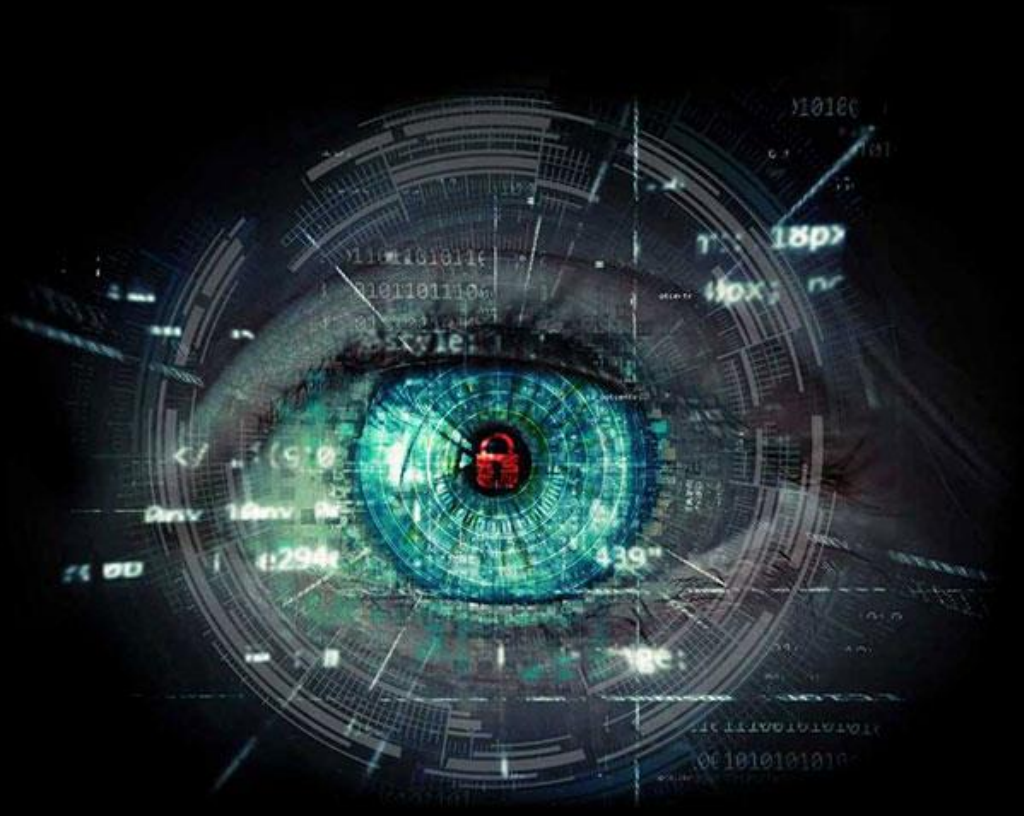
Analyse des Risques de Vulnérabilités en Cybersécurité

Données CISA Juin 2022

AUTEURS :

- MEVENGUE ENGONGOMO FRANCK ANDY
- Christian NGATCHOU-NGUEJIP

SOMMAIRE :



