MATERI L1 SOC ANALYST

UNIT KOMPETENSI 4

Menganalisis Log pada Security Operations Center

MEDIA PEMBELAJARAN L1 SOC ANALYST

Unit Kompetensi

Menganalisis Log pada *Security Operations Center (SOC)*.

Hasil Pembelajaran

Setelah mengikuti pembelajaran peserta didik diharapkan mampu melakukan analisis terhadap keamanan siber untuk menentukan kendali

Indikator Hasil Belajar

- Mengumpulkan informasi terkait efek dari insiden kemanan siber
- Mengidentifikasi dampak insiden siber
- Menentukan kendali terhadap insiden keamanan siber

Elemen Kompetensi

1. Menentukan jenis log
    a. Salinan log disiapkan sesuai kebutuhan.
    b. Jenis log diidentifikasi berdasarkan kebutuhan.
2. Memeriksa log
    a. Parameter kewajaran ditentukan sesuai kebutuhan.
    b. Log artefak diidentifikasi sesuai parameter kewajaran.
3. Mendokumentasikan kegiatan analisis log
    a. Hasil pemeriksaan log didokumentasikan sesuai kebutuhan.
    b. Laporan analisis log disusun sesuai format laporan.

Konteks Variable

1. Kategori jenis log
    a. *Security Software logs*
    Log ini dihasilkan oleh perangkat lunak atau perangkat keras yang dirancang untuk melindungi sistem dari ancaman keamanan. Kategori ini mencakup berbagai alat keamanan yang memantau, mendeteksi, dan mencegah aktivitas mencurigakan. Berikut adalah jenis *Security Software logs* beserta contohnya;

        - *Antimalware software*
        2025-03-24 09:15:32 [INFO] Malware detected: Trojan.Win32.Agent in C:\Users\user\Downloads\file.exe – Quarantined
        Antimalware mendeteksi trojan di file file.exe dan mengkarantinanya.

        - *Intrusion detection and intrusion prevention systems*

2025-03-24 09:16:10 [ALERT] IDS: Port scan detected from 192.168.1.200 targeting 192.168.1.10 on ports 22,80,443
IDS mendeteksi aktivitas pemindaian port dari IP 192.168.1.200.

- *Remote access software*
  2025-03-24 09:17:22 [INFO] VPN: User jdoe connected from 203.0.113.50 to VPN server 192.168.1.1
  Pengguna jdoe terhubung ke VPN dari IP 203.0.113.50.
- *Web proxies*
  2025-03-24 09:18:45 [INFO] Proxy: 192.168.1.50 requested http://malicious-site.com - Blocked (Category: Malware)
  Proxy memblokir akses ke situs berbahaya berdasarkan kategori malware.
- *Vulnerability management software*
  2025-03-24 09:19:10 [WARN] Vulnerability Scan: CVE-2024-12345 detected on 192.168.1.10 (Apache 2.4.29 - Outdated)
  Pemindaian menemukan kerentanan CVE-2024-12345 pada server Apache yang sudah usang.
- *Authentication servers*
  2025-03-24 09:20:01 [ERROR] Authentication Failed: User jdoe from 192.168.1.50 - Invalid credentials
  Upaya login gagal untuk pengguna jdoe karena kredensial salah.
- *Routers*
  2025-03-24 09:21:15 [INFO] Router: Dropped packet from 203.0.113.100 to 192.168.1.10 (Port 445 - SMB)
  Router memblokir paket jaringan pada port 445 (SMB), mungkin karena aturan keamanan.
- *Firewalls*
  2025-03-24 09:22:30 [ALERT] Firewall: Blocked inbound connection from 198.51.100.20 to 192.168.1.10 on port 23 (Telnet)
  Firewall memblokir koneksi masuk pada port 23 (Telnet), yang sering digunakan untuk serangan.
- *Network quarantine servers*
  2025-03-24 09:23:45 [INFO] Quarantine: Device 192.168.1.50 isolated - Reason: Suspicious outbound traffic to 203.0.113.200
  Perangkat diisolasi karena lalu lintas keluar yang mencurigakan.

b. *Operating system logs*
   Log yang dihasilkan oleh sistem operasi (seperti *Windows, Linux, atau macOS*) untuk mencatat aktivitas sistem, seperti login pengguna, perubahan sistem, atau kesalahan kernel. Berikut adalah jenis *Operating system logs* dan contohnya;

- *Windows Event Log*

  Event ID: 4624
  Time Created: 2025-03-24T09:24:32Z
  Source: Microsoft-Windows-Security-Auditing
  Description: An account was successfully logged on.
  Account Name: jdoe
  Logon Type: 2 (Interactive)

- *Linux Syslog*

  Mar 24 09:25:10 my-server kernel: [1234.567890] Out of memory: Kill process 12345 (httpd) score 511 or sacrifice child

c. *Application logs*
Log yang dihasilkan oleh aplikasi tertentu (seperti web server, database, atau aplikasi bisnis) untuk mencatat aktivitas, kesalahan, atau peristiwa penting dalam aplikasi tersebut. Berikut adalah jenis *Application logs* dan contohnya;

- *Apache Access Log*

  192.168.1.100 - - [24/Mar/2025:09:26:32 +0700] "GET /index.html HTTP/1.1" 200 2048 "-" "Mozilla/5.0"
  Pengguna mengakses index.html dengan status sukses (200).

- *MySQL Error Log*

  2025-03-24T09:27:10.123456Z 10 [ERROR] [MY-010123] [Server] Failed to start replication: Access denied for user 'repl'@'192.168.1.10'
  MySQL gagal memulai replikasi karena masalah autentikasi.

- *Custom Application Log*

  2025-03-24 09:28:15 [ERROR] App: User jdoe failed to update profile - Database connection timeout
  Aplikasi mencatat kesalahan saat pengguna jdoe mencoba memperbarui profil karena timeout koneksi database.

