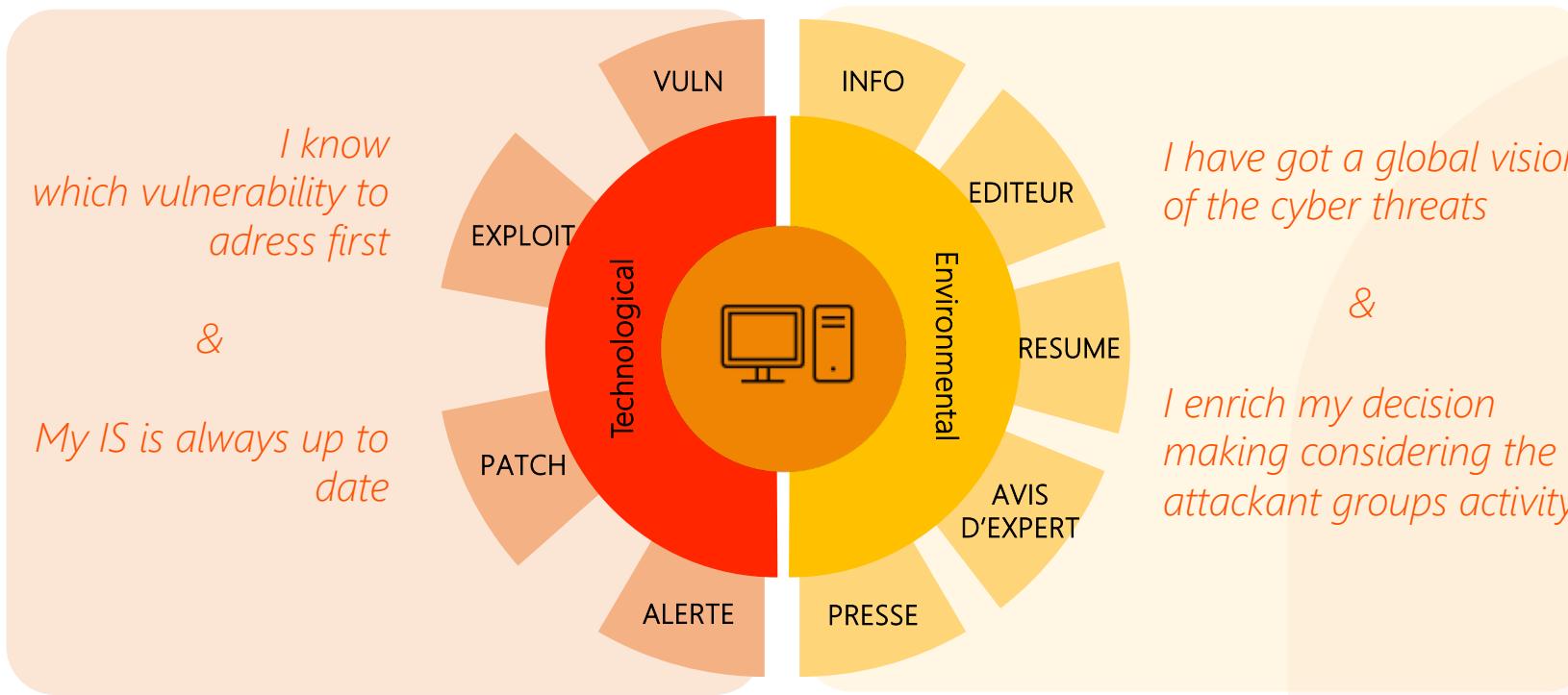


# yuno Module

*By* **xmco**

Management of your cyber-security watch

# yuno : A 360° cybersecurity watch



✓ 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.



[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*

<b>Severity</b>	<b>Damage</b>
	Information disclosure
<b>Platform</b>	<b>Exploitation</b>
Windows	Local
<b>Affected product</b>	
Palo Alto GlobalProtect	
French	English
<b>Description</b>	
A vulnerability has been fixed in Palo Alto GlobalProtect. Its exploitation allowed an attacker to access sensitive information.	
The vulnerability referenced <a href="#">CVE-2022-0021</a> was due to the writing of the login credentials of GlobalProtect App users logging in using the <a href="#">Connect Before Logon</a> 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.	
<b>Recommendation</b>	
The CERT-XMCO recommends installing the version 5.2.9 of GlobalProtect available from the Palo Alto support.	

