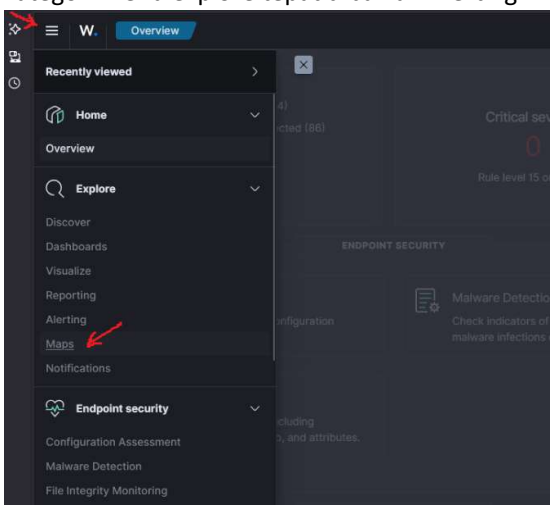
Monitoring log / SIEM dengan fasilitas Pemetaan di Wazuh

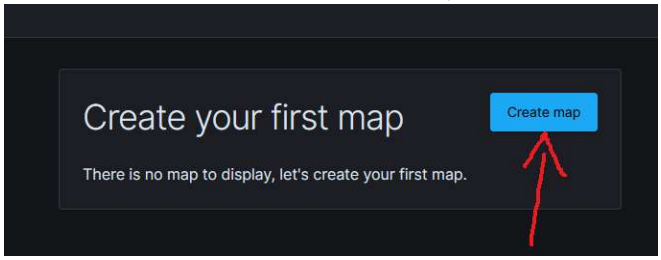
Oleh: Didik Wibawanto (TiTIS-BlitarKab) ®2025

Langkah-langkah

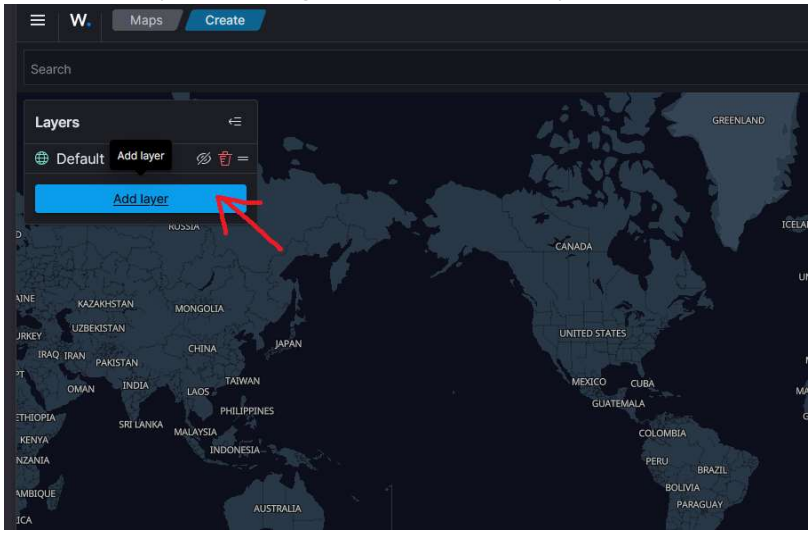
1. Buka menu utama di pojok kiri atas disibelah logo huruf W, kemudian pilih Maps dalam kategori menu explore tepat dibawah Alerting



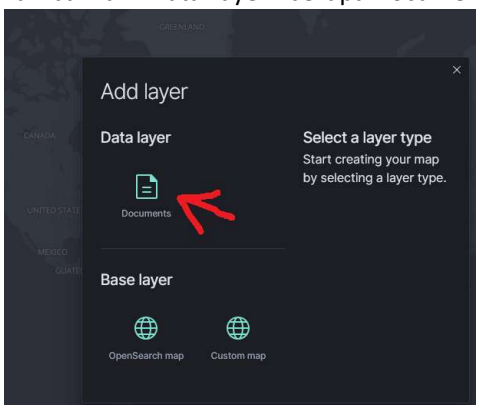
2. Klik tombol biru bertuliskan ”Create Map”



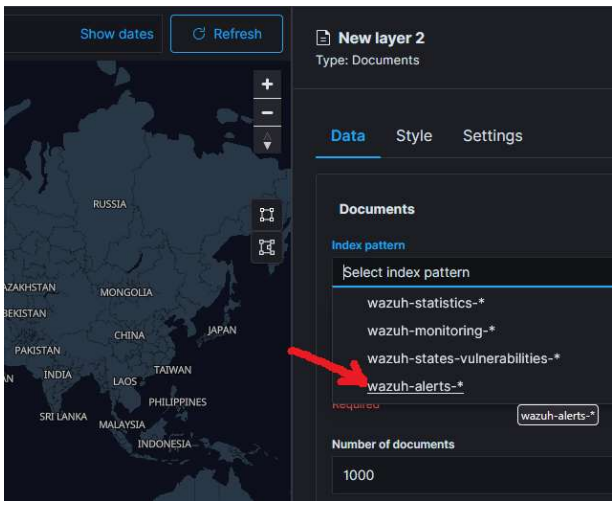
3. Tambahkan layer baru dengan klik tombol ”Add layer”