Introduction

01 ➢ Répartition des Vulnérabilités par Fournisseur de Projet et par Produit

02 ➢ Tendance Temporelle des Scores CVSS

03 ➢ Analyse de la Complexité des Vulnérabilités par Gravité

04 ➢ Nombre de Vulnérabilités Résolues par Rapport à la Date Limite

Conclusion

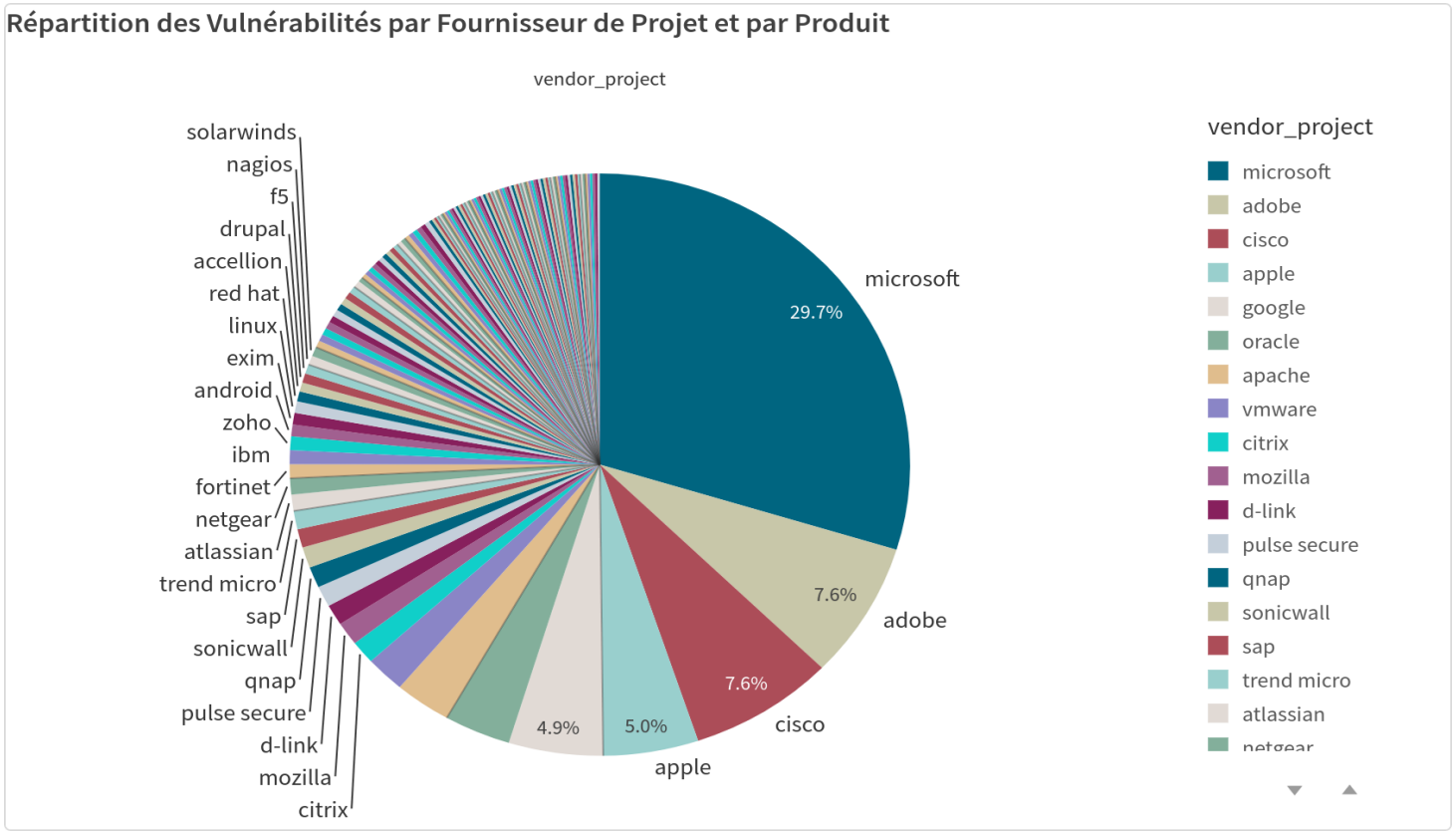
INTRODUCTION :

La cybersécurité est devenue un enjeu majeur dans un monde de plus en plus connecté, où les cybermenaces sont omniprésentes et en constante évolution. Pour mieux comprendre et gérer ces risques, il est crucial de mener une analyse approfondie des vulnérabilités existantes. Dans ce rapport, nous allons examiner les données sur les vulnérabilités de sécurité aux États-Unis à partir du catalogue des vulnérabilités exploitées connues de la CISA pour 2022, en mettant en évidence les tendances, les défis et les opportunités, tout en explorant les possibilités de visualisation des données pour une compréhension plus approfondie.

Répartition des Vulnérabilités par Fournisseur de Projet et par Produit :

