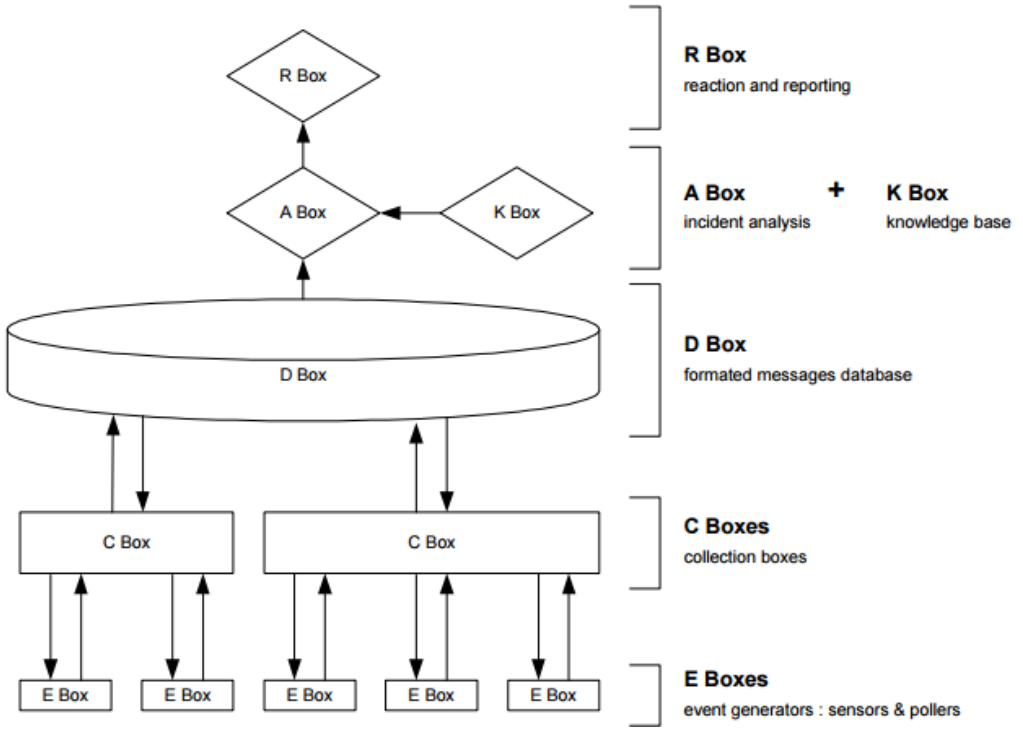
Sebuah Replay attack muncul Ketika attacker mencegat dan menyimpan pesan lama kemudian mencoba mengirimkannya kemballi

nanti. Jenis serangan MitM ini dapat dengan mudah diatasi dengan session timestamps atau nonce (angka acak atau string yang berubah seiring waktu).

### 2.2.2 Security Operation Center (SOC)

*Security Operation Center* (SOC) merupakan salah satu solusi yang populer untuk melakukan *monitor, track,* dan menangani insiden *cyber*. SOC didefinisikan sebagai fasilitas yang dikembangkan secara terpusat yang didedikasikan untuk membantu organisasi dalam hal mengidentifikasi, mengelola, memantau security event dan memulihkan insiden *cyber* (Jacob et al, 2013). Fungsi utama dari SOC adalah untuk mengimplementasi *monitoring*, *analysis*, dan *response* guna mengatasi ancaman *Cyberattack* dan *threats*. Selain itu, SOC juga memiliki fungsi lain yaitu melindungi *confidentiality*, *integrity*, dan *availability* dari informasi melalui pemantauan secara terus menerus[6].

Sebuah SOC haruslah mencakup ketiga aspek yaitu manusia, proses, dan teknologi. Bedasarkan hal tersebut, SOC diwajibkan memiliki personil teknis yang memiliki tanggung jawab untuk memantau sistem dan infrastuktur pada organisasi sesuai dengan proses dan prosedur yang terjamin menggunakan sekumpulan teknologi terbaru. Pemantauan tersebut memiliki tujuaan untuk mencegah penyalahgunaan komputer dan pelanggaran kebijakan(*policy*), mencegah dan mendeteksi *Cyberattack*, mencegah dan mendeteksi *misuse*, mencegah dan mendeteksi kebocoran data, serta memberikan respon terhadap insiden cyber yang terjadi di organisasi[3]. Terdapat 5 modul yang berbeda pada SOC yaitu *event generator*, *event collector*, *message database*, *analysis engine* dan *reaction management software*. Bedasarkan hal tersebut, terdapat 5 operasi yang harus ada di SOC yaitu *Security Event Generation*, *Security Event Collection*, *Security Event Storage*, *Security Event Analysis* dan *Security Event Reaction*. Berikut Gambar 2.4 merupakan model SOC bedasarkan Bidou[14].




