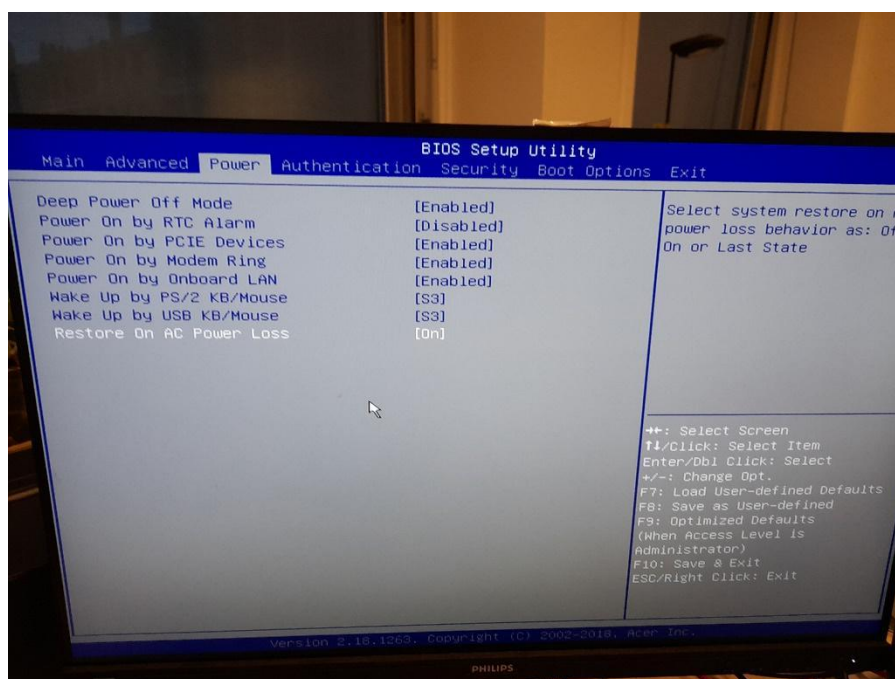


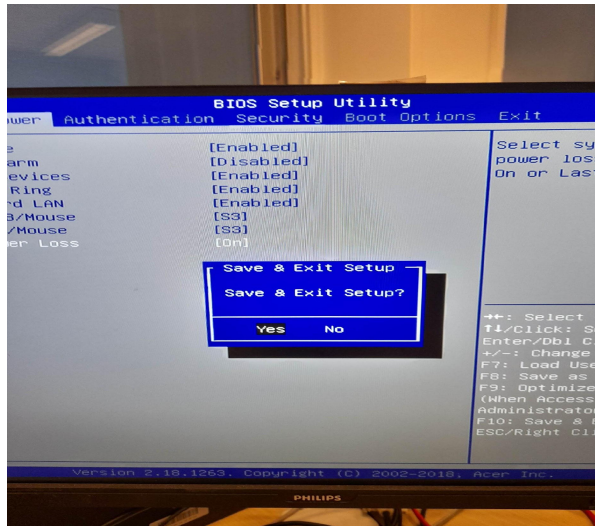
## Préparation postes relais TEHTRIS :

- Dès l'allumage du poste, appuyer plusieurs fois sur la touche « Suppr », afin d'accéder au BIOS :

- o Aller dans menu POWER
- o Au niveau de la ligne « Restore On AC Power LOSS », cliquer sur [Last State]
- o Sélectionner « ON » puis taper sur la touche « Entrée »



- o Taper sur la touche F10 pour sauver la modification effectuée et quitter le BIOS. Appuyer sur la touche Entrée du clavier.

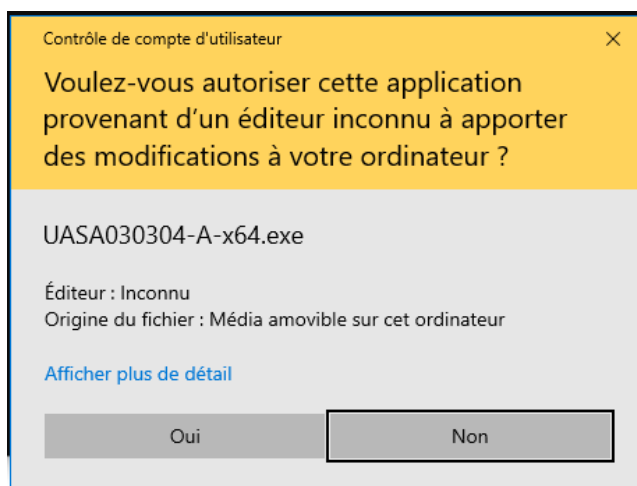


#### - Démarrer la session :

- o Aller dans « Autre Utilisateur » en bas à gauche
  - Identifiant : .\pcasecours
  - Mdp : P0l&su770rtidf

