Project TVM V2 Dashboard

Comment y accéder ?

Sur le SharePoint Teams : « **GLOBAL- Cyber Security & Service Delivery-Tower**”, dans les documents suivre le chemin :
01. Projects → 03 - INFRA TVM_V2 → 03_CrowdStrike Scan → 03_DASHBOARD → Télécharger le fichier

Une fois qu’il sera mis en ligne sur app Powerbi lié à L'Oréal vous pourrez y accéder dans la rubrique espace de travail de la personne qui la mettra en ligne.

Guide d’utilisation

Plusieurs feuilles sont disponible dans ce dashboard :

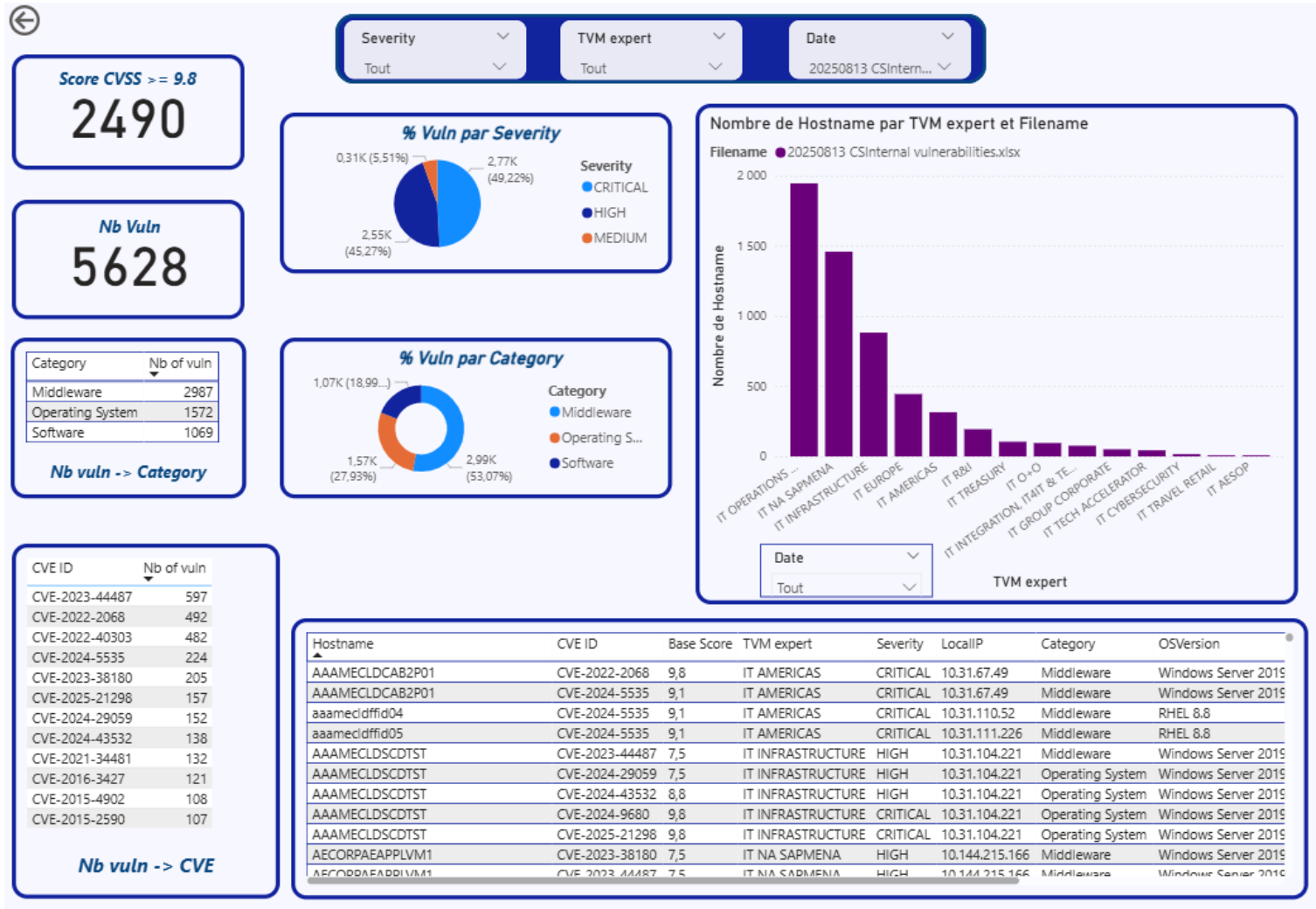
Une feuille ou vous allez retrouver toutes les vulnérabilités de toute les zones

Une feuille ou vous allez retrouver toutes les vulnérabilités liées à la zone INFRASTRUCTURE

Une feuille ou vous allez retrouver tout les operating system liés a toutes les zones avec et leurs managements

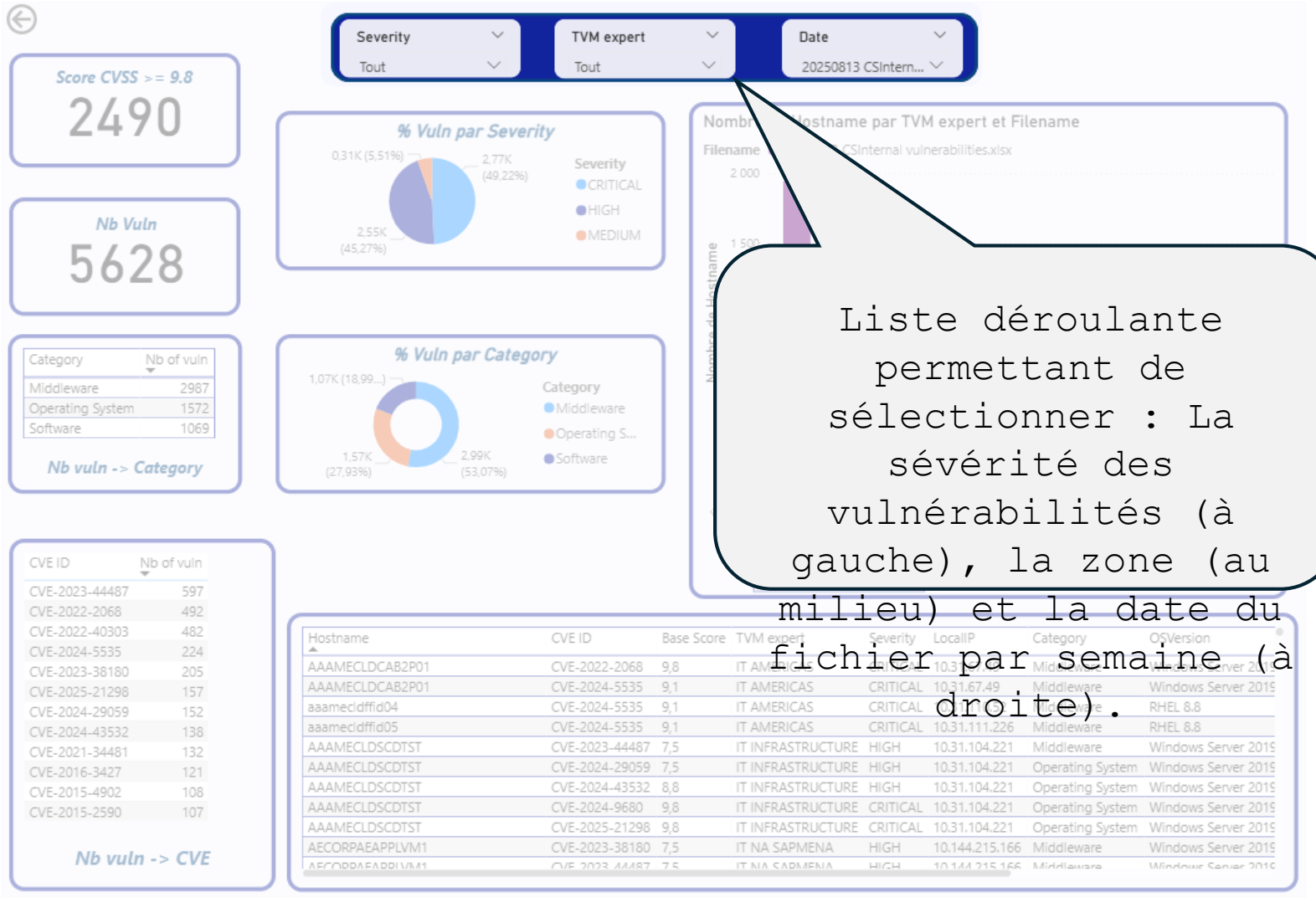
Une feuille ou vous allez retrouver toutes les APP liées a toutes les zones et leurs managements