## 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;
- ...

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



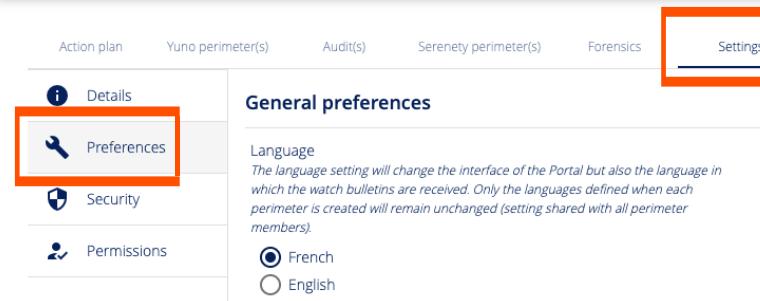
16/12/2021

*CAMPAGNE D'ATTAQUE DU MODE OPÉATOIRE APT31*

<b>Severity</b>	
French	English
<b>Description</b>	
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 <a href="#">Judgment Panda</a> (CrowdStrike) and <a href="#">Zirconium</a> (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 ( <a href="#">IOCs</a> ) related to the campaign conducted by APT31 (see <a href="#">CXN-2021-3418</a> ).	
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:	
<ul style="list-style-type: none"><li>• 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 <a href="#">Pakdoor</a> and presented in an independent report.</li><li>• 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.</li></ul>	

# Configure the reception parameters

Users > Yuno USER



Action plan   Yuno perimeter(s)   Audit(s)   Serenity perimeter(s)   Forensics   **Settings**

**General preferences**

Language  
The language setting will change the interface of the Portal but also the language in which the watch bulletins are received. Only the languages defined when each perimeter is created will remain unchanged (setting shared with all perimeter members).

French  
 English

Email format  
 HTML  
 Text

Details  
Preferences (highlighted)  
Security  
Permissions

## Step 2

Define the parameters related to technical and informational intelligence

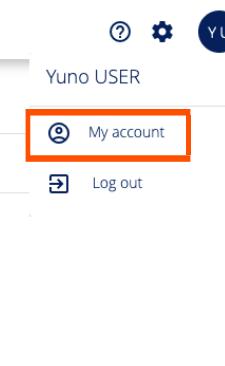


### Environmental Watch

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.