#### - Mettre à jour Passeport : 2 composants :

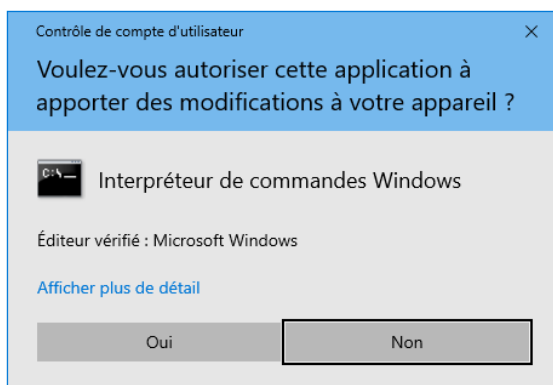
- o **UASA** :
  - A partir de la clé USB, dans répertoire UASA030304, double-cliquer sur gediff.bat
  - Cliquer sur Oui dans la fenêtre qui apparaît :



- Quand la fenêtre DOS (fenêtre noire) disparaît, l'installation est terminée.

#### o **UAST :**

- A partir de la clé USB, copier le répertoire « gpo\_UAST020036 » dans C:\PMF\Install\Cache\
- A l'intérieur de ce répertoire C:\PMF\Install\Cache\gpo\_UAST020036\, clic droit sur « install\_UAST020036.bat », cliquer sur « Exécuter en tant qu'administrateur »
- Cliquer sur « oui » :



- Plusieurs fenêtres DOS noires s'ouvrent, laisser faire jusqu'à l'apparition de cette fenêtre :

Message de 14/10/2022 09:52



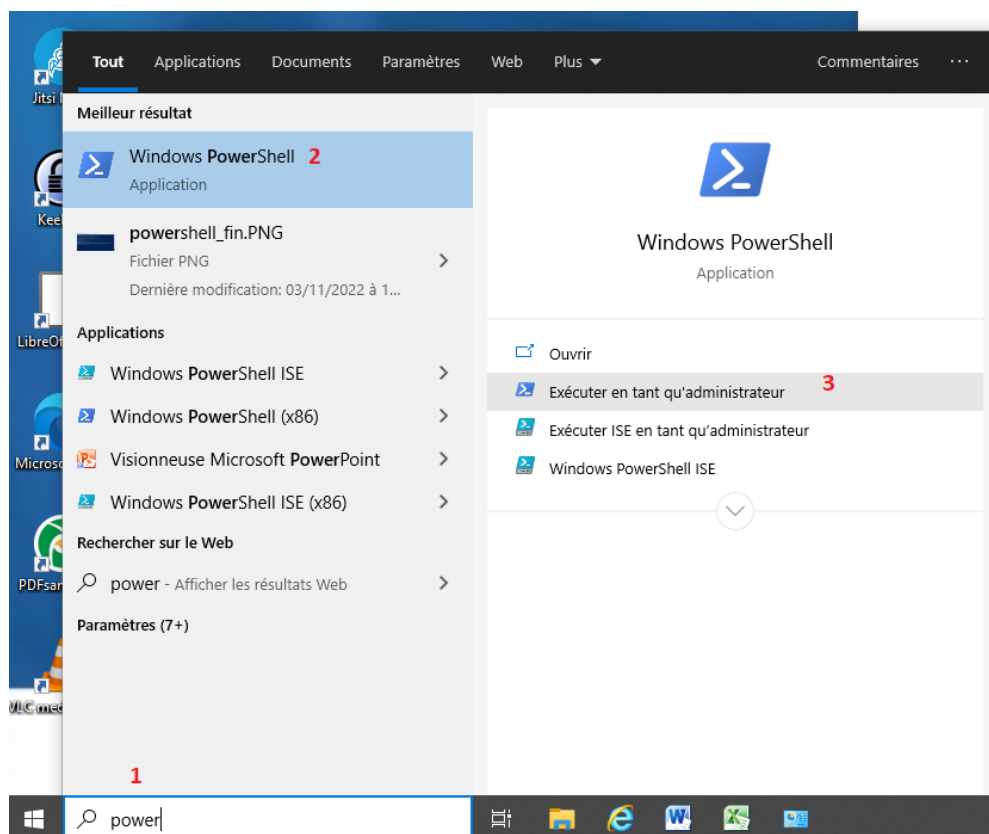
UN COMPOSANT DE SECURITE PASSEPORT A ETE MIS A JOUR SUR  
VOTRE ORDINATEUR. UN REDEMARRAGE DE VOTRE POSTE EST  
NECESSAIRE POUR RECUPERER TOUTES VOS HABILITATIONS PASSEPORT

