yuno Module

By xmco

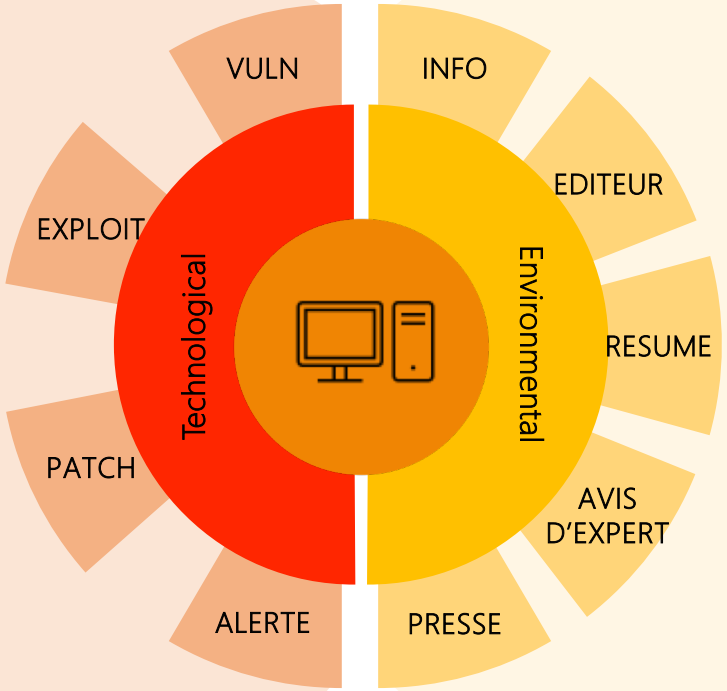
Management of your cyber-security watch

yuno : A 360° cybersecurity watch

I know which vulnerability to adress first

&

My IS is always up to date



I have got a global vision of the cyber threats

&

I enrich my decision making considering the attackant groups activity

- Qualified and exploitable cyberwatch
- Standardised vocabulary
- Remediation management tool
- EN/FR Bulletins

Types of bulletins

The CERT-XMCO offers 2 types of monitoring.

Technical watch

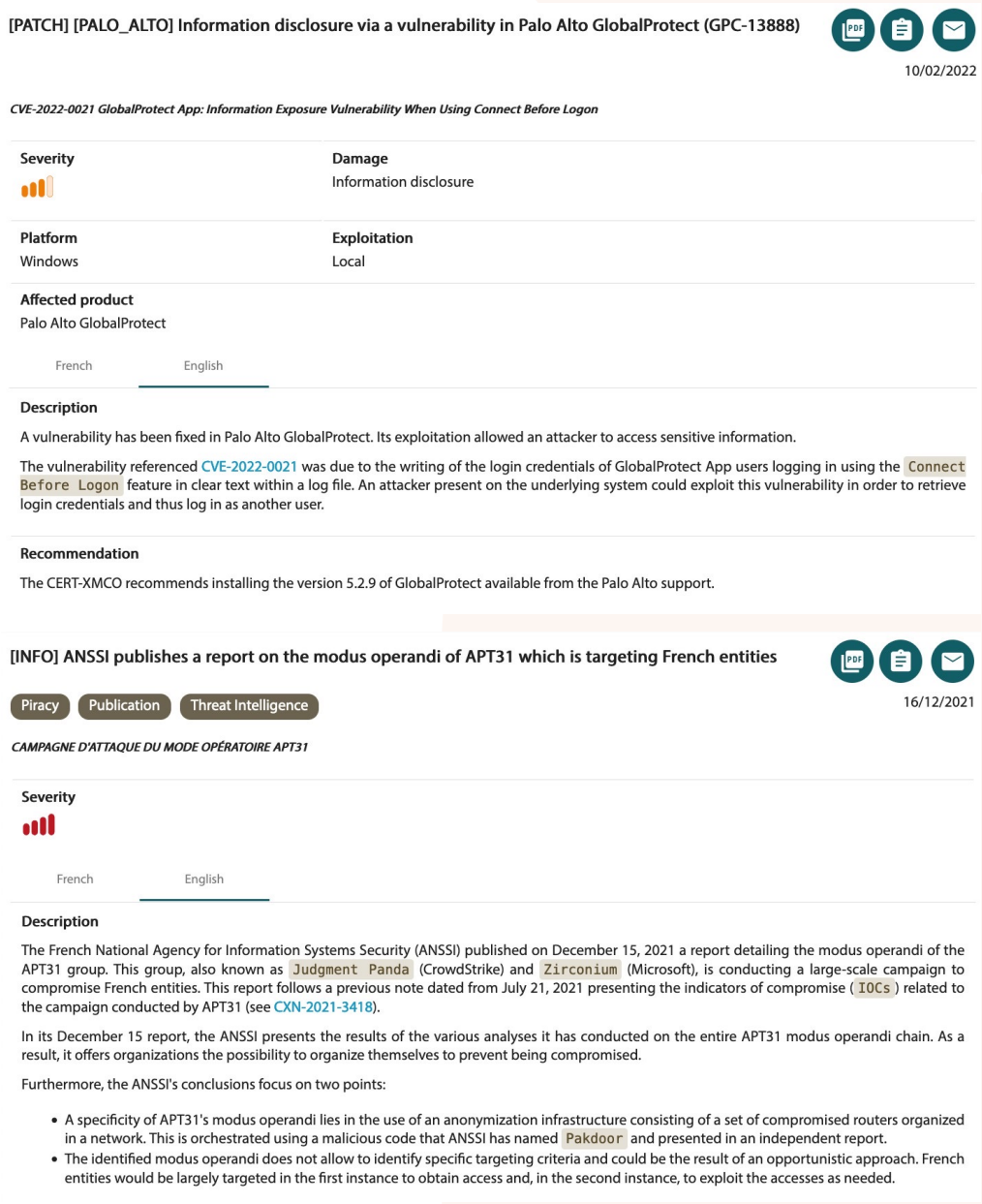
Bulletins are associated with products/technologies:

- the discovery of vulnerabilities ;
- publication of patches;
- publication of exploit codes.

Environmental watch

Bulletins are not associated with products/technologies. They deal with:

- cyber security news;
- publications by researchers
- current attack campaigns;
- CERT-XMCO management bulletins;
- ...



