MODUL 9

SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

9.1 Tujuan Praktikum

1. Dapat memahami dan mengetahui ap aitu SIEM
2. Dapat memahami dan mengetahui manfaat dari SIEM
3. Dapat memahami dan mengetahui implementasi dari SIEM
4. Dapat melakukan monitoring potensi serangan *cyber* menggunakan SIEM
5. Dapat memahami dan mengetahui teori tentang *honeypot technology*

9.2 Alat dan Bahan

1. Laptop
2. Mouse
3. Microsoft Azure

9.3 Dasar Teori

9.3.1 Pengertian SIEM

Security Information and Event Management atau SIEM adalah Solusi yang mmebantu organisasi mendeteksi, menganalisis, dan merespons ancaman keamanan sebelum membahayakan operasi bisnis. SIEM, dibaca “sim”, menggabungkan manajemen keamanan. Teknologi SIEM mengumpulkan data log kejadia dari berbagai sumber, mengidentifikasi aktivitas yang menyimpang dari norma dengan analisis *real time*, dan mengambil Tindakan yang tepat.

Singkatnya, SIEM memberi organisasi visibilitas tentang aktivitas di dalam jaringan agar dapat merespons potensi serangan *cyber* dengan cepat dan memenuhi persyaratan kepatuhan. Dalam sepuluh tahun terakhir, teknologi SIEM telah berkembang dengan memanfaatkan kecerdasan buatan untuk membuat deteksi ancaman dan respons insiden lebih cerdas serta lebih cepat.

Dashboard SIEM adalah tampilan visual yang menampilkan data dari SIEM. Dashboard SIEM memungkinkan pengguna untuk memahami hasil analisis yang penting bagis pebisnis, departemen, atau proyek mereka.

9.3.2 Cara Kerja SIEM

SIEM mengumpulkan, menggabungkan, dan menganlasis volume data dari aplikasi, perangkat, server, dan pengguna ortganisasi secara *real time* sehingga tim keamanan dapat mendeteksi dan memblokir serangan. Data yang diterima kemudian akan dinormalisasi, dikategorikan, dan diklasifikasi menjadi tindakan yang tepat untuk diambil. SIEM menggunakan aturan yang telah ditentukan untuk membantu tim keamanan menentukan ancaman dan menghasilkan peringatan. SIEM menggunakan teknologi kecerdasan buatan (AI) dan pemrosesan bahasa alami (NLP/ *Natural Language Processing*) untuk mengenali pola dan perilaku yang mencurigakan, serta membedakan antara ancaman yang nyata dan palsu.

9.3.3 Manfaat SIEM

SIEM menawarkan beberapa manfaat utama, yaitu:

1. Pemantauan keamanan yang bersifat *real-time*

   SIEM memberikan visibilitas real-time ke posisi keamanan organisasi, memungkinkan tim keamanan untuk memantau peristiwa dan mendeteksi ancaman potensial dengan cepat. Hal ini memungkinkan pencarian ancaman proaktif dengan mengidentifikasi aktivitas mencurigakan, anomali, atau pola yang mungkin menunjukkan pelanggaran keamanan.

2. Manajemen kepatuhan

   SIEM memfasilitasi manajemen kepatuhan dengan mengumpulkan dan mengkorelasi log dari berbagai sumber, sehingga menyederhanakan proses menghasilkan laporan kepatutan. Fitur ini sangat penting bagi perusahaan yang beroperasi di industri yang sangat diatur.

3. Peringatan jika terjadi ancaman keamanan

   SIEM memungkinkan kemampuan respons insiden dengan menyediakan peringatan, tindakan respons otomatis, dan laporan komprehensif. Ini

membantu tim keamanan dalam memprioritaskan dan merespon insiden keamanan secara efektif, mengurangi waktu yang dibutuhkan untuk mengidentifikasi dan mengurangi ancaman.

9.3.4 Fungsi Utama SIEM dalam Keamanan Jaringan

1. Daftar koleksi

   SIEM bertindak sebagai repositori pusat untuk mengumpulkan log dan peristiwa dari berbagai sumber di seluruh jaringan dan sistem organisasi. Sumber-sumber ini termasuk firewall, sistem deteksi intrusion (IDS), perangkat jaringan, server, dan banyak lagi. Dengan menggabungkan data dari berbagai sumber, SIEM memberikan pandangan holistik dari lanskap keamanan organisasi.