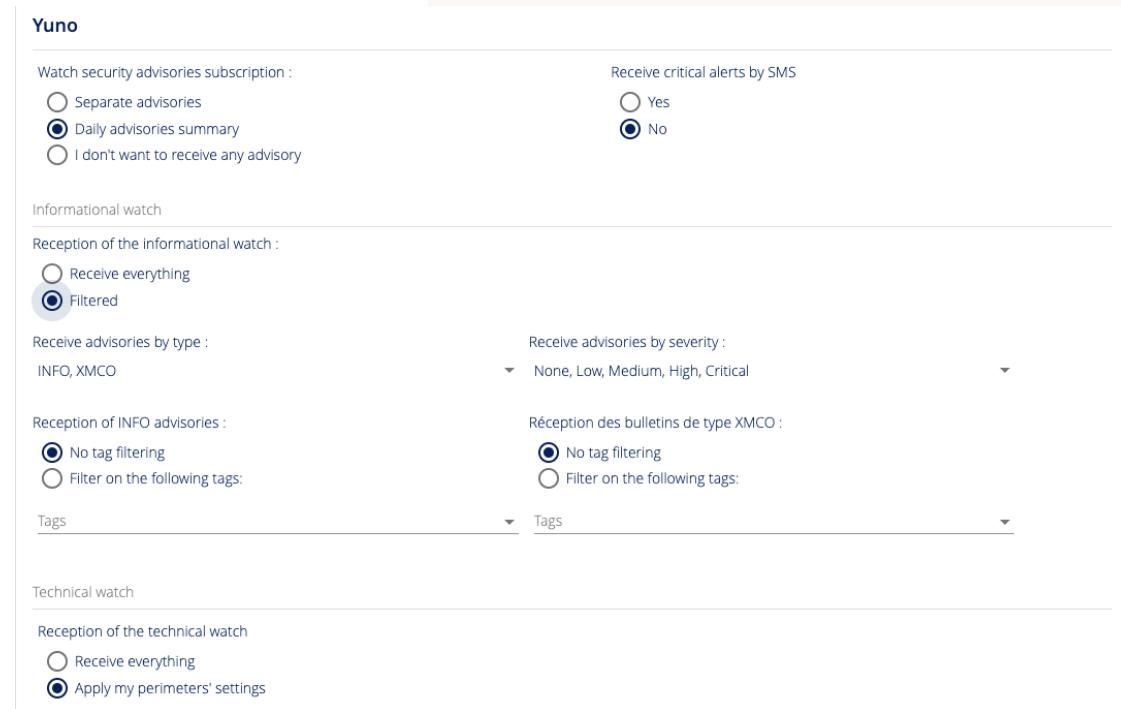


Yuno USER

My account (highlighted)  
Log out

## Step 1

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



Yuno

Watch security advisories subscription :  
 Separate advisories  
 Daily advisories summary  
 I don't want to receive any advisory

Receive critical alerts by SMS  
 Yes  
 No

Informational watch

Reception of the informational watch :  
 Receive everything  
 Filtered

Receive advisories by type :  
INFO, XMCO

Receive advisories by severity :  
None, Low, Medium, High, Critical

Reception of INFO advisories :  
 No tag filtering  
 Filter on the following tags:

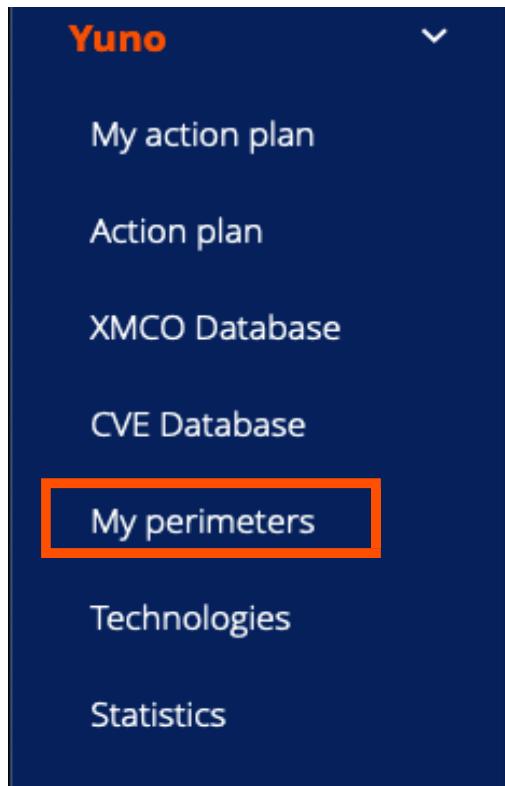
Réception des bulletins de type XMCO :  
 No tag filtering  
 Filter on the following tags:

Tags

Technical watch

Reception of the technical watch  
 Receive everything  
 Apply my perimeters' settings

# Create a perimeter



Perimeters > My YUNO perimeters

Research Abonnements

Database Yuno scope

Export all my action plans Export all my perimeters

My action plan

Adding a perimeter

Scope name \* Champ requis

Subscription \* Champ requis

Owner \*

Parent scope

Description

Scope access  Read only  Read and write

User(s)

Cancel Add

**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.

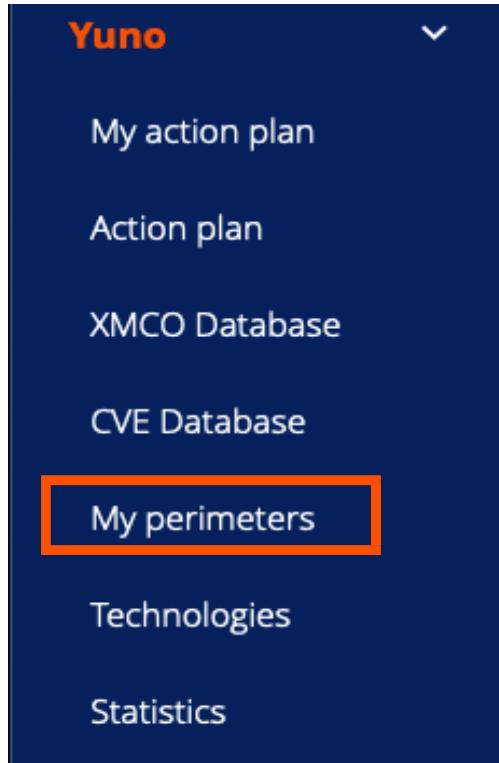


A **scope** is a collection of **technologies** and **users** who wish to monitor them.