[PATCH] [PALO_ALTO] Information disclosure via a vulnerability in Palo Alto GlobalProtect (GPC-13888)

10/02/2022

CVE-2022-0021 GlobalProtect App: Information Exposure Vulnerability When Using Connect Before Logon

Severity

Damage
Information disclosure

Platform
Windows

Exploitation
Local

Affected product
Palo Alto GlobalProtect

French English

Description

A vulnerability has been fixed in Palo Alto GlobalProtect. Its exploitation allowed an attacker to access sensitive information.

The vulnerability referenced CVE-2022-0021 was due to the writing of the login credentials of GlobalProtect App users logging in using the `Connect Before Logon` feature in clear text within a log file. An attacker present on the underlying system could exploit this vulnerability in order to retrieve login credentials and thus log in as another user.

Recommendation

The CERT-XMCO recommends installing the version 5.2.9 of GlobalProtect available from the Palo Alto support.

[INFO] ANSSI publishes a report on the modus operandi of APT31 which is targeting French entities

Piracy Publication Threat Intelligence

16/12/2021

CAMPAGNE D'ATTAQUE DU MODE OPÉRATOIRE APT31

Severity

French English

Description

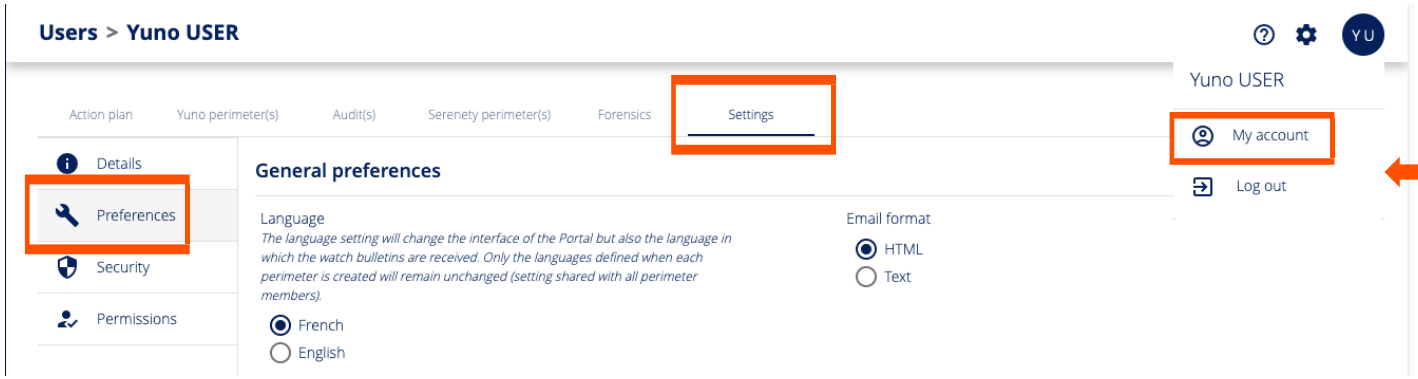
The French National Agency for Information Systems Security (ANSSI) published on December 15, 2021 a report detailing the modus operandi of the APT31 group. This group, also known as `Judgment Panda` (CrowdStrike) and `Zirconium` (Microsoft), is conducting a large-scale campaign to compromise French entities. This report follows a previous note dated from July 21, 2021 presenting the indicators of compromise (`IOCs`) related to the campaign conducted by APT31 (see CXN-2021-3418).

In its December 15 report, the ANSSI presents the results of the various analyses it has conducted on the entire APT31 modus operandi chain. As a result, it offers organizations the possibility to organize themselves to prevent being compromised.

Furthermore, the ANSSI's conclusions focus on two points:

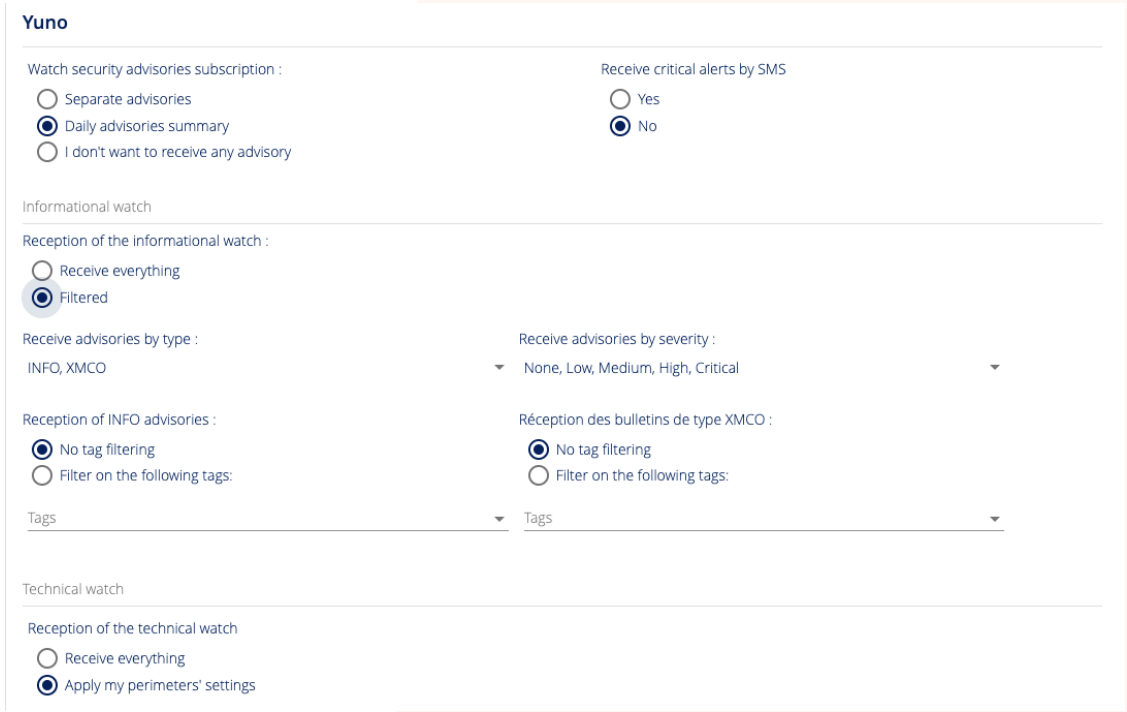
- A specificity of APT31's modus operandi lies in the use of an anonymization infrastructure consisting of a set of compromised routers organized in a network. This is orchestrated using a malicious code that ANSSI has named `Pakdoor` and presented in an independent report.
- The identified modus operandi does not allow to identify specific targeting criteria and could be the result of an opportunistic approach. French entities would be largely targeted in the first instance to obtain access and, in the second instance, to exploit the accesses as needed.

