Module yuno

By xmco

Gestion de votre veille cyber-sécurité

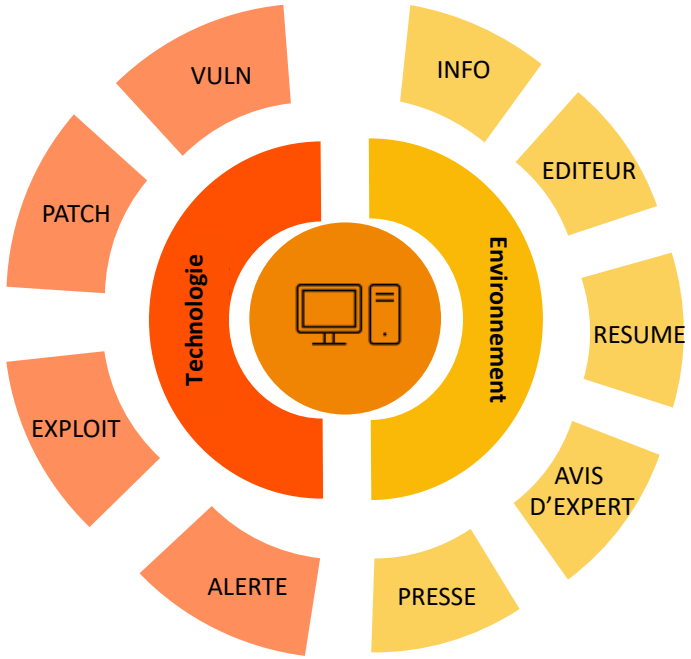
leportail

By xmco

yuno : Une veille 360° de votre actualité cyber

Le SI de mon client est toujours à jour

Je sais quelle vulnérabilité adresser en priorité



J'ai une vision globale des menaces cyber

Je sensibilise en interne sur les problématiques de sécurité

- Veille **quotidienne**
- Veille **qualifiée** et **exploitable**
- Veille **personnalisable**
- Consultation multi-canal (API, Mailing, SaaS)
- Aide à la remédiation dédiée (plan d'action)

Types de bulletins

Deux types de veille sont proposés par le CERT-XMCO.

La veille « technique »

Les bulletins sont associés à des produits/technologies :
- la découverte de vulnérabilités ;
- la publication de correctifs ;
- la publication de codes d'exploitation.

[PATCH] [SAMBA] Prise de contrôle du système via une vulnérabilité au sein de Samba

01/02/2022

Out-of-bounds heap read/write vulnerability in VFS module vfs_fruit allows code execution

Criticité

Dommage
Prise de contrôle d'un système

Plateforme
Indépendant

Exploitation
Distante

Produit concerné
Samba

Français | Anglais

Description

Une vulnérabilité a été corrigée au sein de Samba. Son exploitation permettait à un attaquant de prendre le contrôle du système.

La faille de sécurité référencée CVE-2021-44142 provenait d'une erreur dans le traitement des métadonnées `EA` à l'ouverture d'un fichier dans `smbd`. Un attaquant distant pouvant modifier ces métadonnées pouvait exploiter cette vulnérabilité afin de réaliser des opérations de lecture et d'écriture en dehors des limites prévues sur le tas pour exécuter du code arbitraire avec les privilèges `root`.

Note : cette vulnérabilité impactait la configuration par défaut du module `vfs_fruit` de Samba. Si les options `fruit:metadata` et `fruit:resource` ont toutes les deux des valeurs différentes que celles par défaut (respectivement `fruit:metadata=netatalk` et `fruit:resource=file`), alors le serveur n'est pas vulnérable. Cette opération provoque **la perte des données** stockées.

La veille « environnementale »

Les bulletins ne sont pas associés à des produits/technologies. Ils traitent de :
- l'actualité de la cyber-sécurité ;
- les publications de chercheurs ;
- les campagnes d'attaques en cours ;
- les bulletins managériaux du CERT-XMCO ;
- …

[INFO] Deux vulnérabilités sur le logiciel CWP permettent à un attaquant d'exécuter du code à distance sur des serveurs Linux

Fuite d'informations | Vulnérabilité

02/02/2022

CWP bugs allow code execution as root on Linux servers, patch now

Criticité

Français | Anglais

Description

Le 22 janvier dernier, un chercheur en sécurité de `Octagon Networks` a identifié deux vulnérabilités permettant à un attaquant d'exécuter du code arbitraire à distance, en tant qu'utilisateur `root`, sur un serveur Linux.

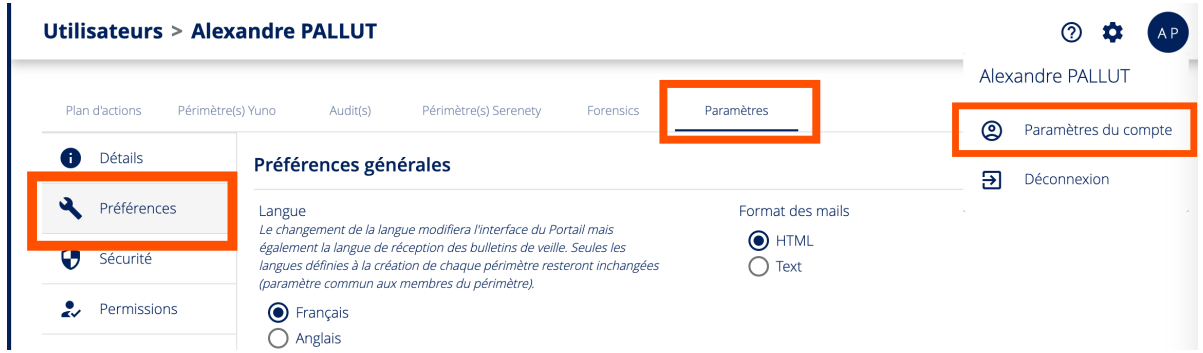
Les vulnérabilités concernent le logiciel `Control Web Panel` (`CWP`), anciennement appelé `CentOS Web Panel`, conçu pour gérer des serveurs d'hébergement web dédiés et des serveurs privés virtuels (`VPS`).

