

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 :

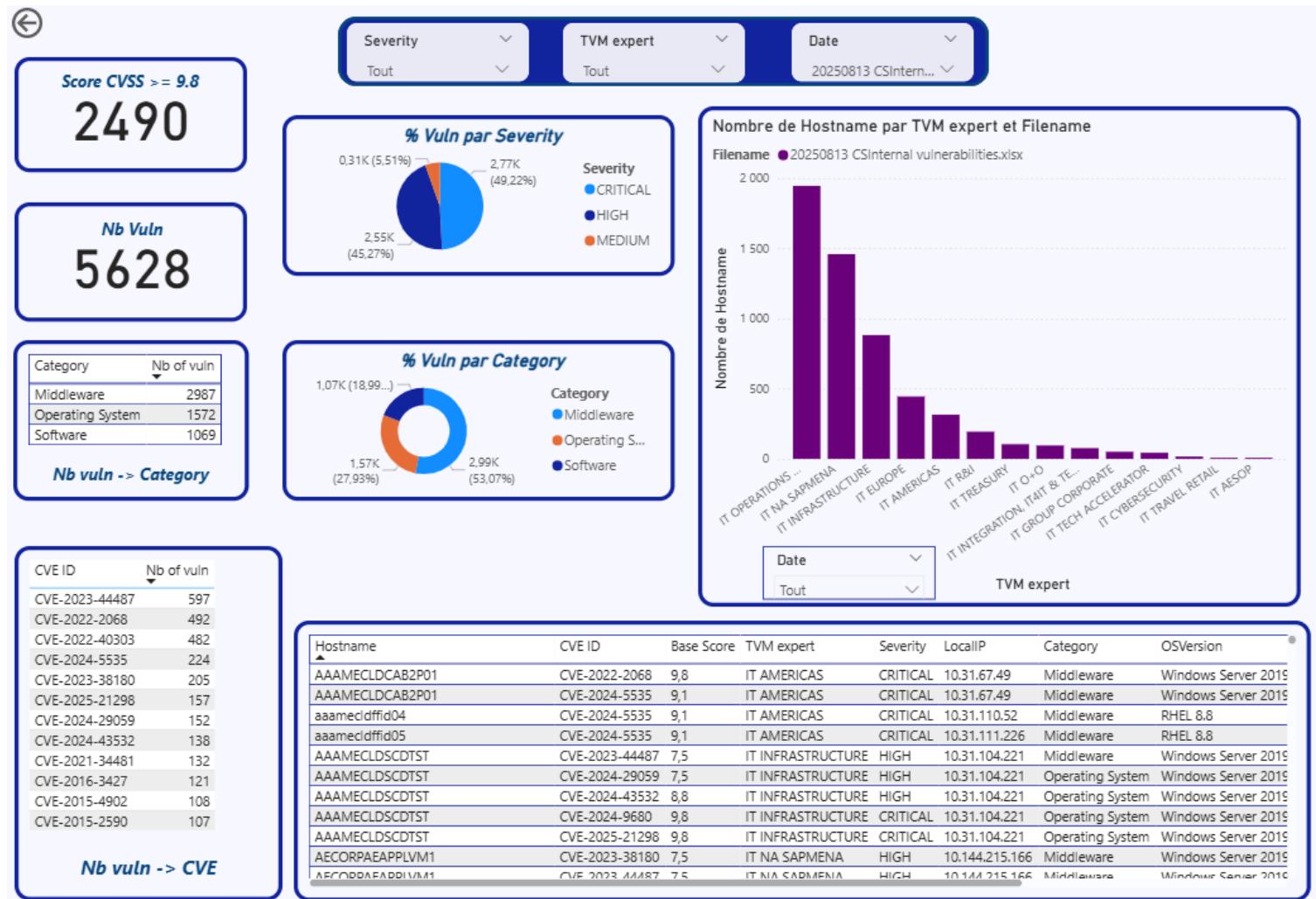
Une feuille où vous allez retrouver toutes les vulnérabilités de toute les zones

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

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

Une feuille où 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.

Score CVSS >= 9.8

2490

Nb Vuln

5628

Category	Nb of vuln
Middleware	2987
Operating System	1572
Software	1069

Nb vuln -> Category

% Vuln par Severity

Severity	Count	Percentage
Critical	2.77K	(49.22%)
High	2.55K	(45.27%)
Medium	0.31K	(5.51%)

% Vuln par Category

Category	Count	Percentage
Software	2.99K	(53.07%)
Operating S.	1.57K	(27.93%)
Middleware	1.07K	(18.99%)