Configure the reception parameters



Step 1
Click on the top right menu, then My Account and finally Preferences.

Step 2
Define the parameters related to technical and informational intelligence



Environmental Watch

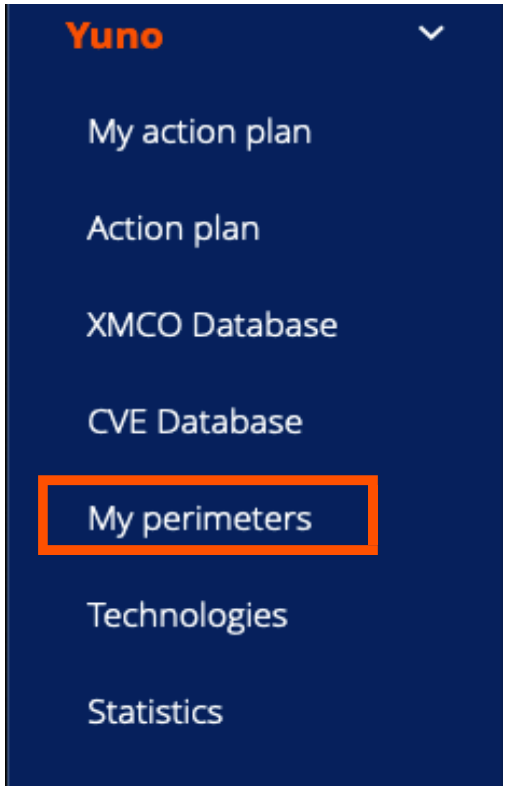
Choose to receive all newsletters, or use the filters to restrict newsletters by criticality, type, or specific tags.

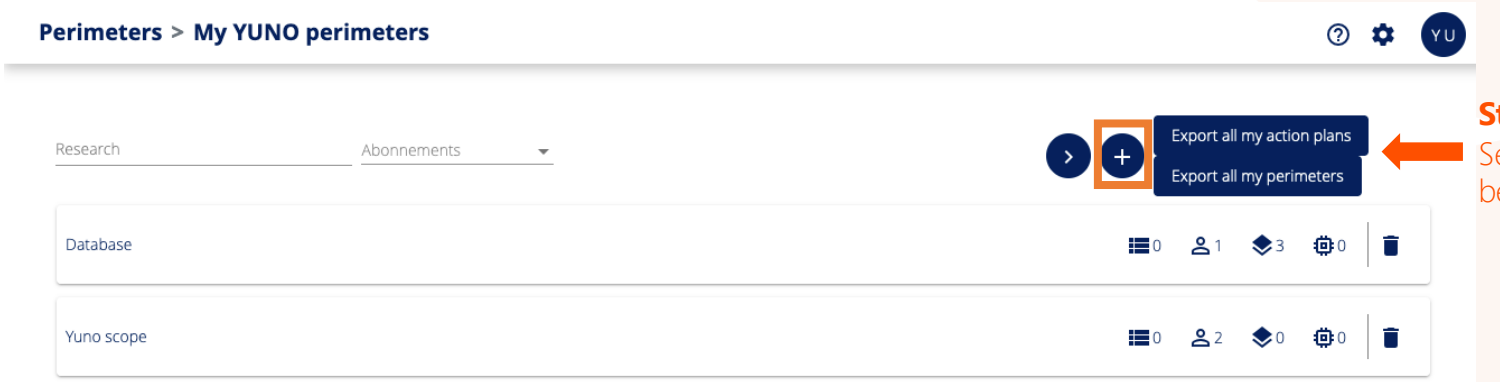
Technical Watch

Choose to receive all technical bulletins, or choose to receive only the bulletins concerning your perimeters. You will need to be part of at least 1 perimeter to receive technical bulletins.

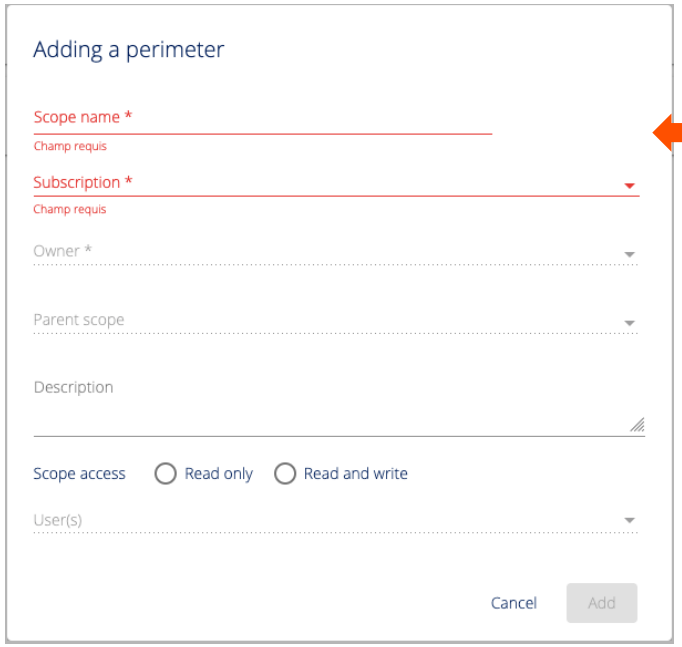
Create a perimeter

Step 1
Click on My Perimeters





Step 2
Select the perimeter to be modified



Step 3
Fill in the available fields and click **add** to confirm the creation.

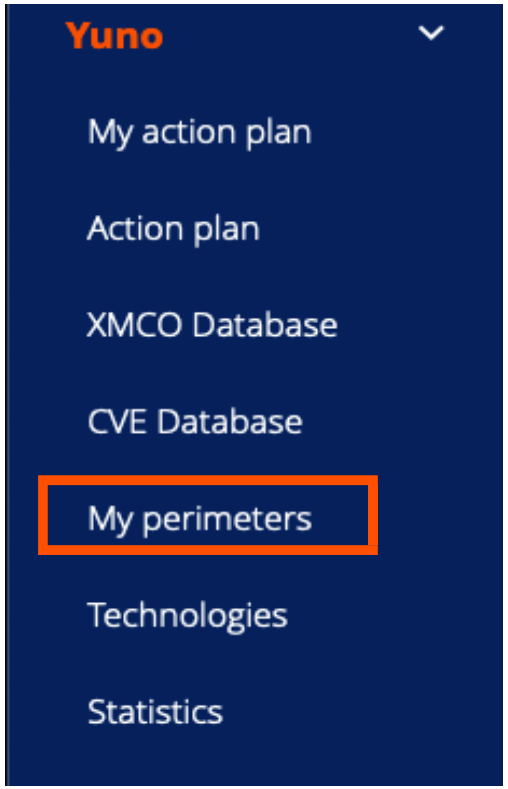
Users added to the scope will receive bulletins about the technologies associated with that scope.