**Gambar 2.4** Model SOC

Bedasarkan model pada Gambar 2.4, operasi yang berjalan pada sebuah SOC direpresentasikan oleh beberapa box, yaitu:

1. E Box

   E Box bertanggung jawab untuk operasi security event generation. E Box dapat dibedakan menjadi 2 tipe, yaitu event based data generation dan status based data generation.

   a. Event Based Data Generation (Sensor)

      Event Based Data Generation atau Sensor menghasilkan event bedasarkan operasi yang dilakukan secara spesifik pada OS, application, atau network. Beberapa contohnya adalah Intrusion Detection System (IDS), Firewalls, Router, Switches, Hub, Radius Server, SNMP Stack, dan lain-lain.

   b. Status Based Data Generation (Poller)

      Status Baased Data Generation atau Poller merupakan sebuah event generator yang spesifik. Poller menghasilkan event bedasarkan

pada reaksi terhadap stimulus eksternal seperti ping, pengecekan data intergrity, atau pengecekan status daemon. Pada konteks keamanan, poller akan bertanggung jawab terhadap pengecekan status service dan data intergrity.

2. C Box

   C Box bertanggung jawab untuk operasi Security Event Collection. Tujuan dari C Box adalah mengumpulkan event dari E Box yang kemudian ditranslasi menjadi sebuah format sehingga memiliki pesan yang berbasis homogen.

3. D Box

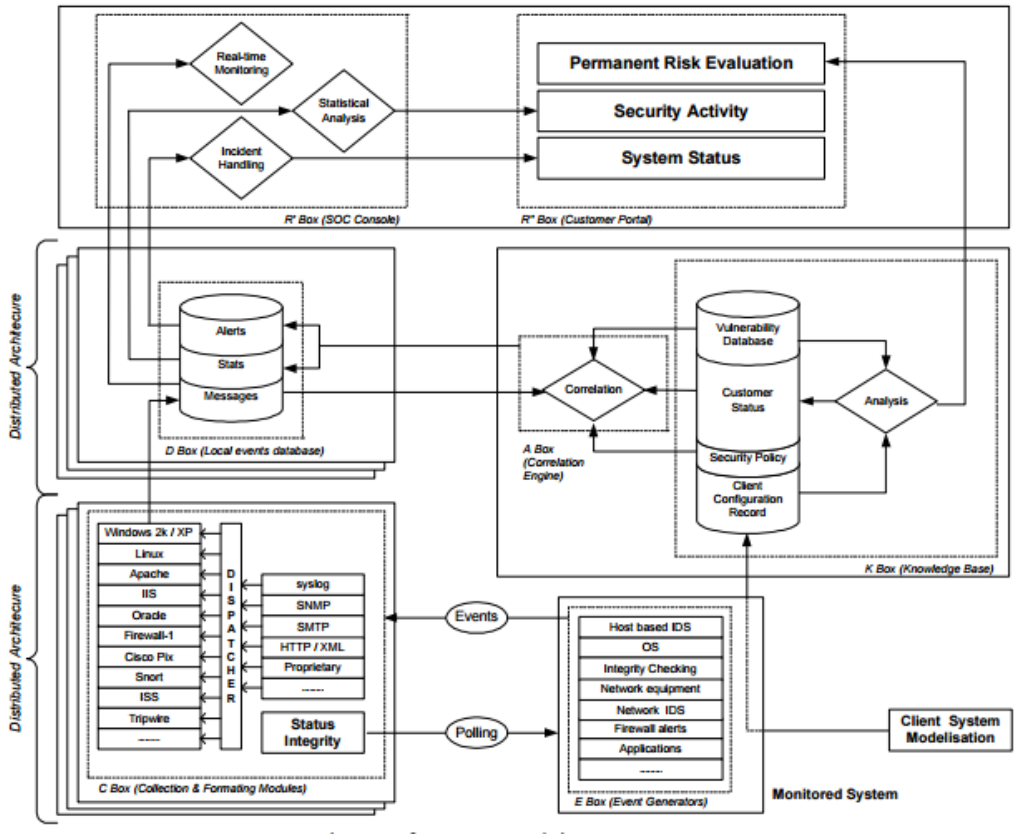
   D Box bertanggung jawab untuk operasi Security Event Storage. Semua security event yang dikumpulkan dan diformat oleh C Box akan disimpan kedalam D Box.