CVE ID

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

Hostname	CVE ID	Base Score	TVM expert	Severity	LocalIP	Category	OSVersion
AAAMECLDCAB2P01	CVE-2022-2068	9,8	IT AMERICAS	CRITICAL	10.31.104.221	Middleware	Windows Server 2019
AAAMECLDCAB2P01	CVE-2024-5535	9,1	IT AMERICAS	CRITICAL	10.31.167.49	Middleware	Windows Server 2019
aaamecldffid04	CVE-2024-5535	9,1	IT AMERICAS	CRITICAL	10.31.111.226	Middleware	RHEL 8.8
aaamecldffid05	CVE-2024-5535	9,1	IT AMERICAS	CRITICAL	10.31.111.226	Middleware	RHEL 8.8
AAAMECLDCDTST	CVE-2023-44487	7,5	IT INFRASTRUCTURE	HIGH	10.31.104.221	Middleware	Windows Server 2019
AAAMECLDCDTST	CVE-2024-29059	7,5	IT INFRASTRUCTURE	HIGH	10.31.104.221	Operating System	Windows Server 2019
AAAMECLDCDTST	CVE-2024-43532	8,8	IT INFRASTRUCTURE	HIGH	10.31.104.221	Operating System	Windows Server 2019
AAAMECLDCDTST	CVE-2024-9680	9,8	IT INFRASTRUCTURE	CRITICAL	10.31.104.221	Operating System	Windows Server 2019
AAAMECLDCDTST	CVE-2025-21298	9,8	IT INFRASTRUCTURE	CRITICAL	10.31.104.221	Operating System	Windows Server 2019
AECORPAEAPLVM1	CVE-2023-38180	7,5	IT NA SAPMENA	HIGH	10.144.215.166	Middleware	Windows Server 2019
AECORPAEADIVM1	CVE-2023-44487	7,5	IT NA SAPMENA	HIGH	10.144.215.166	Middleware	Windows Server 2019

Date

Nombre de Hostname par TVM expert et Filename

CSInternal vulnerabilities.xlsx

Nombre de Hostname

2 000

1 500

1 000

500

0

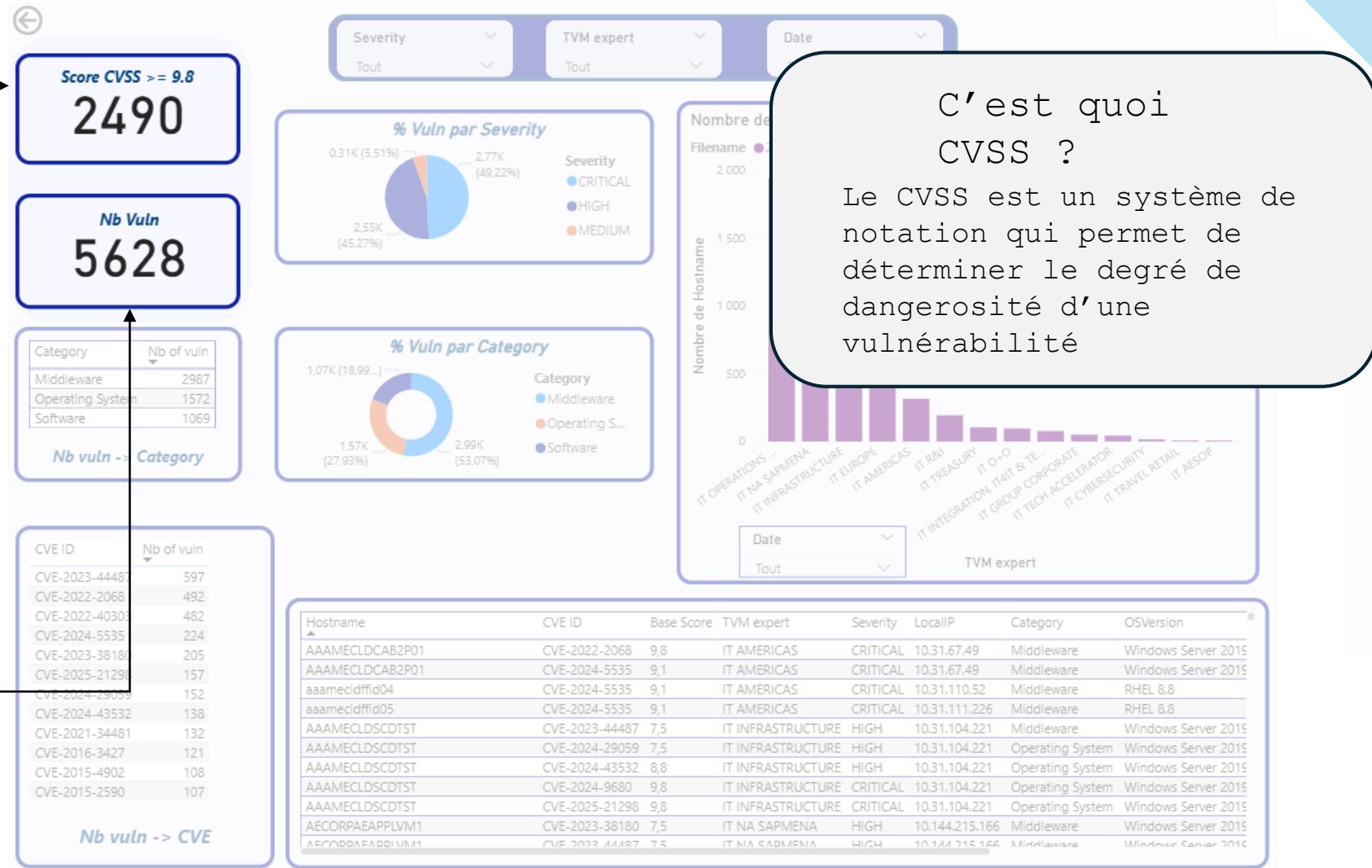
Liste déroulante permettant de sélectionner : La sévérité des vulnérabilités (à gauche), la zone (au milieu) et la date du fichier par semaine (à droite).

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

Score CVSS >= 9.8
2490

Nb Vuln
5628

Category Nb of vuln

- Middleware
- Operating System
- Software

Nb vuln -> CVE

CVE ID

- CVE-2023-44487
- CVE-2022-2068
- CVE-2022-40303
- CVE-2024-5535
- CVE-2023-38180
- 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

Severity Tout TVM expert Tout Date 20250813 CSIntern...

