Elmedin SULTANOVIC
Gabin BECU

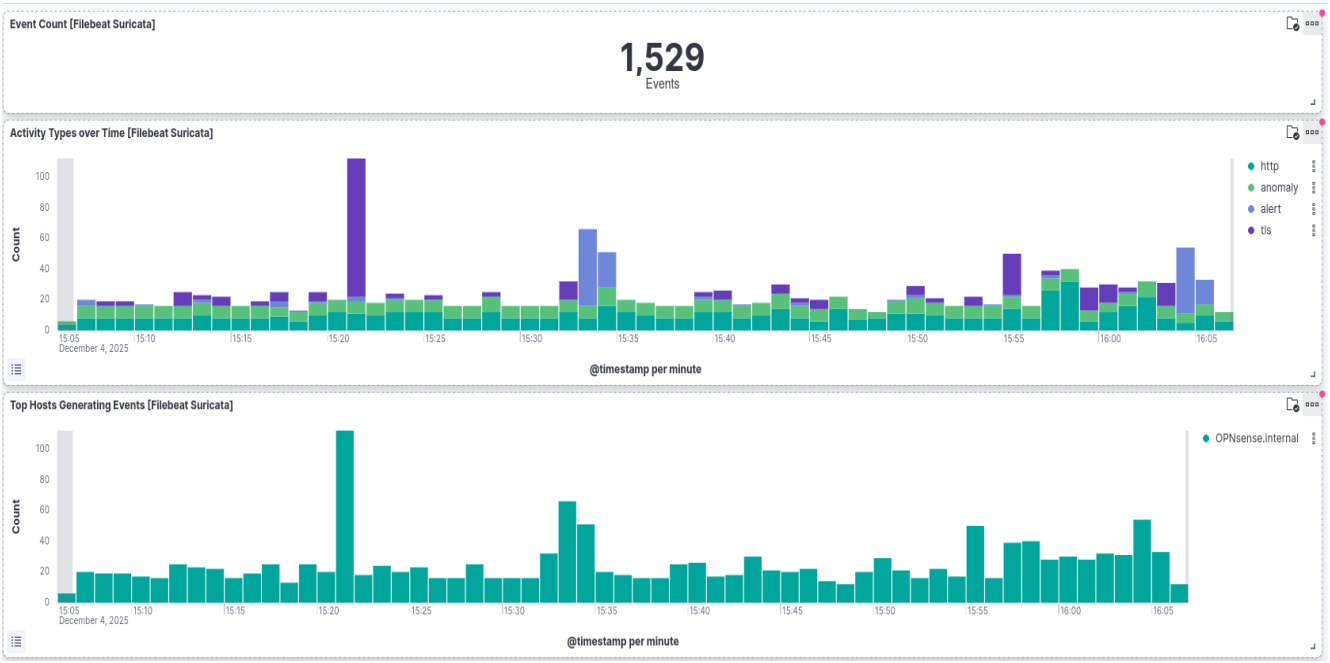
Dashboard Kibana

Nous avons choisi de faire un seul Dashboard mais qui rassemble toutes les informations utiles et nous avons suivi une logique de mettre les informations les plus simples et larges en haut, et plus on descend, plus les informations sont complexes et précises.

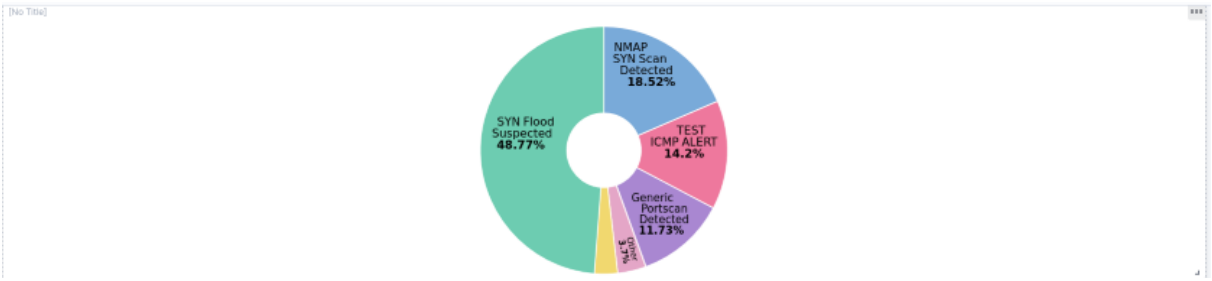
Dans ce premier panel, on a affiché le **nombre de logs reçus** sur la période sélectionnée (ici 15 minutes).

Puis 2 graphiques qui nous permettent de voir :

- Les protocoles utilisés en fonctions du temps.
- Les hosts qui génèrent le plus de logs.



