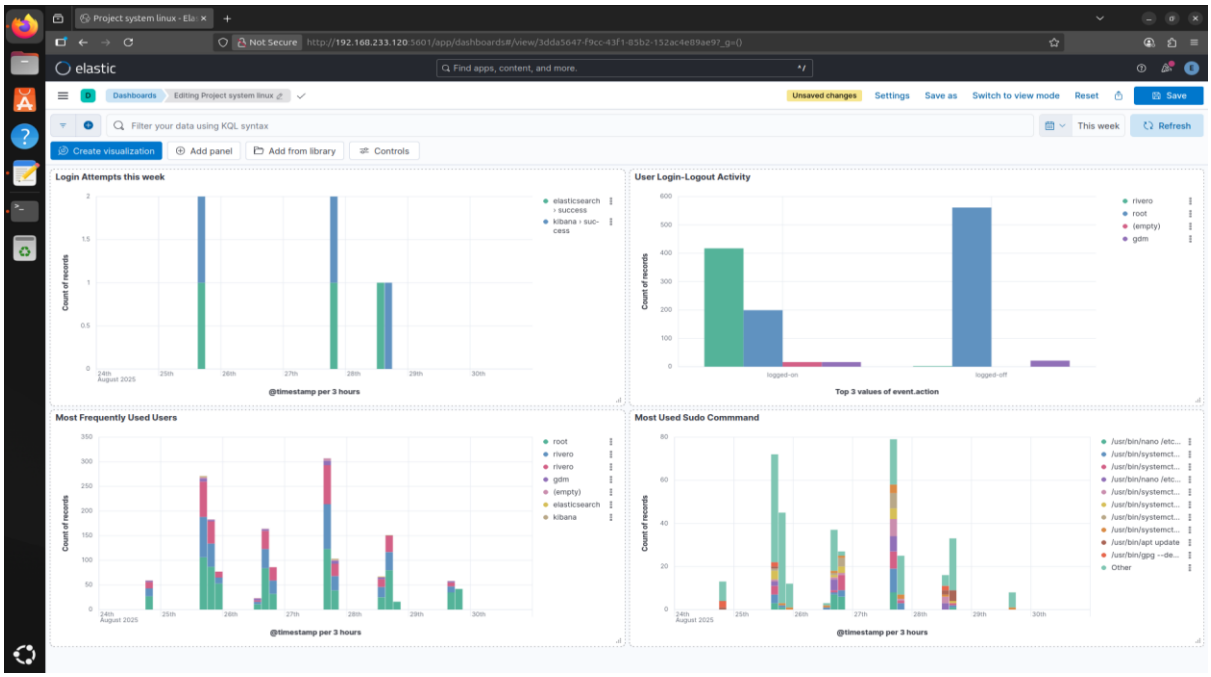
PROJEK SIEM (*Security Information and Event Management*) BERBASIS ELK STACK: MENGANALISIS LOG SISTEM KOMPUTER (Linux Ubuntu)

Laporan ini akan menyajikan hasil analisis aktivitas pengguna pada server ubuntu dalam periode minggu ini. Analisis ini menggunakan data log yang dikumpulkan oleh Elastic Agent dan divisualisasikan menggunakan Kibana. Projek SIEM sederhana ini dibangun menggunakan ELK Stack dikarenakan aplikasinya yang *open source* cocok untuk pembelajaran. Projek SIEM dapat dilihat pada gambar berikut.



TUJUAN PROJEK :

Tujuan utama projek ini adalah untuk memperkuat pemahaman dan keterampilan terkait alur kerja SIEM dan dapat mengidentifikasi dan menganalisis pola aktivitas pengguna terhadap sistem serta memvisualisasikan data log sebagai bentuk laporan dan informasi.

ALAT YANG DIGUNAKAN :

- Elastic Search, Sebagai penyimpanan dan pengindeksan data log
- Elastic Agent, Sebagai pengumpul data dari sumbernya yaitu log sistem
- Kibana, Sebagai alat visualisasi , manajemen dan analisis