4. A Box dan K Box

   A Box dan K Box bertanggung jawab untuk operasi Security Event Analysis. A box dan K Box akan melakukan analisis terhadap Event yang ada di D Box. A box akan melakukan berbagai macam operasi untuk melakukan analisis Event di D Box baik dalam hal korelasi antar algoritma, pendeteksian message false-positive, representasi mataematika ataupun distirbusi Operasi sehingga menghasilkan alert message yang memenuhi syarat. Sedangkan K Box berfungsi sebagai inputan terhadap A Box.

5. R Box

   R Box bertanggung jawab untuk operasi Security Event Reaction. R Box merupakan tools yang digunakan untuk memberikan reaksi terhadap offending event.




**Gambar 2.5** Arsitektur SOC

Bedasarakan Gambar 2.4 dan 2.5, beberapa jurnal sepakat bahwa sistem integral dari sebuah SOC biasanya didasarkan pada sistem Security Information and Event Management (SIEM) [1] [5].

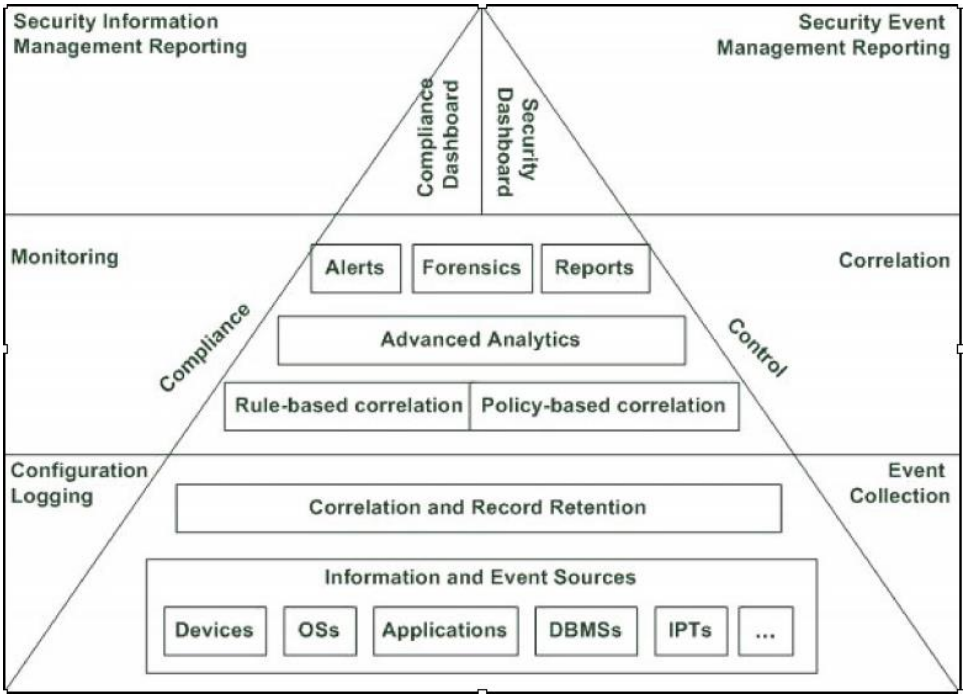
### 2.2.3 Security Information and Event Management (SIEM)

Security Information and Event Management atau yang biasa dikenal dengan SIEM merupakan sebuah sistem yang digunakan untuk menyelesaikan masalah *flow control* dari *event* keamanan informasi yang datang dari *information protection tools* serta untuk mengkomputerasikan proses pengelolaan *Information Security Inci*dent[1]. Sistem SIEM melakukan proses pengumpulan event dari beberapa sensor[15]. Kemudian SIEM akan melakukan korelasi antar event serta memberikan gambaran secara syntethic views dari alert yang dihasilkan untuk digunakan sebagai threat handling dan pembuatan report security. Hal tersebut menyebabkan sistem SIEM menjadi sebuah infrastuktur yang penting dalam

sebuah organisasi. SIEM digunakan sebagai bagian intergral dari sistem yang berjalan pada sebuah SOC di organisasi[1][5][16][17][18].