Après, on a regroupé les panels en « donuts », le premier **étant le plus important**, qui montre les alertes les plus **détectées** et en fait des statistiques.



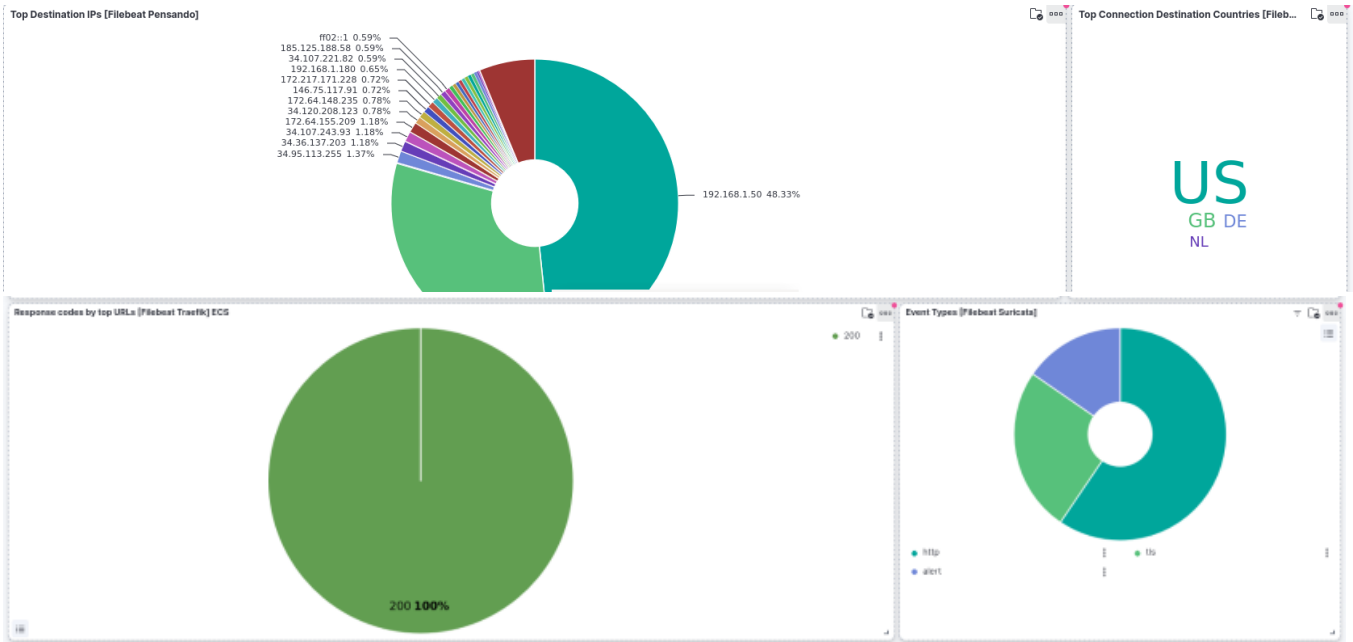
Ensuite, on a ajouté 4 panels qui permettent clairement de voir :

• les IP qui sont concernées par le plus de logs

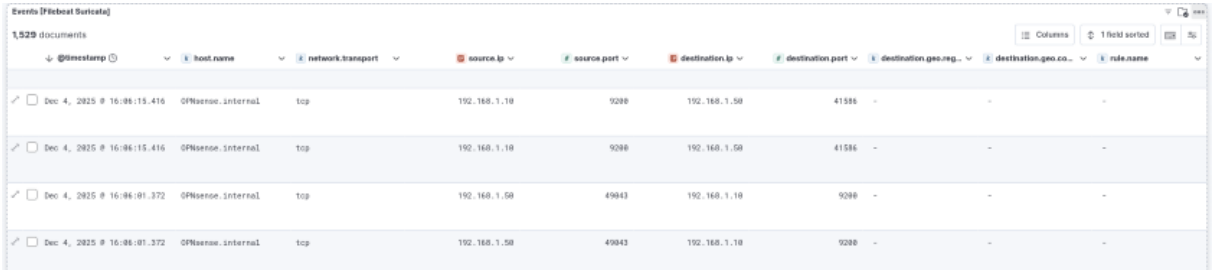
• les pays les plus concernés.

• les codes de status http afin de detecter si des erreurs arrivent

• les protocols les plus utilisés.



Enfin, on a ajouté un panneau de logs avec des filtres pré-paramétrés afin de pouvoir directement constater les logs problématiques repérés avec les panels précédents.



Ce dashboard offre une vision complète et efficace de l'activité des logs. Il permet à la fois :

- une surveillance en temps réel,
- une détection rapide des anomalies,
- et une analyse approfondie des événements critiques.