# Adding technologies to follow in a perimeter

## Step 1

Click on My Perimeters



## Perimeters > My YUNO perimeters

Database	0	1	3	0	
Yuno scope	0	2	0	0	



Export all my action plans  
Export all 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.

## Perimeters > Database

Action plan	Deployed technology(ies)	Technical component(s)	Statistics	User(s)	Details	Preferences

### Deployed technologies

Research

Cisco IOS

Fortios

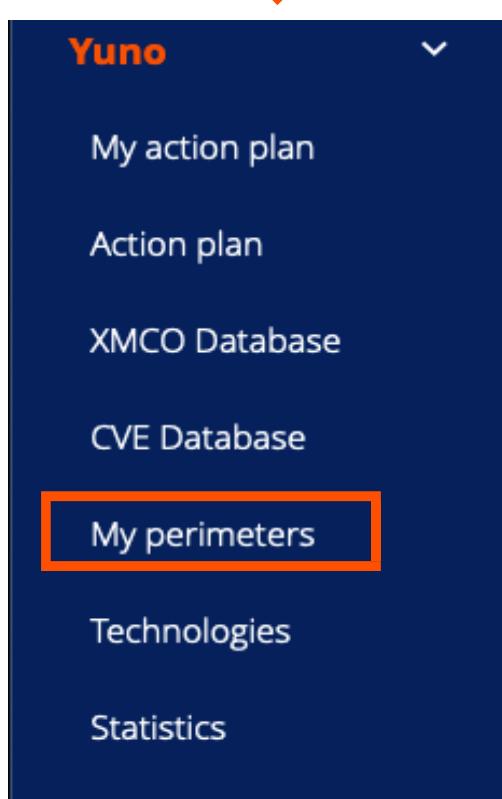


## Step 4

Click here to add or remove one or more technologies.

# Adding users to a perimeter

**Step 1**  
Click on My Perimeters



Perimeters > My YUNO perimeters

- Database
- Yuno scope

?

⚙

YU



Export all my action plans  
Export all my perimeters

0 1 3 0



0 2 0 0



Perimeters > Database

Action plan Deployed technology(ies) Technical component(s) Statistics



Details Preferences

?

⚙

YU

Apply



Research Profiles Account activation Account language

Users have read access on the perimeter. Write access can be granted for each user.

USER Yuno

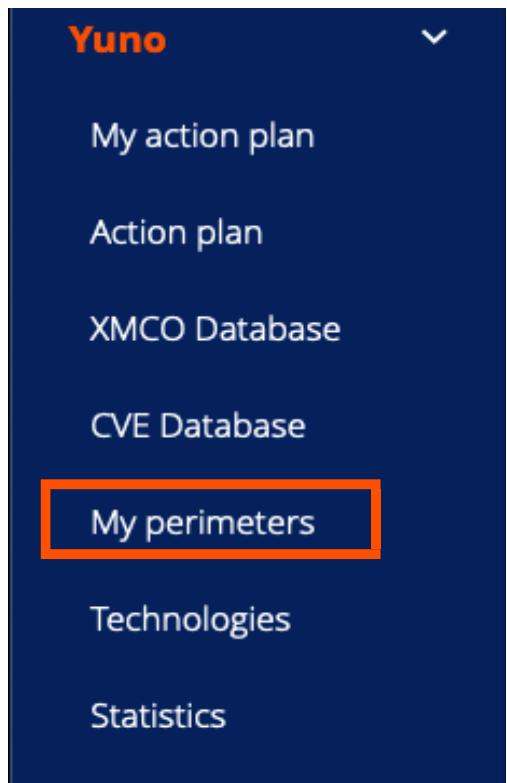
Login : apallut+test1@xmco.fr  
Profiles : Manager Serenety, Manager Veille, manager

0 0 2 0

Write access on this perimeter

# Configure the reception filters for a perimeter

**Step 1**  
Click on My Perimeters



**Perimeters > Database**

This page allows you to manage the options to receive watch advisories and generate tickets for the technologies included in your perimeters. These technologies can be specified by adding a "Technical Component" to your audit perimeter. Dès lors, les bulletins Yuno publiés chaque jour par notre CERT concernant ces technologies vous seront envoyés et viendront enrichir vos plans d'action.