2. Log Artefak
Log artefak bukanlah log asli yang dihasilkan secara langsung oleh sistem, melainkan salinan atau ekstraksi dari log asli yang telah diproses untuk keperluan analisis. Proses ini dilakukan untuk memastikan bahwa log asli tidak diubah (untuk menjaga integritas data) dan untuk mempermudah analisis dengan menambahkan informasi tambahan atau menyusun data dalam format yang lebih terstruktur. Berikut adalah contohnya

a. Log Asli *(Apache Access Log)*
192.168.1.100 - - [24/Mar/2025:09:15:32 +0700] "GET /search?q=<script>alert('XSS')</script> HTTP/1.1" 403 512 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) Chrome/89.0.4389.90"

192.168.1.200 - - [24/Mar/2025:09:16:10 +0700] "POST /login.php HTTP/1.1" 200 1024 "-" "Mozilla/5.0" -d "username=admin' OR '1'='1&password=123"

b. Log Artefak (Dengan Keterangan)

[Incident ID: INC-2025-001]
[Analysis Date: 2025-03-25]
[Source: /var/log/apache2/access.log]
[Hash of Original Log: SHA256: a1b2c3d4e5f6...]

1. *[Timestamp: 2025-03-24 09:15:32 +0700]*
   [IP: 192.168.1.100]
   [Request: GET /search?q=<script>alert('XSS')</script> HTTP/1.1]
   [Status: 403]
   [Note: Suspected XSS attack - Attempt to inject JavaScript code. Blocked by ModSecurity (status 403). Investigate further for potential attacker activity.]

2. *[Timestamp: 2025-03-24 09:16:10 +0700]*
   [IP: 192.168.1.200]
   [Request: POST /login.php HTTP/1.1]
   [Data: username=admin' OR '1'='1&password=123]
   [Status: 200]
   [Note: Suspected SQL Injection attack - Attempt to bypass authentication using 'OR 1=1'. Status 200 indicates possible vulnerability in login.php. Immediate action required to patch application and verify if unauthorized access occurred.]

Penjelasan Log Artefak

- **Metadata Tambahan**: ID insiden, tanggal analisis, sumber log, dan hash untuk verifikasi integritas.
- **Keterangan per Baris**:
  a. Baris 1, menjelaskan bahwa ini adalah upaya *XSS* dan diblokir oleh server.
  b. Baris 2, menjelaskan upaya *SQL Injection*, dengan catatan bahwa status 200 menunjukkan potensi kerentanan yang perlu ditangani.

3. Parameter Kewajaran
   Poin yang perlu diperiksa dalam rangka melakukan analisis log, meliputi:
   a. *Informasi severity log (Emergency, Alert, Critical, Error, Warning, Notice, Informational, Debug)*
   b. Statistik log
   c. Linimasa log
   d. Karakteristik log (sub konten/field/ metadata log)

A. Log Security Management

Apa itu Log Security Management?

Proses pengumpulan, penyimpanan, analisis, dan perlindungan terhadap catatan aktivitas (log) yang dihasilkan oleh sistem dan aplikasi dalam lingkungan teknologi informasi.

Log berisi informasi berharga tentang:

1. Aktivitas pengguna: Login, logout, akses file dan aplikasi
2. Perubahan konfigurasi: Modifikasi pengaturan sistem dan jaringan
3. Transaksi: Aktivitas bisnis dan keuangan yang tercatat
4. Kejadian keamanan: Percobaan login yang gagal, serangan malware, dll

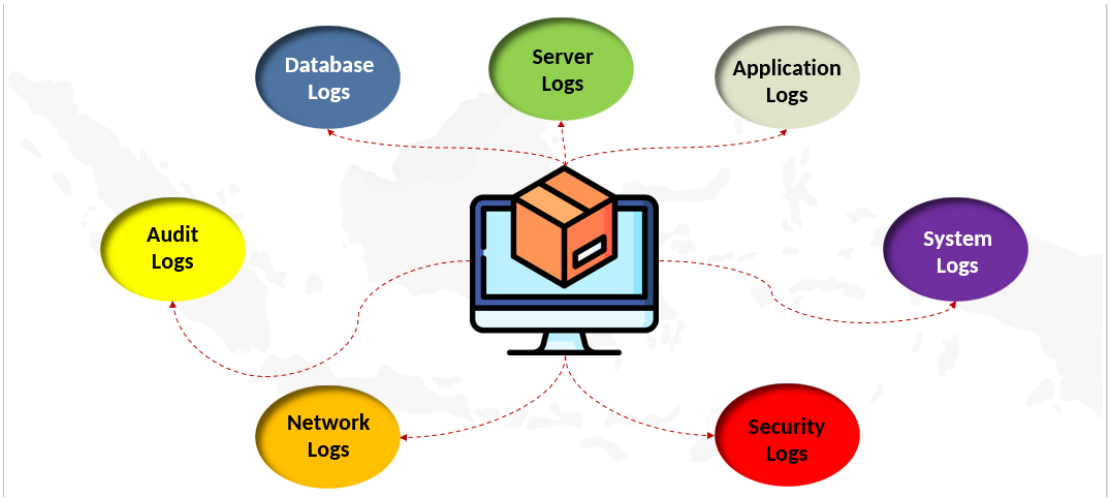
Analisis Log

Proses meninjau, mengintepretasikan, dan memahami log.

Manfaat Log Security Management

1. Meningkatkan keamanan dengan memudahkan proses deteksi dan penanganan ancaman keamanan.
2. Mempercepat penanganan insiden dengan menyediakan jejak audit yang berharga untuk investigasi insiden keamanan.
3. Efisiensi waktu untuk memantau sistem, memonitor error, dan perubahan sistem, dan menentukan troubleshoot.
4. Memperkuat kepatuhan terhadap regulasi yang mengharuskan organisasi menyimpan dan memantau log untuk jangka waktu tertentu.
5. Melakukan penelusuran suatu aktivitas yang terjadi.

Jenis Log



1. Database logs, Log ini dihasilkan oleh sistem manajemen basis data (DBMS) seperti *MySQL, PostgreSQL, atau Microsoft SQL Server*. Log ini mencatat berbagai aktivitas, termasuk transaksi database seperti *INSERT, UPDATE, DELETE,* atau *SELECT*, serta kesalahan yang terjadi, seperti kegagalan koneksi, pelanggaran integritas data, atau query yang gagal. Selain itu, log juga mencatat aktivitas administratif, seperti pembuatan atau penghapusan tabel, serta log replikasi atau backup jika tersedia.