Première feuille : ALL VULN



ALL VULN

En ce qui concerne la date quand vous ne sélectionné aucune date, le résultat de tous les fichiers se présentera donc doublon à prévoir.

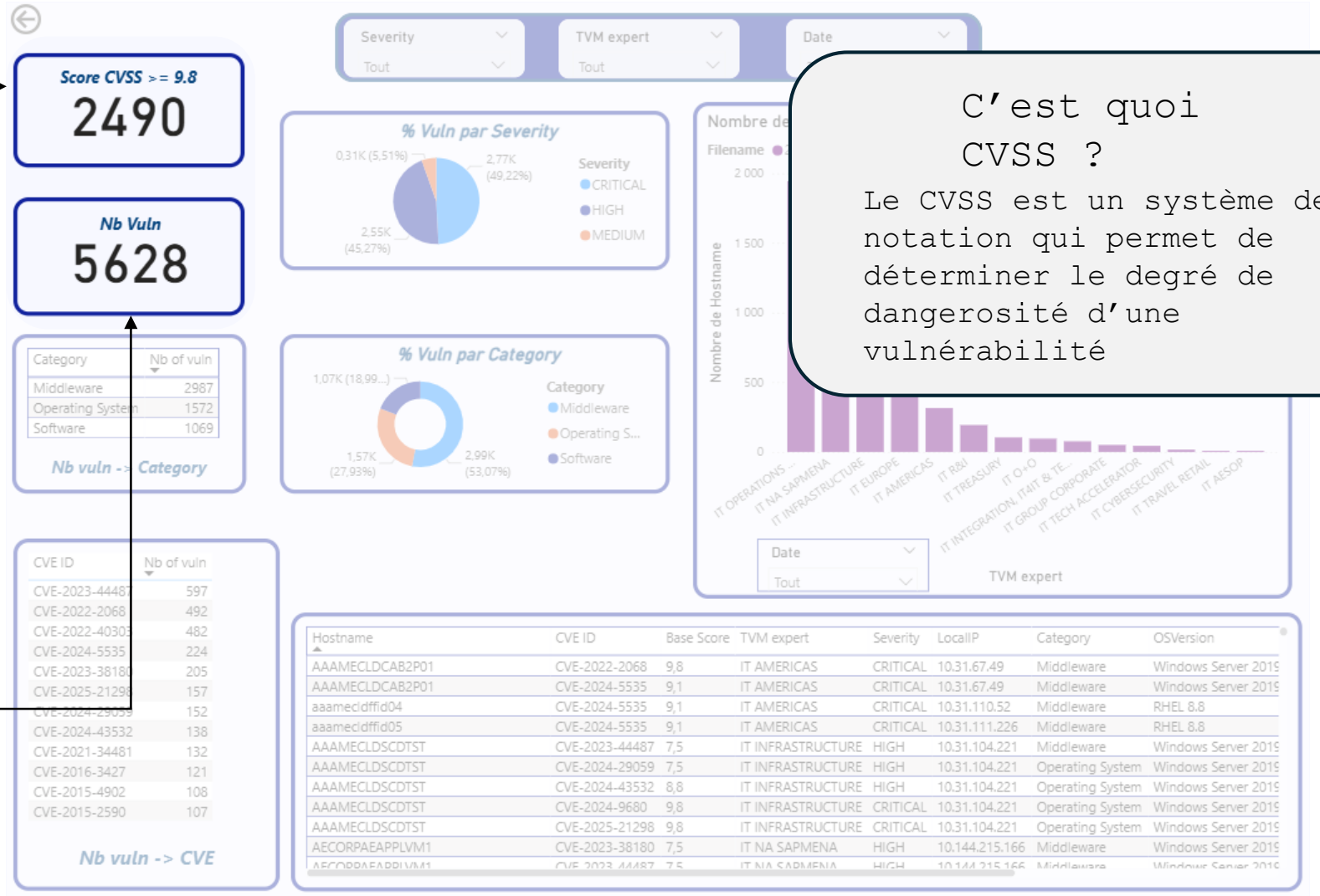


ALL VULN

Score CVSS >= 9,8

Permet de visualiser les vulnérabilités avec les scores CVSS les plus critiques donc les vulnérabilités le plus dangereuse

Nombre de vulnérabilité au total



C'est quoi CVSS ?