% Vuln par Severity

Severity

- CRITICAL
- HIGH
- MEDIUM

% Vuln par Category

Nombre de Hostname par TVM expert et Filename

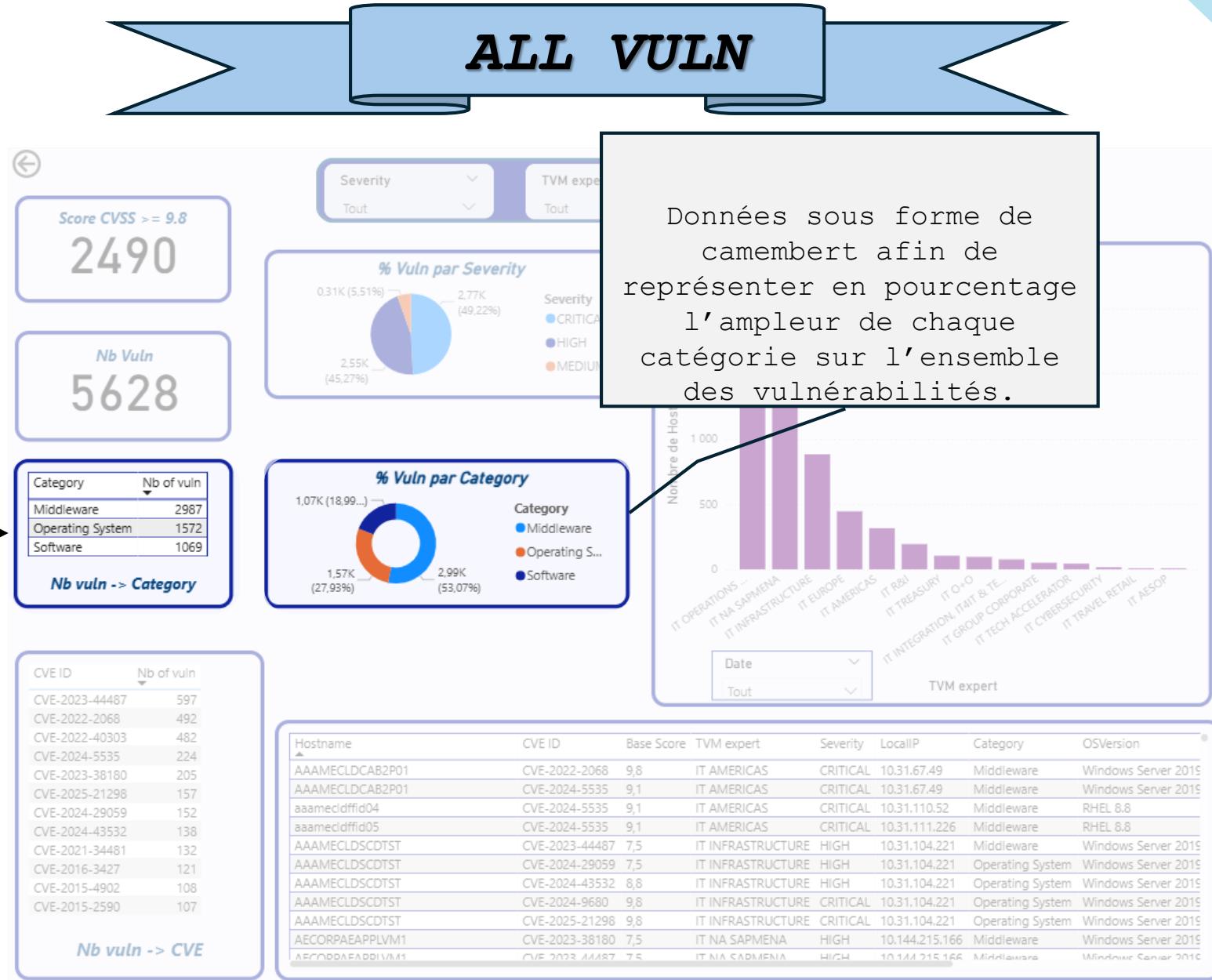
Filename 20250813 CSInternal vulnerabilities.xlsx

Date Tout TVM expert

Base Score	TVM expert	Severity	LocalIP	Category	OSVersion
9,8	IT AMERICAS	CRITICAL	10.31.67.49	Middleware	Windows Server 2019
9,1	IT AMERICAS	CRITICAL	10.31.67.49	Middleware	Windows Server 2019
9,1	IT AMERICAS	CRITICAL	10.31.110.52	Middleware	RHEL 8.8
9,1	IT AMERICAS	CRITICAL	10.31.111.226	Middleware	RHEL 8.8
7,5	IT INFRASTRUCTURE	HIGH	10.31.104.221	Middleware	Windows Server 2019
7,5	IT INFRASTRUCTURE	HIGH	10.31.104.221	Operating System	Windows Server 2019
8,8	IT INFRASTRUCTURE	HIGH	10.31.104.221	Operating System	Windows Server 2019
9,8	IT INFRASTRUCTURE	CRITICAL	10.31.104.221	Operating System	Windows Server 2019
9,8	IT INFRASTRUCTURE	CRITICAL	10.31.104.221	Operating System	Windows Server 2019
7,5	IT NA SAPMENA	HIGH	10.144.215.166	Middleware	Windows Server 2019
7,5	IT NA SAPMENA	HIGH	10.144.215.166	Middleware	Windows Server 2019