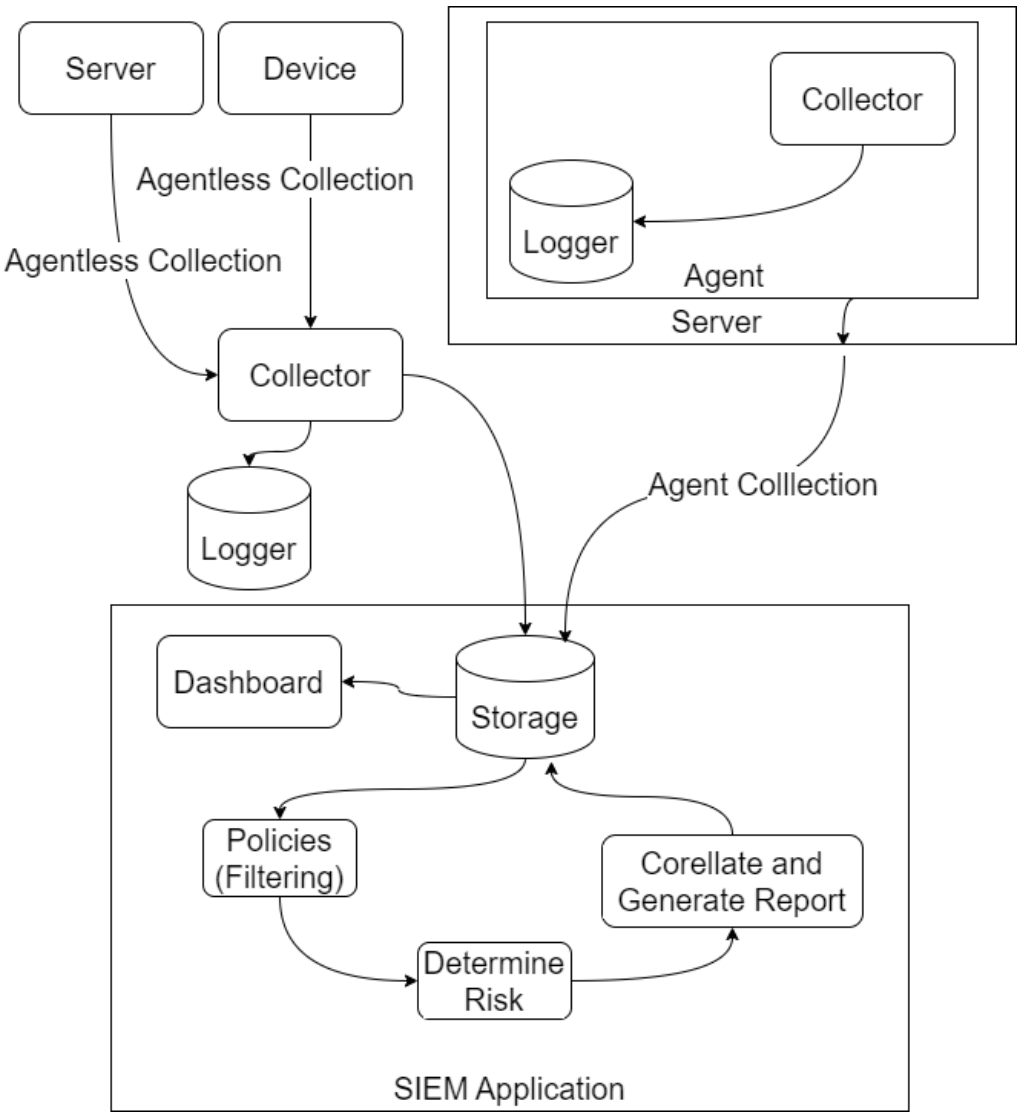
Secara umum SIEM memiliki kapabilitas untuk melakukan operasi *collect*, *aggregate*, *store*, dan *correlate* terhadap event yang dihasilkan oleh infrastruktur suatu organisasi[16]. Sistem SIEM dapat melakukan analisis, audit, penemuan, dan pengantisipasian hardaware, network, dan seluruh aplikasi event secara langsung. SIEM menyediakan analisis security alert dari sebuah network hardware dan aplikasi secara real time. Tujuan dari SIEM's adalah untuk membantu organisasi agar dapat lebih cepat merespon terhadap sebuah serangan serta menghubungkan seluruh event yang terjadi menjadi sebuah rangkaian yang bermakna[19]. Sistem SIEM digunakan secara terus-menerus untuk memantau *user activity* dan *event* sehingga memungkinkan SOC untuk mendeteksi dan menangani *Information Security incident* melalui agregaasi dari ssejumlah besar data mesin secara real time yang digunakan untuk *Information Security Risk Management* [1]. Infromasi pada sistem SIEM diatur menggunakan dashboard sehingga SIEM dapat mengkomunikasikan informasai penting secara sekilas[15].

