

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

A light orange rounded rectangle containing text. A light orange arrow points downwards from its bottom center to the top of the next box.

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

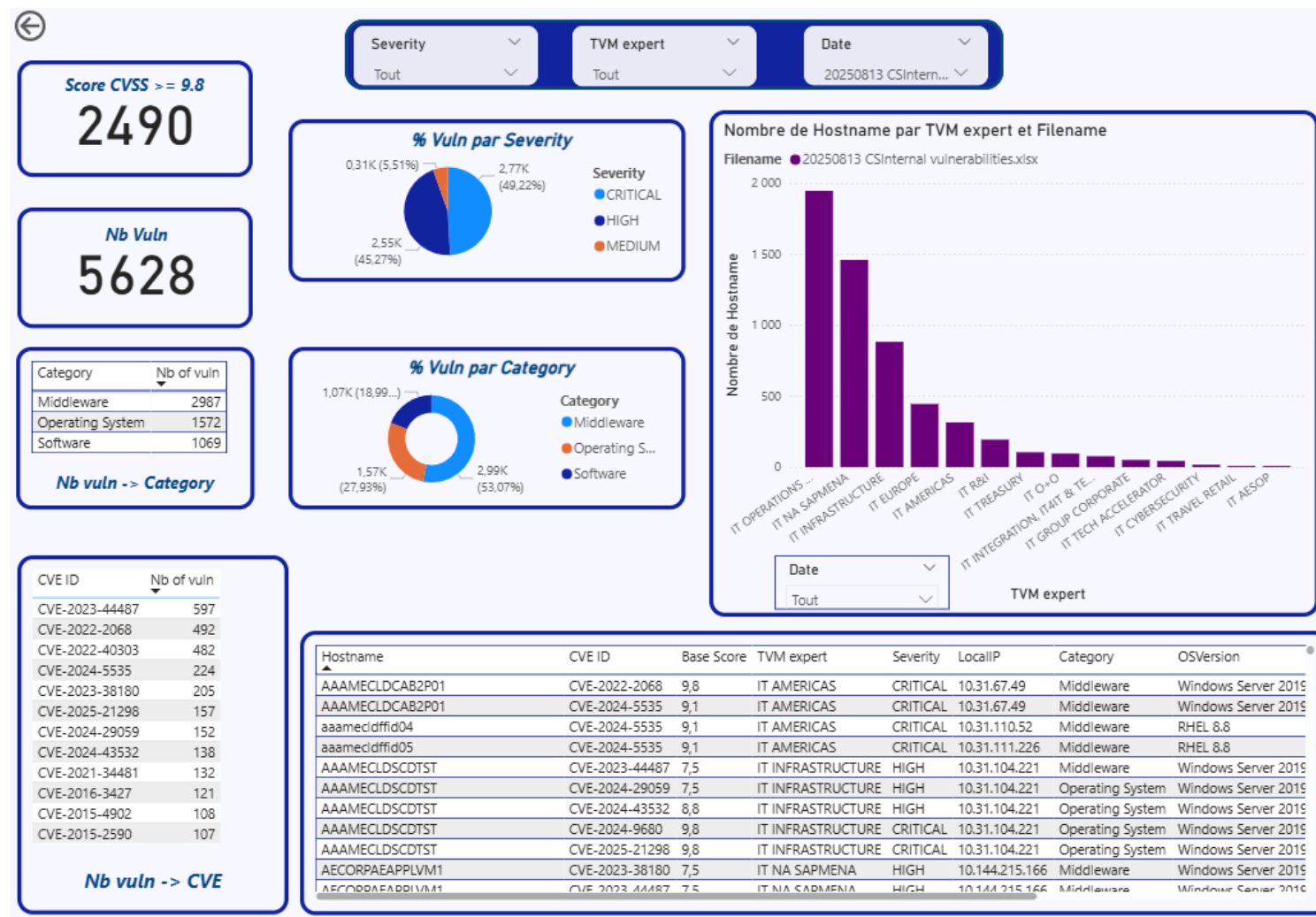
A dark green rounded rectangle containing text. A light green arrow points downwards from its bottom center to the top of the next box.

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

A blue rounded rectangle containing text. A light blue arrow points downwards from its bottom center to the top of the next box.