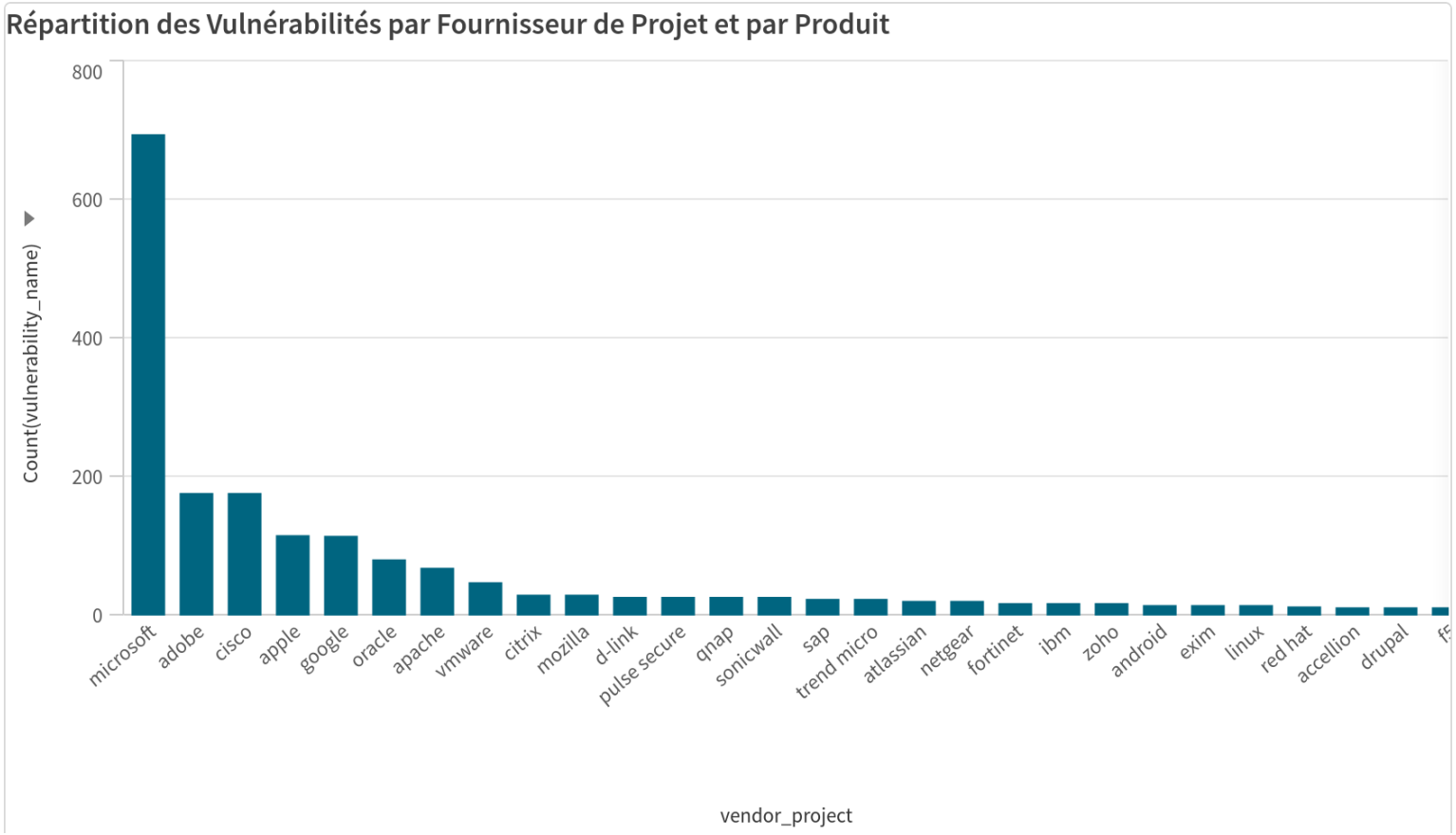
Répartition des Vulnérabilités par Fournisseur de Projet et par Produit :

La première visualisation que nous avons examinée était la répartition des vulnérabilités par fournisseur de projet et par produit. Cette visualisation nous a permis d'identifier les fournisseurs de projet et les produits les plus touchés par les vulnérabilités. Nous avons constaté que certains fournisseurs et produits étaient plus susceptibles de présenter des vulnérabilités que d'autres, ce qui souligne l'importance de choisir des fournisseurs et des produits sécurisés pour réduire les risques.