Istilah SIEM dikenalkan pada tahun 2005 oleh perusahaan yang bergerak pada bidang *research* dan *consulting*[1]. Sistem SIEM merupakan gabungan dari Security Information Management (SIM) dan Security Event Management (SEM)[19][20]. SIM berfokus pada storage jangka panjang dalam hal analisis dan reporting bedasarkan data log. Sedangkan SEM berfokus pada real time monitoring dan notifikasi[1][20]. Berikut Gambar 2.6 merupakan gambaran dari sistem SIEM




**Gambar 2.6** Model SIEM

Gambar 2.6 merupakan Gambaran model SIEM yang menggabungkan fungsi dari SIM dan SEM. Untuk memperjelas model SIEM pada Gambar 2.5 Berikut ini pada Gambar 2.7 merupakan arsitektur model SIEM Environment bedasarkan Dorigo[20] :




**Gambar 2.7** SIEM *Environment*

Adapun penjelasan dari komponen-komponen yang terdapat pada Gambar 2.7 adalah sebagai beriku:

1. Agent

   Agent merupakan sebuah potongan program, ektensi, atau plugin yang disediakan oleh vendor SIEM yang mampu untuk mentransfer dan mengkonversi entri log dari target sistem ke aplikasi SIEM. Fitur utama dari agent adalah kemampuannya untuk melakukan pra-filter entri log. Agent akan melakukan pengiriman entri log melalui koneksi khusus

yang aman. Terdapat alternatif lain untuk mengirimkan log dari device/server ke aplikasi SIEM yaitu melalui agentless.

2. Collector

   Collector mampu melakukan korelasi meskipun fungsi utama collector adalah *normalization* sehingga aplikasi SIEM dapat menerima entri log yang lebih terstuktur. Sesudah dilakukan klasifikiasi, entri log dapat dikirimkan ke logger ataupun ke Apllikasi SIEM.

3. Logger

   Logger berfungsi untuk menyimpan log files. Dengan logger entri log disimpan, diamankan, dan di *signed* untuk dilakukan analisis lebih lanjut.

4. SIEM Application

   Aplikasi SIEM merupakan inti dari SIEM *environtment*. Aplikasi SIEM mangani hal-hal seperti risk assesment, event corellation, vulnerability scanning, data mining, real-time monitoring. Aplikasi SIEM akan menghasilkan report dari security event yang ada. Adapun beberapa fitur pada aplikasi SIEM diantaranya:

   a. Storage

      Semua event yang diterima oleh SIEM environment akan disimpan di database. Biasanya terdapat 2 tipe database, yaitu general storage serta storage untuk backlog yang masih pada tahap korelasi.

   b. Policies

      Terdapat 2 tipe policies, yaitu general server policy dan spesifik policy. General server policy mendefinisikan apa yang harus terjadi kepada semua event yang diterima server. Sedangkan spesifik policy digunakan pada spesifik event yang datang dari spesifik agent atau spesifik device. Penggunaan spesifik policy memungkinkan administrator untuk menyempurnakan flow dari event. Policies server mengotomatisasi proses untuk melakukan pelacakan terhadap apa yang penting. Policies dapat dilakukan

konfigurasi melalui SIEM server sehingga memudahkan proses maintenance.

c. Determine Risk

Pada SIEM, risk dari suatu event ditentukan oleh 3 faktor yaitu prioritas, reliability dan nilai dari aset. Pada semua event, terdapat 2 risk yaitu risk untuk *source* (diukur untuk menentukan kemungkinan mesin di lakukan compromised) dan risk untuk *destination* (diukur untuk menentukan potensi risk akibat dari serangan terhadap mesin.