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

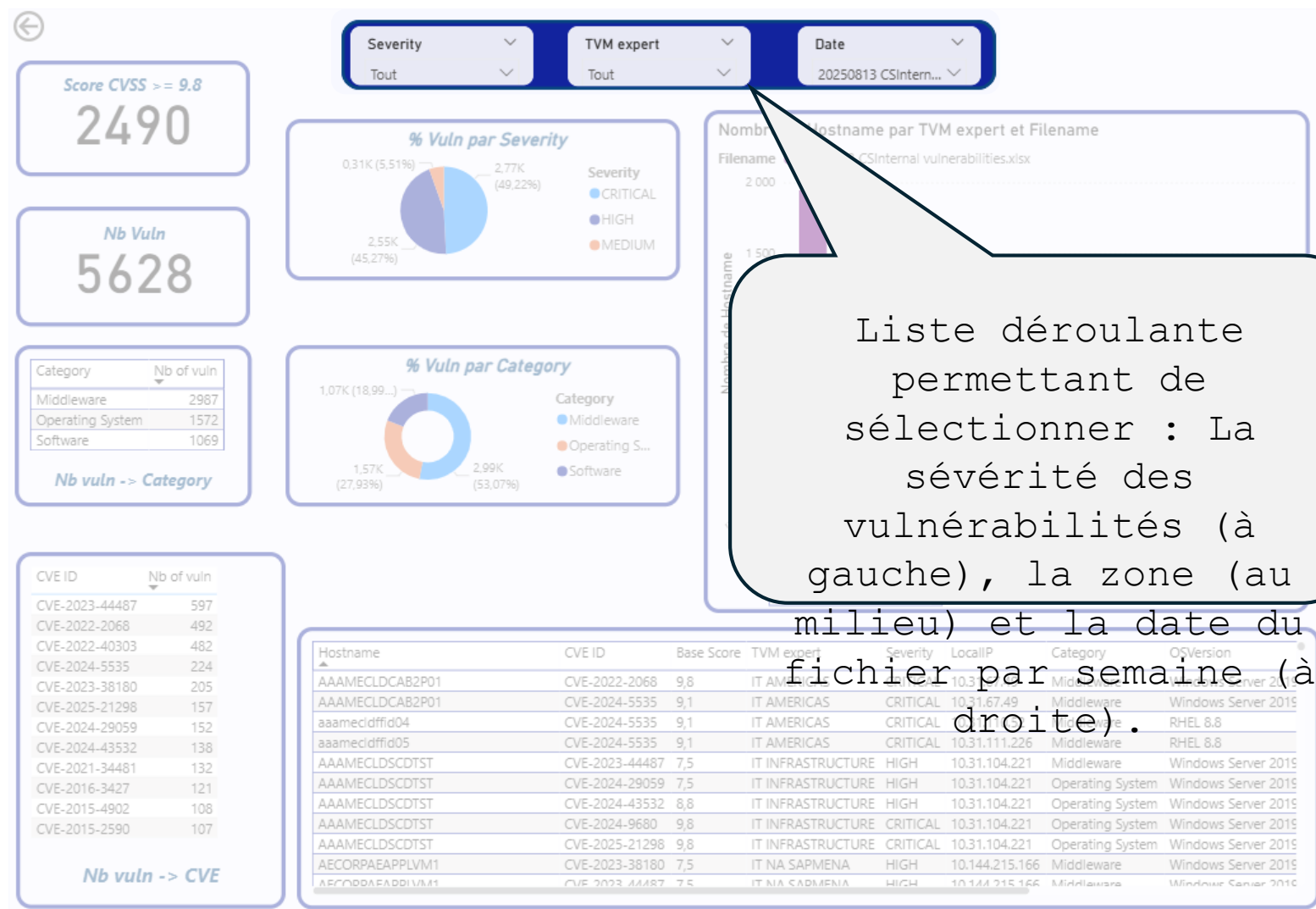
Première feuille : ALL VULN



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.