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 :

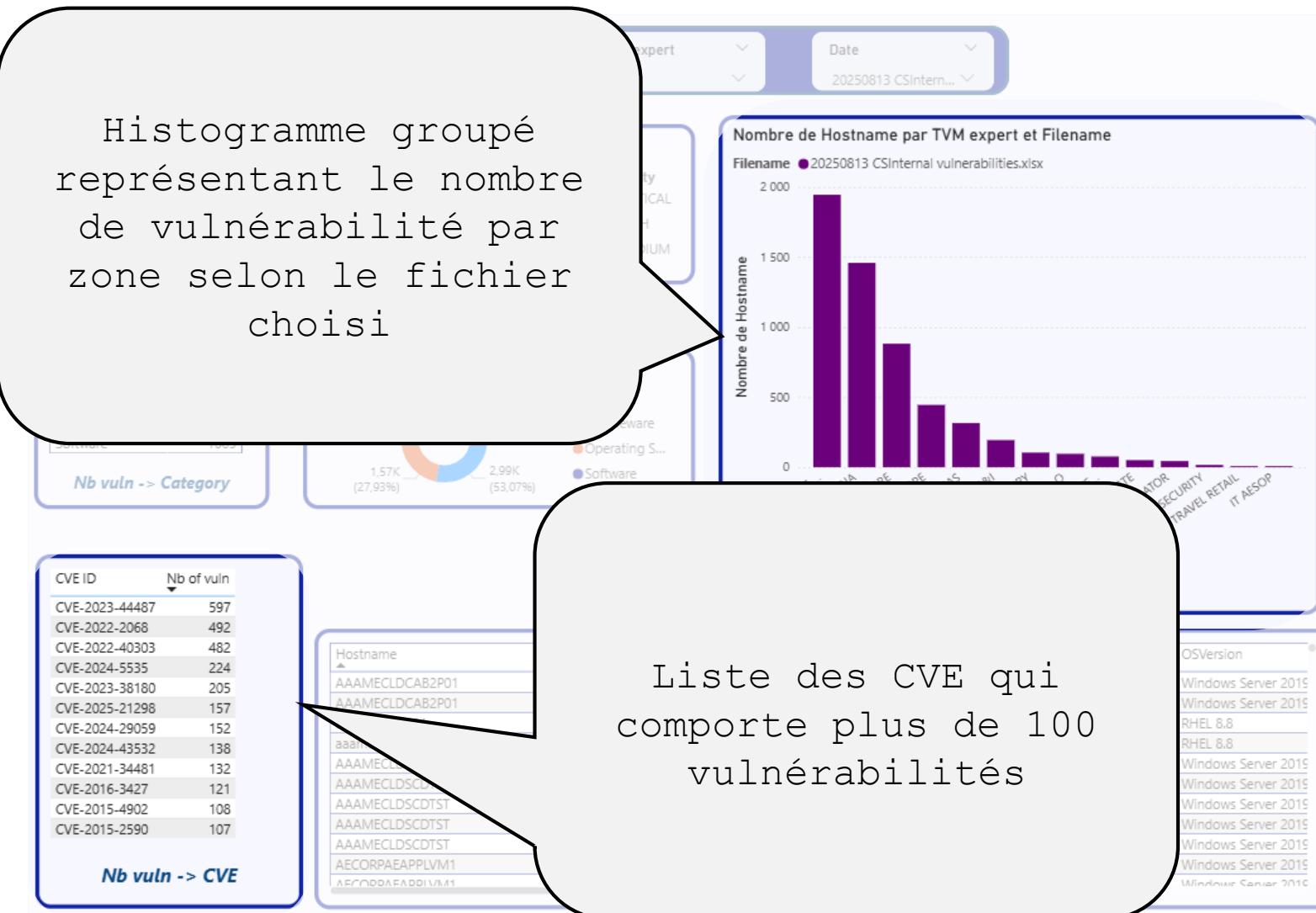
- ❖ Operating System
- ❖ Middleware
- ❖ Software

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

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

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

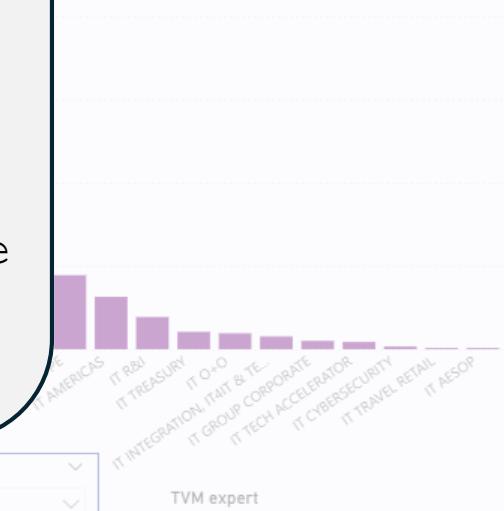
CVE ID	Nb of vuln
CVE-2023-44487	597
CVE-2022-2068	492
CVE-2022-40303	482
CVE-2024-5535	224
CVE-2023-38180	205
CVE-2025-21298	157
CVE-2024-29059	152
CVE-2024-43532	138
CVE-2021-34481	132
CVE-2016-3427	121
CVE-2015-4902	108
CVE-2015-2590	107