d. Correlate and Generate Report

Korelasi merupakan tahap yang penting pada SIEM dikarenakan dengan korelasi, SIEM dapat mengurangi false-positive event. Hal tersebut didukung oleh Sekharan[17] yang mengatakan bahwa komponen utama dari SIEM adalah corellation engine. Biasanya SIEM menghasilkan report pada Dashboard. Selain pada dashboard, report juga dapat dikonfigurasi untuk dikirim ke email kepada orang tertentu.

e. Dashboard

Dashboard menyediakan gambaran umum dari status security, policies dan konfigurasi, serta menyediakan tools untuk analisis security event dan raw log file. SIEM Dashboard biasanya berbasis web yang berjalan di SIEM server.

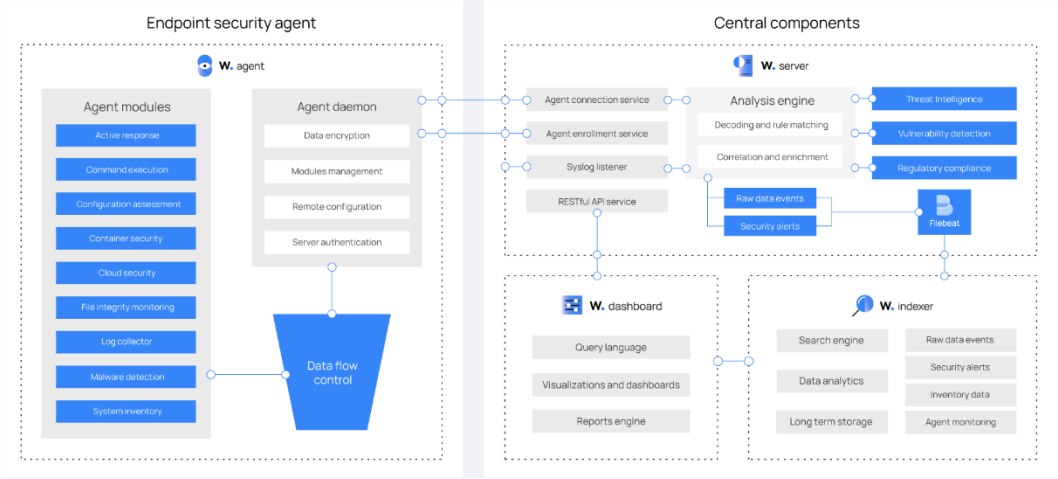
### 2.2.4 Security Event

*Security Event* merupakan sebuah kejadian yang teridentifikasi (diamati) dari suatu keadaan sistem, *service*, atau *network* yang mengidikasikan konsekuensi negatif seperti pelanggaran *pollicies*, pelanggaran sebuah *security practice* atau kegagalan control, atau situasi yang sebelumnya tidak diketahui yang mungkin berkaitan dengan keamanan. Suatu security event dapat dikatakan sebagai bagian dari security incident. Dan sebuah *security incident* dapat dikatakan sebagai kumpulan dari *security event* [1]. Salah satu jenis Information Security Event

adalah anomali *traffic*. Anomali traffic merupakan keaadan abnormalitas yang terjadi pada lalu lintas *network* sehingga dapat menyebabkan penurunan performa jaringan bahkan hingga melumpuhkan jaringan. [2]

### 2.2.5 Wazuh

Wazuh merupakan sebuah platform keamanan *opensource* yang menggabungkan kemampuan XDR dan SIEM secara terpadu untuk mellindungi *endpoints* dan beban kerja cloud. Wazuh membantu organisasi dan individual dalam melindungi aset data mereka dari ancaman keamanan. Beberapa kemampuan wazuh diantaranya analisis data log, *intrusion and malware detection*, pemantauan *file intergrity*, penilaian konfigurasi, *vulnerability detection*, dukungan untuk *requlatory compliance*. Gambar 2.3 berikut ini merepresentasikan komponen apa saja yang ada diwazuh dan bagaimana aliran datanya.




**Gambar 2.8** Wazuh

Tabel 2.1 berikut menampilkan level-level rule yang diguankan pada security event yang dihasilkan oleh Wazuh. Terdapat 15 level yang masing-masing memberikan wawasan terhadap tingkat keparahan dari Security Event pada Wazuh dan juga membantu dalam pembuatan custom rules.