2. Korelasi peristiwa

   SIEM unggul dalam menganalisis dan mengkorelasi peristiwa dari berbagai sumber untuk mengidentifikasi ancaman potensial. Ini mencari pola, anomali, dan indikator kompromi yang mungkin menunjukkan pelanggaran keamanan. Dengan menghubungkan titik-titik di berbagai log, SIEM membantu mendeteksi pola serangan yang kompleks yang mungkin tidak terlihat oleh sistem keamanan individu. Aturan korelasi didefinisikan untuk mengidentifikasi aktivitas mencurigakan, seperti upaya akses yang tidak sah, infeksi malware, atau perilaku pengguna yang abnormal.

3. Pengawasan *real-time*

   SIEM terus memantau peristiwa keamanan secara real time, memberikan tim keamanan dengan visibilitas langsung terhadap ancaman potensial. Ini menawarkan peringatan dan pemberitahuan real-time ketika aktivitas mencurigakan terjadi. Ini memungkinkan analis keamanan untuk segera merespons potensi insiden keamanan dan meminimalkan dampaknya.

4. Integrasi ancaman intelijen

   SIEM mengintegrasikan dengan sumber dan database intelijen ancaman eksternal. Dengan memanfaatkan informasi terkini tentang ancaman yang muncul, SIEM meningkatkan kemampuan deteksi. Ini merujuk peristiwa

dan indikator terhadap vektor serangan yang diketahui, alamat IP berbahaya, domain yang dikompromikan, dan sumber intelijen ancaman lainnya. Integrasi ini memastikan bahwa organisasi terinformasi tentang ancaman terbaru dan dapat merespon secara proaktif terhadapnya.

5. Menajemen kepatuhan

   SIEM memainkan peran penting dalam manajemen kepatuhan dengan mengumpulkan dan mengkorelasi log dari berbagai sumber. Ini menyederhanakan proses menghasilkan laporan kepatuhan, yang sangat penting bagi organisasi yang beroperasi di industri yang diatur. SIEM membantu organisasi memenuhi persyaratan kepatuhan dengan memantau dan melaporkan peristiwa dan insiden keamanan, sehingga mendukung proses audit dan regulasi.

6. Reaksi insiden

   SIEM memfasilitasi respons insiden dengan menyediakan peringatan, tindakan respons otomatis, dan laporan komprehensif. Ketika insiden keamanan terjadi, SIEM dapat memicu tindakan otomatis, seperti memblokir alamat IP atau mengisolasi sistem yang terpengaruh. Ini membantu tim keamanan dalam memprioritaskan dan merespon insiden keamanan secara efektif, mengurangi waktu yang dibutuhkan untuk mengidentifikasi dan mengurangi ancaman.

9.3.5 Keuntungan Penggunaan SIEM

SIEM menawarkan banyak keuntungan yang dapat membantu memperkuat postur keamanan organisasi secara keseluruhan, termasuk:

1. Tampilan potensi ancaman yang terpusat
2. Identifikasi dan respons ancaman secara *real-time*
3. Inteligensi ancaman Tingkat lanjut
4. Audit dan pelaporan kepatuhan peraturan
5. Transparansi yang lebih besar memantau pengguna, aplikasi, dan perangkat.

9.3.6 Contoh Penyedia Jasa Layanan SIEM

A. Wazuh

Wazuh adalah *platform* SIEM *open source* gratis yang dikembangkan dari OSSEC. Wazuh menawarkan deteksi kerentanan, analisis log keamanan, penilaian konfigurasi, dan kemampuan kepatuhan terhadap peraturan. Wazuh dapat mengimplementasikan perangkat lunak pada sistem operasi Linux, dan mendukung metode *on-premise*, berbasis cloud, dan *hybrid*. Meskipun Wazuh versi gratis tersedia, terdapat Wazuh opsi untuk berbayar dengan platform cloud yang dihosting yang menawarkan UI yang menarik, pengaturan langsung, dan ancaman sumber terbuka.