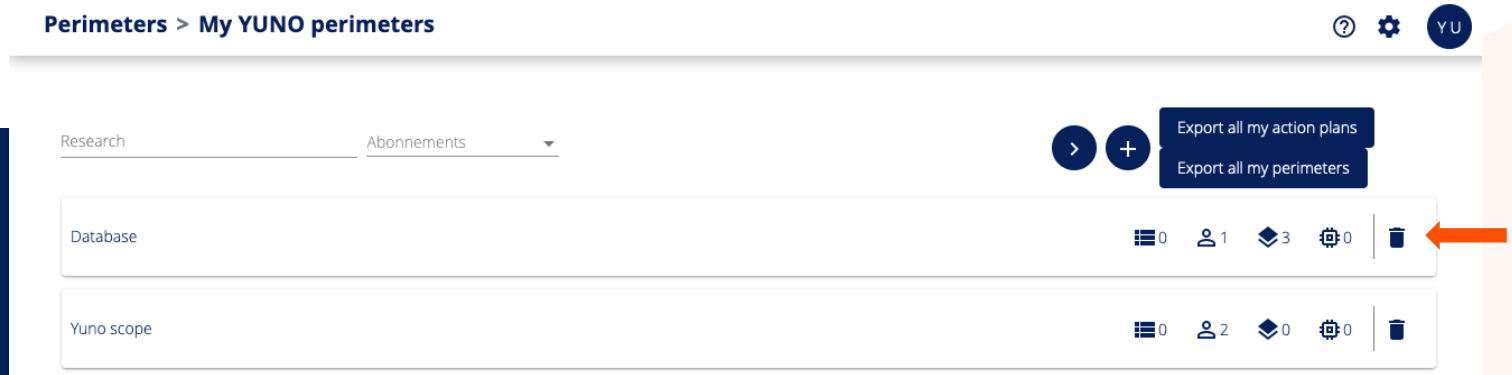
Users with "read/write" access will be able to remove any technologies or add new ones.
This action will not be possible for a user with "read only" mode.

A scope is a collection of technologies and users who wish to monitor them.

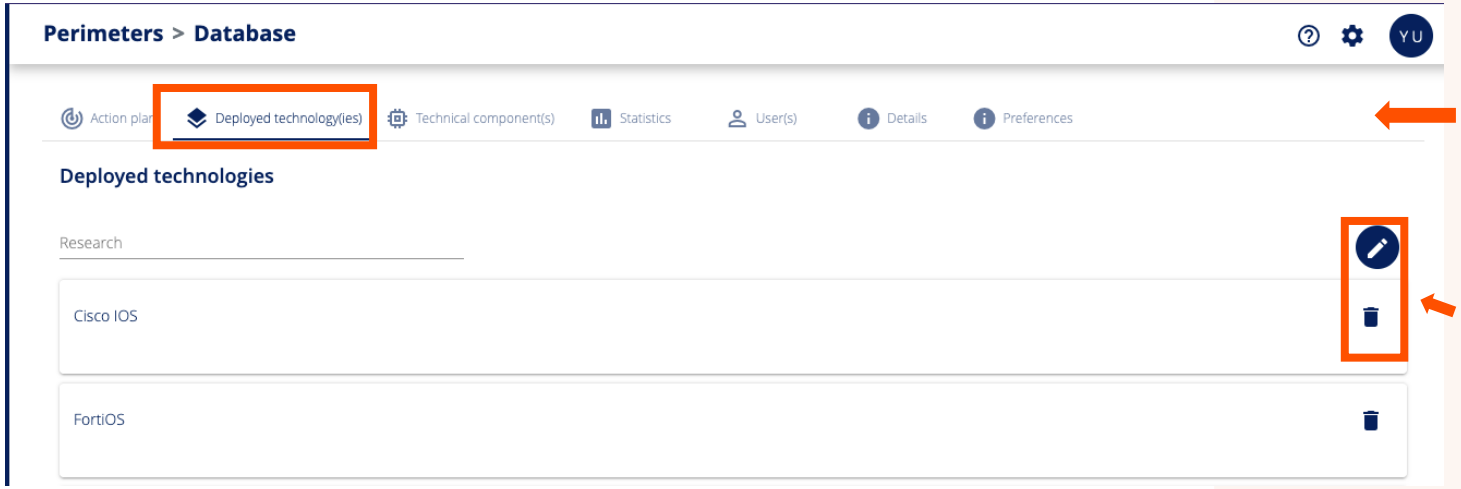
Adding technologies to follow in a perimeter