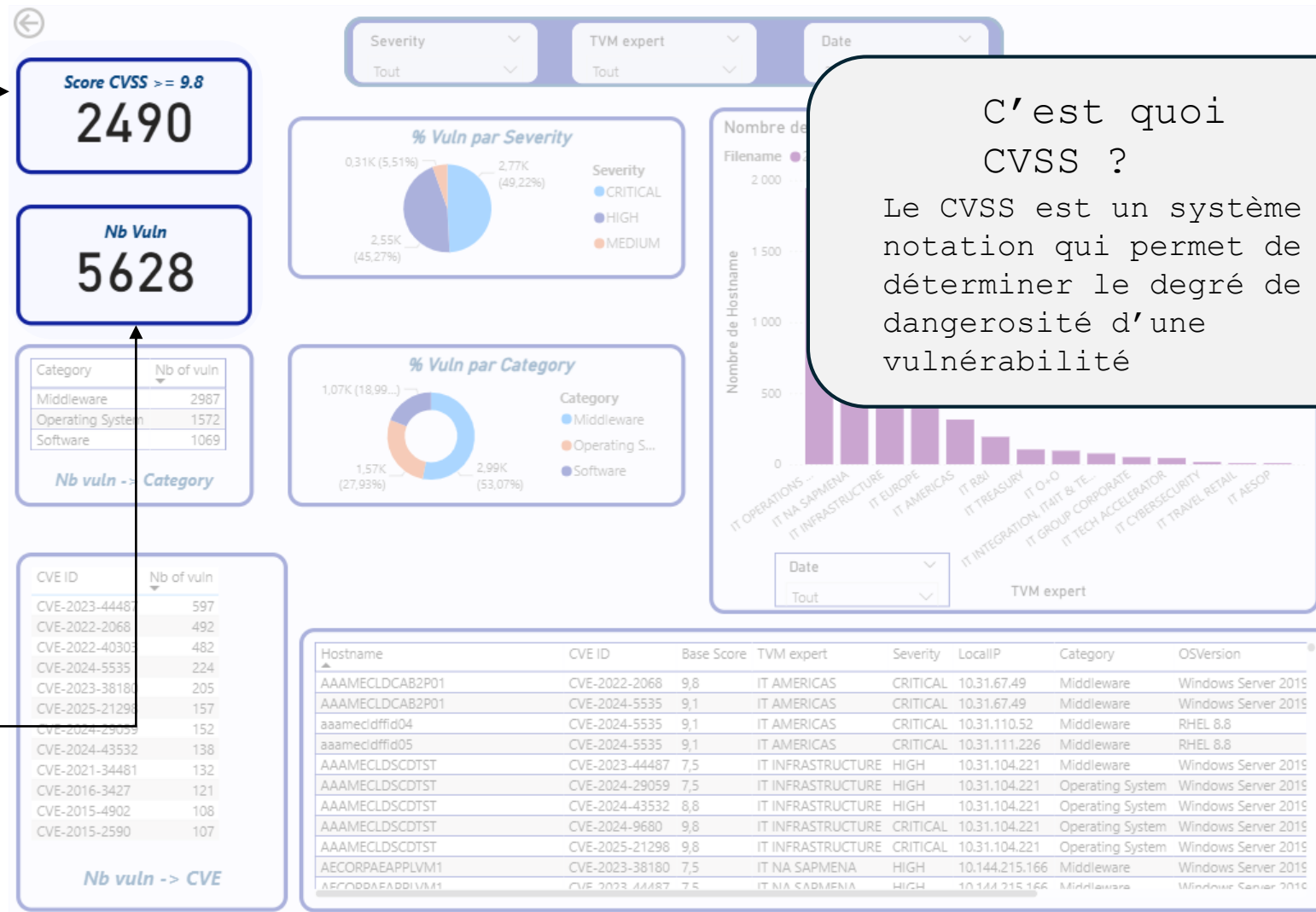


ALL VULN

Score CVSS $\geq 9,8$

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

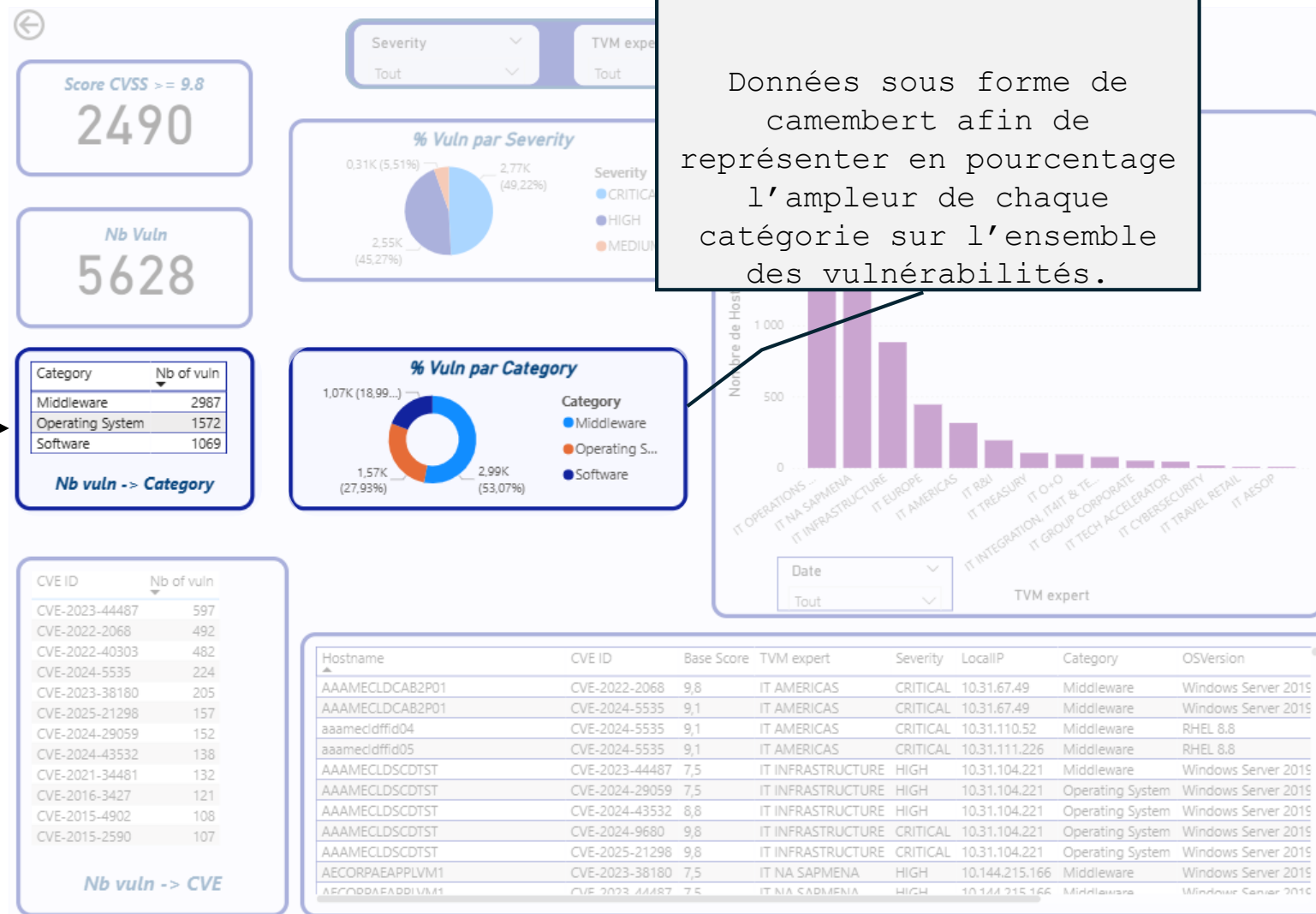


Dans ce cas, la
moitié des
vulnérabilités
sont en état
CRITIQUE



ALL VULN

Visualisation du nombre de vulnérabilités par catégorie



Nous avons ici 3 sortes de catégories :

- ❖ Operating System
- ❖ Middleware
- ❖ Software

Qui entre dans 2 grandes cases :

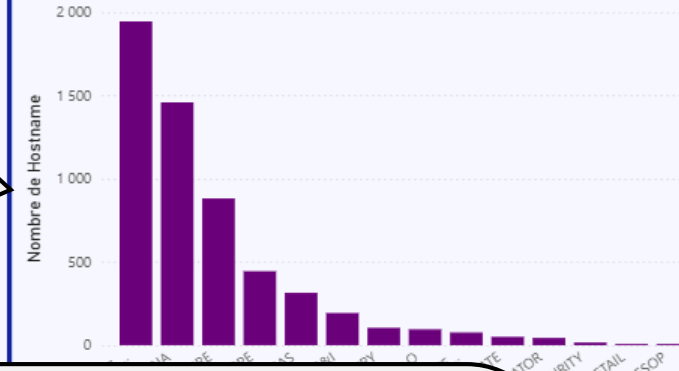
- OS = Operating System
- APP = Middleware et Software

ALL VULN

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