**Reception of Yuno advisories by email**

Receive advisories by type:  PATCH,  EXPLOIT,  VULN

Receive advisories by severity:  None,  Low,  Medium,  High,  Critical

Yuno Rewind: Receive a summary of the latest advisories that affect your scope by email and leverage your first action tickets. [Activate Yuno Rewind](#)

**Action tickets creation**

Language for tickets issued by the Yuno service:  French,  English

Do not generate an action ticket  
 Generate action tickets for all perimeter advisories  
 Generate action tickets for specific advisories (mail-independent filters)

Notes:

- Yuno advisories email send parameters do not affect action tickets generation.
- The locale setting only applies to the generated action ticket and not e-mails reception.
- The modification of the language of the perimeter would impact the language of future tickets issued by our Yuno service.

**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**.

### Technical watch

#### Reception of the technical watch

- Receive everything
- Apply my perimeters' settings

Informational watch

Reception of the informational watch :

Receive everything  
 Filtered

Receive advisories by type :

INFO, XMCO

Receive advisories by severity :

Medium, High, Critical

Reception of INFO advisories :

No tag filtering  
 Filter on the following tags:

Tags

× Finance × Regulatory and Legal

× Tags

Réception des bulletins de type XMCO :

No tag filtering  
 Filter on the following tags:

Tags

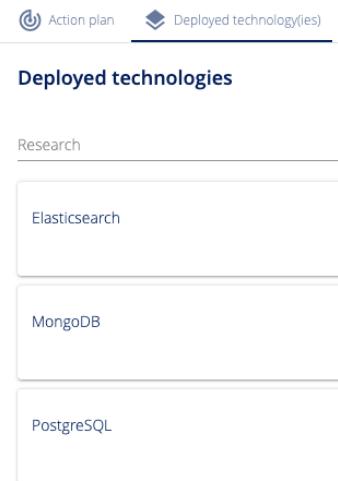
According to my preferences, the reception of technical bulletins follows the parameters defined within my perimeters.

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).

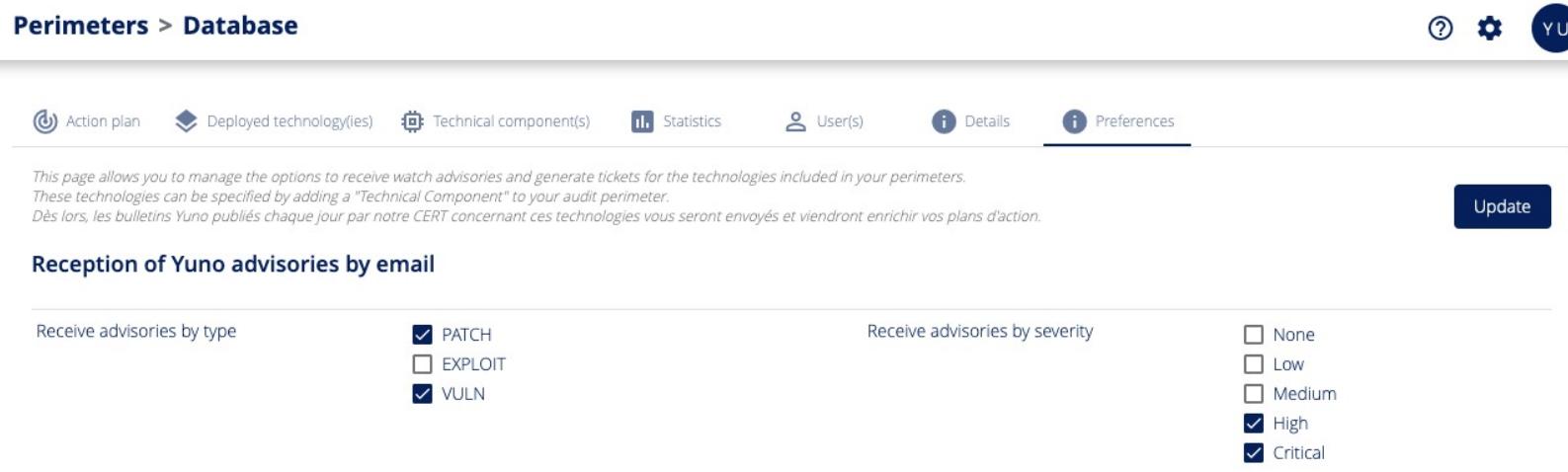
I will therefore **only receive technical bulletins** referring to these 3 technologies.