Le CVSS est un système de notation qui permet de déterminer le degré de dangerosité d'une vulnérabilité

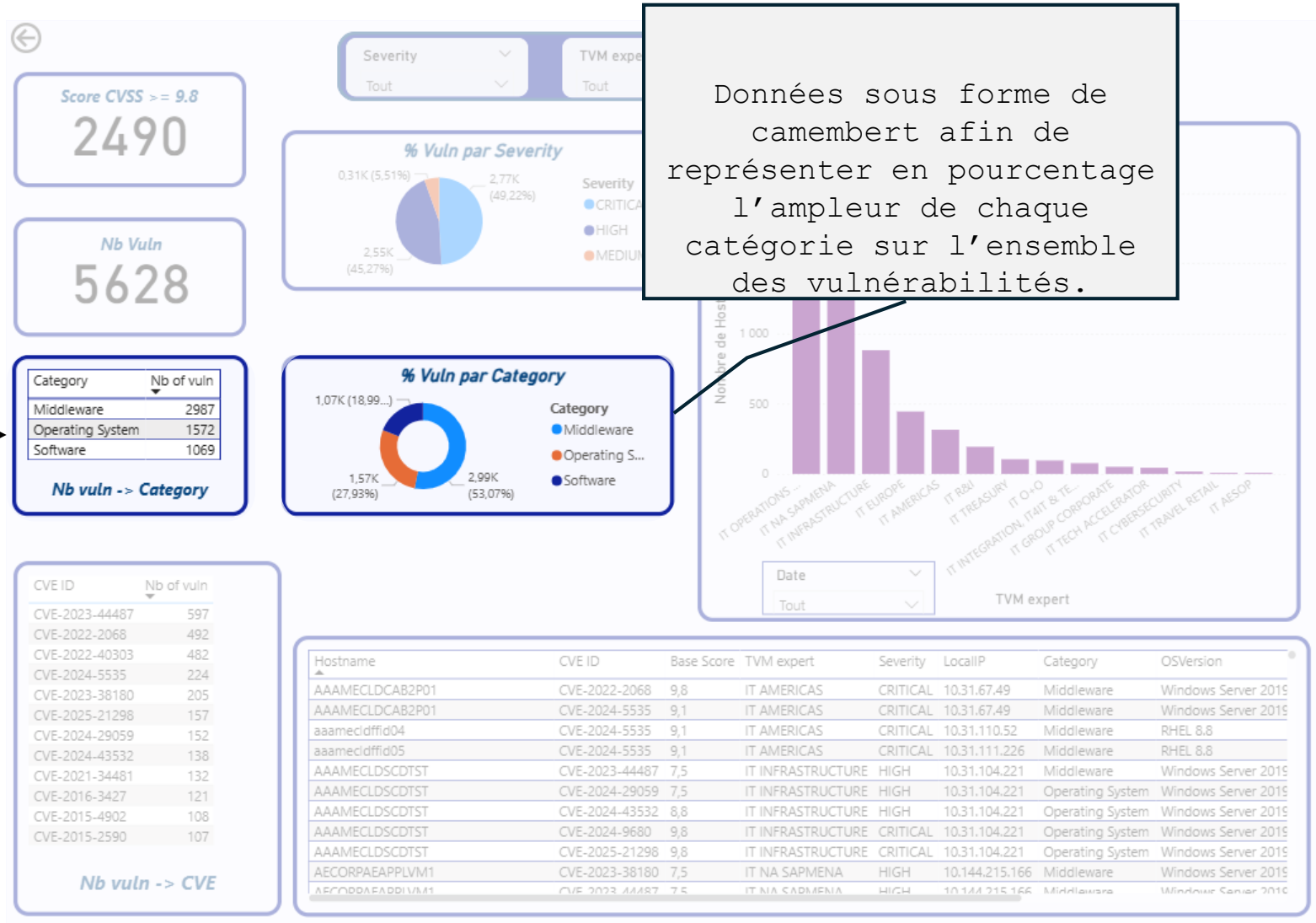
ALL VULN

Dans ce cas, la moitié des vulnérabilités sont en état CRITIQUE

Données sous forme de camembert afin de représenter en pourcentage l'ampleur de chaque niveau de dangerosité sur l'ensemble des vulnérabilités.

ALL VULN

Visualisation du nombre de vulnérabilités par catégorie



Données sous forme de camembert afin de représenter en pourcentage l'ampleur de chaque catégorie sur l'ensemble des vulnérabilités.

Nous avons ici 3 sortes de catégories :

- Operating System
- Middleware
- Software

Qui entre dans 2 grandes cases :

- OS = Operating System
- APP = Middleware et Software

ALL VULN

Histogramme groupé représentant le nombre de vulnérabilité par zone selon le fichier choisi

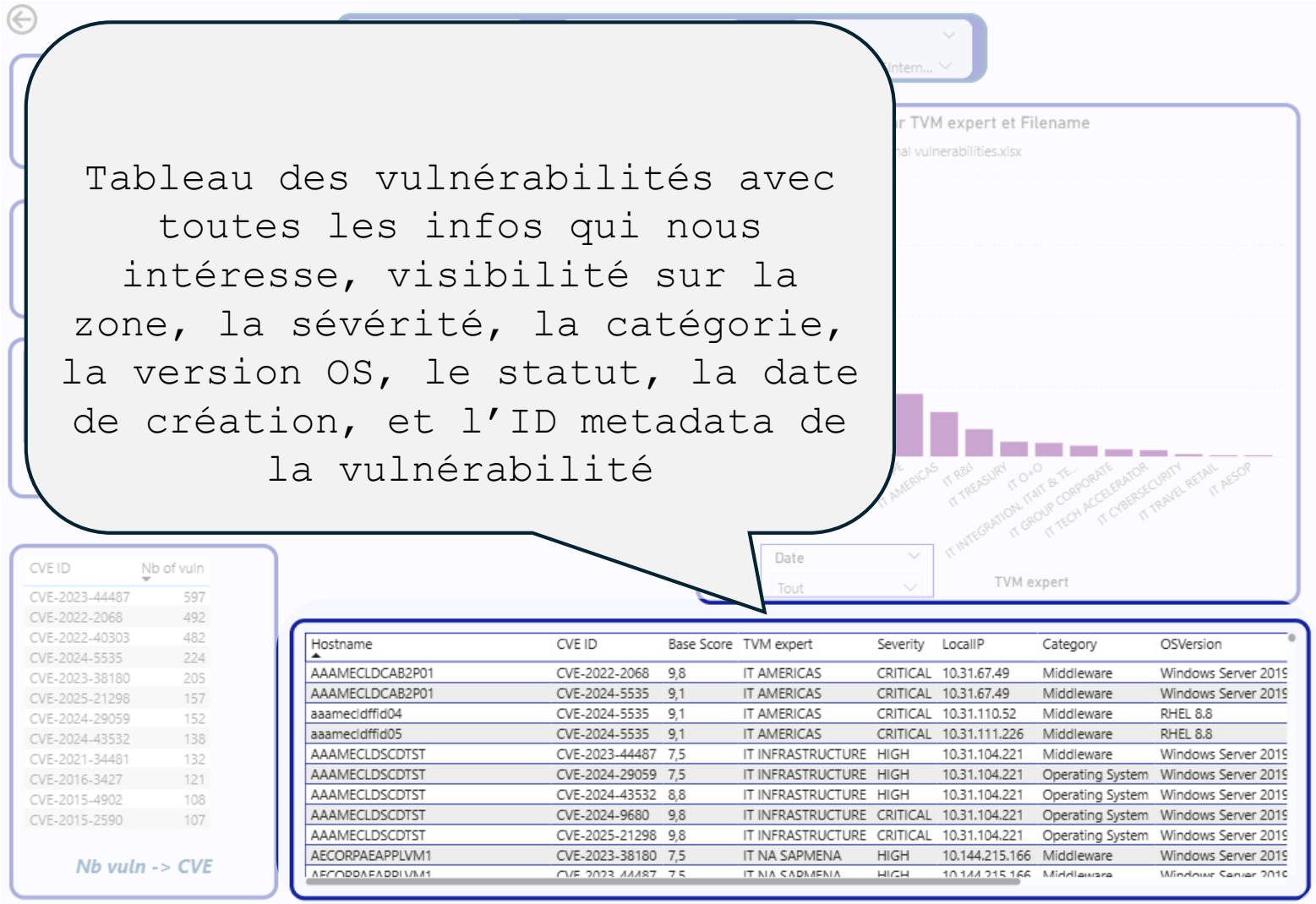
Liste des CVE qui comporte plus de 100 vulnérabilités