Nombre de Hostname par TVM expert et Filename

Filename ● 20250813 CSInternal vulnerabilities.xlsx



Nb vuln -> Category

CVE ID	Nb of vuln
CVE-2023-44487	597
CVE-2022-2068	492
CVE-2022-40303	482
CVE-2024-5535	224
CVE-2023-38180	205
CVE-2025-21298	157
CVE-2024-29059	152
CVE-2024-43532	138
CVE-2021-34481	132
CVE-2016-3427	121
CVE-2015-4902	108
CVE-2015-2590	107

Nb vuln -> CVE

Liste des CVE qui
comporte plus de 100
vulnérabilités



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

ALL VULN



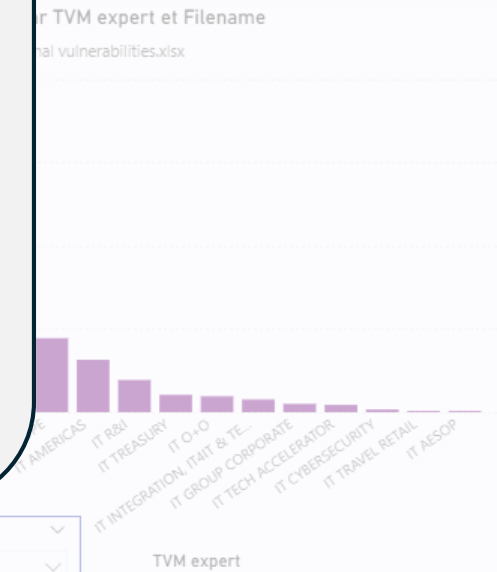
Le tableau s'actualise à chaque item qu'on touche dans le Dashboard pour cibler nos recherches