Nb vuln -> CVE

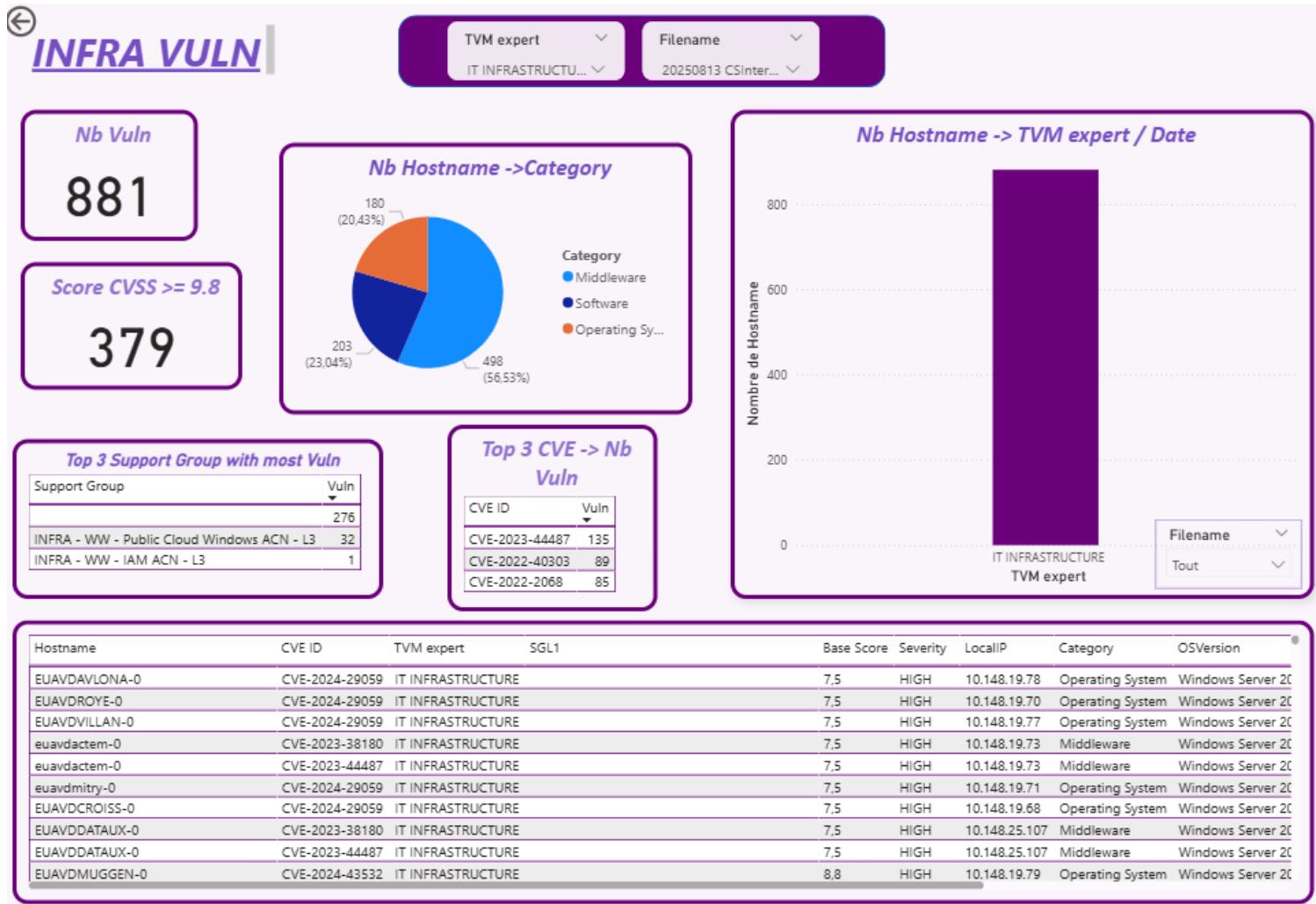
Hostname	CVE ID	Base Score	TVM expert	Severity	LocalIP	Category	OSVersion
AAAMECLDCAB2P01	CVE-2022-2068	9,8	IT AMERICAS	CRITICAL	10.31.67.49	Middleware	Windows Server 2019
AAAMECLDCAB2P01	CVE-2024-5535	9,1	IT AMERICAS	CRITICAL	10.31.67.49	Middleware	Windows Server 2019
aaamecldffid04	CVE-2024-5535	9,1	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
AECORPAEAAPLVM1	CVE-2023-38180	7,5	IT NIA SAPMENA	HIGH	10.144.215.166	Middleware	Windows Server 2019
AECORPAEAAPLVM1	CVE-2023-44487	7,5	IT NIA SAPMENA	HIGH	10.144.215.166	Middleware	Windows Server 2019