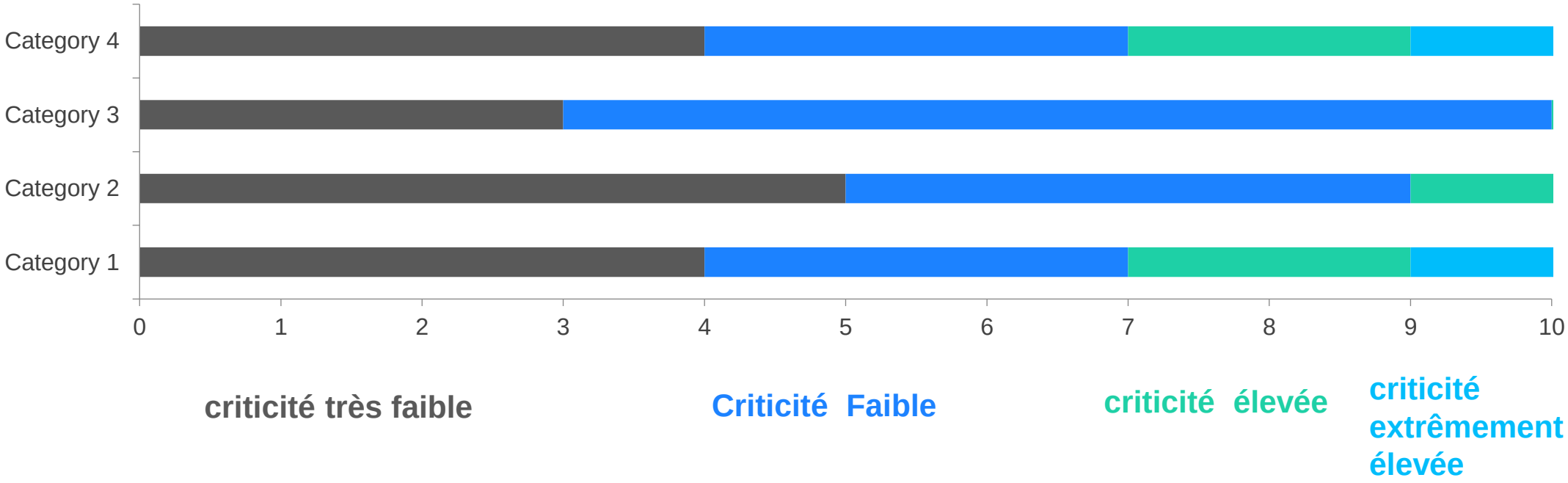


Répartition des Vulnérabilités par Fournisseur de Projet et par Produit :

Cette visualisation permettra de cartographier la répartition des vulnérabilités en fonction des fournisseurs de projet, mettant en évidence ceux qui sont les plus touchés par les vulnérabilités. De plus, elle permettra également d'identifier les produits associés à ces vulnérabilités, offrant ainsi une vue holistique des domaines les plus sensibles en termes de sécurité.

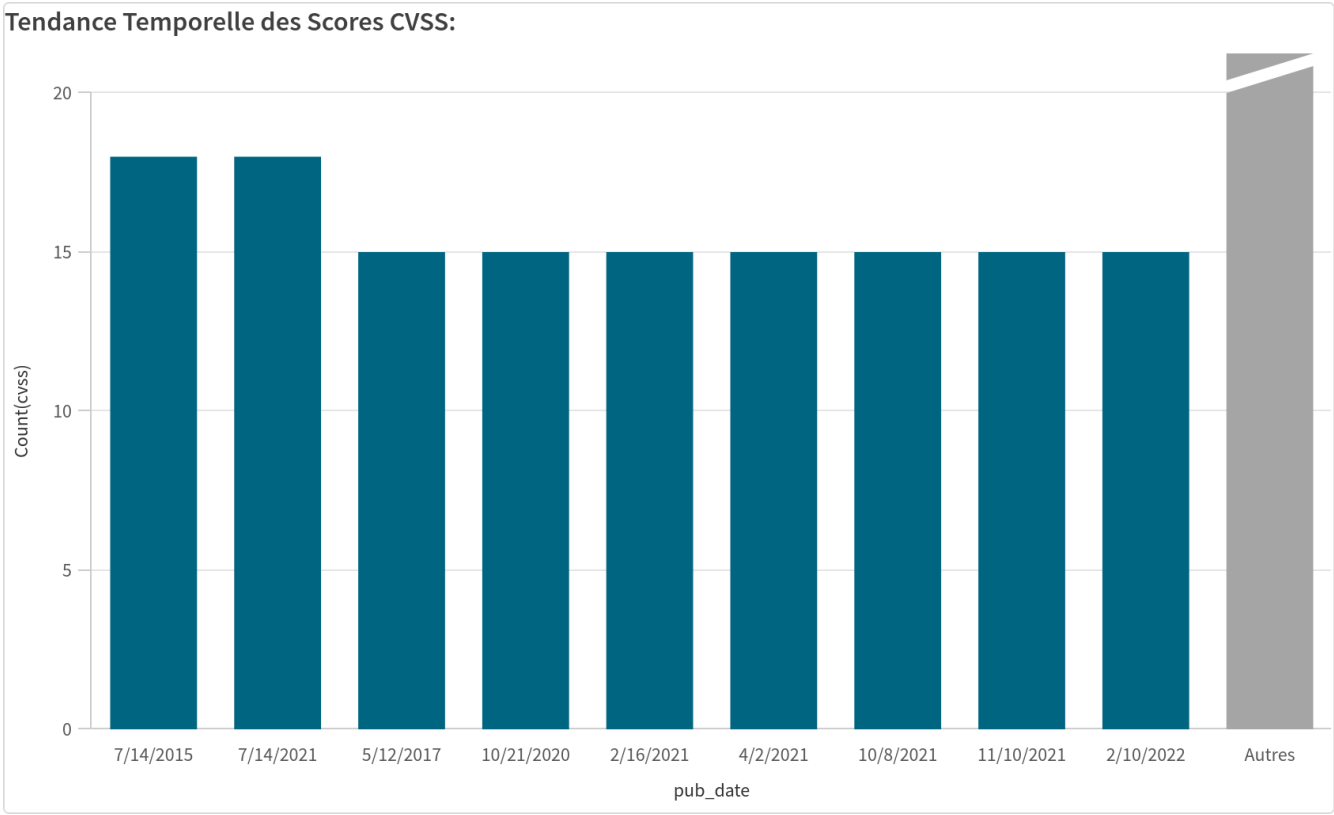


Tendance Temporelle des Scores CVSS:



Évaluation du score et de la gravité CVSS : La CISA calcule ces deux indicateurs (score et gravité du Common Vulnerability Scoring System (CVSS)) en fonction de certains paramètres en attribuant des notes pondérées afin de comprendre sa visibilité sur le type et l'ampleur (niveau d'impact probable, indiquant clairement le statut gris, Bleu, vert et bleu ciel} selon le calcul interne). Les cotes vont généralement de 0 à 10 (0-20), ce qui indique l'ordre de désignation; 0 étant **très faible**, 10 – 20 (échelle) - **Gravité ou criticité extrêmement élevée**.