Les deux failles, référencées CVE-2021-45467 et CVE-2021-45466, permettent la lecture (pour la première) et l'écriture (pour la seconde) de fichiers conduisant, lorsqu'elles sont combinées, à une exécution de code arbitraire.

Bien qu'un correctif ait été publiée pour la première vulnérabilité, `Octagon Networks` affirme qu'il est possible de contourner la solution apportée.

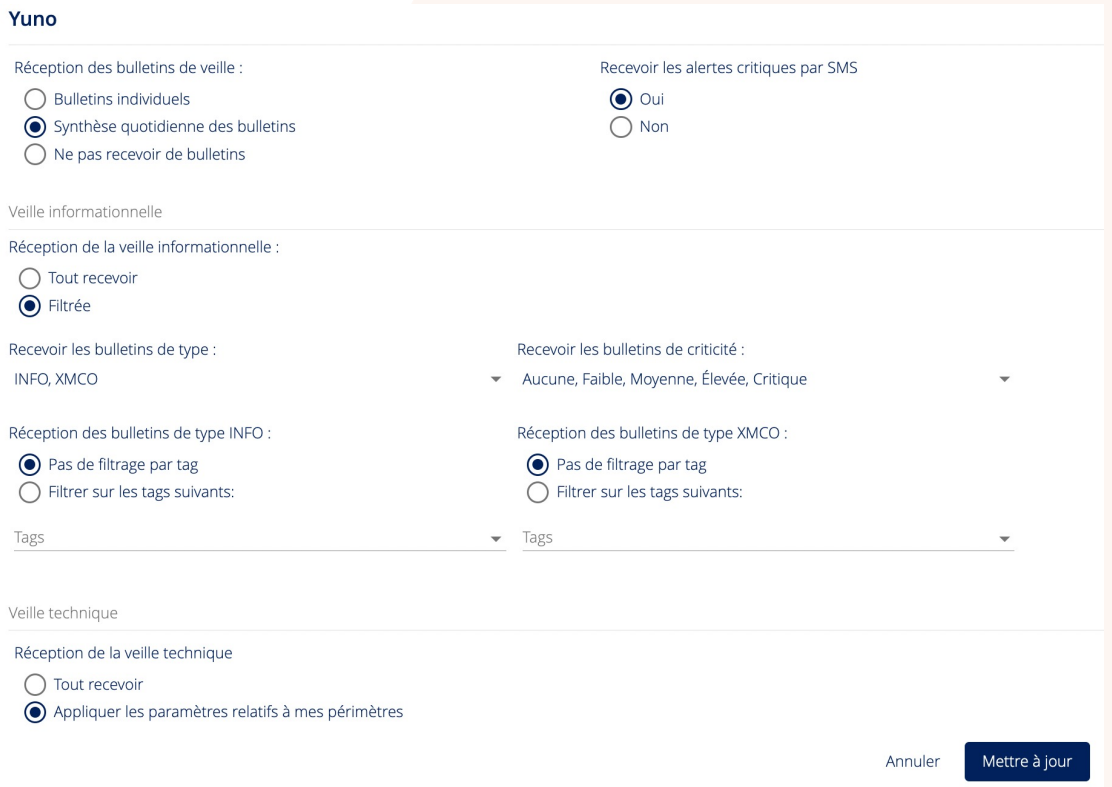
De plus, même si le site de CWP affirme que seuls 30 000 serveurs sont concernés par les failles, des chercheurs en ont identifié plus de 200 000.

Configurer les paramètres de réception



Étape 1
Cliquez sur le menu en haut à droite, puis **Paramètres du compte** et enfin **Préférences**.

Étape 2
Définir les paramètres relatifs à la veille technique et environnementale



Veille environnementale

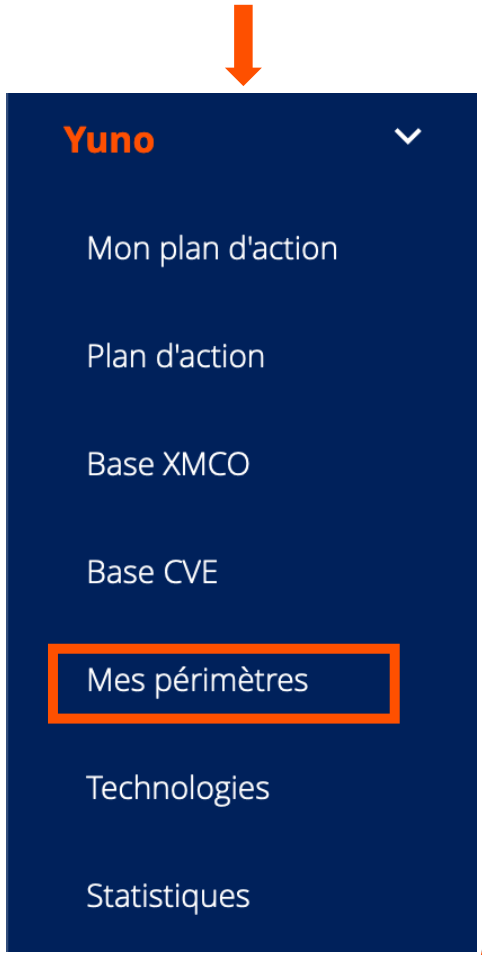
Choisissez de recevoir tous les bulletins de veille environnementale, ou utiliser les filtres pour restreindre les bulletins par criticité, par type, ou par thématiques (tags) spécifiques.