A noter qu'il est possible de comparer dans l'histogramme groupé, les différents fichiers en faisant CTRL dans le choix des dates

ALL VULN

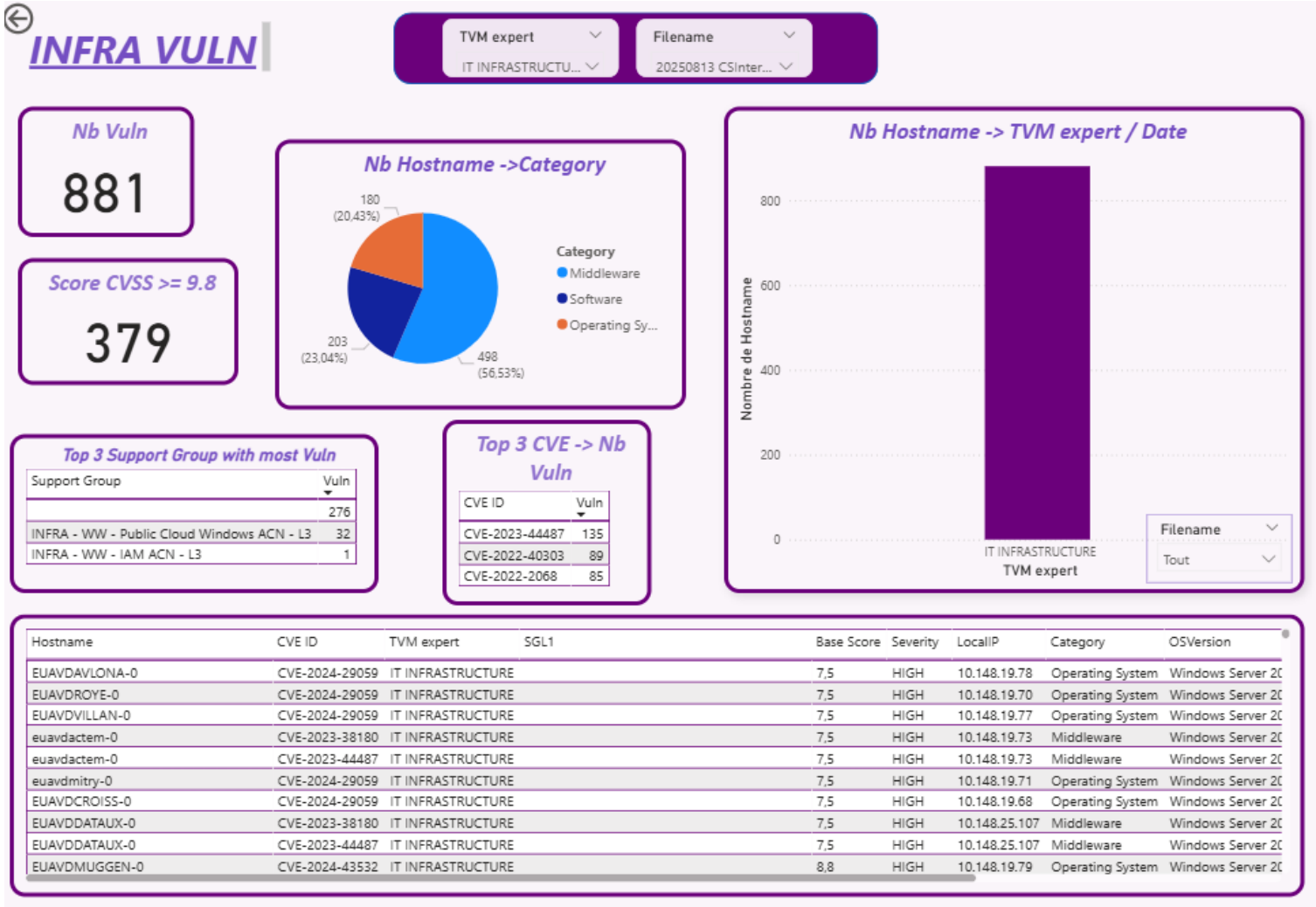
Le tableau s'actualise à chaque item qu'on touche dans le Dashboard pour cibler nos recherches