OK

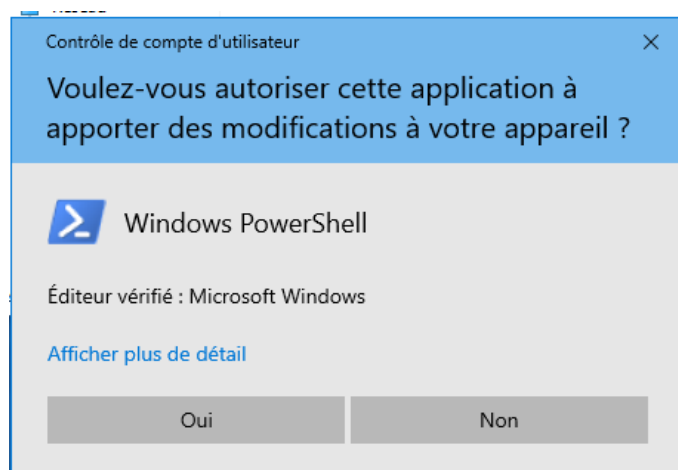
- Cliquer sur OK et redémarrer le poste.

#### **INSTALLATION TEHTRIS EDR :**

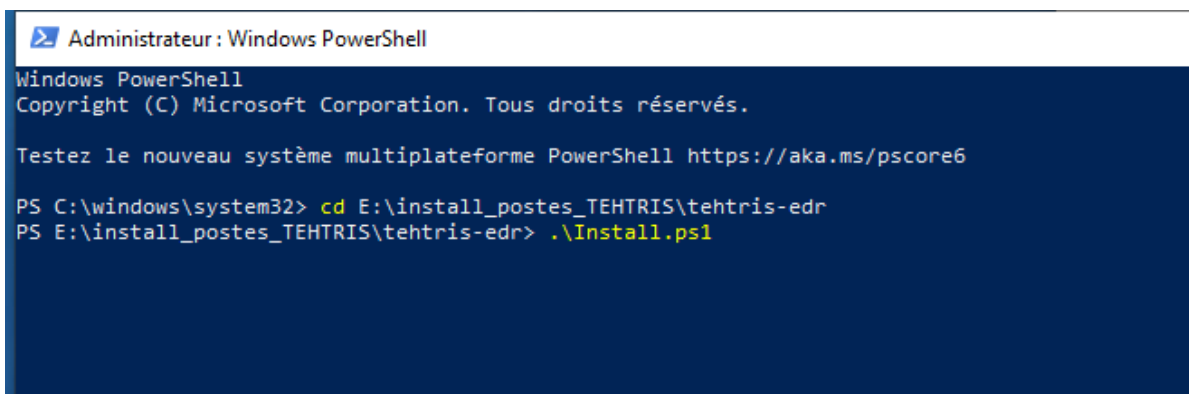
- A partir de la clé, copier le répertoire TEHTRIS-EDR dans c:\APPLINAT\
- Dans Recherche taper « POWER » **1**, « Windows Powershell » apparaît **2**, cliquer sur « Exécuter en tant qu'administrateur » **3** :



- Cliquer sur OUI dans la fenêtre qui apparaît :