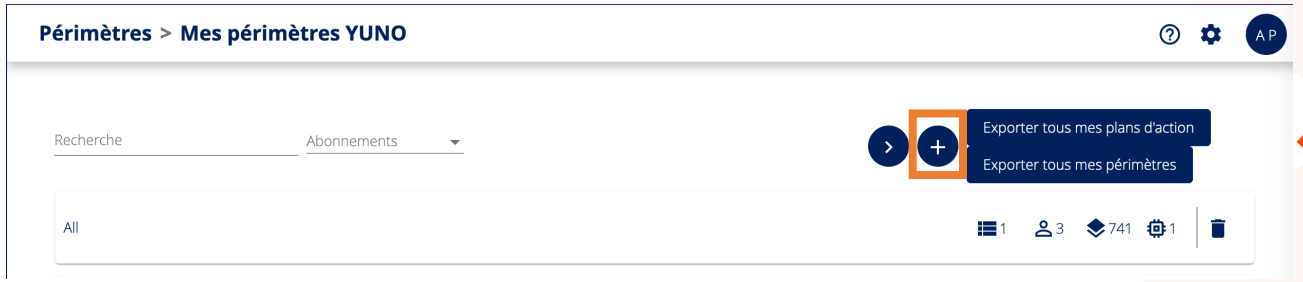
Veille technique

Choisissez de recevoir tous les bulletins de veille technique, ou choisissez de ne recevoir uniquement les bulletins concernant vos périmètres. Vous devrez alors faire partie d'au moins 1 périmètre pour pouvoir recevoir des bulletins techniques.

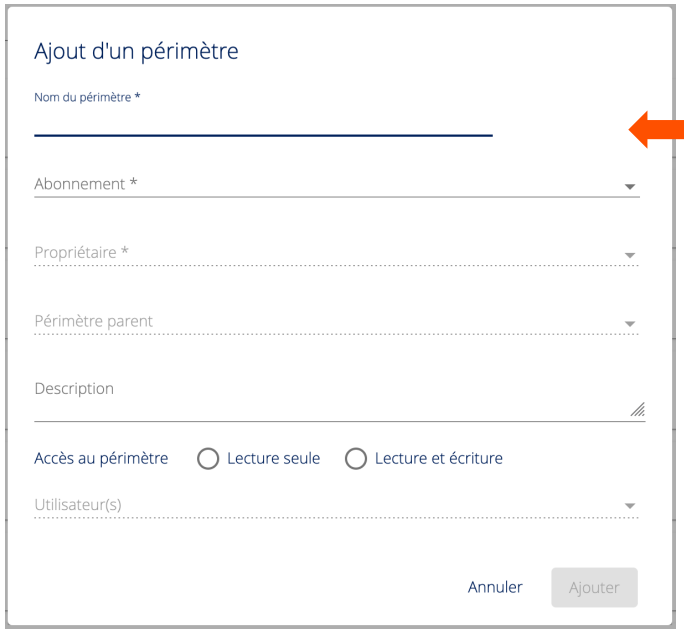
Créer un périmètre

Étape 1
Cliquez sur Mes Périmètres





Étape 2
Ajouter un périmètre



Étape 3
Renseignez les champs proposés et cliquez sur **ajouter** pour confirmer l'ajout.

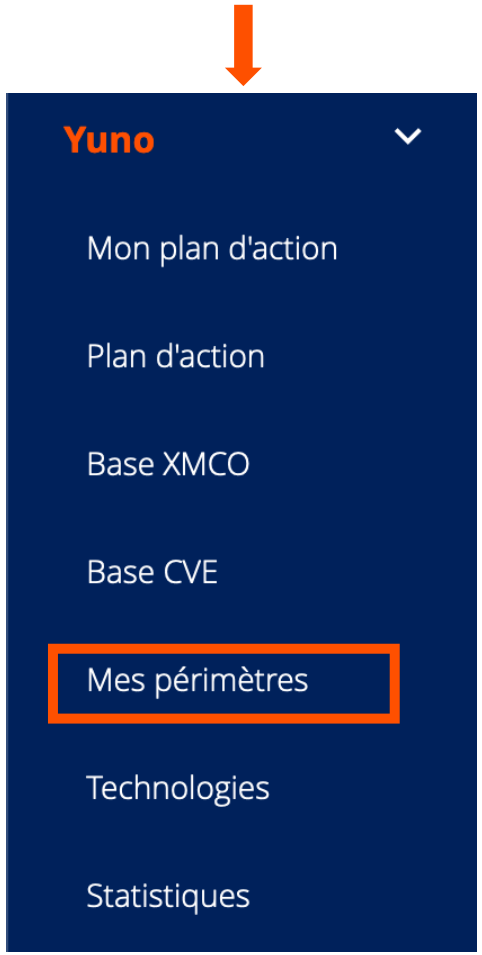
Les utilisateurs ajoutés au périmètre recevront les bulletins concernant les technologies associées à ce périmètre.

Les utilisateurs désignés avec un accès en mode « lecture/écriture » seront en mesure de supprimer une technologie ou d'en ajouter de nouvelles.
Cette action ne sera pas possible pour un utilisateur en mode « lecture seule ».