Tendance Temporelle des Scores CVSS:



Nous avons examinée la tendance temporelle des scores CVSS. Cette visualisation nous a permis de suivre l'évolution des scores CVSS moyens au fil du temps. Nous avons observé que les scores CVSS moyens variaient au cours des années, ce qui indique que certaines périodes peuvent être plus propices aux vulnérabilités que d'autres. Cette information est cruciale pour comprendre les tendances des attaques et ajuster les mesures de sécurité en conséquence.

Distribution des Types de Vulnérabilités les Plus Courants :

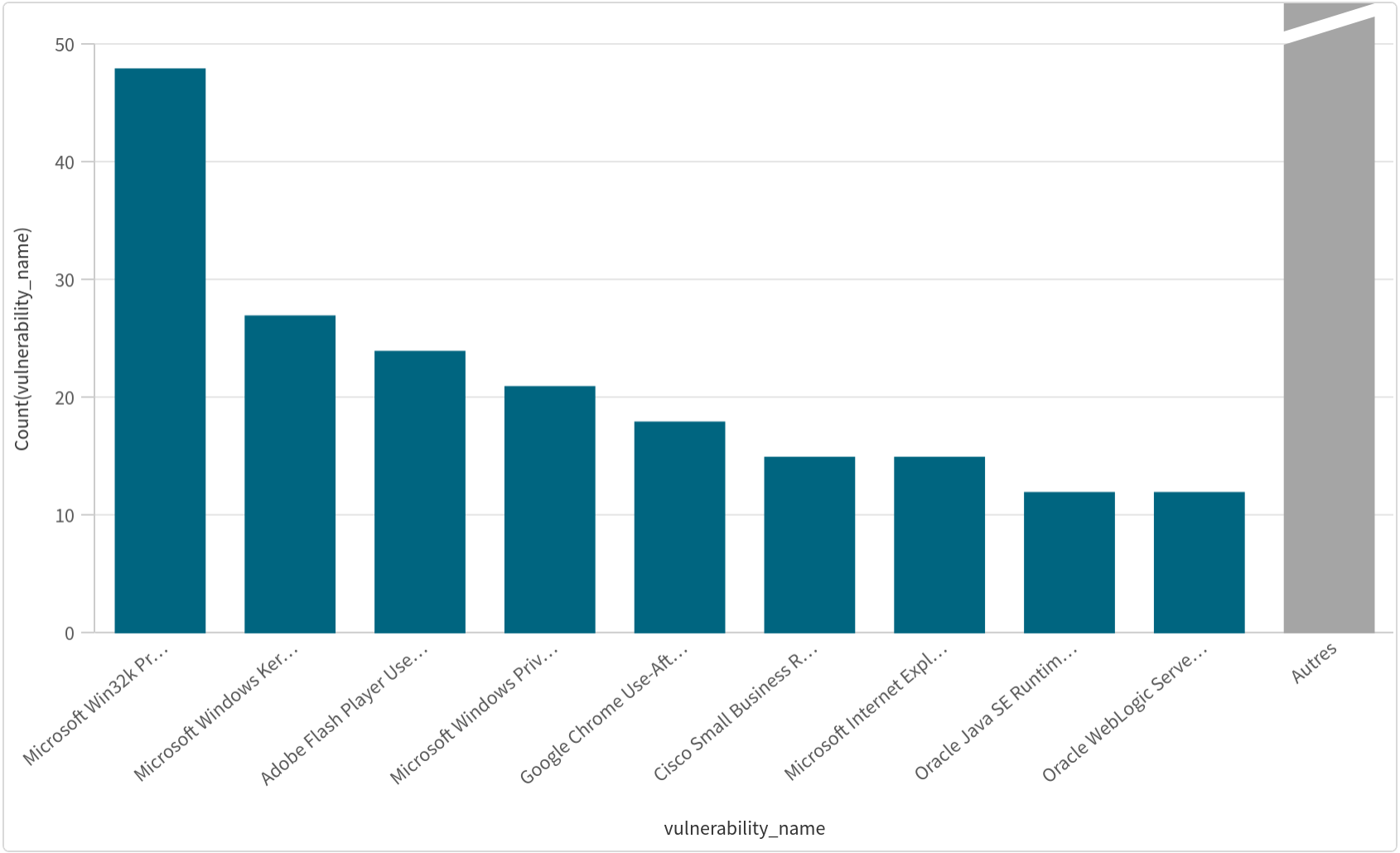
La distribution des types de vulnérabilités les plus courants était une autre visualisation importante que nous avons examinée. Cette visualisation nous a permis d'identifier les types de vulnérabilités les plus fréquemment rencontrés, ce qui nous a aidés à orienter nos efforts de sécurité pour se prémunir contre ces types spécifiques de menaces. Nous avons constaté que certaines vulnérabilités étaient plus courantes que d'autres, ce qui souligne l'importance de se concentrer sur les vulnérabilités les plus critiques et les plus exploitées.