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

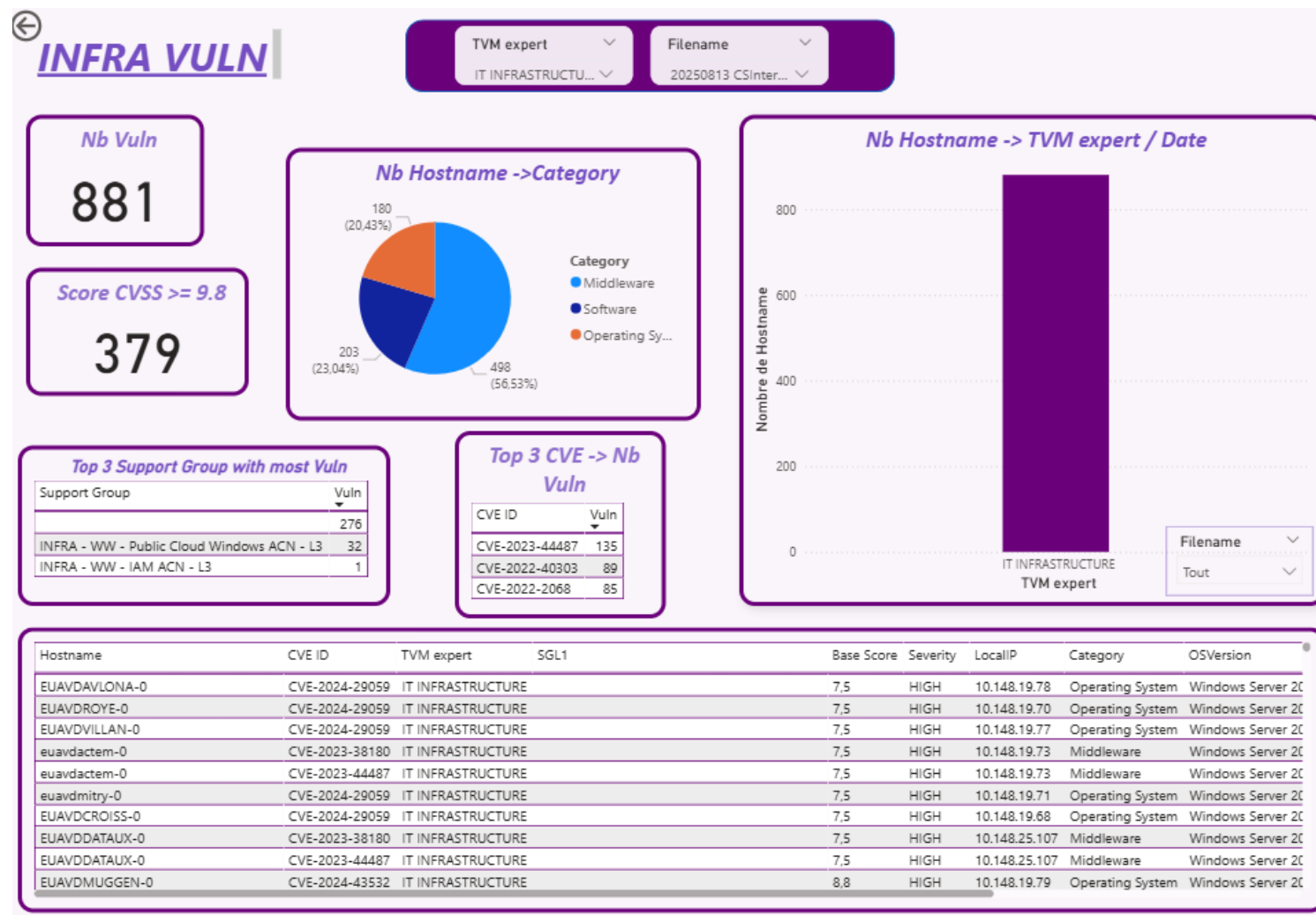
CVE ID	Nb of vuln
CVE-2023-44487	597
CVE-2022-2068	492
CVE-2022-40303	482
CVE-2024-5535	224
CVE-2023-38180	205
CVE-2025-21298	157
CVE-2024-29059	152
CVE-2024-43532	138
CVE-2021-34481	132
CVE-2016-3427	121
CVE-2015-4902	108
CVE-2015-2590	107

Nb vuln -> CVE

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
aaamecidffid04	CVE-2024-5535	9,1	IT AMERICAS	CRITICAL	10.31.110.52	Middleware	RHEL 8.8
aaamecidffid05	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
AECORPAEAPPLVM1	CVE-2023-44487	7,5	IT NA SAPMENA	HIGH	10.144.215.166	Middleware	Windows Server 2019



Deuxieme feuille : INFRA VULN





INFRA VULN

Nb Vuln

881

Score CVSS >= 9.8

379

Top 3 Support Group with most Vuln

Support Group	Vuln
	276
INFRA - WW - Public Cloud Windows ACN - L3	32
INFRA - WW - IAM ACN - L3	1