Step 1
Click on My Perimeters





Step 2
Select the perimeter to be modified

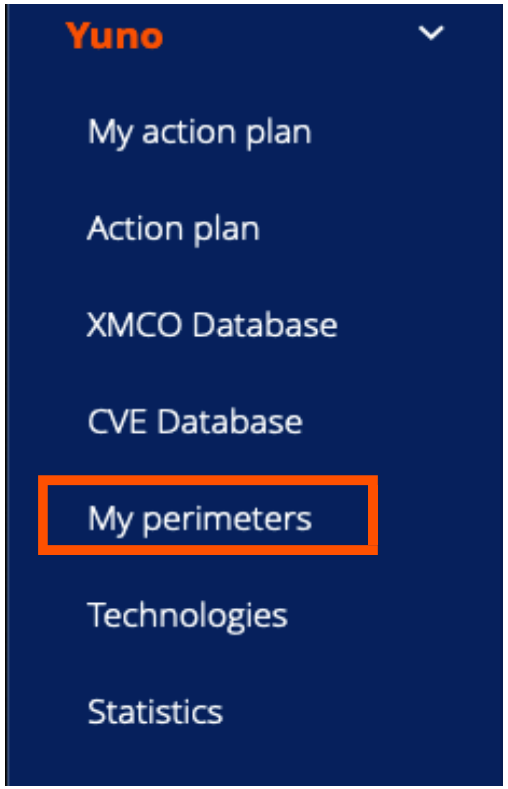


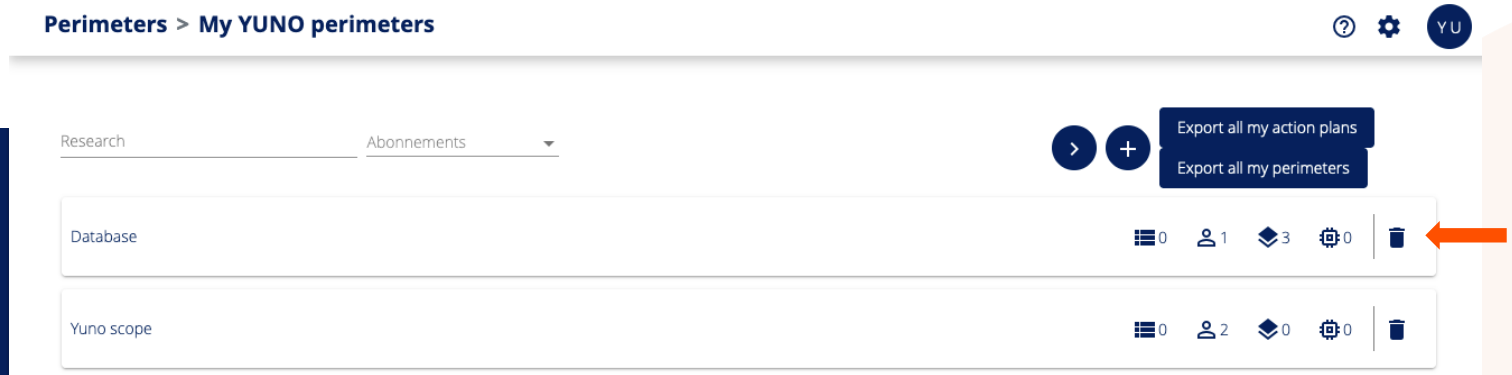
Step 3
You can access the list of technologies associated with your scope via the "Deployed Technologies" tab.

Step 4
Click here to add or remove one or more technologies.