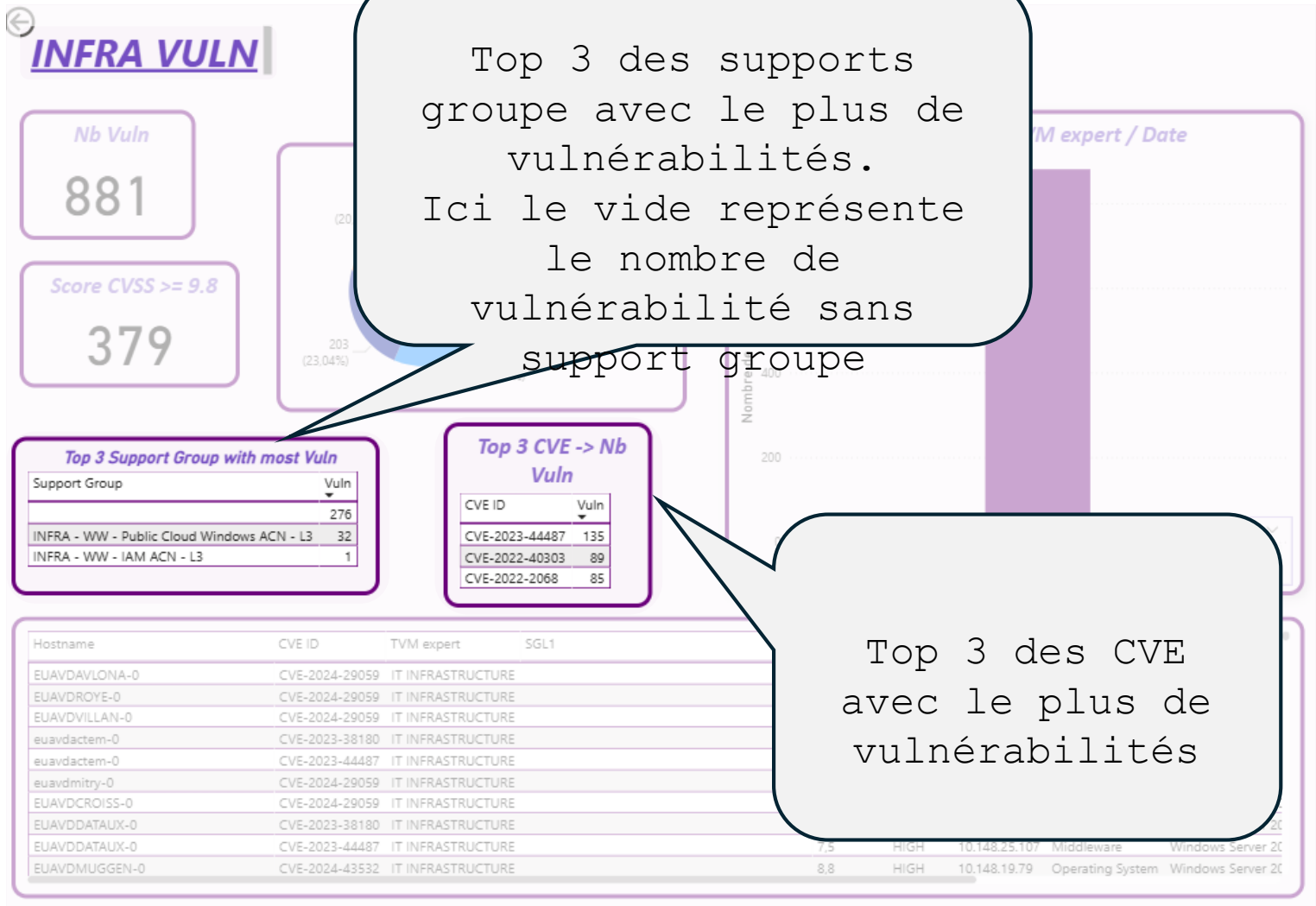
Tableau des vulnérabilités avec toutes les infos qui nous intéresse, visibilité sur la zone, la sévérité, la catégorie, la version OS, le statut, la date de création, et l'ID metadata de la vulnérabilité



Hostname	CVE ID	Base Score	TVM expert	Severity	LocalIP	Category	OSVersion
AAAMECLDCAB2P01	CVE-2022-2068	9,8	IT AMERICAS	CRITICAL	10.31.67.49	Middleware	Windows Server 2019
AAAMECLDCAB2P01	CVE-2024-5535	9,1	IT AMERICAS	CRITICAL	10.31.67.49	Middleware	Windows Server 2019
aaamecldffid04	CVE-2024-5535	9,1	IT AMERICAS	CRITICAL	10.31.110.52	Middleware	RHEL 8.8
aaamecldffid05	CVE-2024-5535	9,1	IT AMERICAS	CRITICAL	10.31.111.226	Middleware	RHEL 8.8
AAAMECLDSCDTST	CVE-2023-44487	7,5	IT INFRASTRUCTURE	HIGH	10.31.104.221	Middleware	Windows Server 2019
AAAMECLDSCDTST	CVE-2024-29059	7,5	IT INFRASTRUCTURE	HIGH	10.31.104.221	Operating System	Windows Server 2019
AAAMECLDSCDTST	CVE-2024-43532	8,8	IT INFRASTRUCTURE	HIGH	10.31.104.221	Operating System	Windows Server 2019
AAAMECLDSCDTST	CVE-2024-9680	9,8	IT INFRASTRUCTURE	CRITICAL	10.31.104.221	Operating System	Windows Server 2019
AAAMECLDSCDTST	CVE-2025-21298	9,8	IT INFRASTRUCTURE	CRITICAL	10.31.104.221	Operating System	Windows Server 2019
AECORPAEAPPLVM1	CVE-2023-38180	7,5	IT NA SAPMENA	HIGH	10.144.215.166	Middleware	Windows Server 2019