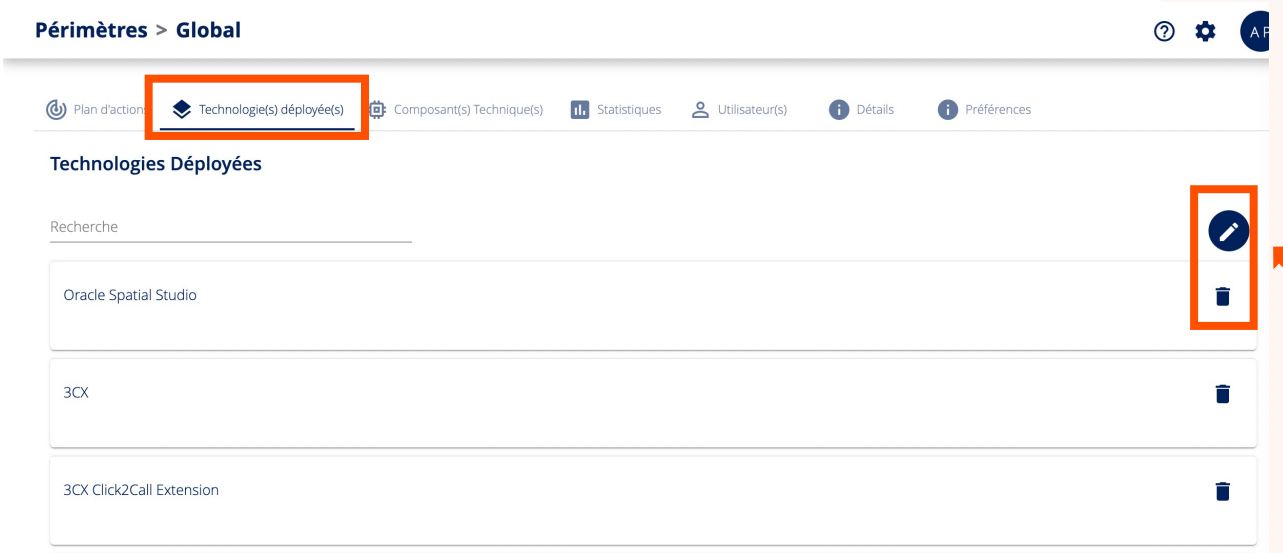
Un périmètre est un regroupement de technologies et d'utilisateurs qui souhaitent les surveiller.

Ajouter des technologies à suivre dans un périmètre

Étape 1
Cliquez sur Mes Périmètres



Étape 2
Sélectionnez le périmètre à modifier

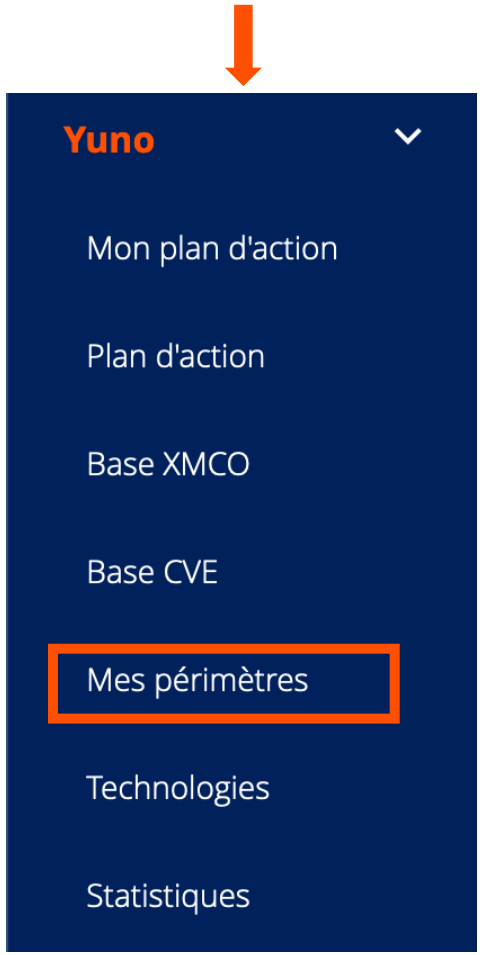


Étape 3
Vous pouvez accéder à la liste des technologies associées à votre périmètre via l'onglet « Technologies Déployées ».

Étape 4
Cliquez ici pour ajouter ou supprimer une ou plusieurs technologies.

Ajouter des utilisateurs dans un périmètre

Étape 1
Cliquez sur Mes Périmètres



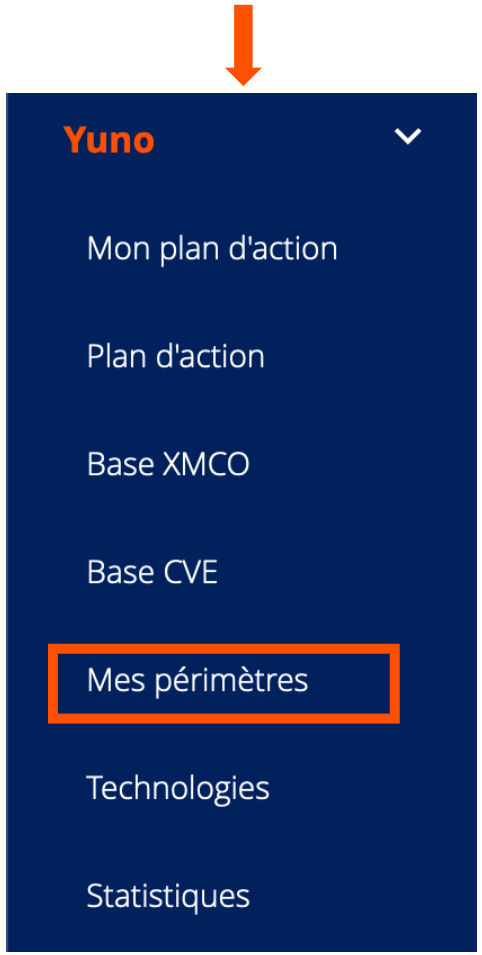
Étape 2
Sélectionnez le périmètre à modifier