Filter TVM expert et Filename

Global vulnerabilities.xlsx



Deuxieme feuille : **INFRA VULN**



INFRA VULN

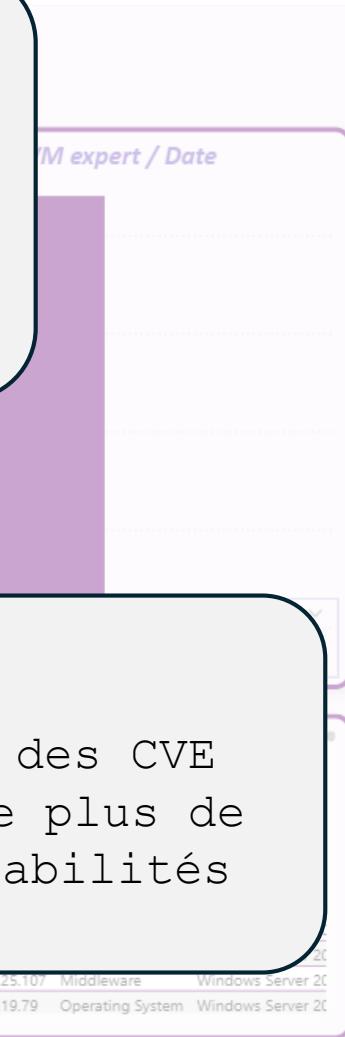
Nb Vuln
881

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

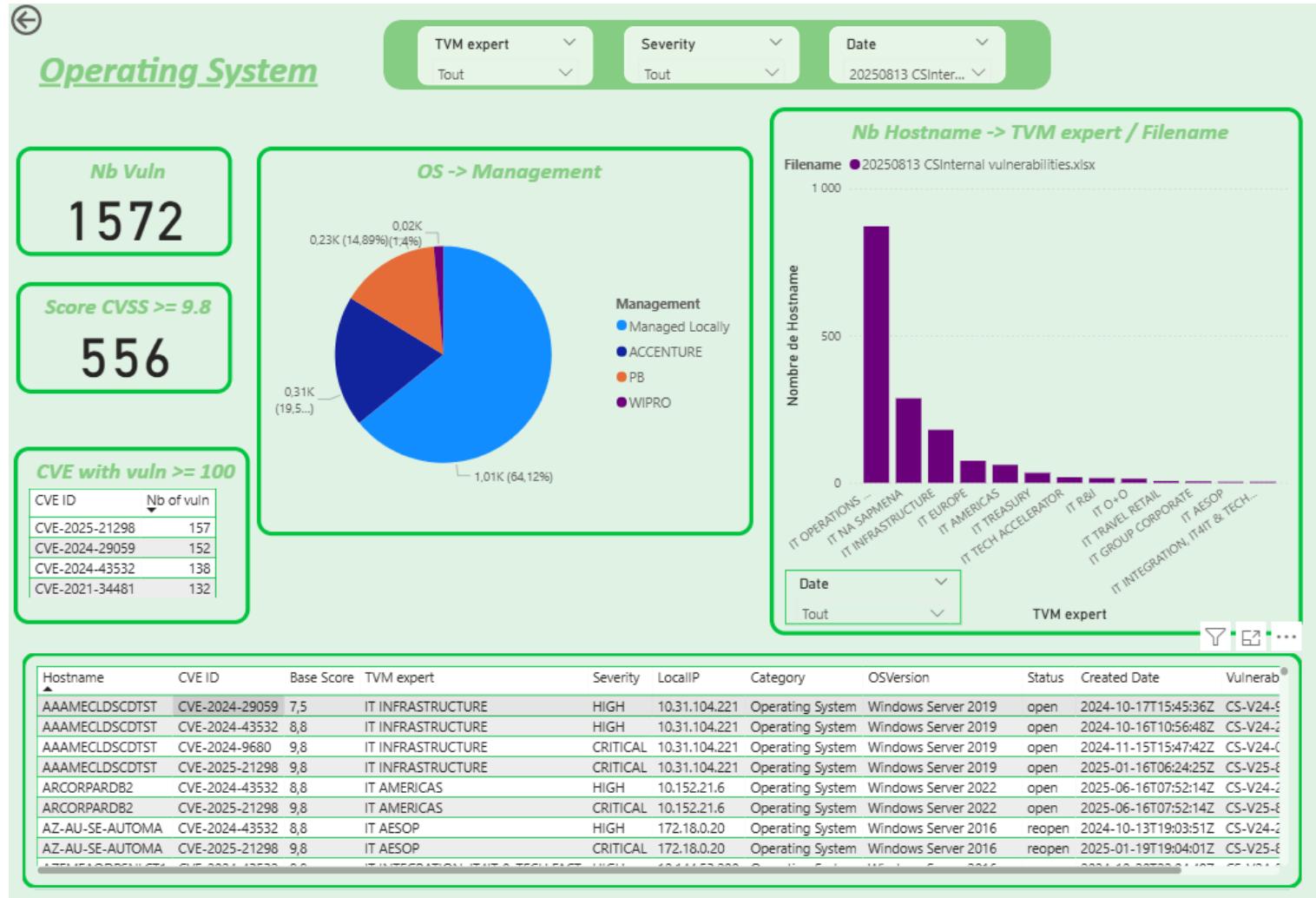
Hostname	CVE ID	TVM expert	SGL1
EUAVDAVLONA-0	CVE-2024-29059	IT INFRASTRUCTURE	
EUAVDROYE-0	CVE-2024-29059	IT INFRASTRUCTURE	
EUAVDVILLAN-0	CVE-2024-29059	IT INFRASTRUCTURE	
euavdactem-0	CVE-2023-38180	IT INFRASTRUCTURE	
euavdactem-0	CVE-2023-44487	IT INFRASTRUCTURE	
euavdmity-0	CVE-2024-29059	IT INFRASTRUCTURE	
EUAVDCROISS-0	CVE-2024-29059	IT INFRASTRUCTURE	
EUAVDDATAUX-0	CVE-2023-38180	IT INFRASTRUCTURE	
EUAVDDATAUX-0	CVE-2023-44487	IT INFRASTRUCTURE	
EUAVDMUGGEN-0	CVE-2024-43532	IT INFRASTRUCTURE	