- Dans la fenêtre Powershell qui s'ouvre saisir (ou copier-coller) la ligne suivante puis taper la touche Entrée :
  - o `cd C:\APPLINAT\TEHTRIS-EDR`
- Taper « ins » puis sur la touche TAB, pour faire s'afficher :



```

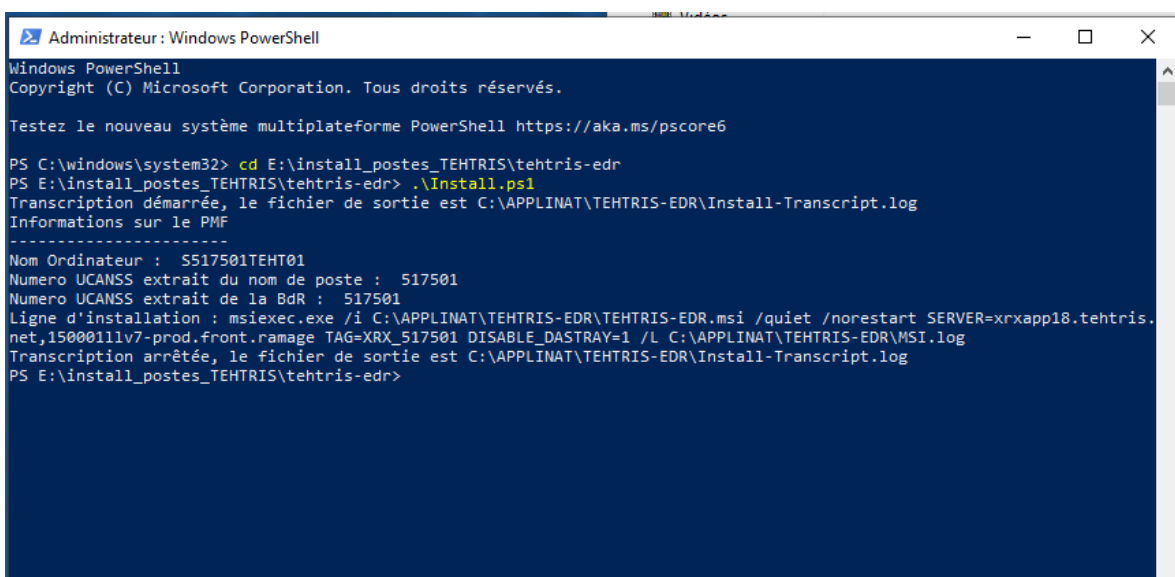
Administrateur : Windows PowerShell

Windows PowerShell
Copyright (C) Microsoft Corporation. Tous droits réservés.

Testez le nouveau système multiplateforme PowerShell https://aka.ms/pscore6

PS C:\windows\system32> cd E:\install_postes_TEHTRIS\tehttris-edr
PS E:\install_postes_TEHTRIS\tehttris-edr> .\Install.ps1
  
```

- Laisser se dérouler l'installation pendant quelques minutes, jusqu'à ce que la fenêtre s'affiche ainsi :



```

Administrateur : Windows PowerShell

Windows PowerShell
Copyright (C) Microsoft Corporation. Tous droits réservés.

Testez le nouveau système multiplateforme PowerShell https://aka.ms/pscore6

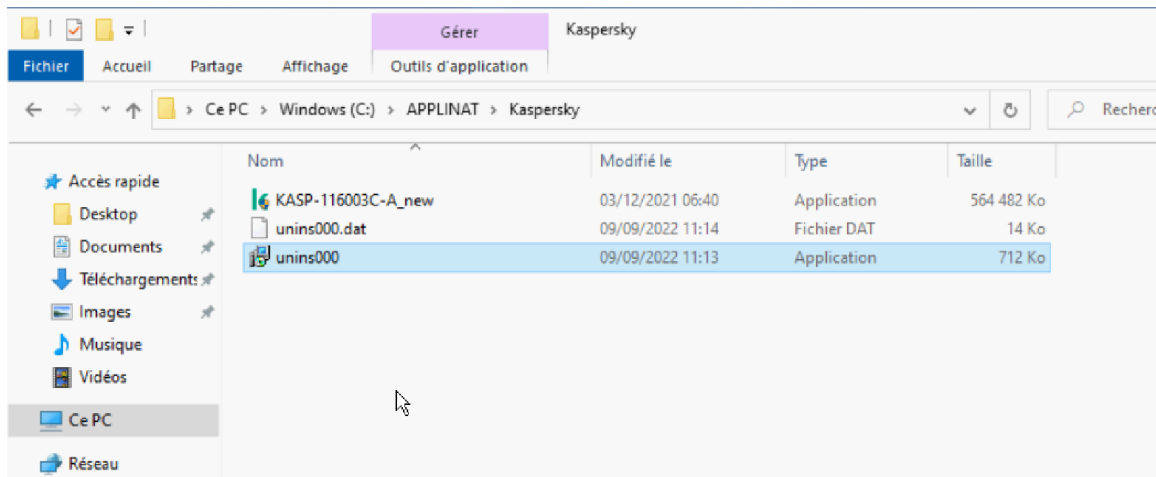
PS C:\windows\system32> cd E:\install_postes_TEHTRIS\tehttris-edr
PS E:\install_postes_TEHTRIS\tehttris-edr> .\Install.ps1
Transcription démarrée, le fichier de sortie est C:\APPLINAT\TEHTRIS-EDR\Install-Transcript.log
Informations sur le PMF
-----
Nom Ordinateur : S517501TEHT01
Numero UCANSS extrait du nom de poste : 517501
Numero UCANSS extrait de la BdR : 517501
Ligne d'installation : msixec.exe /i C:\APPLINAT\TEHTRIS-EDR\TEHTRIS-EDR.msi /quiet /norestart SERVER=xrxapp18.tehttris.
net,15000111v7-prod.front.ramag TAG=XRX_517501 DISABLE_DASTRAY=1 /L C:\APPLINAT\TEHTRIS-EDR\MSI.log
Transcription arrêtée, le fichier de sortie est C:\APPLINAT\TEHTRIS-EDR\Install-Transcript.log
PS E:\install_postes_TEHTRIS\tehttris-edr>
  