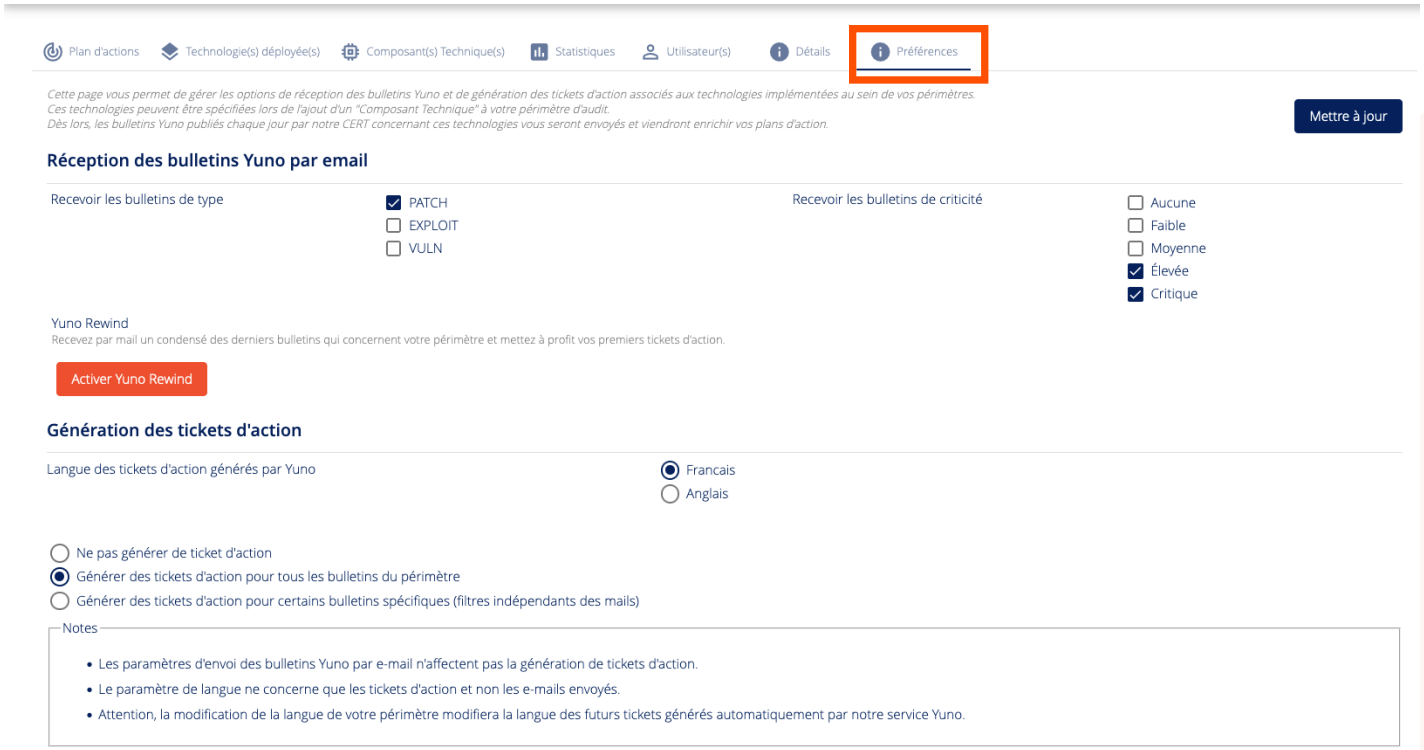
Étape 3
Cliquez sur l'onglet Utilisateurs

Étape 4
Cliquez ici pour ajouter ou supprimer des utilisateurs.

Configurer les filtres de réception pour un périmètre

Étape 1
Cliquez sur Mes Périmètres





Étape 2
Cliquez sur Préférences

Étape 3
Vous pouvez ici filtrer les bulletins techniques par criticité ou par type.

Ces filtres concerneront tous les utilisateurs du périmètre.

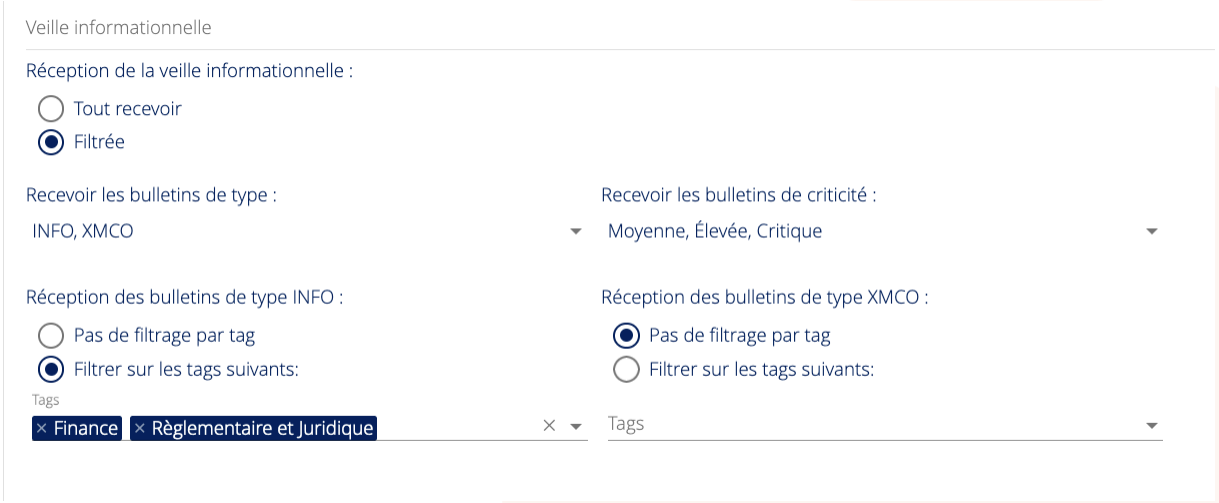
Étape 4
Vous pouvez ici choisir de générer des tickets d'action (selon le type ou la criticité des bulletins) afin d'alimenter le plan d'action associé à ce périmètre lors de la publication d'un bulletin de Veille.