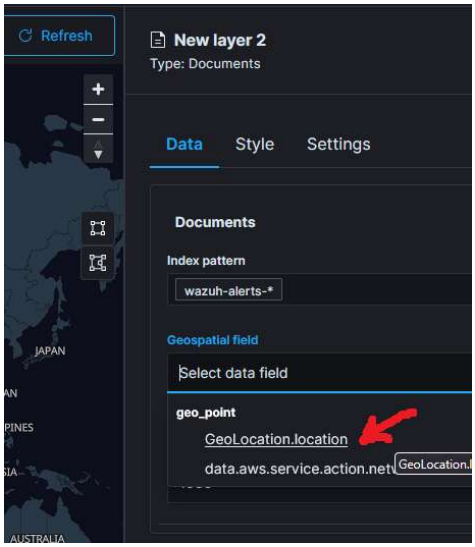
4. Tambahkan ”Data Layer” berupa Documents



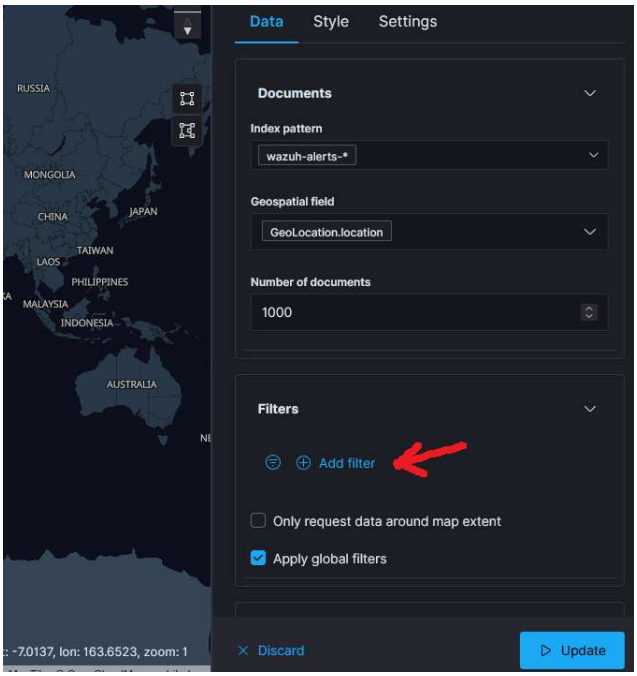
5. Akan muncul menu baru di kanan sebagai ”New Layer2” dengan typeL Documents Pilih pada drop-down menu “wazuh-alerts-*”



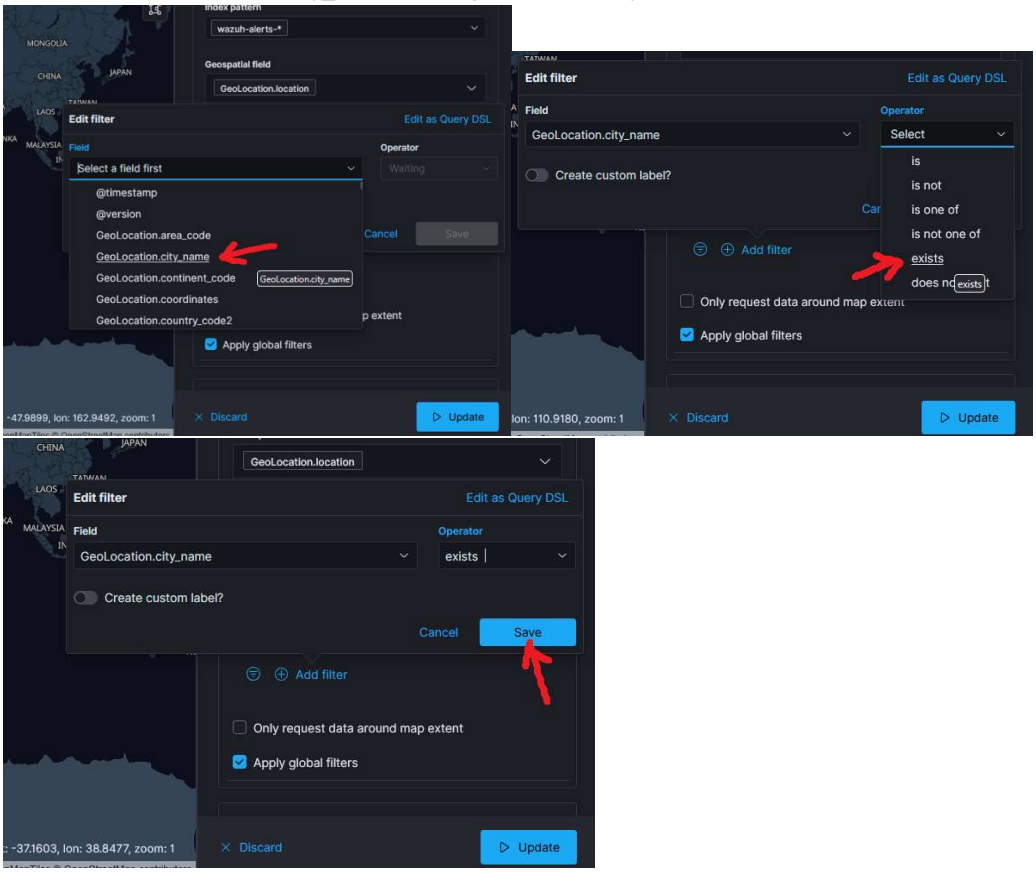
6. Pilih ”GeoLocation.location” pada menu drop-down Geospatial field