   Tujuan utama dari log ini adalah untuk memantau performa database, membantu dalam diagnosis masalah seperti query yang lambat atau kegagalan transaksi, serta melacak aktivitas mencurigakan, misalnya upaya *SQL Injection.* Sebagai contoh, log berikut menunjukkan adanya percobaan *SQL Injection* yang gagal karena akses ditolak:

   *2025-03-24T10:15:32.123456Z 5 [ERROR] [MY-010123] [Server] Query failed: SELECT * FROM users WHERE id = '1' OR '1'='1' -- Access denied.*

2. Server logs, Log ini dihasilkan oleh server, baik itu server web, email, maupun file, seperti *Apache, Nginx,* atau *Microsoft IIS*. Log ini mencatat berbagai informasi penting, termasuk *Access Logs*, yang merekam permintaan yang diterima server, seperti metode *HTTP (GET/POST)*, URL yang diakses, alamat IP klien, kode status (misalnya 200 atau 404), serta *User-Agent* yang digunakan. Selain itu, *Error Logs* mencatat kesalahan yang terjadi di server, seperti file yang tidak ditemukan, kesalahan skrip, atau kegagalan konfigurasi.

   Tujuan utama dari log ini adalah untuk memantau lalu lintas server dan performanya, mendeteksi serangan seperti *XSS, SQL Injection,* atau *Directory Traversal*, serta membantu dalam diagnosis masalah server, seperti crash

atau overload. Sebagai contoh, *Apache Access Log* berikut mencatat akses normal ke file *index.html* dengan status 200 (sukses):

192.168.1.100 - - [24/Mar/2025:10:16:10 +0700] "GET /index.html HTTP/1.1" 200 2048 "-" "Mozilla/5.0"

Sementara itu, *Apache Error Log* berikut mencatat kesalahan PHP karena fungsi *db_connect()* tidak ditemukan:

[Tue Mar 24 10:17:22.654321 2025] [php:error] [pid 5678] [client 192.168.1.50:54321] PHP Fatal error: Uncaught Error: Call to undefined function db_connect() in /var/www/html/db.php:15

3. Application logs, Log ini dihasilkan oleh aplikasi tertentu, seperti aplikasi bisnis, perangkat lunak kustom, atau aplikasi pihak ketiga. Log ini mencatat berbagai informasi penting, termasuk aktivitas pengguna, seperti login, logout, atau transaksi dalam aplikasi. Selain itu, log juga mencatat kesalahan aplikasi, seperti crash, timeout, atau bug, serta peristiwa penting, seperti pembaruan data atau eksekusi tugas tertentu.

   Tujuan utama dari log ini adalah untuk debugging aplikasi, membantu menemukan dan memperbaiki bug, serta melacak aktivitas pengguna untuk keperluan audit atau analisis. Selain itu, log juga digunakan untuk mendeteksi penyalahgunaan aplikasi. Sebagai contoh, log berikut mencatat bahwa pengguna "jdoe" berhasil login dari alamat IP 192.168.1.50:

   2025-03-24 10:18:15 [INFO] App: User jdoe logged in successfully from 192.168.1.50

   Sementara itu, log berikut mencatat kegagalan dalam memproses pembayaran karena timeout koneksi ke database:

   2025-03-24 10:18:20 [ERROR] App: Failed to process payment for user jdoe - Database connection timeout

4. System logs, Log ini dihasilkan oleh sistem operasi, seperti *Windows, Linux, atau macOS*, untuk mencatat aktivitas sistem secara keseluruhan. Log ini mencatat berbagai informasi penting, termasuk aktivitas sistem, seperti startup, shutdown, atau pembaruan sistem, serta *login* dan *logout* pengguna, baik secara lokal maupun jarak jauh. Selain itu, log juga mencatat kesalahan sistem, seperti kegagalan perangkat keras, crash kernel, atau kehabisan memori, serta peristiwa keamanan, seperti upaya login yang gagal.

   Tujuan utama dari log ini adalah untuk memantau kesehatan dan performa sistem, melacak aktivitas pengguna guna meningkatkan keamanan, serta mendiagnosis masalah sistem, seperti crash atau kegagalan layanan. Sebagai contoh, log berikut mencatat upaya login SSH yang gagal untuk pengguna "jdoe" dari alamat IP 192.168.1.100:

   Mar 24 10:19:32 my-server sshd[12345]: Failed password for user jdoe from 192.168.1.100 port 54321 ssh2

5. Security logs, Log ini dihasilkan oleh alat atau sistem keamanan, seperti *firewall*, *IDS/IPS*, atau perangkat lunak antimalware, untuk mencatat berbagai peristiwa keamanan. Log ini mencatat deteksi ancaman, pemblokiran koneksi, atau upaya login yang mencurigakan, serta aktivitas jaringan yang diblokir atau diizinkan oleh firewall. Selain itu, log juga merekam deteksi malware, serangan *XSS, SQL Injection*, atau aktivitas mencurigakan lainnya.

   Tujuan utama dari log ini adalah untuk mendeteksi dan merespons ancaman keamanan, melacak aktivitas penyerang untuk analisis forensik, serta memastikan kepatuhan terhadap kebijakan keamanan. Sebagai contoh, log berikut mencatat bahwa firewall telah memblokir koneksi *Telnet* yang mencurigakan dari alamat IP 198.51.100.20 ke 192.168.1.10 pada port 23:

   2025-03-24 10:21:45 [ALERT] Firewall: Blocked inbound connection from 198.51.100.20 to 192.168.1.10 on port 23 (Telnet)

6. Network logs, Log ini dihasilkan oleh perangkat jaringan, seperti router, switch, atau alat pemantau jaringan, untuk mencatat berbagai aktivitas dan kejadian dalam jaringan. Log ini mencatat lalu lintas jaringan, termasuk alamat IP sumber dan tujuan, port, protokol, serta jumlah data yang dikirim atau diterima. Selain itu, log juga mencatat peristiwa jaringan, seperti koneksi yang diizinkan atau diblokir, serta kesalahan jaringan, seperti kegagalan koneksi atau kelebihan beban.