Vous pouvez retrouver vos tickets d'action et suivre leur évolution dans le menu Plan d'Action, ou directement dans Mon plan d'action dans le menu latéral.

Exemple de configuration (1/2)

D'après mes préférences ci-contre, je vais recevoir tous les bulletins de veille environnementale de type INFO et XMCO, et disposant des criticités « moyenne, élevée et alerte ».

Pour les bulletins de type INFO, je ne recevrai que les bulletins disposant des tags Finace ou Juridique.

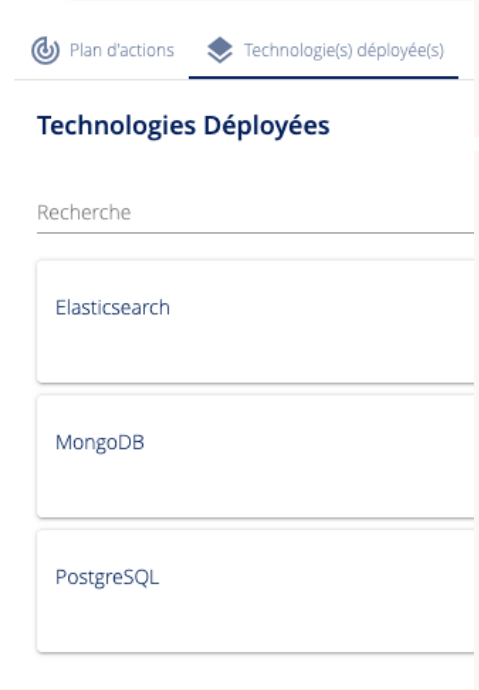


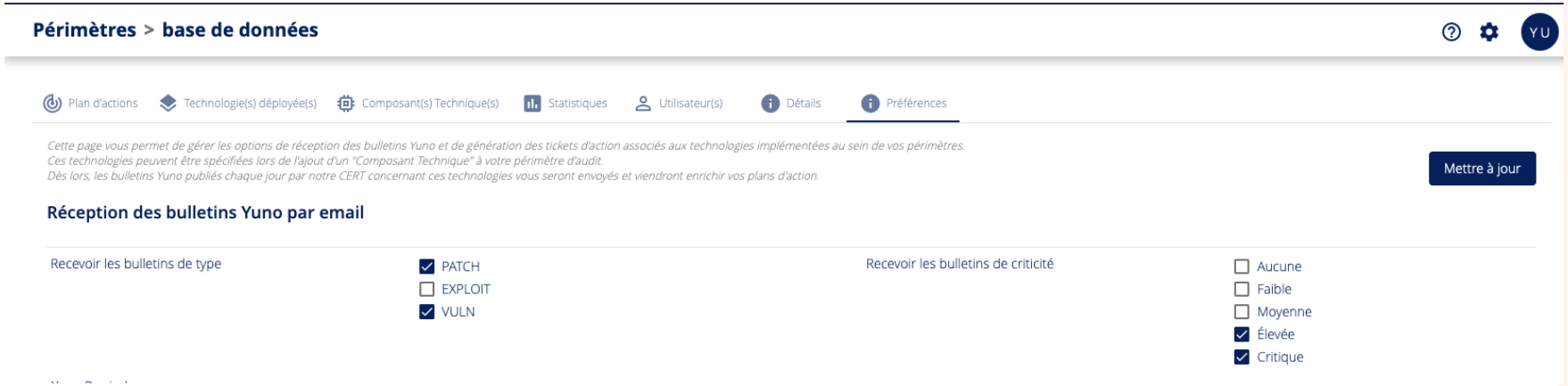
D'après mes préférences, la réception de bulletins techniques suit les paramètres définis au sein de mes périmètres. C'est donc les périmètres auxquels je suis associé qui vont déterminer la liste des bulletins techniques que je vais recevoir.

Exemple de configuration (2/2)

Je fais partie du périmètre « base de données » qui recense 3 technologies (Elasticsearch, MongoDB et PostgreSQL).

Je recevrai donc uniquement des bulletins techniques faisant référence à ces 3 technologies.