B. AlienVault OSSIM

OSSIM (*open source security information management*) oleh AlienVault adalah platform SIEM *open source* yang gratis dan terkemuka. OSSIM juga memiliki versi berbayar, USM Anywhere, dengan fitur yang lebih canggih. OSSIM dapat menggunakan versi gratis pada satu server, tetapi meningkatkannya ke versi berbayar memungkinkan penskalaan ke server tambahan. Platform ini terdiri dari kerangka kerja keamanan seperti OSSEC, Nagios, Snort dan OpenVAS. OSSIM memiliki fitur pengumpulan peristiwa, korelasi, normalisasi dan ancaman intelligen.

C. Mozilla Defense Platform (MozDef)

Mozilla Defense Platform adalah seperangkat layanan mikro gratis yang digunakan sebagai platform SIEM yang *open source*. MozDef dibangun di atas platform pihak ketiga seperti Meteor dan Kibana. MozDef menawarkan kemampuan seperti korelasi peristiwa dan peringatan keamanan dan bertujuan untuk mengotomatiskan respon insiden. MozDef juga dapat menyesuaikan preferensi peringatan dengan plugin Python. Sistem ini menawarkan model penyebaran yang dihost sendiri tetapi tidak termasuk dukungan seluler.

D. Graylog Open

Graylog Open adalah platform SIEM *open source* gratis yang menawarkan kemampuan manajemen log terpusat. Graylog Open mengumpulkan,

menyimpan, meningkatkan dan menganalisis peristiwa keamanan dan data log. Fitur teratas termasuk dasbor, pencarian lanjutan, toleransi kesalahan, paket konten, dan sespan graylog. Graylog Open juga menyediakan dasbor untuk menampilkan data pemantauan keamanan waktu nyata, metrik penting, dan tren pada satu halaman.

E. Prelude OSS

Prelude OSS adalah versi SIEM *open source* gratis dari perangkat lunak kelas perusahaan vendor. Prelude OSS mendukung berbagai format log dan dapat dengan mudah diintegrasikan dengan alat pihak ketiga seperti Suricata, OSSEC dan Snort. Format IDMEF memungkinkan pengguna menggunakan data intrusion detection system (IDS). Prelude OSS menawarkan kemampuan seperti pemantauan data, penyelidikan hukum, peringatan, pelaporan, dan integrasi pihak ketiga.

9.3.7 Honeypot Technology

Honeypot adalah server atau sistem jaringan yang dipasang sebagai umpan untuk memikat hacker saat akan melakukan upaya penyerangan atau peretasan. Honeypot dirancang agar terlihat seperti target yang menarik dan diletakan di sekitar server asli. Sehingga dapat mengelabui hacker dan menyerang target yang salah.

9.3.8 Cara Kerja *Honeypot Technology*

Honeypot dibuat semirip mungkin dengan sistem komputer pada umumnya, lengkap dengan aplikasi maupun data yang dapat menarik perhatian *hacker*. Seperti misalnya *honeypot* yang meniru sistem keuangan perusahaan dan lain sebagainya. Untuk memancing perhatian peretas, *honeypot* sengaja dibuat dengan tingkat keamanan yang rendah. Salah satunya dengan penggunaan port yang rentan terhadap pemindaian port. Kemudian port yang lemah tersebut dibiarkan terbuka agar hacker terpancing untuk menyerangnya. Perlu dipahami jika *honeypot* bukanlah bentuk *cyber security* yang dapat mencegah serangan hacker secara langsung. Tujuan diciptakannya *honeypot* adalah untuk membantu menyempurnakan *Intrusion Detection System (IDS)–software* yang dapat mendeteksi jaringan keamanan agar dapat mengatasi

serangan dengan lebih baik lagi. Ada dua tahap utama dalam *honeypot: production* dan *research*. Pada tahap produksi, honeypot fokus sebagai server yang menyamar dan mengelabui peretas. Sedangkan pada tahap penelitian, *honeypot* akan melakukan penelitian terhadap serangan yang berhasil masuk ke dalam *honeypot*.

9.3.9 Fungsi *Honeypot Technology*

Honeypot memiliki beberapa fungsi penting untuk membantu mencegah serangan *hacker* pada server. Berikut penjelasannya:

1. Mengalihkan perhatian

   Honeypot adalah sistem jaringan yang dibuat semirip mungkin dengan server asli. Dengan begitu, kamu dapat menjadikan *honeypot* sebagai pengalih perhatian dari target utama serangan *hacker*.