```

- Fermer la fenêtre Powershell.

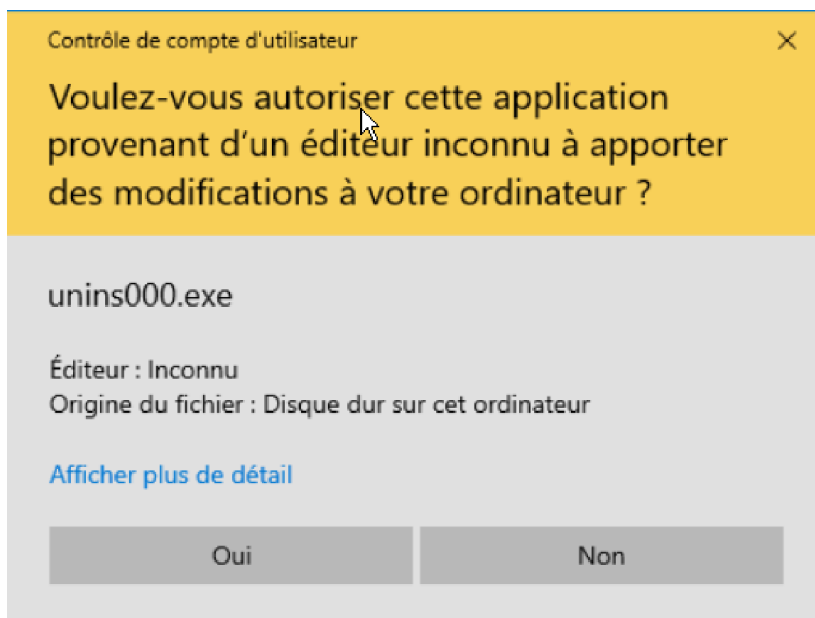
## DESINSTALLATION KASPERSKY :

Selon la version Kaspersky installée sur le serveur, il est parfois nécessaire de passer par le menu **Démarrer, Kaspersky Security for Windows Server, Modification ou Suppression de Kaspersky Security for Windows Server**.