   Tujuan utama dari log ini adalah untuk memantau performa jaringan, mendeteksi aktivitas mencurigakan, seperti pemindaian port atau serangan DDoS, serta mendiagnosis masalah jaringan, seperti latensi tinggi atau kehilangan paket. Sebagai contoh, log berikut mencatat bahwa router telah memblokir paket pada port 445 (SMB), kemungkinan karena aturan keamanan:

   2025-03-24 10:23:15 [INFO] Router: Dropped packet from 203.0.113.100 to 192.168.1.10 (Port 445 - SMB)

7. Audit logs, Log ini mencatat berbagai aktivitas penting terkait keamanan dan kepatuhan dalam sistem, termasuk aktivitas pengguna seperti login, logout, atau perubahan data, serta perubahan konfigurasi pada sistem atau aplikasi. Selain itu, log juga merekam akses ke data sensitif, seperti file atau database.

   Tujuan utama dari log ini adalah untuk memastikan kepatuhan terhadap kebijakan dan regulasi, melacak siapa yang melakukan apa dan kapan guna meningkatkan akuntabilitas, serta mendukung investigasi jika terjadi pelanggaran. Sebagai contoh, log berikut mencatat bahwa pengguna "admin" melakukan perubahan pada file /etc/passwd dari alamat IP 192.168.1.1, yang merupakan aktivitas sensitif:

   2025-03-24 10:24:30 [AUDIT] User admin modified file /etc/passwd from 192.168.1.1

Komponen Log

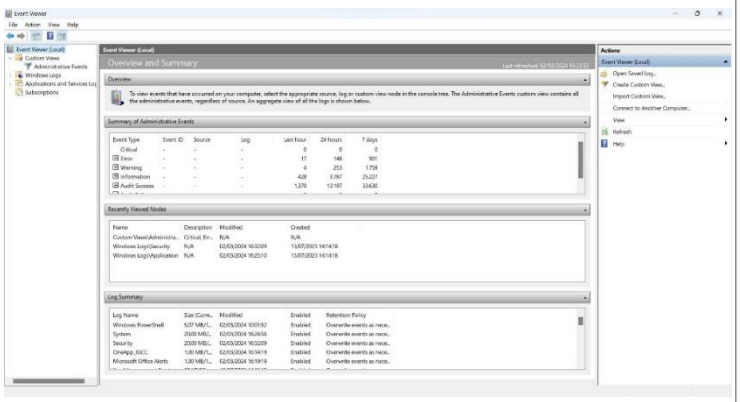
1. *When,* Kapan event terjadi pada sistem dan kapan event dicatat dalam log management
2. *Where,* Dimana event dicatat, atau dimana lokasi event tersebut
3. *Who,* Sumber dari subjek yang menimbulkan event (IP Address, Device, atau FQDN)
4. *What,* Informasi detail mengenai event
5. *Why,* Penjelasan mengenai kondisi event, beserta statusnya (success, failure, error, critical, etc)

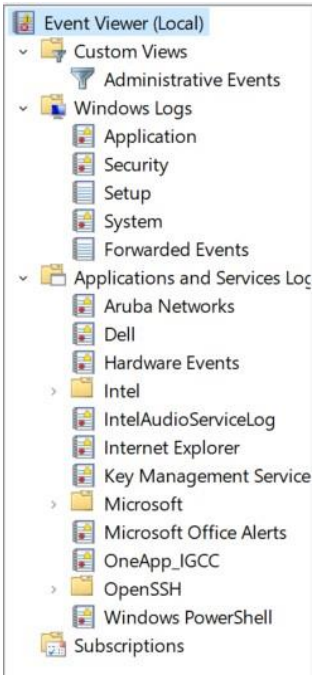
B. Contoh Log

Windows Event Logs

Windows Vista dan versi terbaru

C:\Windows\System32\winevt\logs





C:\Windows\System32\winevt\logs, merupakan lokasi default untuk menyimpan file log peristiwa (event logs) pada Windows Vista dan versi yang lebih baru. File log ini berisi catatan aktivitas sistem, aplikasi, keamanan, dan lainnya, yang dapat digunakan untuk analisis forensik, pemecahan masalah, atau audit sistem.

Terdapat juga berbagai kategori log yang tersedia, seperti **Windows Logs** (Application, Security, Setup, System, Forwarded Events) dan **Applications and Services Logs** (termasuk log dari vendor seperti Dell, Intel, Microsoft, dll.).

Hasil yang didapatkan pada gambar bahwa Sistem mencatat total 1,789 kesalahan (error) dan 22,527 peringatan (warning), dengan 17 kesalahan dan 428 peringatan terjadi dalam 24 jam terakhir. Log System memiliki ukuran 20,480 KB dan terakhir dimodifikasi pada 02/03/2024, menunjukkan aktivitas sistem yang signifikan.

Mengingat Windows Vista sudah tidak didukung sejak 2017, sistem ini berisiko tinggi terhadap ancaman keamanan. Disarankan untuk memeriksa log System dan Application guna mengidentifikasi penyebab kesalahan, serta mempertimbangkan peningkatan ke sistem operasi yang lebih baru untuk meningkatkan keamanan dan stabilitas.

Linux logs

/var/log

Terdapat beberapa jenis log yang terdapat pada linux berupa

1. Log Os
2. Log Services
3. Log Aplikasi

Dapat dilihat pada gambar merupakan isi direktori /var/log. Direktori ini berisi berbagai file log, termasuk auth.log (aktivitas autentikasi), syslog (pesan sistem), msfconsole.log (aktivitas Metasploit Framework), dan log dari layanan seperti Apache2, Nginx, MySQL, PostgreSQL, dan OpenVPN.