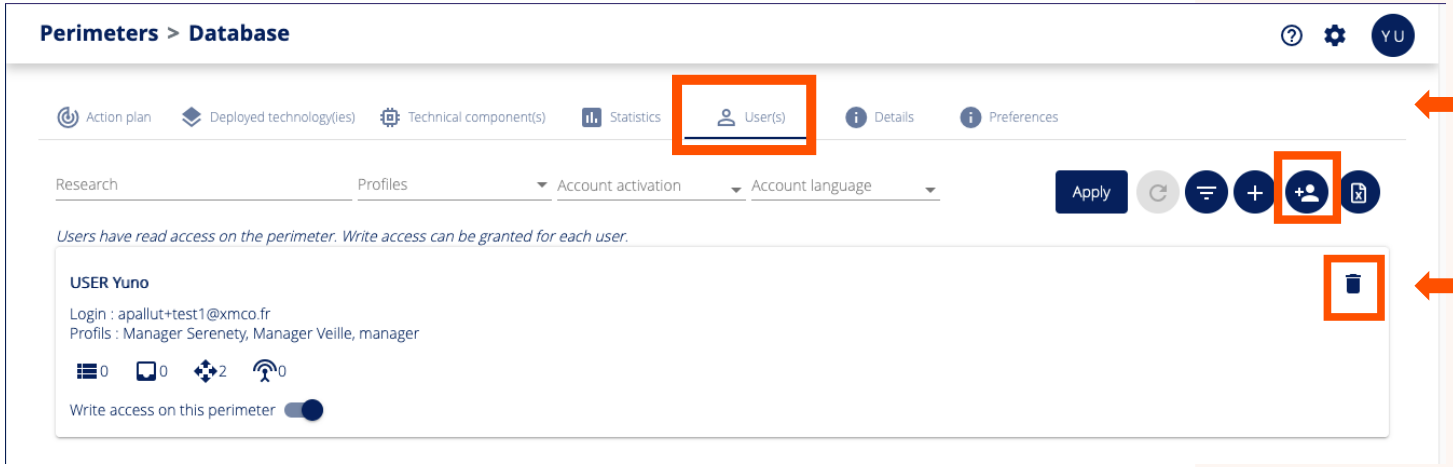
Adding users to a perimeter

Step 1
Click on My Perimeters





Step 2
Select the perimeter to be modified

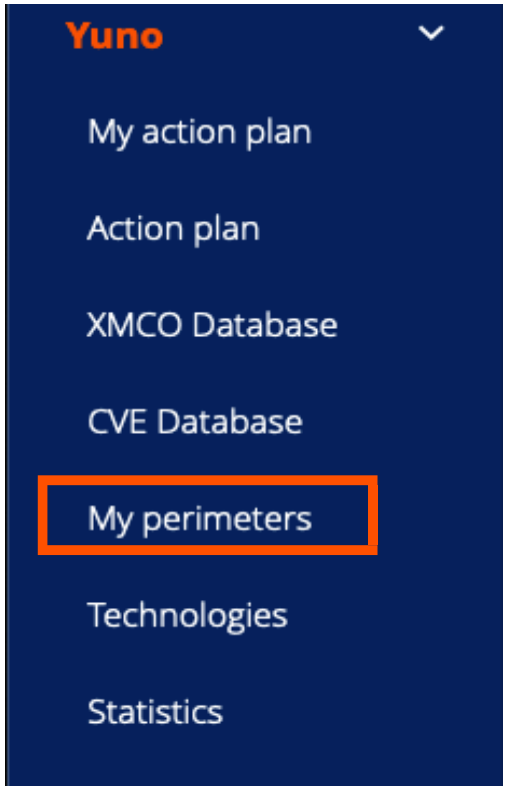


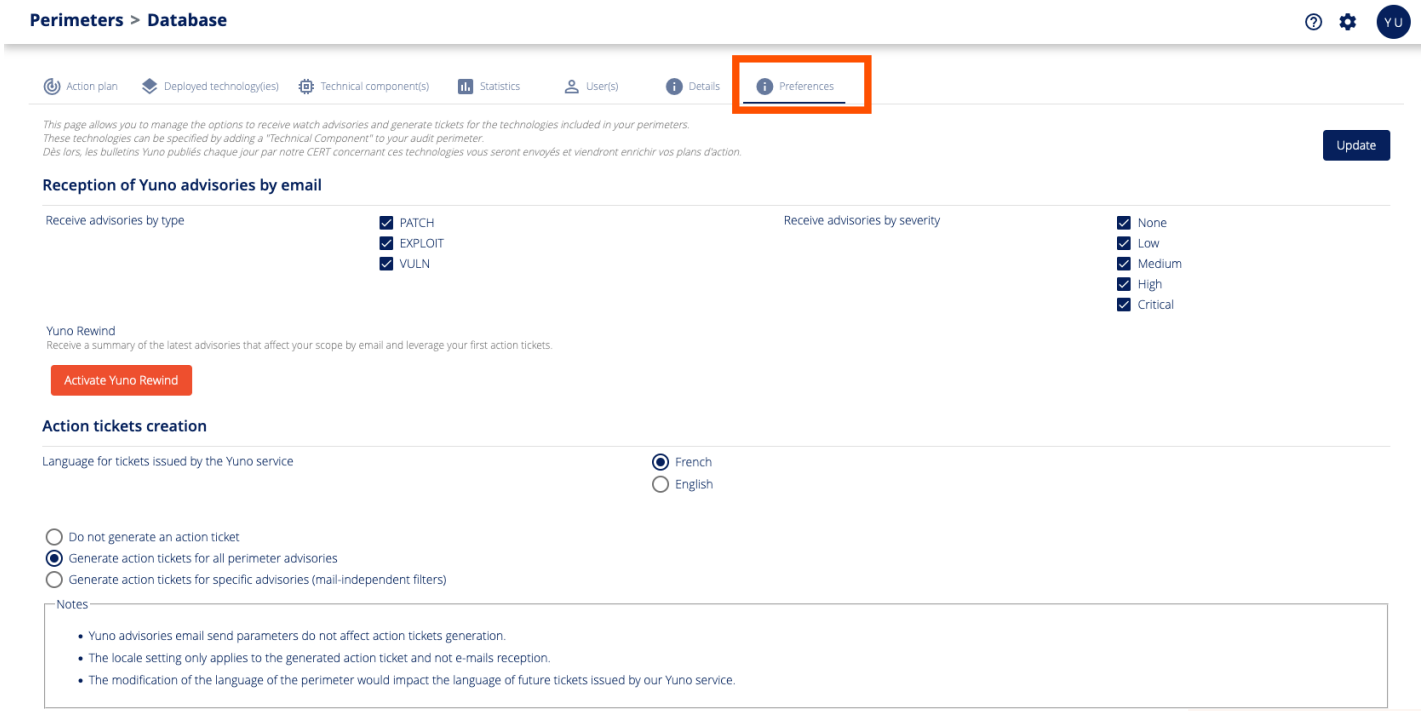
Step 3
Click on the Users tab

Step 4
Click here to add or remove users.

Configure the reception filters for a perimeter

Step 1
Click on My Perimeters





Step 2
Click on Preferences

Step 3
You can filter the technical bulletins by criticality or by type.

These filters will affect all users in the scope.

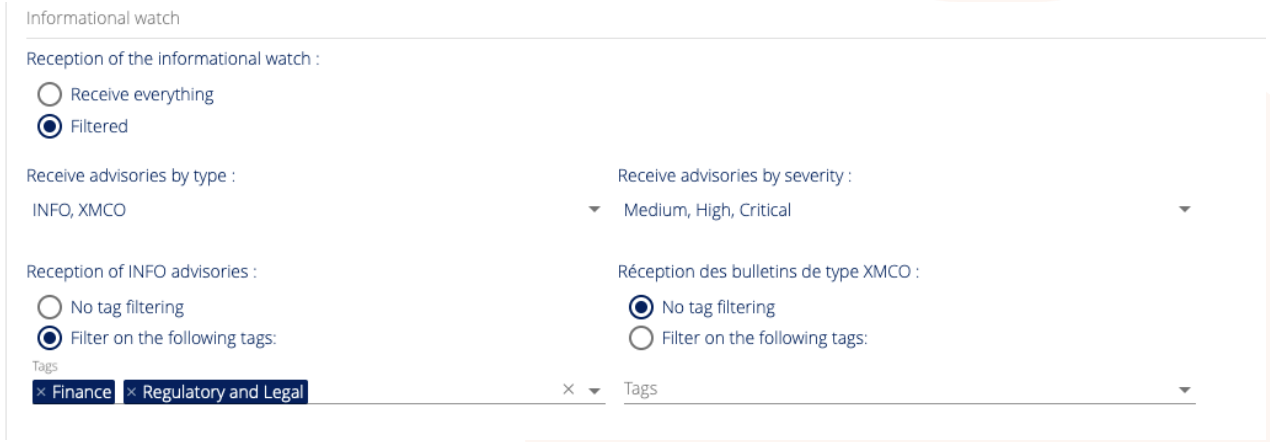
Step 4
Here you can choose to generate action tickets (depending on the type or criticality of the bulletins) in order to feed the action plan associated with this scope when a Watch bulletin is published.

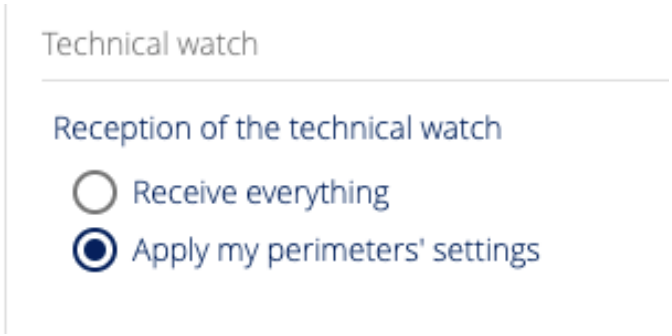
You can find your action tickets and follow their evolution in the Action Plan tab, or directly in My Action Plan in the side menu.

Example of configuration (1/2)

According to my preferences on the left, I will receive all INFO and XMCO newsletters with the criticality "medium, high and alert".

For INFO bulletins, I will only receive bulletins with the tags Finance or Legal.