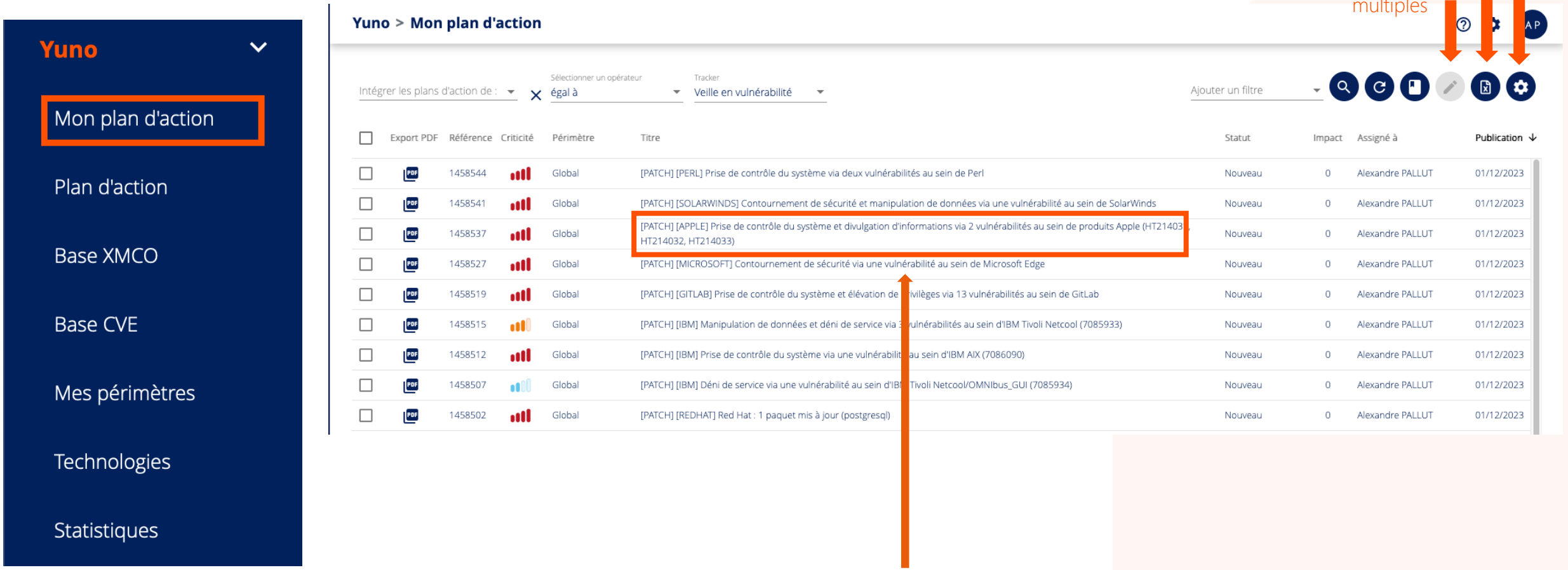




Les préférences de mon périmètre « base de données » indiquent que je vais recevoir les bulletins techniques de type PATCH ou VULN et disposant des criticités Élevée ou Alerte.

Consulter le plan d'action

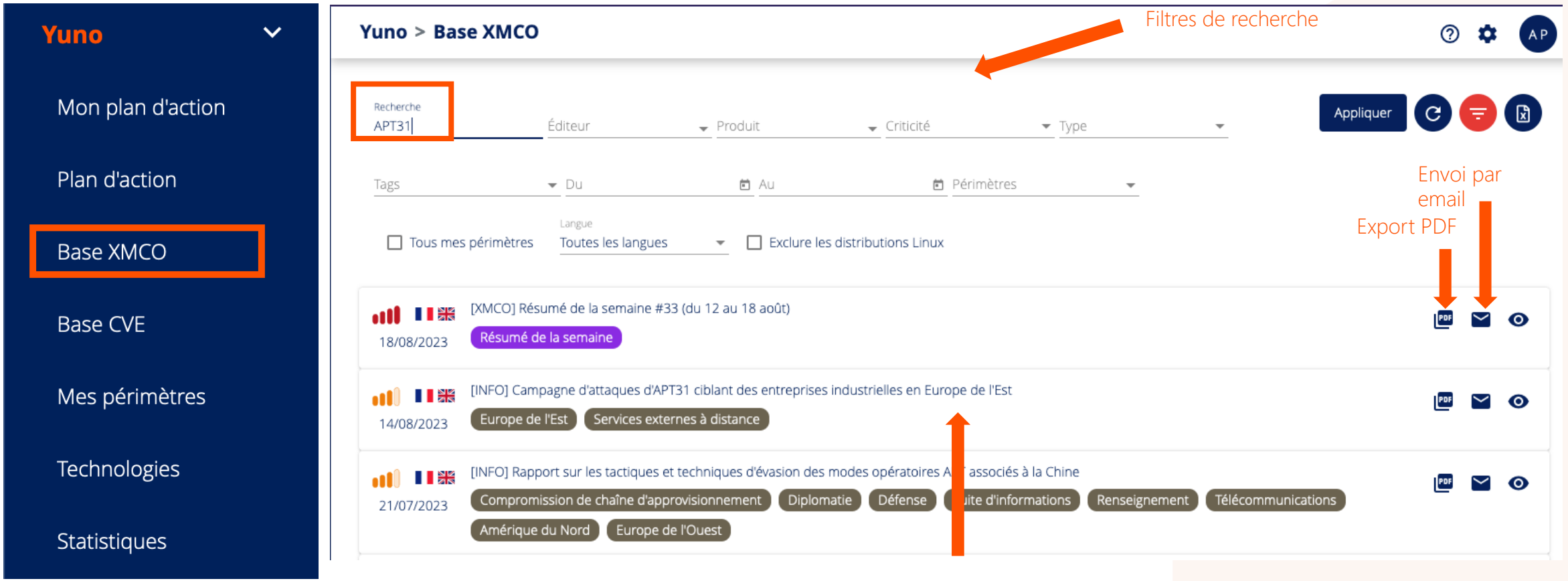
Le plan d'action vous permet d'accéder à l'ensemble des bulletins émis par le CERT-XMCO depuis le lancement du service de veille.