1. alternatives.log: Log perubahan konfigurasi alternatif perangkat lunak (via update-alternatives).
2. apache2/: Log server web Apache2 (access dan error log untuk permintaan HTTP dan kesalahan).
3. auth.log: Log autentikasi (login pengguna, sesi SSH, kegagalan login).
4. boot.log: Log proses booting sistem (layanan yang dimulai/gagal).
5. boot.log.[1-4]: Arsip log booting sebelumnya.
6. btmp: Log upaya login gagal (format biner, dibaca dengan lastb).
7. daemon.log: Log aktivitas daemon/layanan (misalnya cron, sshd).
8. debug: Log pesan debug dari sistem/layanan untuk troubleshooting.
9. dpkg.log: Log aktivitas manajer paket dpkg (instalasi/pembaruan paket).
10. faillog: Log jumlah login gagal per pengguna (dibaca dengan faillog).
11. fontconfig.log: Log aktivitas pustaka fontconfig (pengelolaan font).
12. installer/: Log proses instalasi sistem/perangkat lunak.
13. journal/: Log biner dari systemd-journald (pesan sistem, dibaca dengan journalctl).
14. kern.log: Log pesan kernel (perangkat keras, driver, kesalahan kernel).
15. lastlog: Log login terakhir pengguna (format biner, dibaca dengan lastlog).

16. lightdm/: Log manajer tampilan lightdm (login grafis, sesi desktop).
17. messages: Log pesan umum sistem (mirip syslog).
18. mysql/: Log server database MySQL (kesalahan, query, administrasi).
19. nginx/: Log server web Nginx (access dan error log).
20. ntpstats/: Log statistik sinkronisasi waktu NTP.
21. openvpn/: Log layanan OpenVPN (koneksi/pemutusan VPN).
22. postgresql/: Log server database PostgreSQL (query, kesalahan).
23. private/: Log sensitif yang memerlukan izin khusus (misalnya autentikasi).
24. run/: Log sementara dari layanan yang berjalan.
25. samba/: Log layanan Samba (berbagi file dengan Windows).
26. speech-dispatcher/: Log layanan sintesis suara untuk aksesibilitas.
27. stunnel4/: Log stunnel (terowongan SSL/TLS).
28. syslog: Log utama sistem (pesan dari kernel, daemon, aplikasi).
29. syslog.[1-7]: Arsip log syslog sebelumnya.
30. user.log: Log aktivitas pengguna (perintah yang dijalankan).
31. wtmp: Log sesi login/logout (format biner, dibaca dengan last).
32. Xorg.[0-1].log: Log server Xorg (inisialisasi grafis, driver layar).
33. Xorg.[0-1].log.old: Arsip log Xorg sebelumnya.

Contoh Linux Logs : Apache Log Access

1. SQL Injection

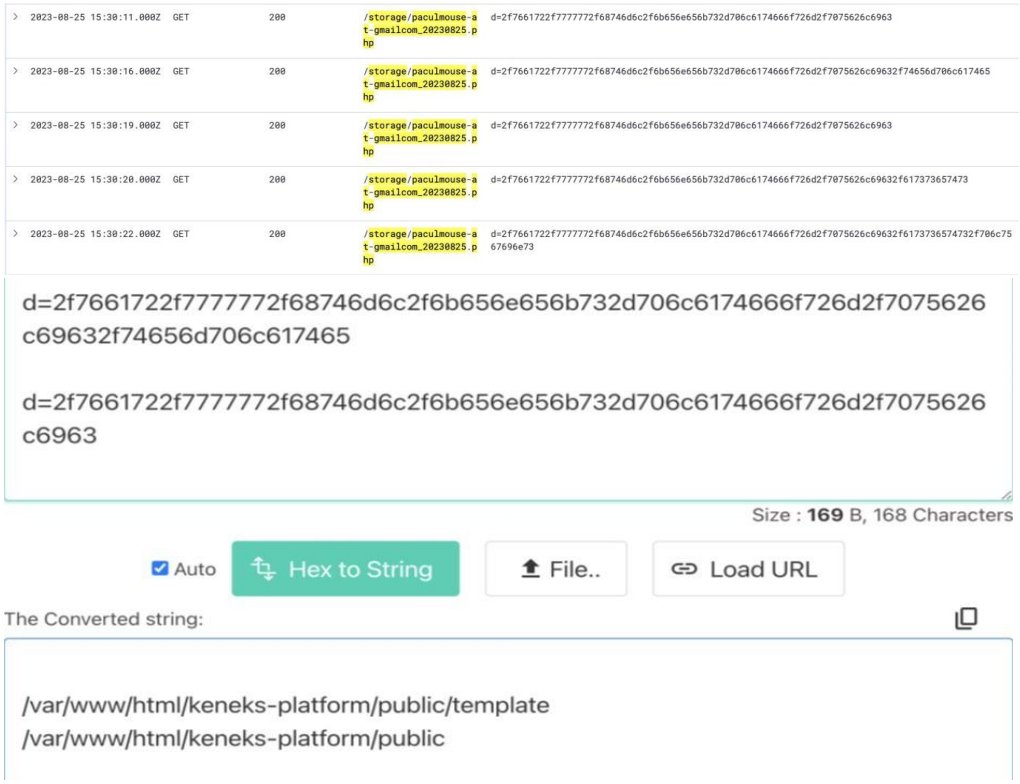
```
115.178.205.90 - - [28/Sep/2020:01:34:21 +0700] "GET
/ecut/admin/detail-karyawan.php?id=-
1013349%27+union+select+1,2,0x3C6868696464656E223E3C2F...
8746D6C3E20,4,5,6,7,8,9,10,11,12,13,14,15,16,17+into+outf
ile+%27C:/xampp/htdocs/y.php%27--+- HTTP/1.1" 200 17515 "-
" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/85.0.4183.101 Safari/537.36"

115.178.205.90 [28/Sep/2020:01:48:56 +0700] "GET
/ecut/admin/detail-karyawan.php?id=-
1013349%27+union+select+1,2,0x236661726965645F417A0D0A446
9726563746F7279496E64657820792E706870,4,5,6,7,8,9,10,11,1
2,13,14,15,16,17+into+outfile+%27C:/xampp/htdocs/.htacces
s%27--+- HTTP/1.1" 200 17515 "-" "Mozilla/5.0 (X11; Linux
x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/85.0.4183.101 Safari/537.36"
```

   Pada gambar dapat dilihat adanya indikasi serangan SQL Injection, terlihat adanya parameter id dalam URL yang dimanipulasi dengan menggunakan perintah SQL UNION SELECT. Kemudian penyerang mencoba memasukkan payload hexadecimal (0x3C6868696464656E223E3C... dan 0x236661726965645F417A...) yang dapat dikonversi menjadi string teks. Payload yang digunakan mengindikasikan bahwa penyerang berusaha menulis file ke dalam server dengan menggunakan perintah INTO OUTFILE. File yang ditargetkan termasuk .htaccess, yang bisa digunakan untuk

mengeksekusi skrip berbahaya atau mendapatkan akses lebih lanjut ke server. Jika serangan berhasil, penyerang dapat menanamkan skrip berbahaya di server.