Deuxieme feuille : INFRA VULN



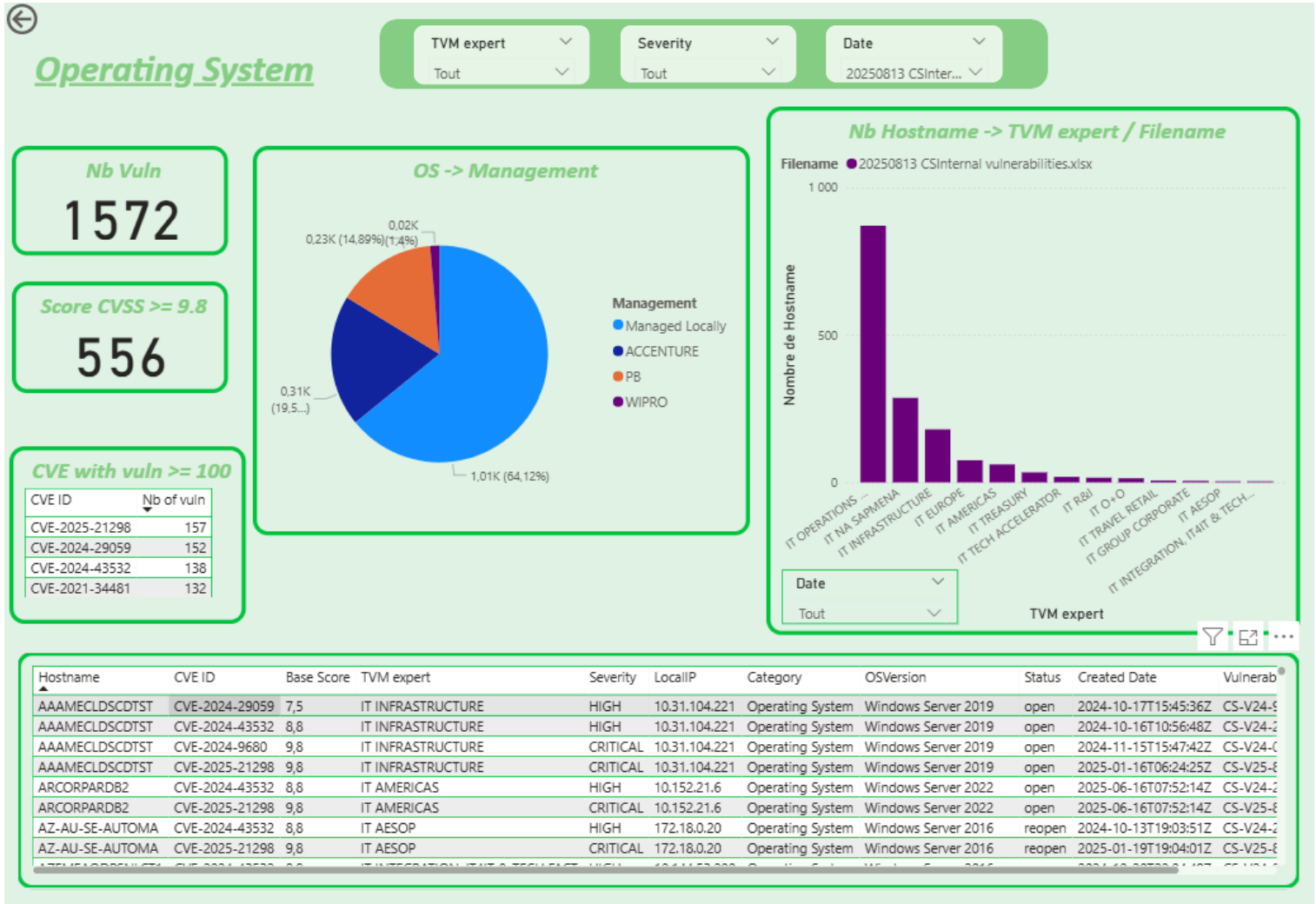


Top 3 des supports groupe avec le plus de vulnérabilités.
Ici le vide représente le nombre de vulnérabilité sans support groupe

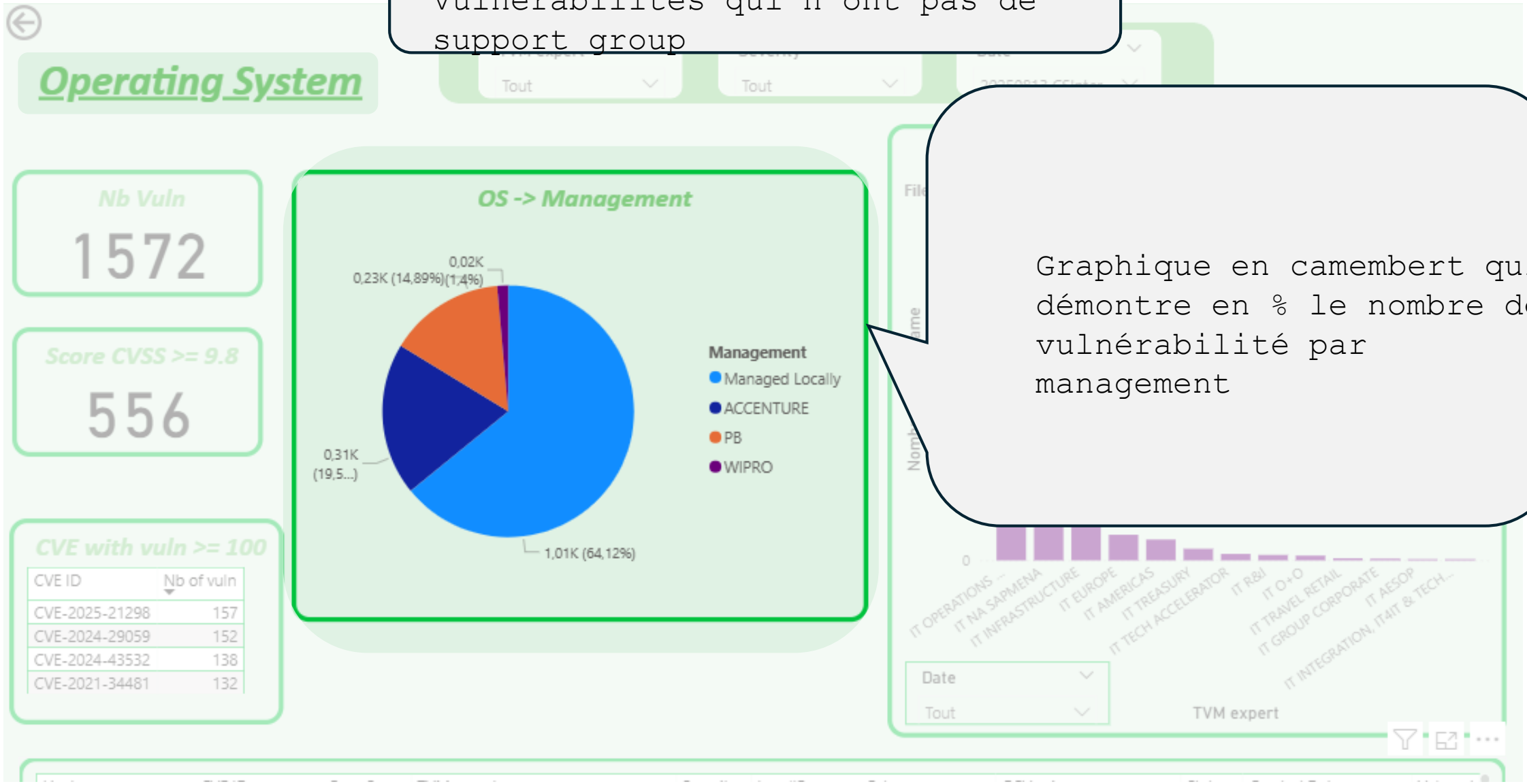
Top 3 des CVE avec le plus de vulnérabilités