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

Top 3 CVE -> Nb Vuln

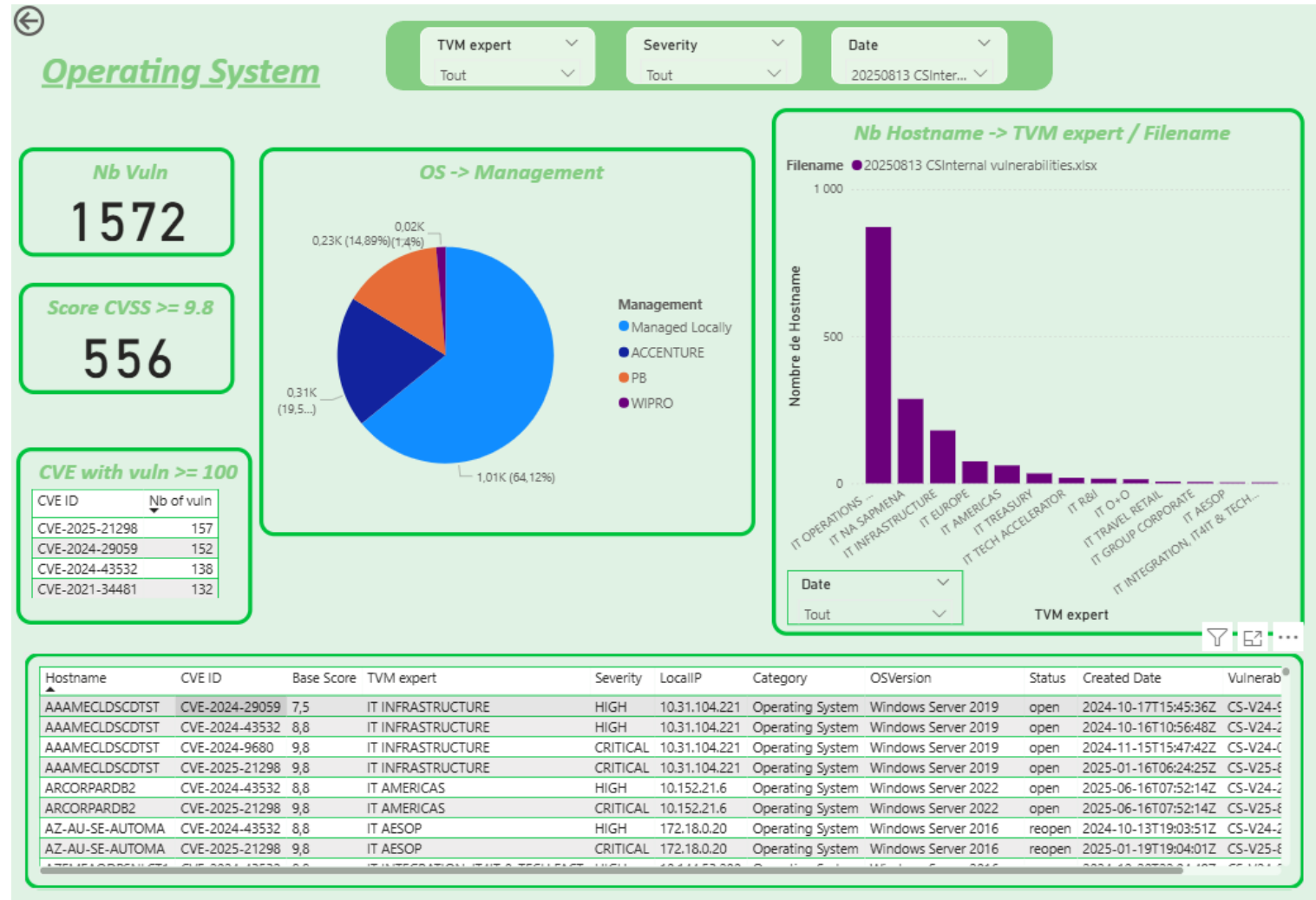
CVE ID	Vuln
CVE-2023-44487	135
CVE-2022-40303	89
CVE-2022-2068	85

Top 3 des CVE avec le plus de vulnérabilités

Hostname	CVE ID	TVM expert	SGL1
EUAVIDAVLONA-0	CVE-2024-29059	IT INFRASTRUCTURE	
EUAVIDROYE-0	CVE-2024-29059	IT INFRASTRUCTURE	
EUAVIDVILLAN-0	CVE-2024-29059	IT INFRASTRUCTURE	
euavdactem-0	CVE-2023-38180	IT INFRASTRUCTURE	
euavdactem-0	CVE-2023-44487	IT INFRASTRUCTURE	
euavdmity-0	CVE-2024-29059	IT INFRASTRUCTURE	
EUAVIDCROISS-0	CVE-2024-29059	IT INFRASTRUCTURE	
EUAVIDDATAUX-0	CVE-2023-38180	IT INFRASTRUCTURE	
EUAVIDDATAUX-0	CVE-2023-44487	IT INFRASTRUCTURE	
EUAVIDMUGGEN-0	CVE-2024-43532	IT INFRASTRUCTURE	