2. XSS
   192.168.1.100 - - [23/Mar/2025:08:16:10 +0700] "GET /search?q=<script>alert('XSS')</script> HTTP/1.1" 400 512 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) Chrome/89.0.4389.90"
   - Kueri q=<script>alert('XSS')</script> menunjukkan upaya XSS, mencoba menyisipkan skrip JavaScript.
   - Status 400 (Bad Request) menunjukkan server menolak permintaan, mungkin karena filter keamanan.
3. Directory Traversal
   192.168.1.150 - - [23/Mar/2025:08:18:45 +0700] "GET /../../etc/passwd HTTP/1.1" 403 256 "-" "curl/7.68.0"
   - ../../etc/passwd adalah upaya Directory Traversal untuk mengakses file sistem di luar direktori web.
   - Status 403 (Forbidden) menunjukkan server menolak akses, yang bagus untuk keamanan.
4. Brute Force pada Login
   192.168.1.120 - - [23/Mar/2025:08:20:01 +0700] "POST /login.php HTTP/1.1" 401 512 "-" "Mozilla/5.0" -d "username=admin&password=pass123"
   192.168.1.120 - - [23/Mar/2025:08:20:02 +0700] "POST /login.php HTTP/1.1" 401 512 "-" "Mozilla/5.0" -d "username=admin&password=admin123"
   192.168.1.120 - - [23/Mar/2025:08:20:03 +0700] "POST /login.php HTTP/1.1" 401 512 "-" "Mozilla/5.0" -d "username=admin&password=letmein"
   - Beberapa permintaan POST dari IP yang sama dalam waktu singkat dengan kredensial berbeda menunjukkan upaya brute force.
   - Status 401 (Unauthorized) menunjukkan login gagal.
5. File Upload Exploitation
   192.168.1.180 - - [23/Mar/2025:08:21:30 +0700] "POST /upload.php HTTP/1.1" 500 1024 "-" "Mozilla/5.0" -d "file=shell.php"
   - Upaya mengunggah file shell.php (kemungkinan shell berbahaya untuk remote access).
   - Status 500 (Internal Server Error) menunjukkan ada masalah di server, mungkin karena file ditolak atau ada bug di upload.php.

6. Web Upload



Pada gambar dapat dilihat bahwa terdapat indikasi adanya serangan Webshell Upload, yang merupakan teknik eksploitasi di mana penyerang mengunggah file PHP berbahaya ke server untuk mendapatkan akses kendali. Berdasarkan log yang ditampilkan, terdapat beberapa permintaan GET yang berhasil dengan kode status 200, yang mengarah ke file bernama paclmouse.t-gmailcon_20230825.php di dalam direktori /storage/. Hal ini menunjukkan bahwa file PHP yang diduga sebagai webshell telah berhasil diunggah dan dapat diakses melalui URL tertentu.

Setelah itu string dalam format heksadesimal yang setelah dikonversi mengarah ke direktori server /var/www/html/keneks-platform/public/template dan /var/www/html/keneks-platform/public. Ini mengindikasikan bahwa webshell kemungkinan ditanam di dalam sistem yang terkait dengan aplikasi berbasis web. Jika file ini berisi kode berbahaya, maka penyerang dapat mengeksekusi perintah di server, mencuri data, atau melakukan eskalasi hak akses lebih lanjut.

Contoh Linux Logs : Apache Error Log

1. Kesalahan PHP (Fatal Error)
   [Sun Mar 23 08:15:32.123456 2025] [php:error] [pid 5678] [client 192.168.1.100:54321] PHP Fatal error: Uncaught Error: Call to undefined function db_connect() in /var/www/html/db.php:15

- Kesalahan PHP: fungsi db_connect() tidak ditemukan di file db.php baris 15.
- [client 192.168.1.100:54321] menunjukkan IP klien yang memicu kesalahan.

2. Serangan XSS Ditolak oleh Mod_Security
   [Sun Mar 23 08:17:22.987654 2025] [security2:error] [pid 7890] [client 192.168.1.200:54321] ModSecurity: Access denied with code 403 (phase 2). Pattern match "<script>" at ARGS:q. [file "/etc/modsecurity/rules/xss.conf"] [line "10"] [id "950901"] [msg "XSS Attack Detected"]
   - ModSecurity (firewall aplikasi web) mendeteksi dan memblokir upaya XSS dengan pola <script>.
   - Status 403 (Forbidden) diberikan, dan aturan yang cocok ada di file xss.conf.
3. SQL Injection Ditolak oleh Mod_Security
   [Sun Mar 23 08:19:10.321654 2025] [security2:error] [pid 9012] [client 192.168.1.150:54321] ModSecurity: Access denied with code 403 (phase 2). Pattern match "UNION.*SELECT" at ARGS:query. [file "/etc/modsecurity/rules/sql_injection.conf"] [line "20"] [id "950001"] [msg "SQL Injection Attack Detected"]
   - ModSecurity mendeteksi pola SQL Injection (UNION SELECT) dan memblokirnya.
   - Aturan yang cocok ada di file sql_injection.conf.

C. Security Solution

EDR x XDR x SIEM x SOAR

1. Endpoint Detection and Response (EDR)

- Mendeteksi, menyelidiki, dan merespons ancaman pada endpoint.
- Merekam perilaku yang relevan untuk mendeteksi insiden.
- Pengguna dapat melihat semua aktivitas terkait keamanan pada endpoint, seperti koneksi jaringan, process launches, driver loading, perubahan registri, akses disk, dan akses memori.

2. Extended Detection and Response (XDR)

   - Mengidentifikasi, menyelidiki, dan merespon ancaman yang berasal dari berbagai sumber (cloud, jaringan, email, dll).
   - Mengumpulkan data telemetri dari berbagai teknologi (aplikasi cloud, keamanan email, kontrol akses, dll) dan diintegrasikan untuk meningkatkan visibilitas ancaman dan mengurangi waktu untuk mendeteksi dan merespon serangan.