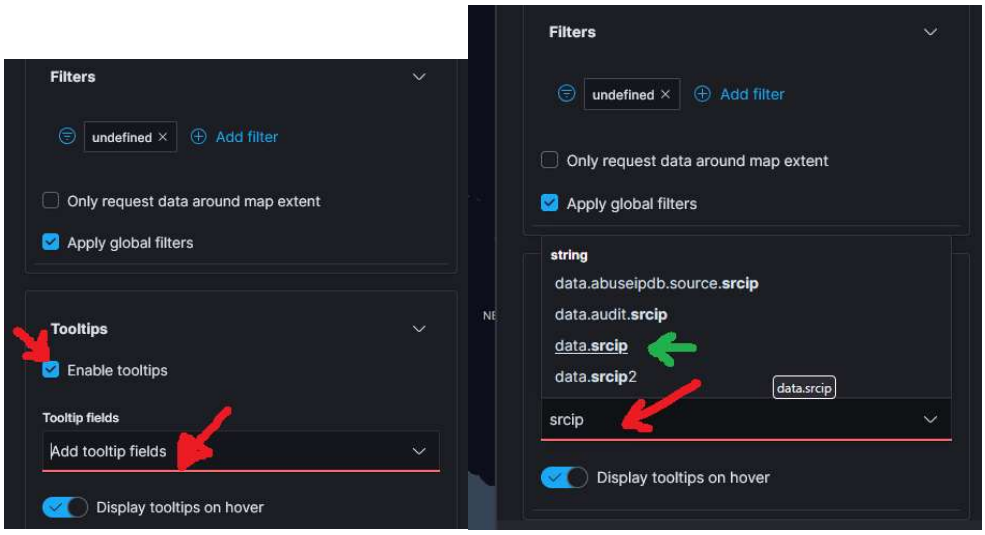
7. Kemudian lengkapi tambahan filter



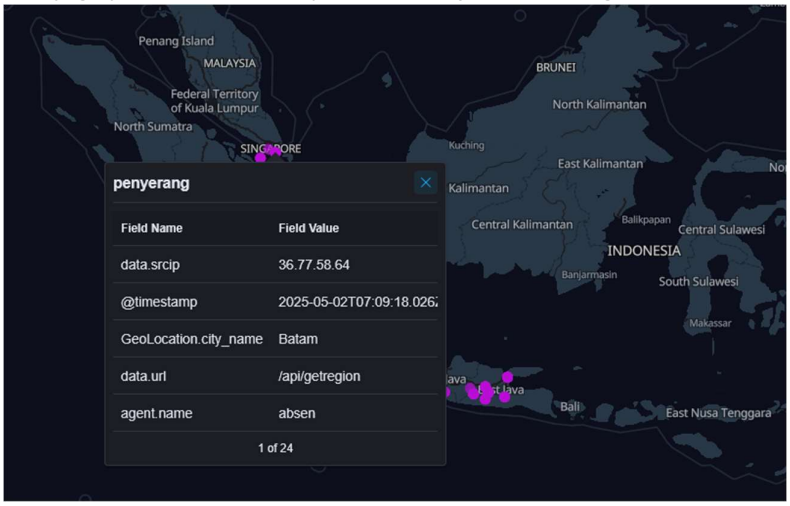
8. Masukkan “GeoLocation.city_name” sebagai filter dan operator “exists”



9. Tambahkan tooltips



Pilih tooltips -> ketik di menu drop-down "**srcip**" (panah merah)
Pilih "**data.srcip**" dari string yang muncul
Bisa juga pilihan lain misalnya: **timestamp, data.url, agent.name**, dan sebagainya



10. Simpan