Le reste des graphiques est semblables à la 1ère feuille

Troisième feuille : Operating System



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

Operating System

Nb Vuln

1572

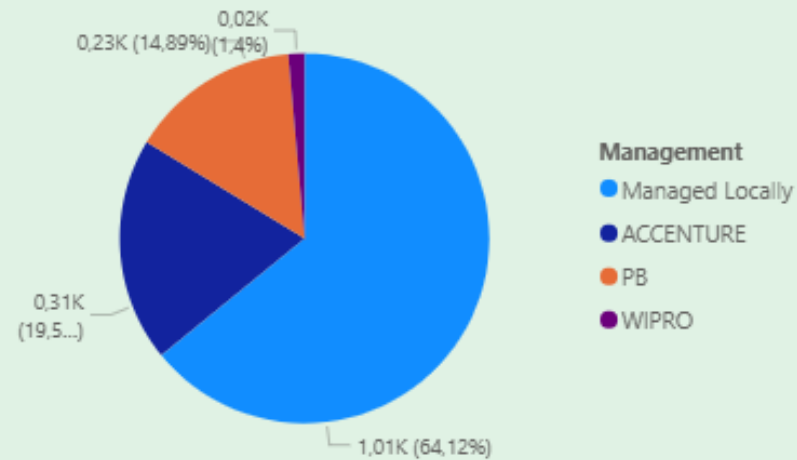
Score CVSS >= 9.8

556

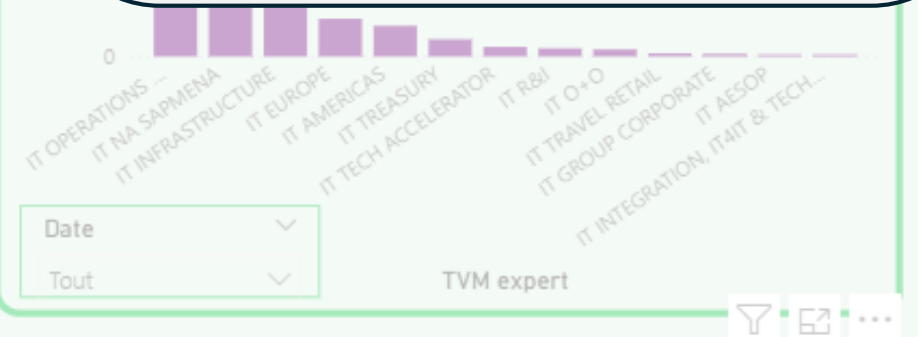
CVE with vuln >= 100

CVE ID	Nb of vuln
CVE-2025-21298	157
CVE-2024-29059	152
CVE-2024-43532	138
CVE-2021-34481	132