Deployed technologies

Research

- Elasticsearch
- MongoDB
- PostgreSQL



Perimeters > Database

Action plan Deployed technology(ies) Technical component(s) Statistics User(s) Details Preferences

This page allows you to manage the options to receive watch advisories and generate tickets for the technologies included in your perimeters. These technologies can be specified by adding a "Technical Component" to your audit perimeter. Dès lors, les bulletins Yuno publiés chaque jour par notre CERT concernant ces technologies vous seront envoyés et viendront enrichir vos plans d'action.

Reception of Yuno advisories by email

Receive advisories by type

- PATCH
- EXPLOIT
- VULN

Receive advisories by severity

- None
- Low
- Medium
- High
- Critical

Update

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

Yuno > My action plan

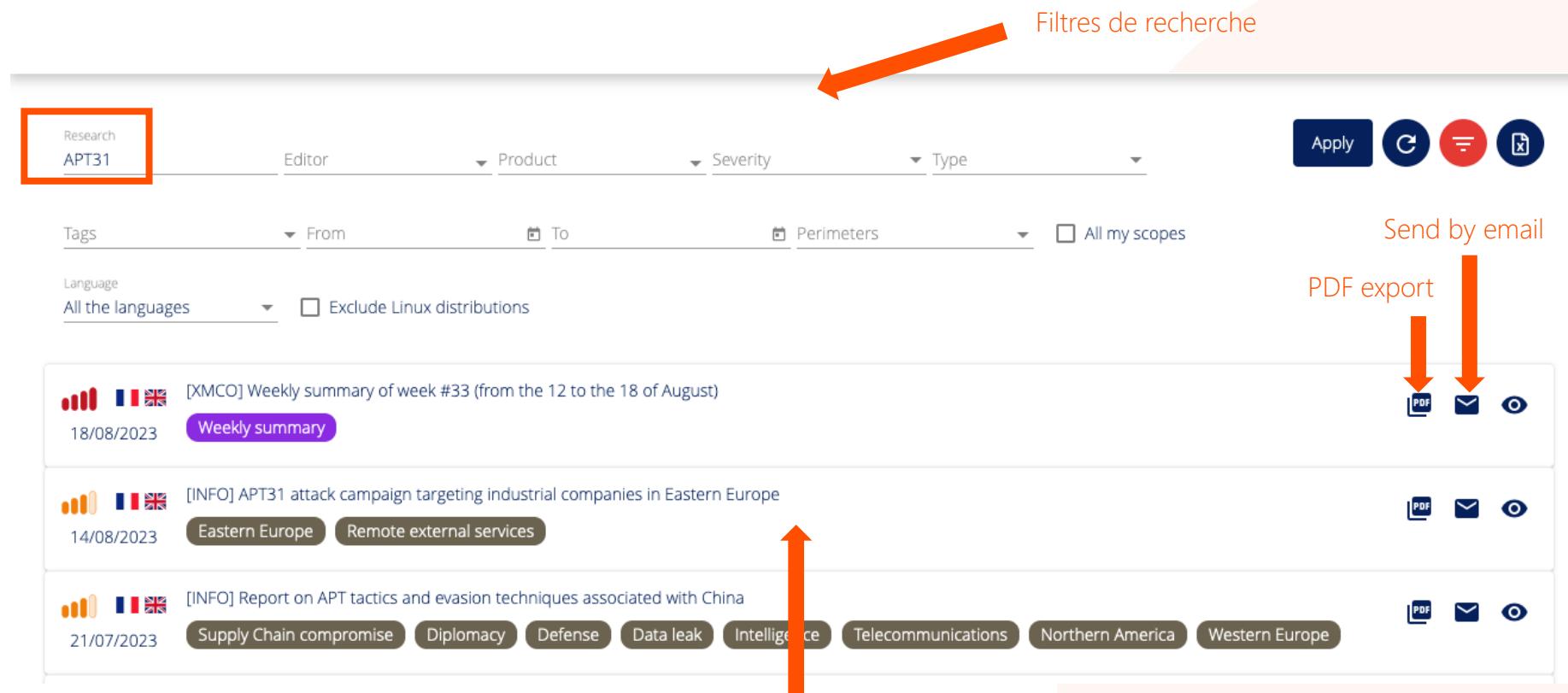
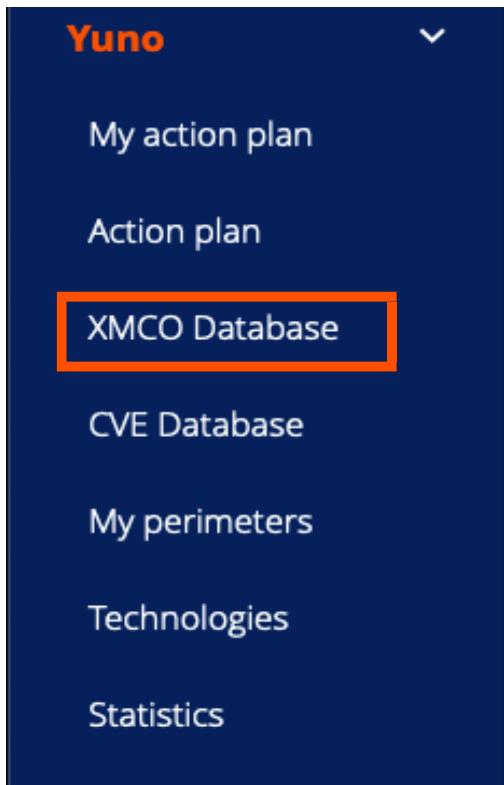
Include the action plans of :  Select an operator  Tracker  Add a filter