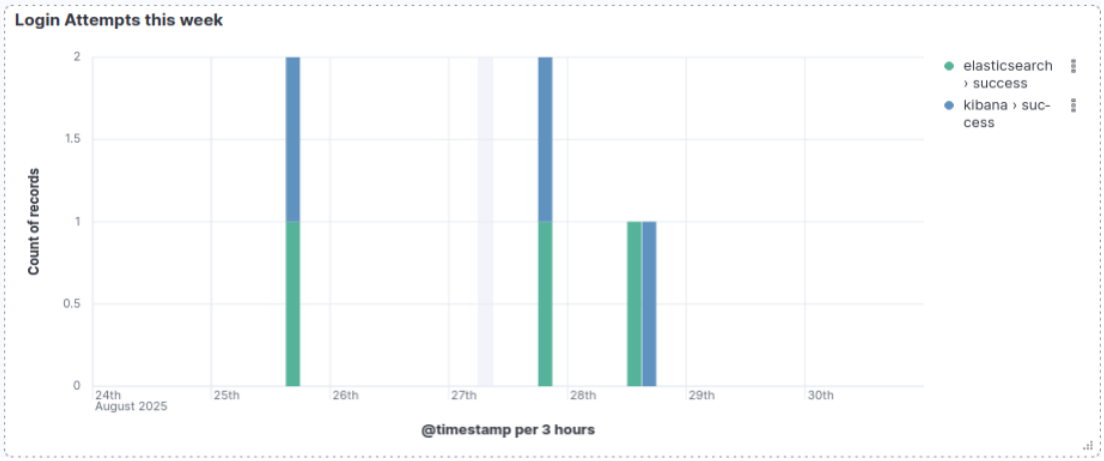
RUANG LINGKUP :

1. Projek ini menganalisis data log sistem yang dihasilkan dalam rentang waktu minggu ini yaitu pada tanggal 24/08/2025 sampai dengan 30/08/2025.
2. Sistem operasi menggunakan linux ubuntu yang berjalan di mesin virtual.

HASIL ANALISIS :

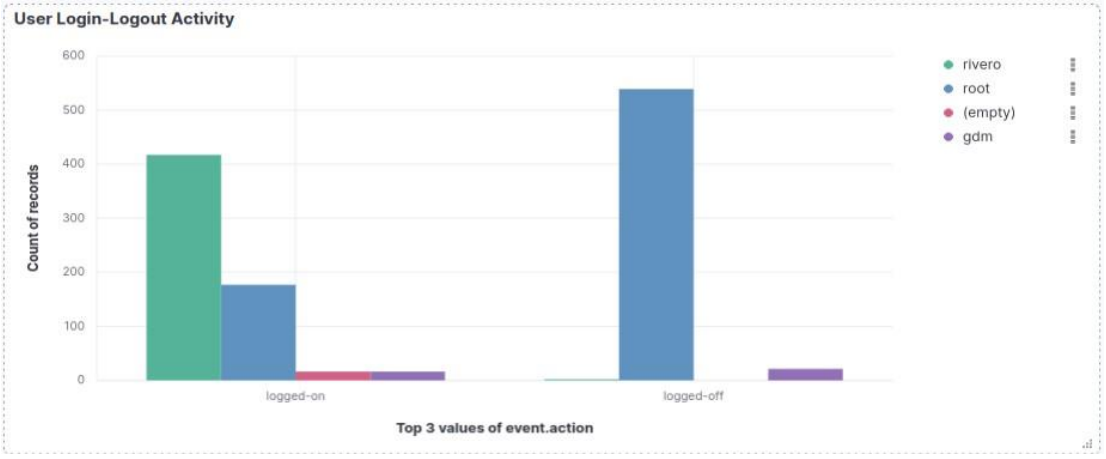
1. **Analisis upaya *Login* user**

   Analisis ini menunjukkan status upaya *login* dalam minggu ini. Terdapat 2 user yang melakukan *login* yaitu elasticsearch dan kibana dengan hasil sukses tanpa adanya kegagalan. Grafik dapat dilihat pada gambar berikut.