3. Security Information and Event Management (SIEM)

   - Digunakan untuk mengidentifikasi, menilai, dan merespons ancaman keamanan
   - Untuk meningkatkan visibilitas lingkungan TI sehingga tim dapat bekerja secara lebih efisien

4. Security Orchestration, Automation, and Response (SOAR)

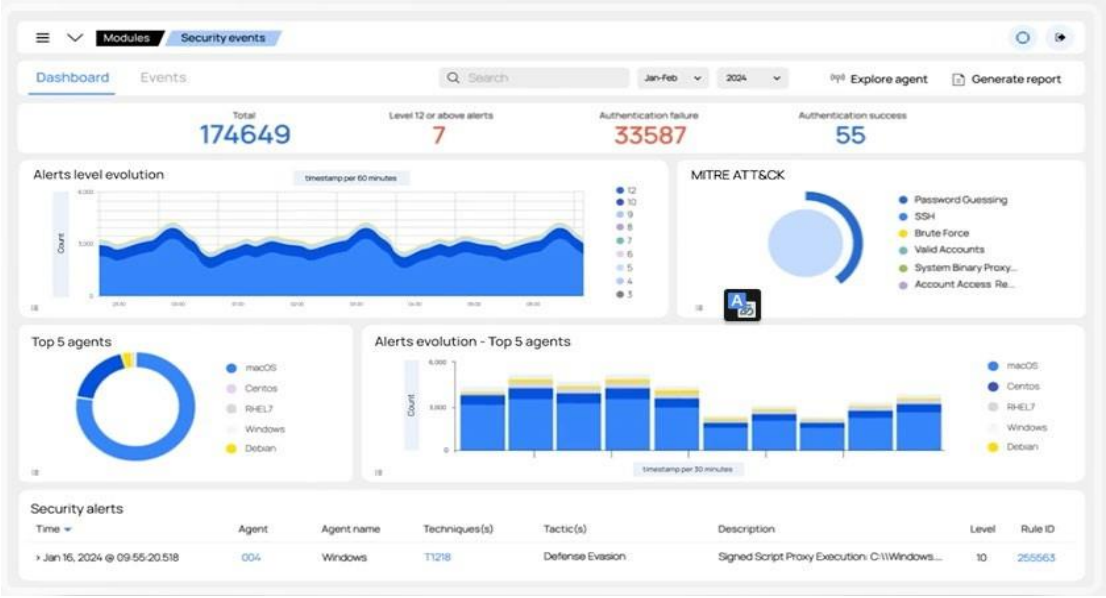
Perangkat yang memungkinkan dilakukannya pengumpulan informasi ancaman keamanan dan respon terhadap peristiwa keamanan tanpa campur tangan manusia, untuk meningkatkan efektivitas operasi keamanan fisik dan digital.

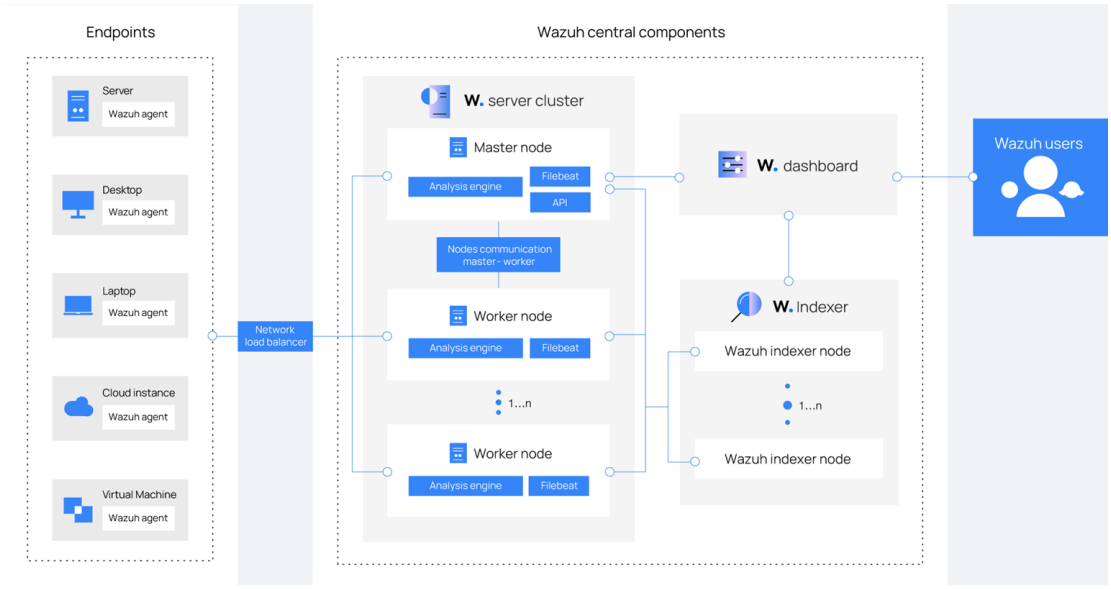
Perbandingan EDR x XDR x SIEM x SOAR

1. EDR, Mengumpulkan dan menghubungkan aktivitas endpoint untuk mendeteksi, menganalisis, dan merespons ancaman keamanan.
2. XDR, Evolusi EDR yang memiliki kemampuan deteksi, analitik, dan respons.
3. SIEM, Mengumpulkan, menggabungkan, menganalisis, dan menyimpan data log dalam jumlah besar dari seluruh perusahaan.
4. SOAR, Mengotomatiskan dan menyederhanakan respons insiden dan operasi keamanan

Wazuh (Endpoint and Cloud Workload Protection)

Wazuh adalah platform XDR dan SIEM open-source yang fleksibel dan scalable, untuk membantu organisasi meningkatkan keamanan jaringan dan endpoint melalui pemantauan dan pendeteksian ancaman, investigasi dan respon insiden, serta analisis log untuk memenuhi persyaratan kepatuhan.