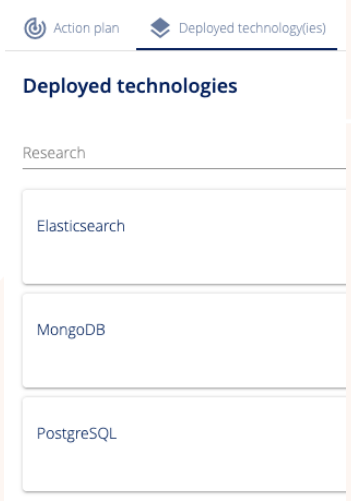


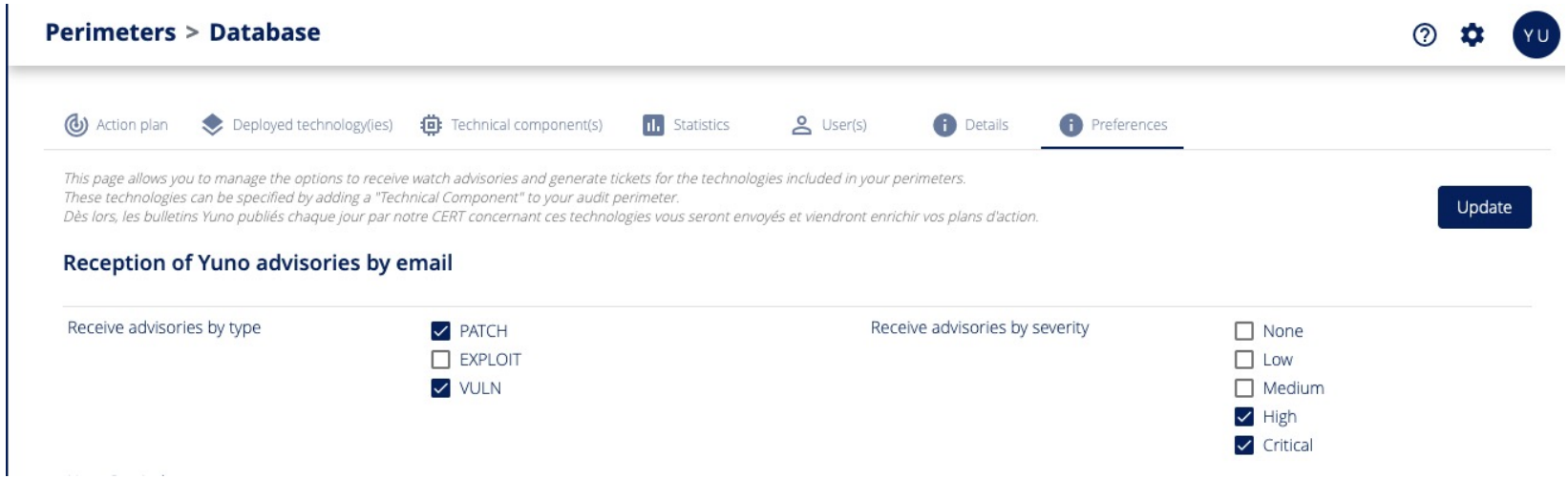
According to my preferences, the reception of technical bulletins follows the parameters defined within my perimeters.
The perimeters I am associated with will determine the list of technical bulletins I will receive.

Example of configuration (2/2)

I am part of the "database" perimeter which includes 3 technologies (Elasticsearch, MongoDB and PostgreSQL).

I will therefore only receive technical bulletins referring to these 3 technologies.





My "database" perimeter preferences indicate that I will receive technical bulletins of type PATCH or VULN and with High or Alert criticalities.

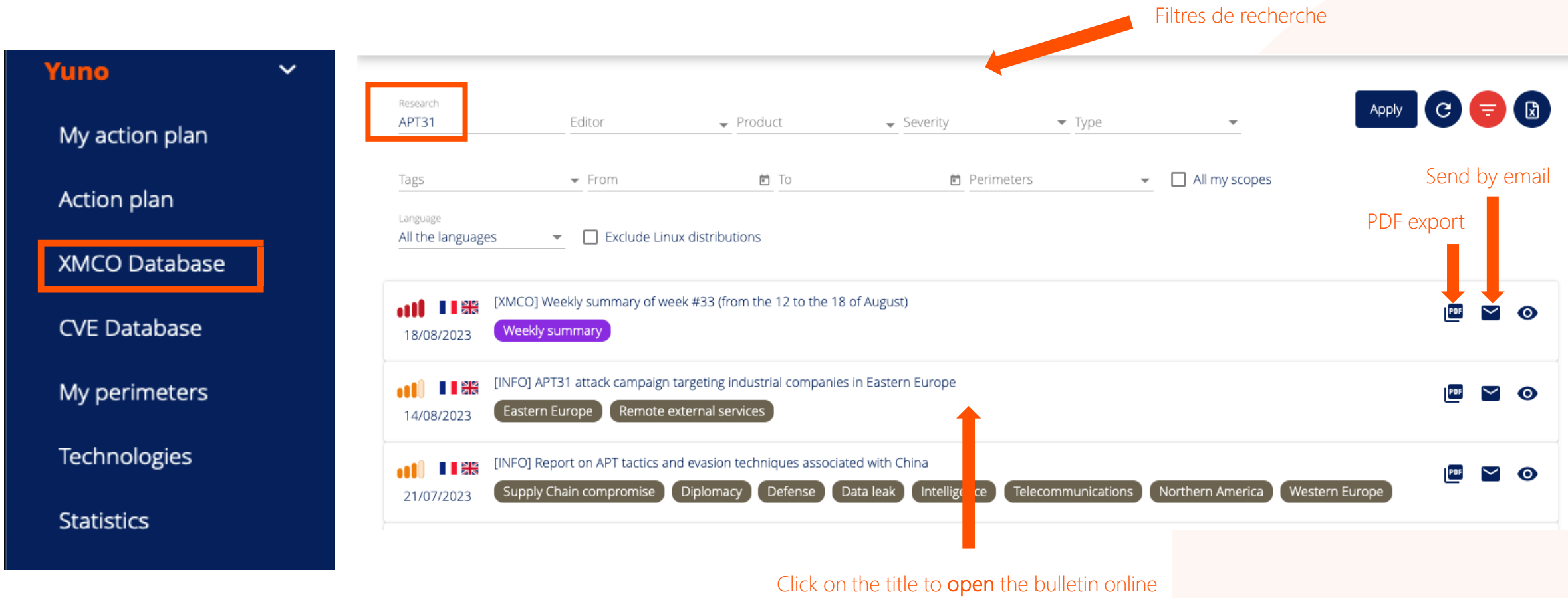
Consult the action plan

The action plan gives you access to all bulletins issued by CERT-XMCO since the launch of the monitoring service