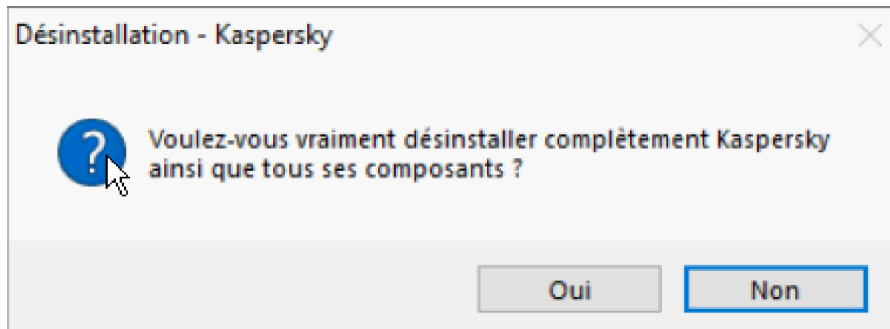
1. Aller dans C:\APPLINAT\Kaspersky et exécuter unins000.exe en administrateur



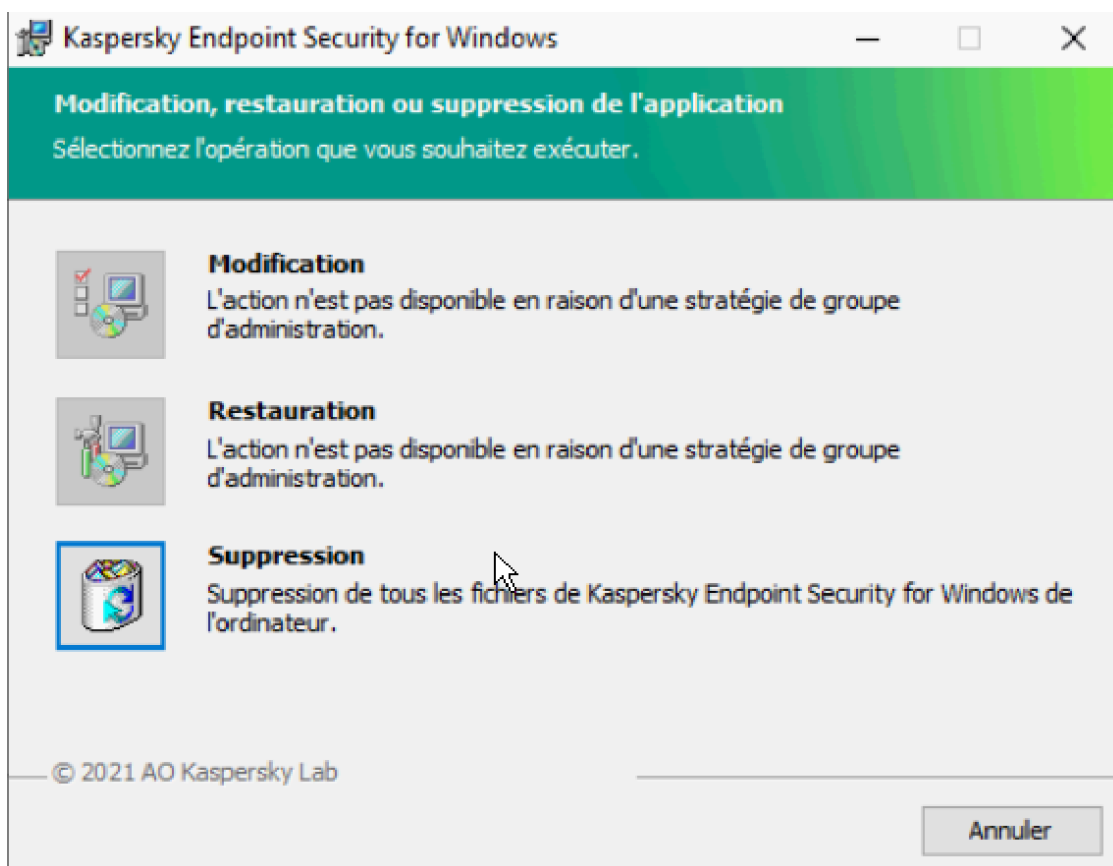
2. Autoriser le lancement de unins000.exe en cliquant sur « Oui ».