Distribution des Types de Vulnérabilités les Plus Courants :

La distribution des types de vulnérabilités les plus courants était une autre visualisation importante que nous avons examinée. Cette visualisation nous a permis d'identifier les types de vulnérabilités les plus fréquemment rencontrés, ce qui nous a aidés à orienter nos efforts de sécurité pour se prémunir contre ces types spécifiques de menaces. Nous avons constaté que certaines vulnérabilités étaient plus courantes que d'autres, ce qui souligne l'importance de se concentrer sur les vulnérabilités les plus critiques et les plus exploitées.

vulnerability_name	Count(vulnerability_name)
Totaux	**2099**
Microsoft Win32k Privilege Escalation Vulnerability	48
Microsoft Windows Kernel Privilege Escalation Vulnerability	27
Adobe Flash Player Use-After-Free Vulnerability	24
Microsoft Windows Privilege Escalation Vulnerability	21
Google Chrome Use-After-Free Vulnerability	18
Cisco Small Business RV Series Routers Stack-based Buffer Overflow Vulnerability	15
Microsoft Internet Explorer Use-After-Free Vulnerability	15
Oracle Java SE Runtime Environment (JRE) Arbitrary Code Execution Vulnerability	12
Oracle WebLogic Server Remote Code Execution Vulnerability	12
Autres	1907

Distribution des Types de Vulnérabilités les Plus Courants :



Analyse de la Complexité des Vulnérabilités par Gravité :

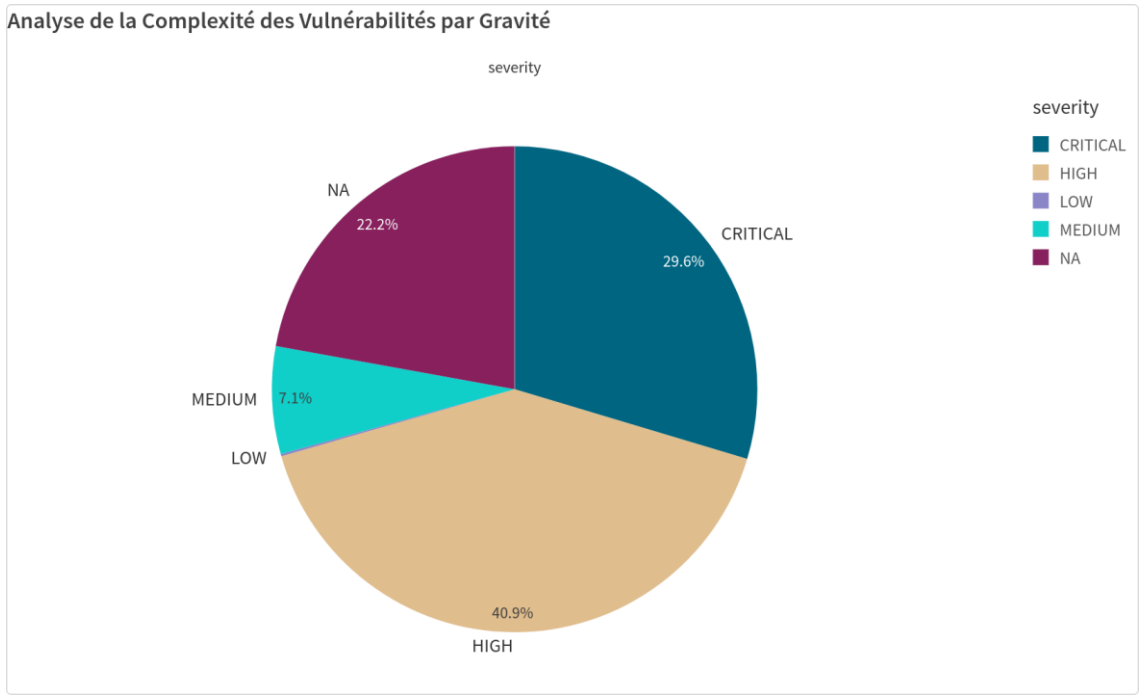
L'analyse de la complexité des vulnérabilités par gravité nous a permis de comprendre si les vulnérabilités les plus graves étaient également les plus complexes à exploiter. Cette visualisation nous a aidés à évaluer les priorités en matière de correction et de prévention, en identifiant les vulnérabilités les plus critiques qui nécessitent une attention immédiate.