**Tabel 2.1** Rule Level pad Wazuh

| Level | Jenis Rule |
|---|---|

| | |
|---|---|
| 0 | Ignored |
| 2 | System Low Priority Notification |
| 3 | Successful/Authorized Event |
| 4 | System Low Priority Error |
| 5 | User Generator Error |
| 6 | Low Relevance Error |
| 7 | Bad Word Matching |
| 8 | First Time Seen |
| 9 | Error From Invalid Source |
| 10 | Multiple User Generated Error |
| 11 | Integrity Checking Warning |
| 12 | High Importance Event |
| 13 | Unusual Error (high Importance) |
| 14 | High Importance Security Event |
| 15 | Sever Attack |

Komponen dari Wazuh terdiri dari Wazuh Agent yang di deploy pada endpoints dan 3 komponen utama yaitu Wazuh server, Wazuh indexer, dan Wazuh Dashboard. Berikut ini penjelasan masing-masing komponennya:

#### 2.2.5.1 Wazuh agents

Wazuh agents akan diinstall pada endpoints seperti laptop, desktops, server, cloud instances, atau virtual machine. Wazuh agents menyediakan kemampuan pencegahan, pendetekisan, dan pemberian respons terhadap ancaman.

#### 2.2.5.2 Wazuh server

Wazuh server bertugas untuk menganilisis data yang diterima dari Wazuh agents. Wazuh server akan memproses data melalui decoder dan *rule*, menggunakan threat intelligence untuk mencari *indicator of compromise* (IoC) yang terkenal. Indicator of comprimse (IoC) adalah bukti digital yang menunjukan kemungkinan terjadinya pelanggaran keamanan pada sistem atau

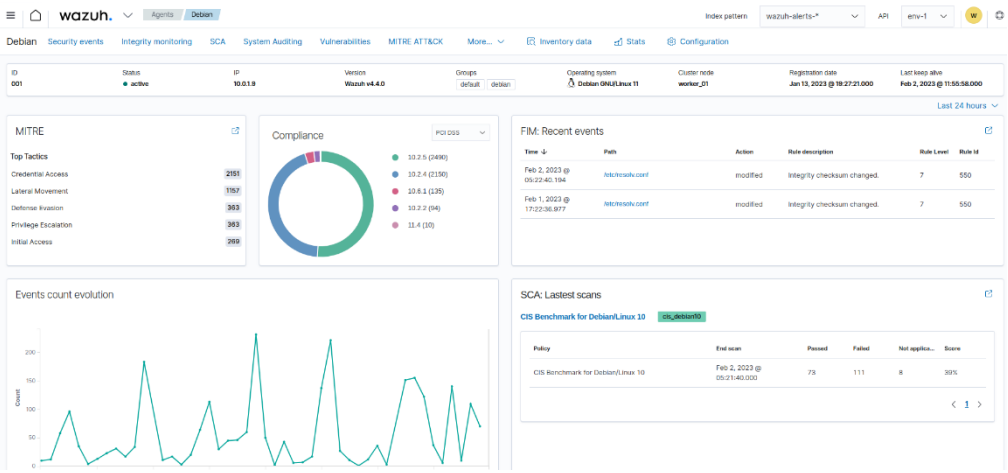
jaringan. Wazuh server juga dapat digunakan untuk mengelola agents secara remote.

### 2.2.5.3 Wazuh indexer

Wazuh indexes merupakan sebuah mesin analisis dan full-text search yang sangat skalabel. Wazuh indexes menyimpan alerts yang dihasilkan oleh wazuh server dan menyediakan kemampuan pencarian dan analisis data secara hampir *real-time*.

### 2.2.5.4 Wazuh dashboard

Wazuh dashboard merupakan sebuah *web user interface* yang digunakan untuk data visualisasi dan analisis event keamanan dan *alerts data*. Hal tersebut mencakup event keamanan, *regulatory compliance*, vulnerability aplikasi yang terdeteksi, data pemantauan *file integrity*, hasil penilaian konfigurasi, pemantauan event infrastuktur cloud, dan lain-lain. Gambar 2.4 berikut merupakan tampilan dari Wazuh dashboard.




**Gambar 2.9** Tampilan Wazuh dashboard.