<input type="checkbox"/> PDF Export	Reference	Severity	Perimeter	Title	Status	Impact	Assigned to	Publication
<input type="checkbox"/>	<a href="#">PDF</a> 1458544		Global	[PATCH] [PERL] Prise de contrôle du système via deux vulnérabilités au sein de Perl	New	0	Alexandre PALLUT	01/12/2023
<input type="checkbox"/>	<a href="#">PDF</a> 1458541		Global	[PATCH] [SOLARWINDS] Contournement de sécurité et manipulation de données via une vulnérabilité au sein de SolarWinds	New	0	Alexandre PALLUT	01/12/2023
<input type="checkbox"/>	<a href="#">PDF</a> 1458537		Global	[PATCH] [APPLE] Prise de contrôle du système et divulgation d'informations via 2 vulnérabilités au sein de produits Apple (HT214031, HT214032, HT214033)	New	0	Alexandre PALLUT	01/12/2023
<input type="checkbox"/>	<a href="#">PDF</a> 1458527		Global	[PATCH] [MICROSOFT] Contournement de sécurité via une vulnérabilité au sein de Microsoft Edge	New	0	Alexandre PALLUT	01/12/2023
<input type="checkbox"/>	<a href="#">PDF</a> 1458519		Global	[PATCH] [GITLAB] Prise de contrôle du système et élévation de priviléges via 13 vulnérabilités au sein de GitLab	New	0	Alexandre PALLUT	01/12/2023
<input type="checkbox"/>	<a href="#">PDF</a> 1458515		Global	[PATCH] [IBM] Manipulation de données et déni de service via 3 vulnérabilités au sein d'IBM Tivoli Netcool (7085933)	New	0	Alexandre PALLUT	01/12/2023

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.



The search interface includes the following fields and filters:

- Tags: **Research APT31** (highlighted with an orange box)
- Editor
- Product
- Severity
- Type
- Tags: From, To, Perimeters,  All my scopes
- Language: All the languages,  Exclude Linux distributions

On the right, there are buttons for **Apply**, **C**, **Send by email**, and **PDF export**. The **PDF export** button is highlighted with an orange box and an arrow pointing to it.

Below the search interface, three bulletins are listed:

- [XMCO] Weekly summary of week #33 (from the 12 to the 18 of August)  
18/08/2023 Weekly summary
- [INFO] APT31 attack campaign targeting industrial companies in Eastern Europe  
14/08/2023 Eastern Europe, Remote external services
- [INFO] Report on APT tactics and evasion techniques associated with China  
21/07/2023 Supply Chain compromise, Diplomacy, Defense, Data leak, Intelligence, Telecommunications, Northern America, Western Europe

An orange arrow points to the title of the second bulletin, and another orange arrow points to the "Click on the title to open the bulletin online" text at the bottom.

# 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.

The screenshot shows the Yuno interface with the 'CVE Database' option selected. The search filters at the top are set to 'Editor: Microsoft', 'Product: Edge chromium', and 'Version: 88.0.705.74'. The table below lists vulnerabilities, with the first two rows highlighted. Red arrows point from the text labels to the corresponding parts of the interface: one arrow points to the 'Associated XMCO bulletins' label, another to the 'The CVE vulnerabilities come from the official MITRE database' label, and a third to the 'Search filters' label.