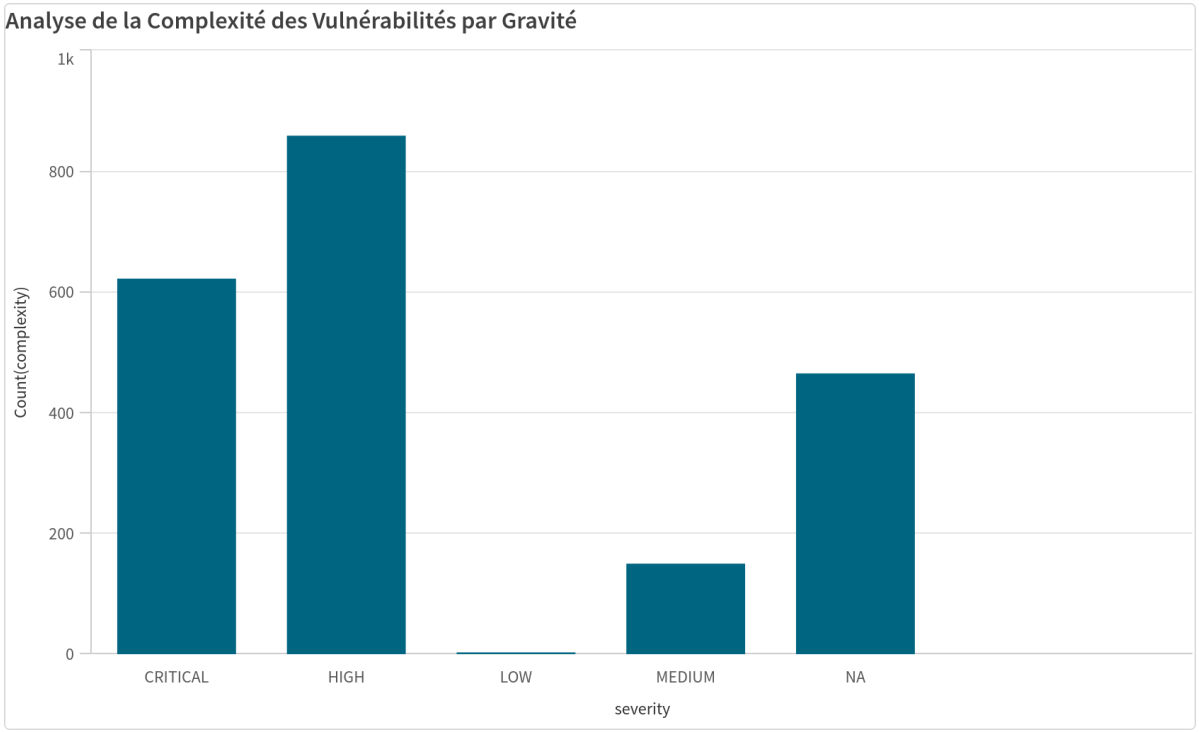
Analyse de la Complexité des Vulnérabilités par Gravité

severity	Count(complexity)
Totaux	**2099**
CRITICAL	622
HIGH	859
LOW	3
MEDIUM	150
NA	465

Analyse de la Complexité des Vulnérabilités par Gravité :

Cette visualisation aiderait à comprendre si les vulnérabilités les plus graves sont également les plus complexes à exploiter, ce qui pourrait influencer les stratégies de correction et de prévention.





Nombre de Vulnérabilités Résolues par Rapport à la Date Limite:

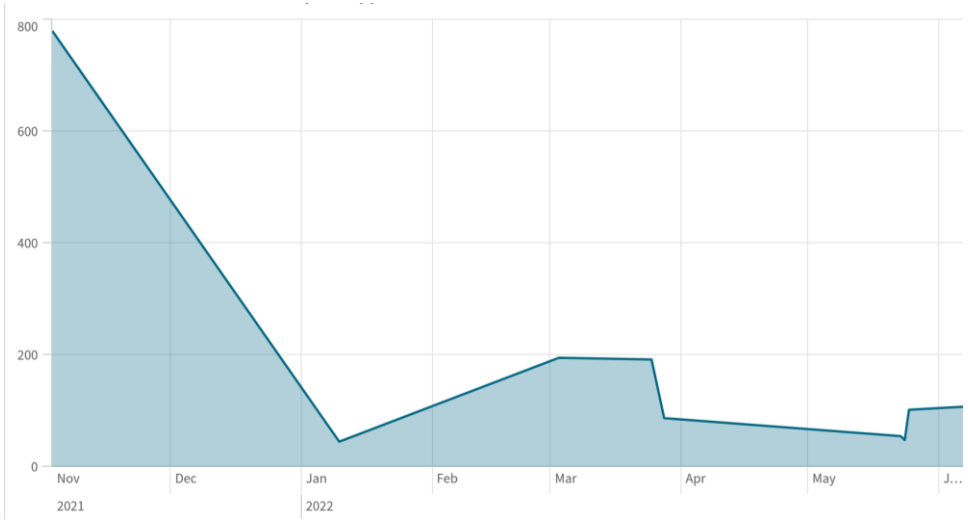
Nombre de Vulnérabilités Résolues par Rapport à la Date Limite:

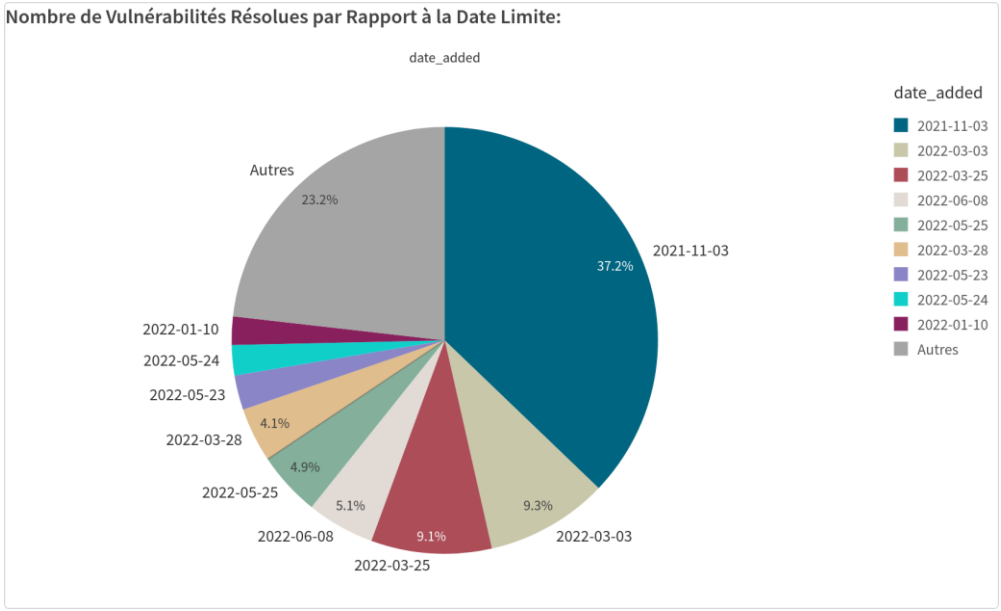
date_added	Count(vulnerability_name)
Totaux	**2099**
2021-11-03	780
2022-03-03	195
2022-03-25	192
2022-06-08	108
2022-05-25	102
2022-03-28	87
2022-05-23	55
2022-05-24	48
2022-01-10	45
Autres	487

Enfin, nous avons examiné le nombre de vulnérabilités résolues par rapport à la date limite. Cette visualisation nous a permis de suivre l'efficacité des processus de gestion des vulnérabilités dans notre organisation. Nous avons constaté que certaines vulnérabilités étaient résolues avant la date limite, tandis que d'autres étaient en attente de correction. Cette information nous a aidés à identifier les lacunes dans nos processus de gestion des vulnérabilités et à prendre des mesures correctives pour améliorer notre posture de sécurité.

Nombre de Vulnérabilités Résolues par Rapport à la Date Limite:

Cette visualisation permettra de suivre l'efficacité des processus de gestion des vulnérabilités en identifiant le nombre de vulnérabilités résolues avant ou après la date limite. Elle aidera à repérer les éventuelles lacunes dans les processus de correction et à prendre des mesures correctives pour améliorer la posture de sécurité globale.





Conclusion :

En conclusion, notre analyse des risques de vulnérabilités dans le monde nous a fourni des informations précieuses sur les tendances, les risques et les priorités en matière de cybersécurité. Les visualisations que nous avons examinées nous ont permis d'identifier les fournisseurs de projet et les produits les plus touchés par les vulnérabilités, de suivre l'évolution des scores CVSS moyens, d'identifier les types de vulnérabilités les plus courants, d'évaluer la complexité des vulnérabilités par gravité, et de suivre l'efficacité de nos processus de gestion des vulnérabilités. Ces informations sont cruciales pour renforcer notre posture de sécurité et nous protéger contre les cyberattaques

THANK YOU