Le reste des graphiques est semblables à la 1ère feuille

Troisième feuille : Operating System

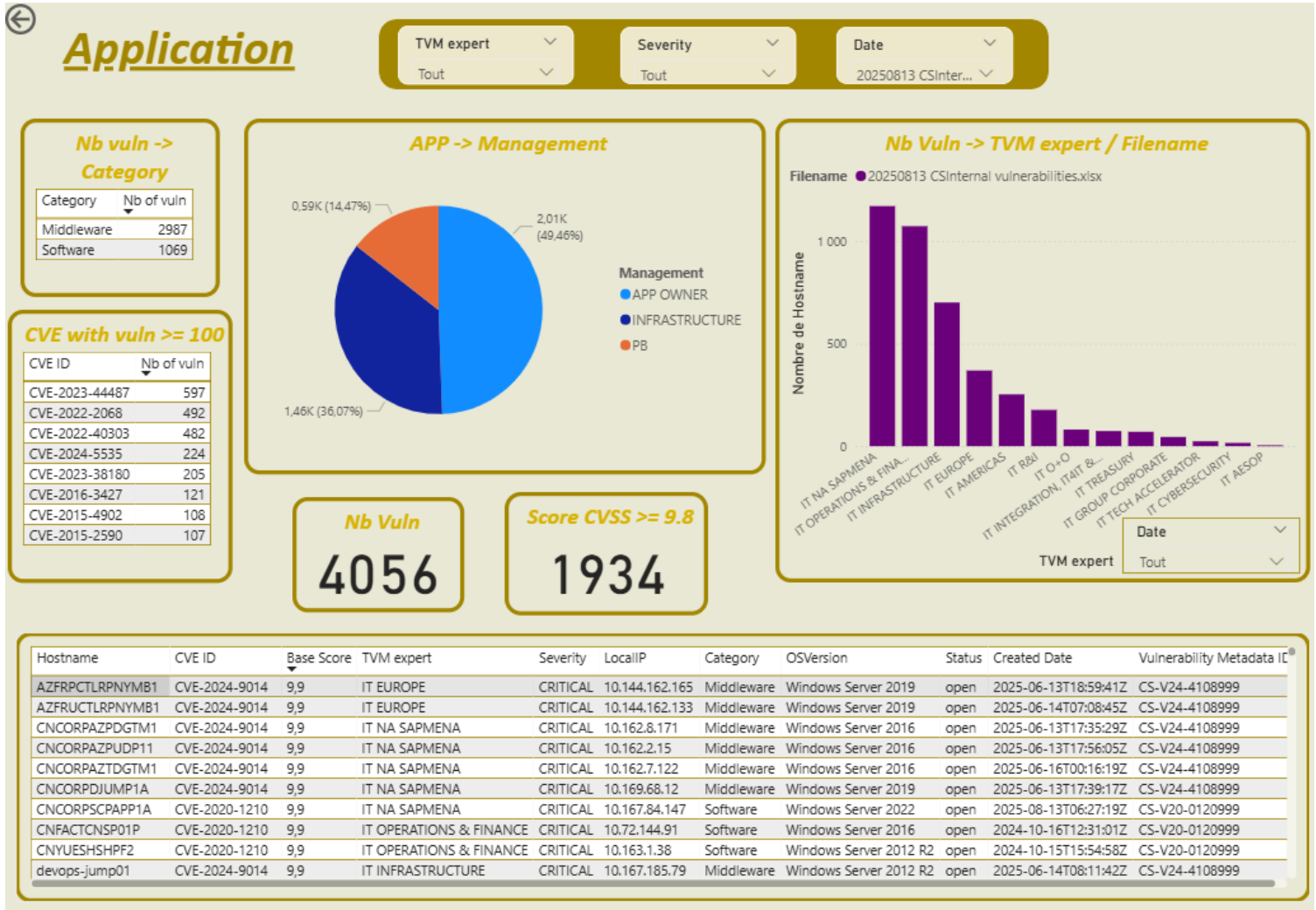


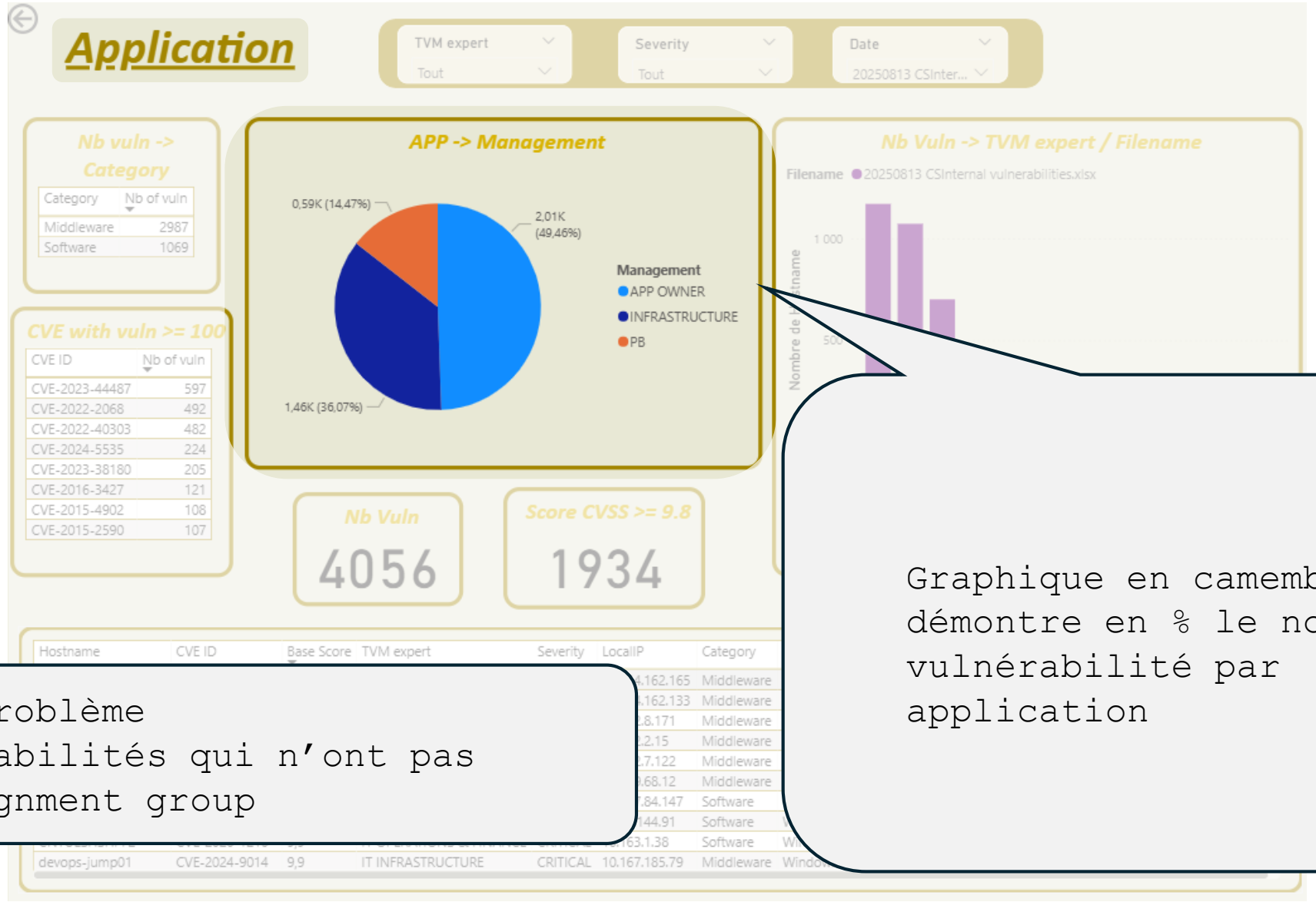
PB = Problème
Vulnérabilités qui n'ont pas de support group