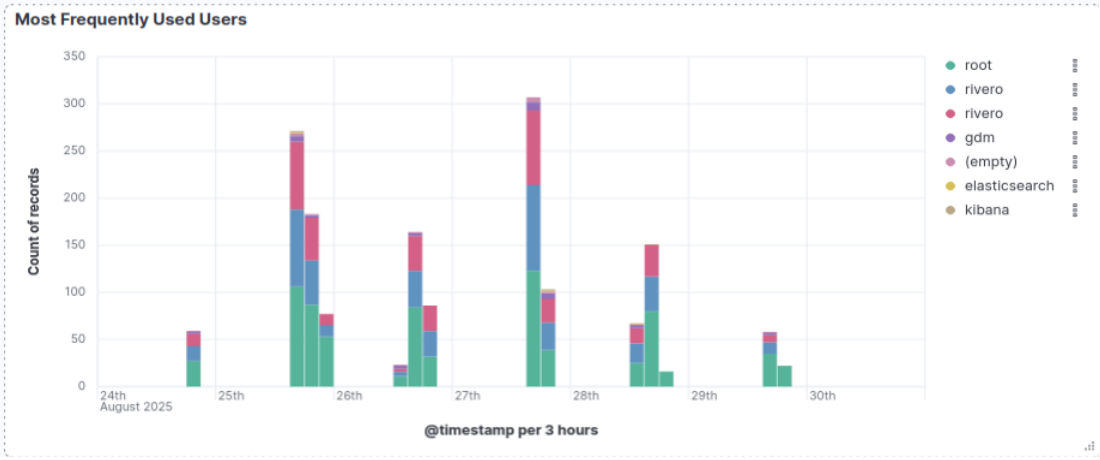


2. **Analisis aktivitas *login & logout* user**

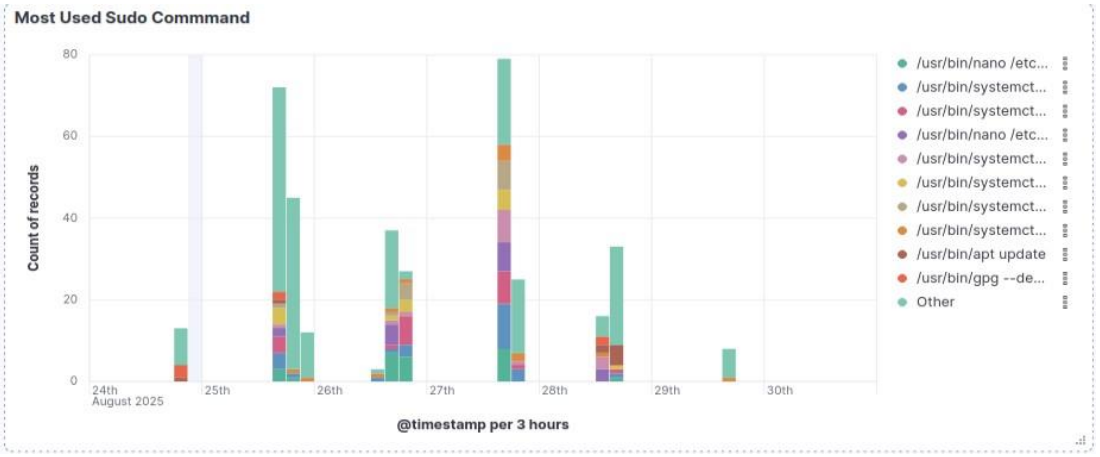
   Analisis ini menunjukkan seberapa banyak user melakukan *login* & *logout* pada sistem. Terdapat 4 user yaitu rivero, root, empty (kosong) dan gdm. Dalam grafik tersebut rivero adalah user yang sering melakukan *login* sebanyak 417 kali dan user root melakukan *logout* sebanyak 547 kali. Hal ini dapat mendeteksi berapa kali user melakukan *login* serta *logout* dalam rentang waktu tertentu. Grafik dapat dilihat pada gambar berikut.



3. **Analisis user yang paling sering digunakan.**
   Analisis ini menunjukkan user yang paling banyak digunakan di dalam sistem. Terdapat 7 user yang digunakan. Hasil analisis ini berfungsi untuk mendeteksi siapa saja user yang paling sering digunakan untuk mengakses atau menggunakan sistem. Grafik dapat dilihat pada gambar berikut.



4. **Analisis perintah sudo yang sering digunakan**
   Analisis ini bertujuan untuk mengetahui perintah sudo yang sering digunakan dari waktu ke waktu oleh user. Hal ini dapat berfungsi untuk mendeteksi dan mencegah adanya perintah berbahaya yang diinput oleh user menggunakan sudo. Grafik dapat dilihat pada gambar berikut.



KESIMPULAN

Berdasarkan hasil analisis yang dilakukan, dengan membangun sebuah teknologi SIEM menggunakan ELK Stack maka kita dapat mengidentifikasi,memonitoring serta menganalisis aktivitas pengguna terhadap sistem. Data log yang dikumpulkan telah berhasil divisualisasikan untuk menghasilkan informasi yang bermanfaat. Dengan membangun SIEM maka dapat mengidentifikasi jika adanya aktivitas berbahaya yang dilakukan pengguna terhadap sistem seperti penggunaan sudo command berbahaya serta aktivitas login yang mencurigakan.