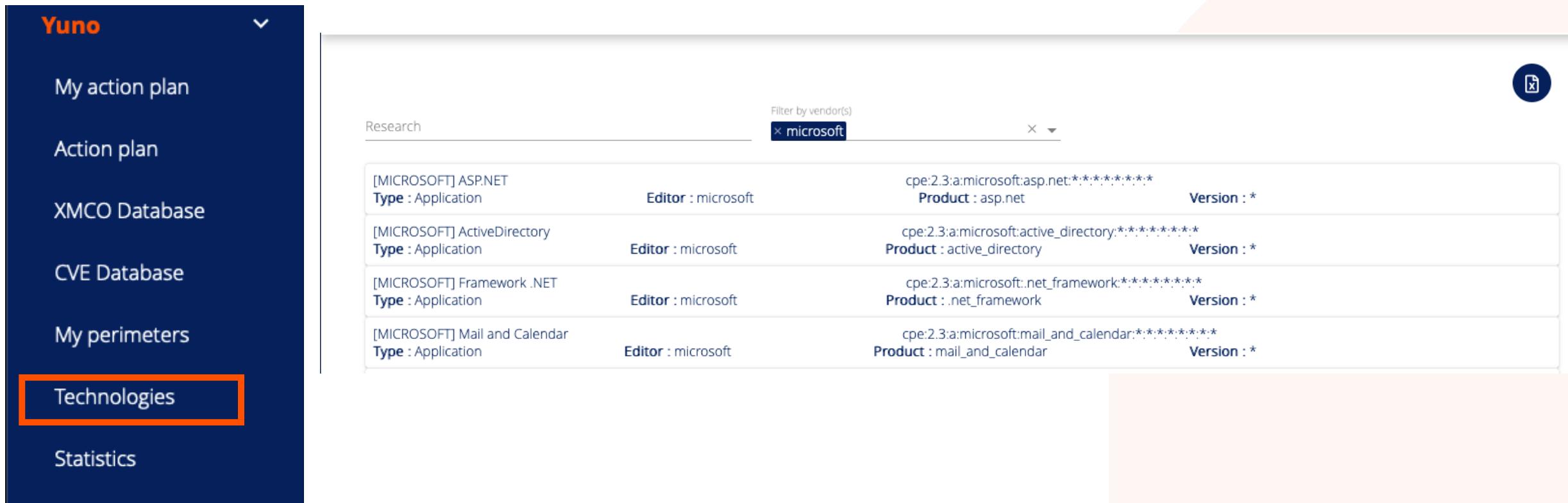
Publication date ↓	CVE ID	CVSS	Editor	Product	Version	Minor version	CXA	Exploitation code
11/04/2023	CVE-2023-24935	0	Microsoft	Edge_chromium	88.0.705.74	*****	CXA-2023-1848	
11/10/2022	CVE-2022-41035	5.3	Microsoft	Edge_chromium	88.0.705.74	*****	CXA-2022-4762	, ...
29/06/2022	CVE-2022-33638	8.3	Microsoft	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.



The screenshot shows the Yuno interface with a sidebar on the left and a main content area on the right.

**Sidebar (Left):**

- Yuno
- My action plan
- Action plan
- XMCO Database
- CVE Database
- My perimeters
- Technologies** (highlighted with an orange border)
- Statistics

**Main Content Area (Right):**

Research

Filter by vendor(s)  (X)

Product	Version
cpe:2.3:a:microsoft:asp.net:***:***:***	Product : asp.net
cpe:2.3:a:microsoft:active_directory:***:***:***	Product : active_directory
cpe:2.3:a:microsoft:.net_framework:***:***:***	Product : .net_framework
cpe:2.3:a:microsoft:mail_and_calendar:***:***:***	Product : mail_and_calendar

**Table Data (Visible Rows):**

Product	Version
cpe:2.3:a:microsoft:asp.net:***:***:***	Product : asp.net
cpe:2.3:a:microsoft:active_directory:***:***:***	Product : active_directory
cpe:2.3:a:microsoft:.net_framework:***:***:***	Product : .net_framework
cpe:2.3:a:microsoft:mail_and_calendar:***:***:***	Product : mail_and_calendar

# Consult the statistics

The [statistics page](#) allows you to obtain information and KPIs on the bulletins received during a given period.