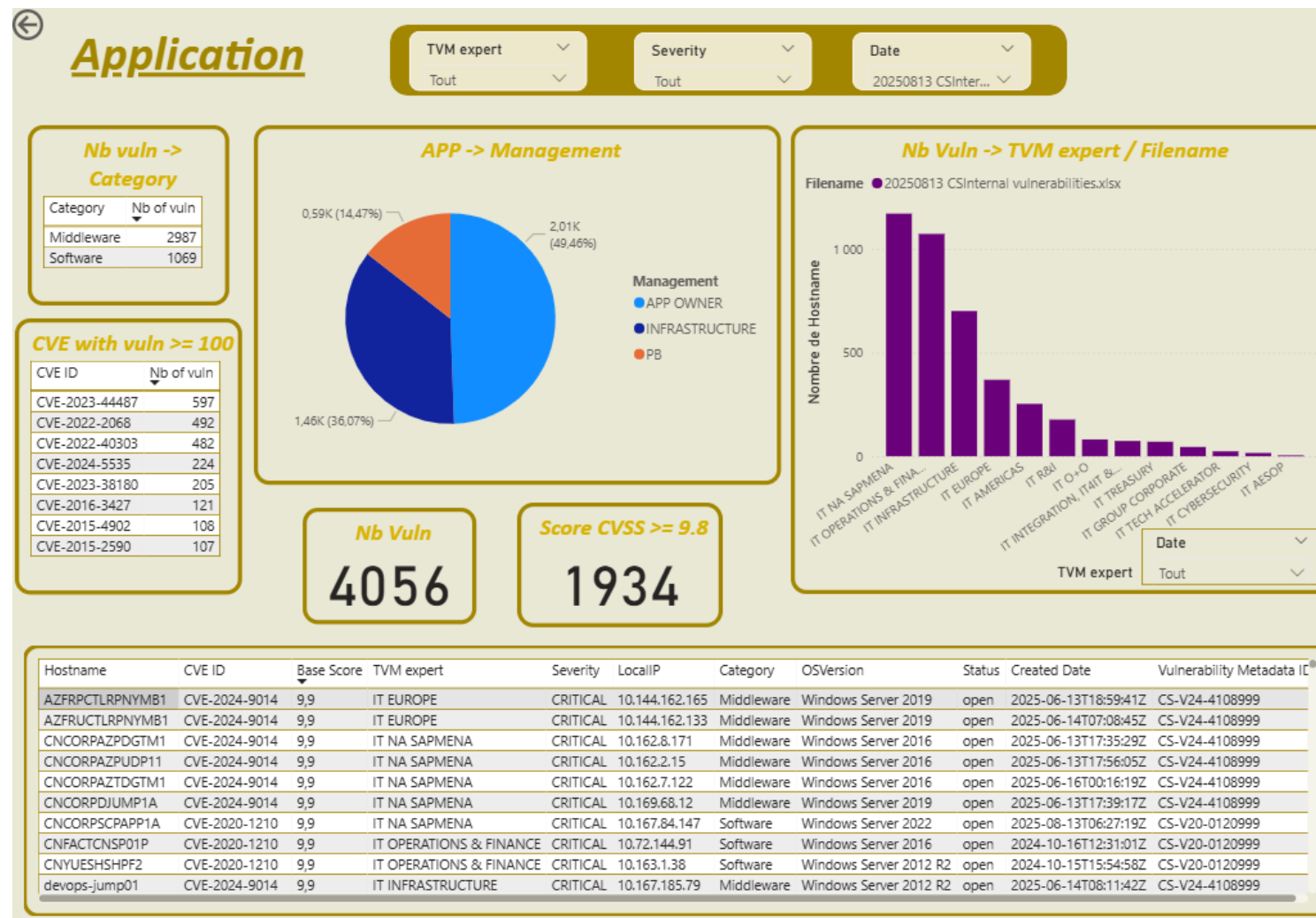
OS -> Management

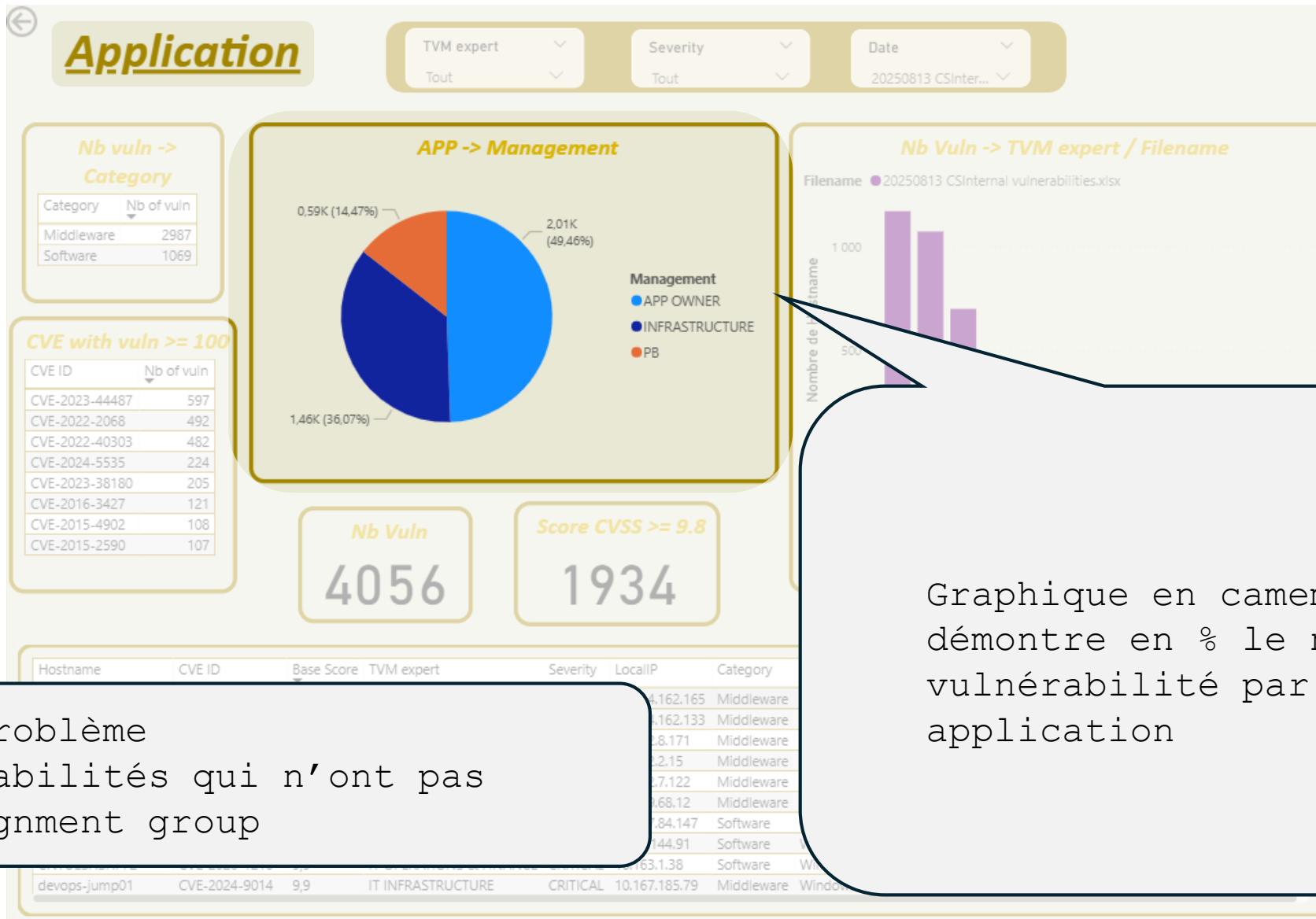


Graphique en camembert qui
démontre en % le nombre de
vulnérabilité par
management



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

Filtres

Rechercher

Filtres dans cette page

assignment group
est (Tout)

Base Score
est (Tout)

Category
est Middleware ou So...

Hostname
est (Tout)

SGL1
est (Tout)

Ajouter des champs de do...

Filtres dans toutes les pages

Ajouter des champs de do...

Visualisations

Données

Rechercher

> 20250731 CSInternal v...

> Requête1

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 »

The screenshot shows a data visualization interface with two main panels: 'Filtres' (Filters) on the left and 'Données' (Data) on the right. A central vertical bar labeled 'Visualisations' separates the two panels. The 'Filtres' panel has a search bar 'Rechercher' and a section 'Filtres dans cette page' containing several filter boxes: 'assignment group est (Tout)', 'Base Score est (Tout)', 'Category est Middleware ou So...', 'Hostname est (Tout)', and 'SGL1 est (Tout)'. Below these is a button 'Ajouter des champs de do...'. The 'Données' panel also has a search bar 'Rechercher' and a list of data columns: '20250731 CSInternal v...' and 'Requête1'. A red circle highlights the 'Filtres dans cette page' section in the 'Filtres' panel. A blue arrow points from the 'Category' filter box to the 'Requête1' data column in the 'Données' panel.

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