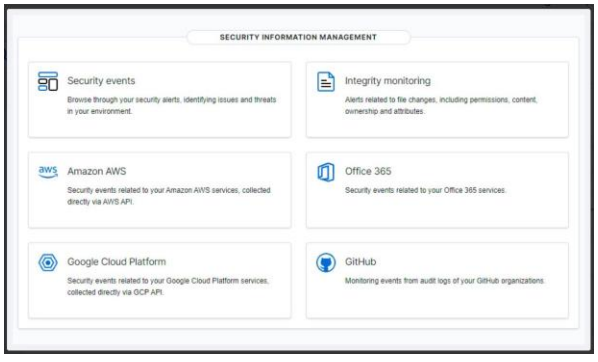


Dapat dilihat dalam gambar arsitektur wazuh terdiri dari tiga komponen utama: Endpoints, Wazuh Central Components, dan Wazuh Users.

Pada bagian Endpoints, berbagai jenis perangkat seperti server, desktop, laptop, cloud instance, dan virtual machine menjalankan Wazuh Agent. Agen ini berfungsi untuk mengumpulkan data keamanan dan mengirimkannya ke Wazuh Server Cluster melalui Network Load Balancer, yang memastikan distribusi lalu lintas jaringan secara optimal.

Wazuh Central Components terdiri dari Wazuh Server Cluster, Wazuh Indexer, dan Wazuh Dashboard. Wazuh Server Cluster memiliki Master Node dan beberapa Worker Node, di mana Master Node bertanggung jawab atas analisis data, komunikasi dengan worker nodes, serta menyediakan API untuk integrasi. Worker nodes menangani pemrosesan analitik dan pengiriman data menggunakan Filebeat.

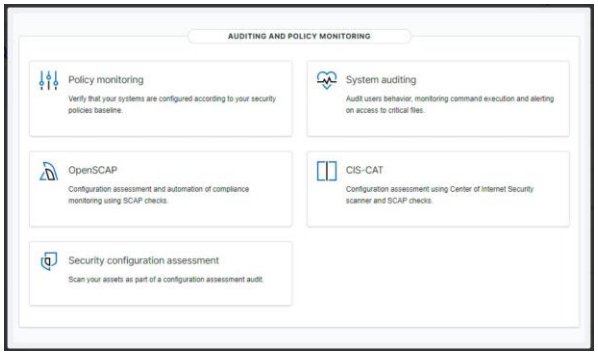
Wazuh Indexer digunakan untuk menyimpan dan mengindeks data yang dikumpulkan oleh agen, yang memungkinkan pencarian dan analisis lebih lanjut. Data yang telah diproses dapat diakses melalui Wazuh Dashboard, yang menyediakan antarmuka bagi pengguna untuk memantau ancaman dan mengelola keamanan sistem.

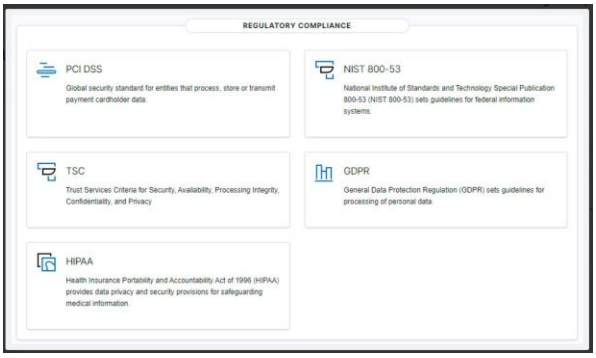


Pada gambar dapat dilihat bahwa terdapat dua bagian utama dari sistem manajemen informasi keamanan dan deteksi ancaman. Bagian pertama, Security Information Management (SIM), mencakup berbagai fitur pemantauan keamanan, seperti Security Events untuk mengidentifikasi ancaman, Integrity Monitoring untuk mendeteksi perubahan file dan izin, serta integrasi dengan layanan cloud seperti Amazon AWS, Google Cloud Platform, Office 365, dan GitHub. Dengan fitur ini, organisasi dapat memantau aktivitas keamanan di berbagai lingkungan IT mereka.

Bagian kedua, Threat Detection and Response (TDR), berfokus pada deteksi dan respons ancaman. Fitur Vulnerabilities membantu dalam mengidentifikasi aplikasi yang rentan, sementara Osquery memungkinkan eksplorasi sistem operasi sebagai database relasional. MITRE ATT&CK digunakan untuk menganalisis taktik dan teknik serangan berdasarkan skenario nyata. Selain itu, integrasi dengan VirusTotal memungkinkan analisis file mencurigakan, sedangkan Docker Listener memantau aktivitas dalam lingkungan container.

Dengan adanya fitur-fitur ini, sistem memberikan solusi komprehensif untuk pemantauan keamanan, deteksi ancaman, serta respons cepat terhadap insiden keamanan dalam berbagai lingkungan IT, baik di on-premise maupun cloud.





Pada gambar dapat dilihat bahwa terdapat dua bagian utama dari sistem pemantauan keamanan dan kepatuhan regulasi. Bagian pertama, Auditing and Policy Monitoring, mencakup fitur-fitur untuk memastikan konfigurasi keamanan sistem sesuai dengan kebijakan yang ditetapkan. Fitur Policy Monitoring digunakan untuk memverifikasi bahwa sistem telah dikonfigurasi sesuai dengan kebijakan keamanan yang berlaku. System Auditing memungkinkan pemantauan perilaku pengguna, termasuk eksekusi perintah dan akses ke file penting. OpenSCAP dan CIS-CAT digunakan untuk menilai konfigurasi keamanan dengan SCAP checks, sedangkan Security Configuration Assessment membantu dalam melakukan audit terhadap aset yang ada.

Bagian kedua, Regulatory Compliance, berfokus pada kepatuhan terhadap berbagai standar keamanan dan regulasi. PCI DSS menetapkan standar keamanan global untuk entitas yang menangani data kartu pembayaran. NIST 800-53 memberikan pedoman keamanan informasi untuk sistem federal. TSC (Trust Services Criteria) mengatur aspek keamanan, ketersediaan, dan privasi dalam pemrosesan data. HIPAA menetapkan aturan keamanan untuk melindungi informasi medis, sementara GDPR mengatur pemrosesan data pribadi sesuai dengan regulasi perlindungan data di Uni Eropa.

Mitre Att&ck

https://attack.mitre.org/matrices/enterprise/