2. Mendeteksi serangan

   Ketika serangan *hacker* masuk ke dalam perangkat *honeypot*, sistem jaringan *honeypot* akan memberikan sinyal atau tanda bahaya sehingga server asli dapat meningkatkan keamanannya.

3. Menganalisis serangan

   Serangan yang terperangkap kemudian dianalisis untuk mendapatkan informasi seperti jenis serangan apa yang dilakukan maupun metode apa yang dilakukan.

4. Memprediksi serangan

   Jika sudah memiliki informasi terkait serangan hacker tersebut, di lain waktu kamu akan dapat memprediksi serangan tersebut kembali datang dan meningkatkan keamanan sehingga lebih sulit untuk diserang.

9.3.10 Jenis-Jenis *Honeypot*

Honeypot dibedakan berdasarkan target serangan peretas yang akan ditipunya. Berikut ini beberapa jenis *honeypot*:

1. *Spam Honeypot*

Spam honeypot adalah jenis *honeypot* yang dirancang untuk menarik *spammer* menggunakan *proxy* terbuka dan *mail relay*. Nantinya, *hacker* akan mencoba mengirimkan email menggunakan *mail relay*. Jika berhasil, *hacker* akan mengirimkan spam dalam jumlah besar. *Spam honeypot* dapat menganalisis tes *spammer* dan memblokir spam yang dicoba dikirimkan oleh *hacker*.

2. *Malware Honeypot*

   Honeypot jenis *malware* akan menggunakan vektor serangan yang sudah dikenal untuk menarik *malware*. *Malware honeypot* dapat meniru perangkat USB. Ketika *malware* mulai menyerang, *honeypot* akan mengelabui *malware* tersebut agar menyerang USB yang sudah dimodifikasi.

3. *Database Honeypot*

   Honeypot jenis ini sengaja membuat database palsu untuk menarik *cybercrime* yang menargetkan database seperti *SQL Injection*. Kamu dapat memanfaatkan *firewall* database untuk membuatnya.

4. *Client Honeypot*

   Honeypot jenis *client* akan mencoba untuk menarik perhatian *hacker* yang menargetkan *client* sebagai korbannya. *Honeypot client* akan berpura-pura menjadi *client* untuk mengamati bagaimana penyerang membuat modifikasi ke server selama serangan. *Honeypot* client biasanya dijalankan di lingkungan virtual dan memiliki perlindungan penahanan untuk mengurangi risiko paparan ke penelitinya.

5. *Honeynet*

   Honeynet adalah jenis *honeypot* yang terdiri dari beberapa jaringan *honeypot*. Fungsinya adalah untuk mempelajari beberapa serangan seperti *Distributed Denial of Service* (DDoS), serangan ke *Content Delivery Network* (CDN), atau serangan *Ransomware*. Meskipun *honeynet* digunakan untuk mempelajari berbagai jenis serangan, *honeynet* juga berisi semua *traffic* masuk dan keluar, untuk melindungi sistem jaringan lainnya.

9.3.11 Kelebihan Honeypot

- Mengumpulkan data secara aktual dari serangan yang sebelumnya masuk ke dalam perangkap *honeypot*.
- Mendeteksi serangan dengan cukup akurat, karena *honeypot* bukanlah sistem jaringan yang dapat dengan mudah diakses pengguna umum. Hanya hacker dengan niat menyerang yang akan mengaksesnya
- Biaya yang lebih hemat, karena *honeypot* dapat menjadi investasi jangka panjang dalam mencegah serangan dan tidak memerlukan banyak sumber daya
- Menangkap aktivitas berbahaya, bahkan jika penyerang menggunakan enkripsi.

9.3.12 Kekurangan Honeypot

- Data yang terbatas, karena *honeypot* hanya mengumpulkan data saat terjadi serangan
- Jaringan yang terisolasi, sehingga terkadang hacker dapat mencurigainya sebagai *honeypot*
- Dapat menempatkan server asli dalam risiko, meskipun *honeypot* adalah jaringan yang terisolasi, namun secara tidak langsung sistem jaringan tersebut terhubung dengan server asli. Sehingga ketika *honeypot* diserang, server asli tetap perlu diamankan.