Graphique en camembert qui démontre en % le nombre de vulnérabilité par management

Quatrième feuille : Application

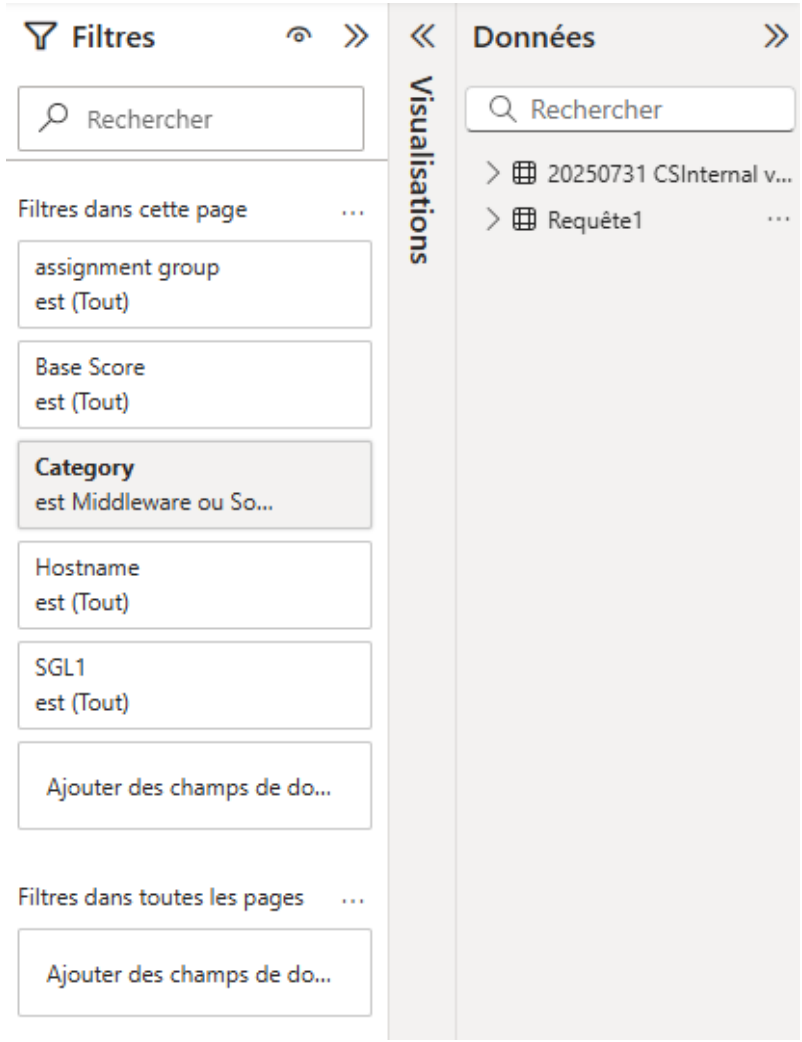




PB = Problème
Vulnérabilités qui n'ont pas d'assignment group

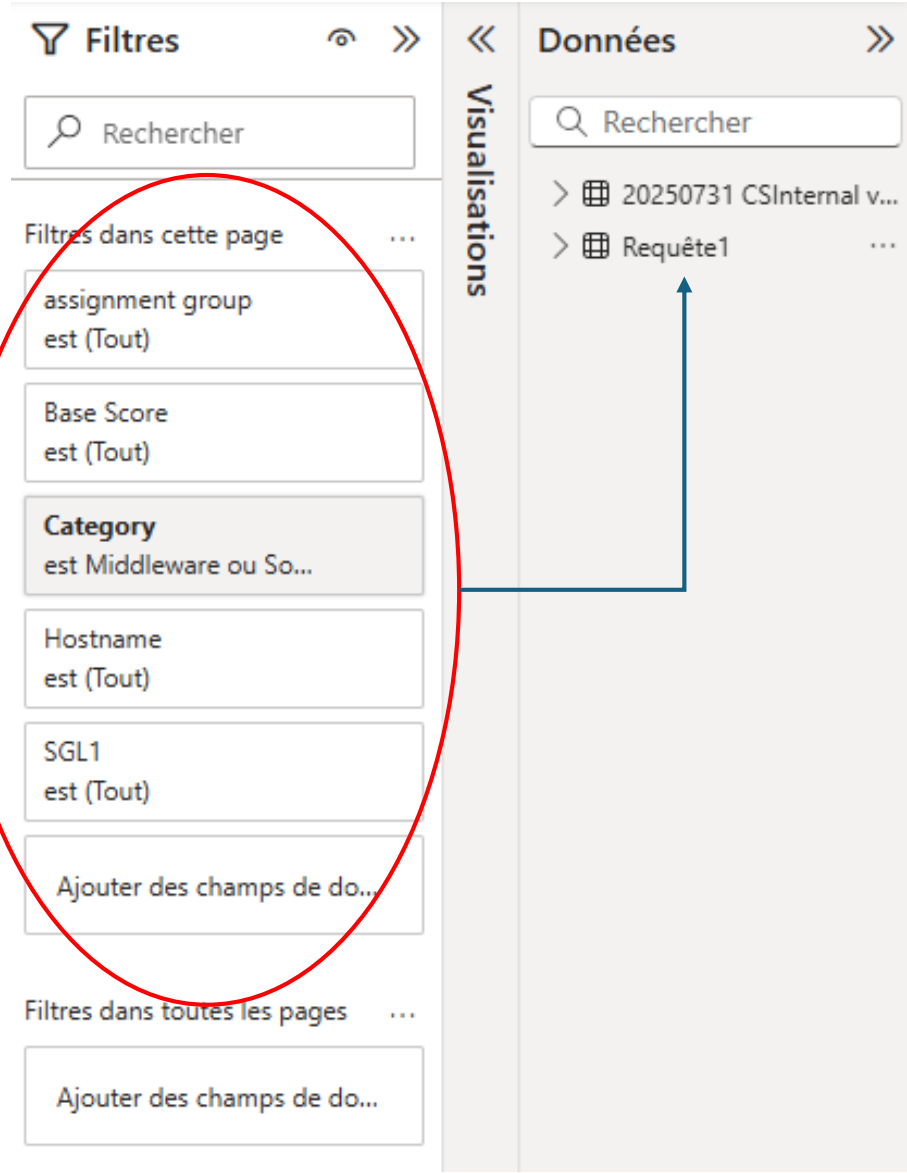
Graphique en camembert qui démontre en % le nombre de vulnérabilité par application

Filtres et données



Dans toutes les feuilles, les filtres proposés sont les suivants.

Possibilité de rajouté des filtres dans la colonne « Données » en utilisant les données de la liste « Requête1 »



Base Score = Score CVSS
Hostname = Nom de la vulnérabilité
SLG1 = Support Group