Click on the title to **view** the action ticket

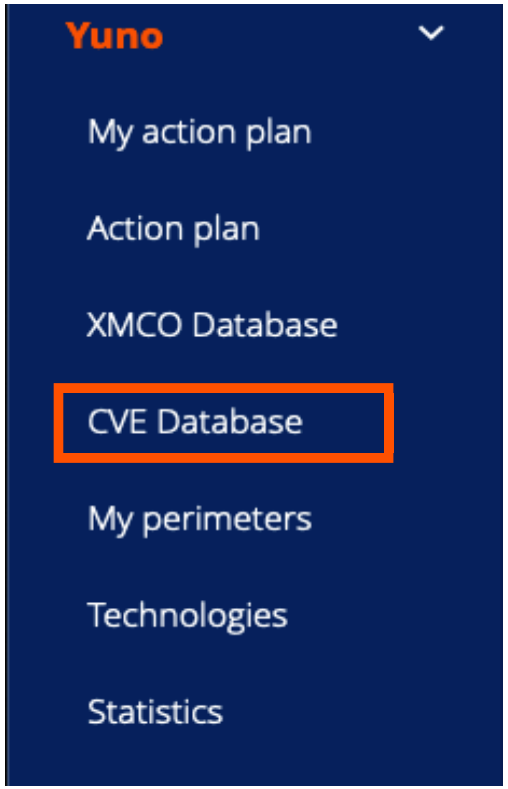
Consult the XMCO database

The XMCO database gives you access to all bulletins issued by the CERT-XMCO since the launch of the monitoring service.



Consult the CVE database

The CVE database allows you to search for vulnerabilities associated with a specific version of a technology, as well as XMCO bulletins that have addressed those vulnerabilities.



Search filters

Editor: Microsoft | Product: Edge chromium | Version: 88.0.705.74 | Search

CVE ID | Score CVSS (>=) | From | To

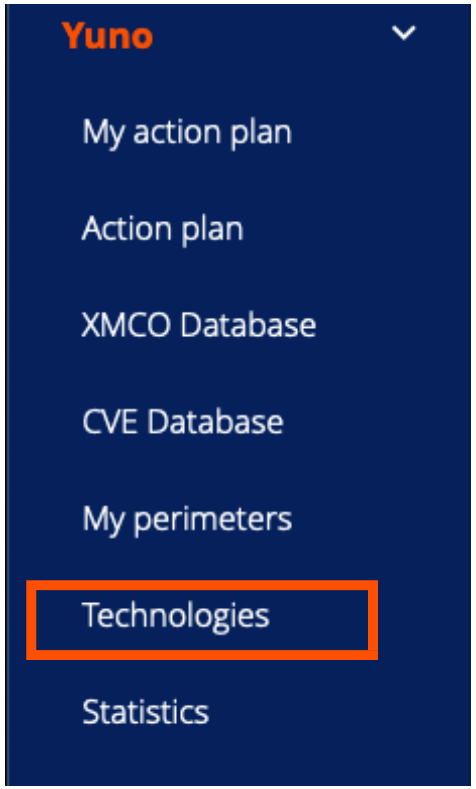
Publication date	CVE ID	CVSS	Editor	Product	Version	Minor version	CXA	Exploitation code
11/04/2023	CVE-2023-24935	0	Microsoft	Edge_chromium	88.0.705.74	*.*.*.*.*.*	CXA-2023-1848	
11/10/2022	CVE-2022-41035	5.3	Microsoft	Edge_chromium	88.0.705.74	*.*.*.*.*.*	CXA-2022-4762 , ...	
29/06/2022	CVE-2022-33638	8.3	Microsoft	Edge_chromium	88.0.705.74	*.*.*.*.*.*	CXA-2022-3078	
29/06/2022	CVE-2022-33639	8.3	Microsoft	Edge_chromium	88.0.705.74	*.*.*.*.*.*	CXA-2022-3078	
29/06/2022	CVE-2022-30192	8.3	Microsoft	Edge_chromium	88.0.705.74	*.*.*.*.*.*	CXA-2022-3078	
16/06/2022	CVE-2022-22021	5.1	Microsoft	Edge_chromium	88.0.705.74	*.*.*.*.*.*	CXA-2022-2800 , ...	
01/06/2022	CVE-2022-30128	8.3	Microsoft	Edge_chromium	88.0.705.74	*.*.*.*.*.*	CXA-2022-2688	

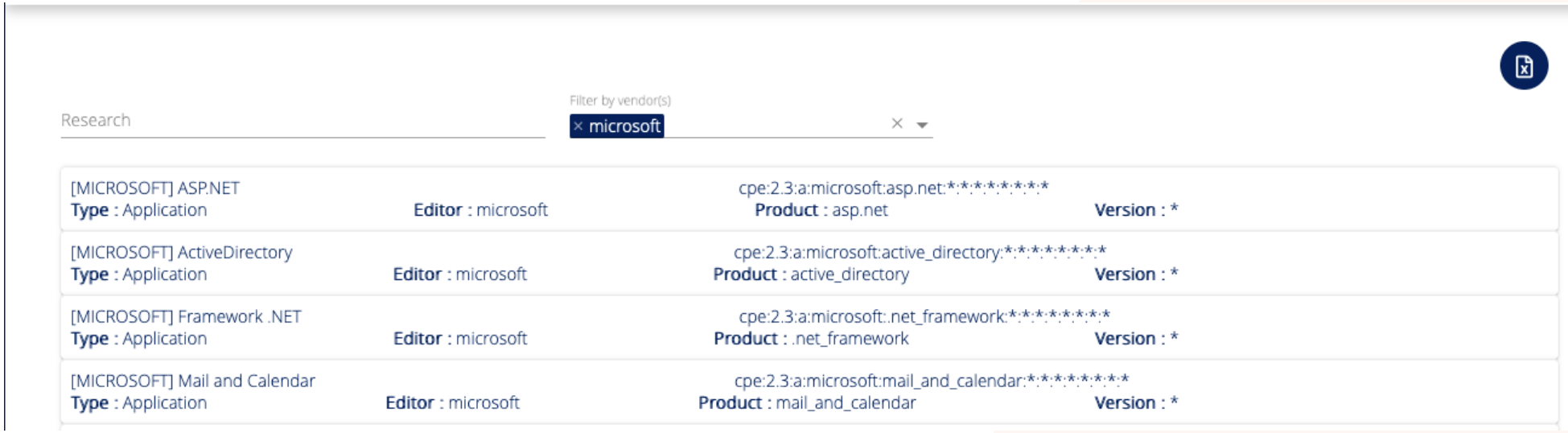
The CVE vulnerabilities come from the official MITRE database

Associated XMCO bulletins

Technologies monitored by the CERT-XMCO

The Technologies database allows you to browse all the products and vendors monitored by the CERT-XMCO for the cyber-security watch service.





Consult the statistics

The statistics page allows you to obtain information and KPIs on the bulletins received during a given period.