Cliquez sur le titre pour consulter l'action

Consulter la base XMCO

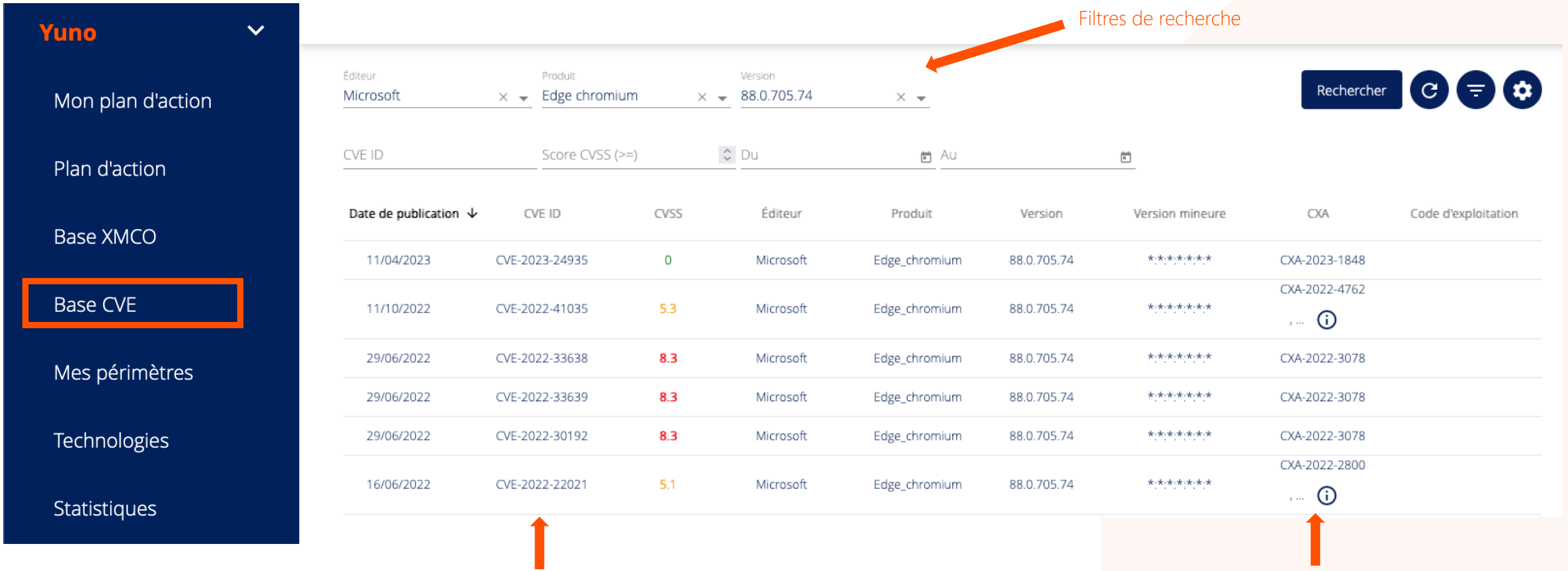
La base XMCO vous permet d'accéder à l'ensemble des bulletins émis par le CERT-XMCO depuis le lancement du service de veille.



Cliquez sur le titre pour consulter le bulletin en ligne

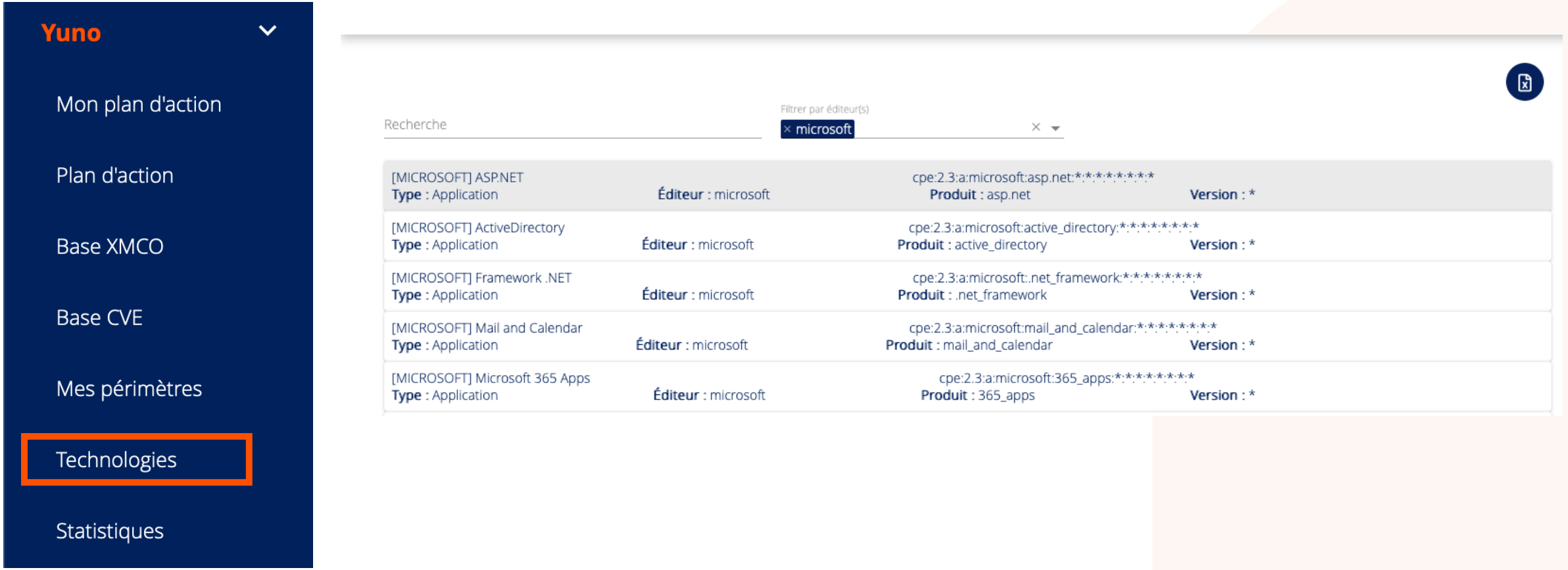
Consulter la base CVE

La base CVE vous permet de rechercher les vulnérabilités associées à une version spécifique d'une technologie, ainsi que les bulletins XMCO ayant traité ces vulnérabilités.



Technologies surveillées par le CERT-XMCO

La page des technologies vous permet de naviguer parmi l'ensemble des technologies et éditeurs suivis par le CERT-XMCO dans le cadre du service de veille.



Consulter les statistiques

La page des statistiques vous permet d'obtenir des informations et KPI sur les bulletins reçus durant une période donnée