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



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

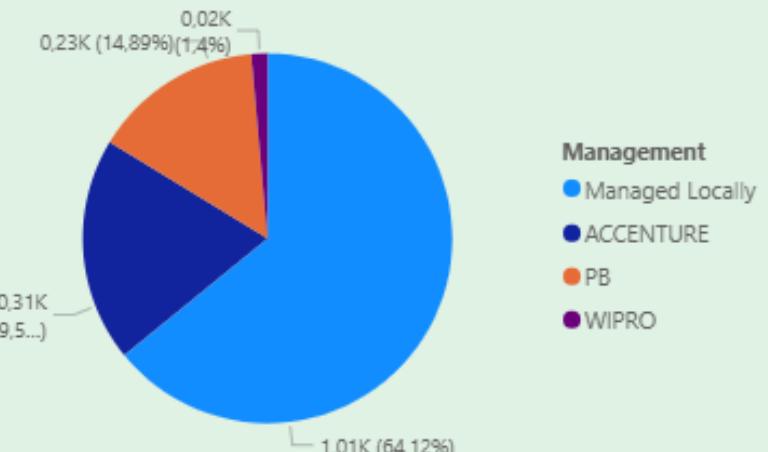
Score CVSS >= 9.8

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

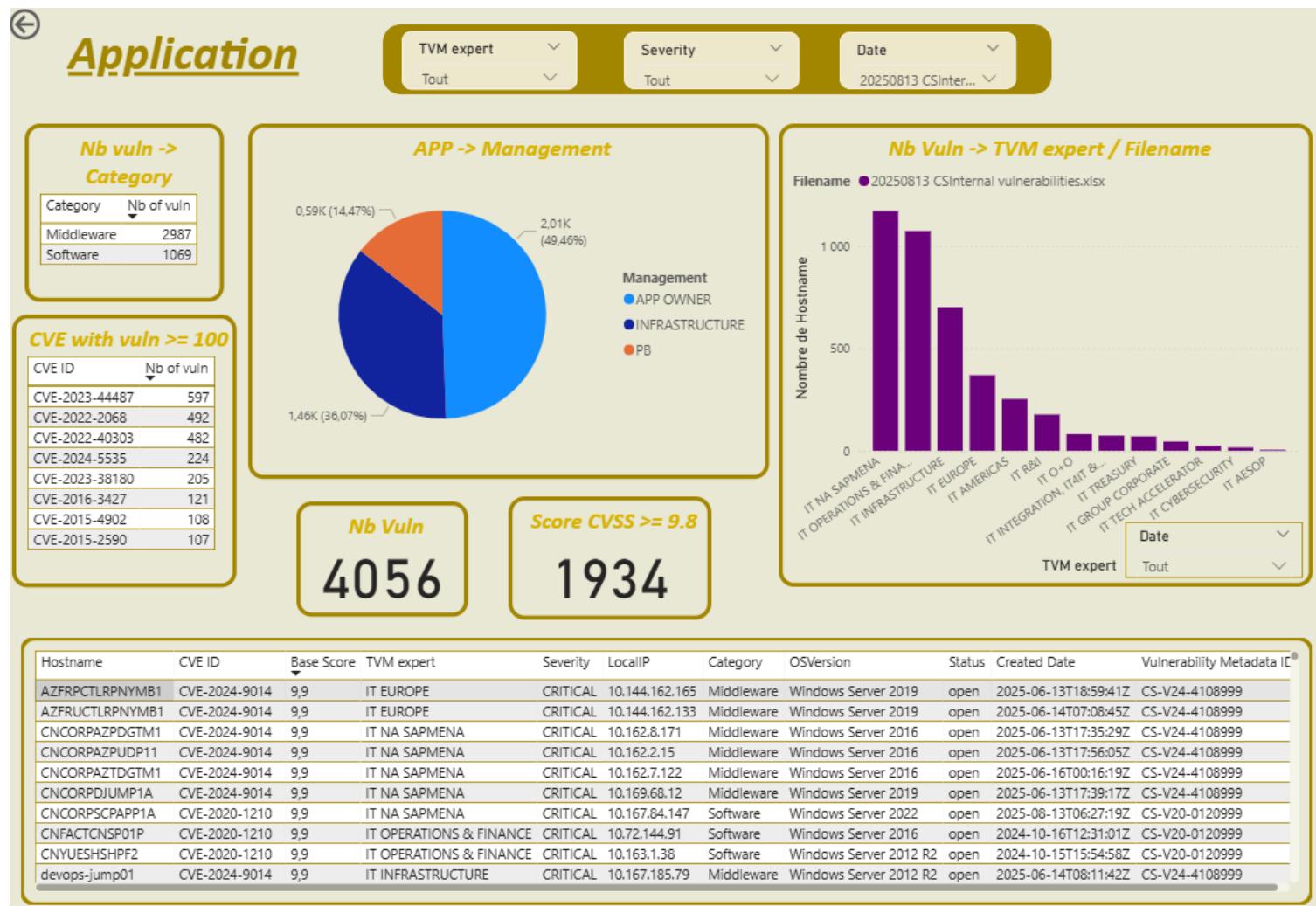


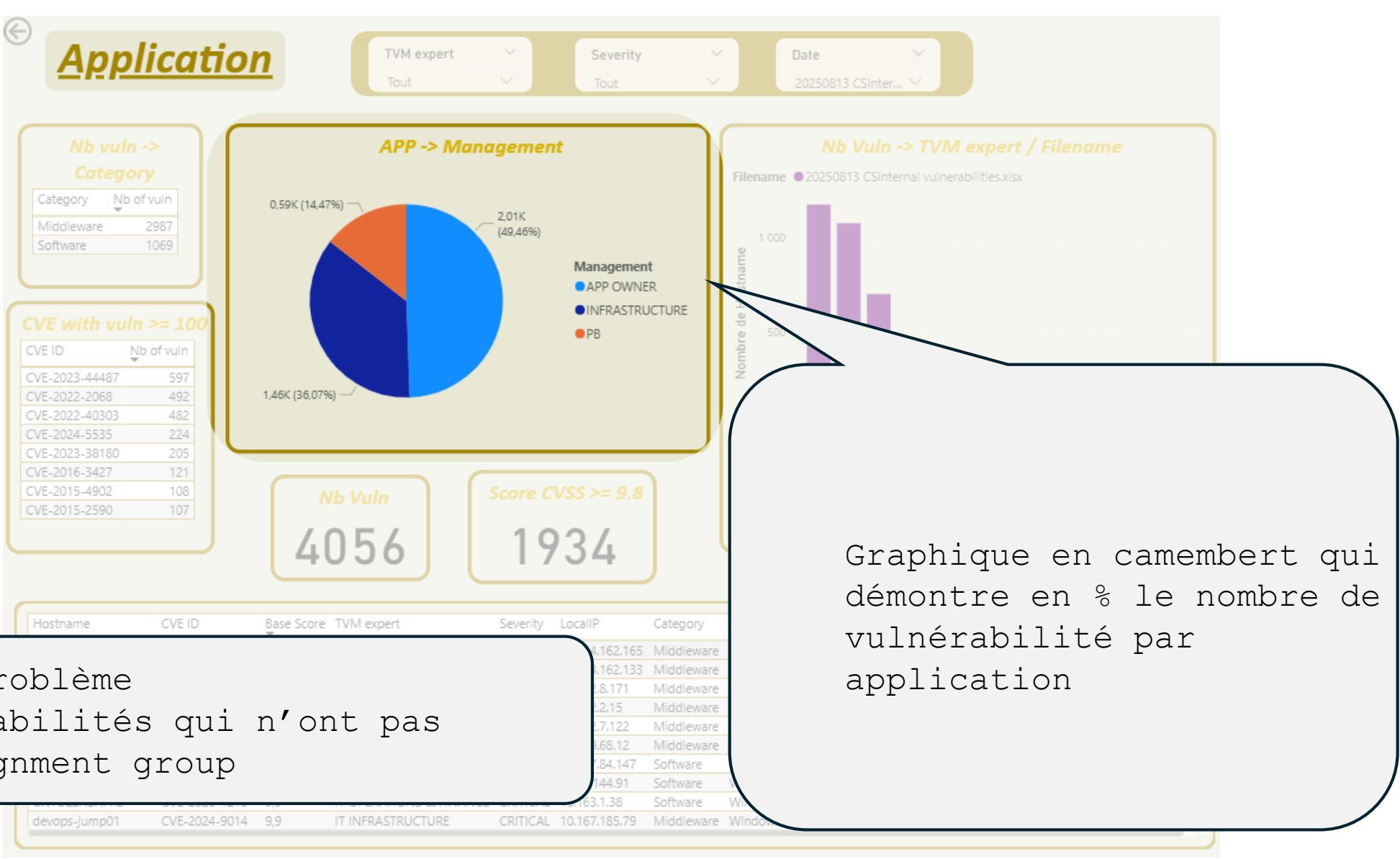
Date

Tout

TVM expert

Quatrième feuille : Application





Filtres et données

The screenshot shows a user interface for managing filters and data. On the left, a dark circular overlay contains the text "Filtres et données". To the right, there are two main sections: "Filtres" and "Données".

Filtres Panel:

- Search bar: Rechercher
- Section: Filtres dans cette page
- Filter items:
 - assignment group est (Tout)
 - Base Score est (Tout)
 - Category est Middleware ou So...
 - Hostname est (Tout)
 - SGL1 est (Tout)
- Text: Ajouter des champs de do...
- Section: Filtres dans toutes les pages
- Text: Ajouter des champs de do...

Données Panel:

- Search bar: Rechercher
- Items:
 - > 20250731 CSInternal v...
 - > Requête1 ...

A vertical sidebar on the right is labeled "Visualisations".

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 the Power BI interface with two main panes: 'Filtres' (Filters) on the left and 'Données' (Data) on the right. The 'Filtres' pane contains a search bar and two sections of filters: 'Filtres dans cette page' (Filters in this page) and 'Filtres dans toutes les pages' (Filters in all pages). The 'Filtres dans cette page' section includes filters for 'assignment group', 'Base Score', 'Category', 'Hostname', and 'SGL1'. The 'Filtres dans toutes les pages' section has an 'Ajouter des champs de do...' (Add fields from do...) button. The 'Données' pane also has a search bar and lists '20250731 CSInternal v...' and 'Requête1' under 'Visualisations' (Visualizations).

Base Score = Score CVSS
Hostname = Nom de la vulnérabilité
SGL1 = Support Group