3. Cliquer sur OUI :

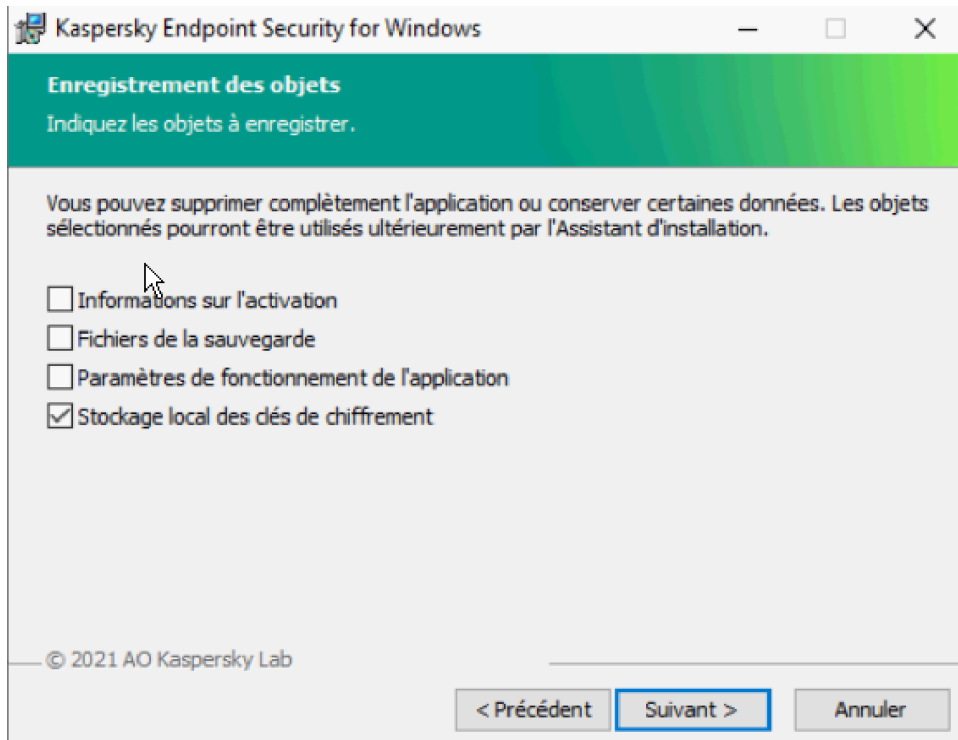


4. Cliquer sur « Suppression »

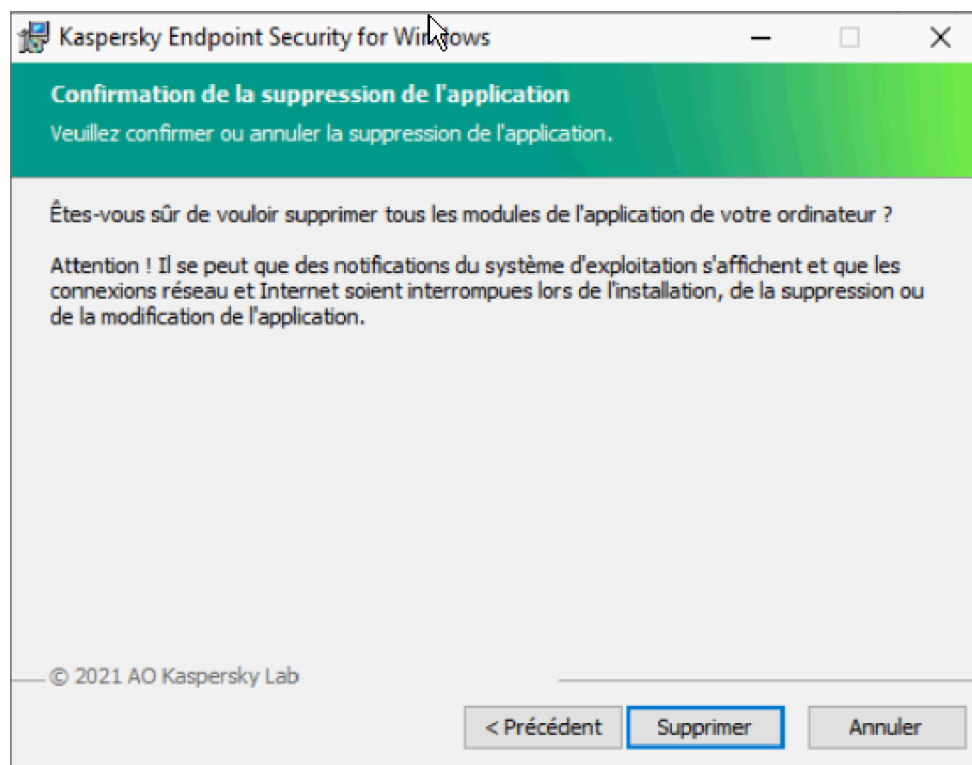


5. Cliquer sur « Suivant »

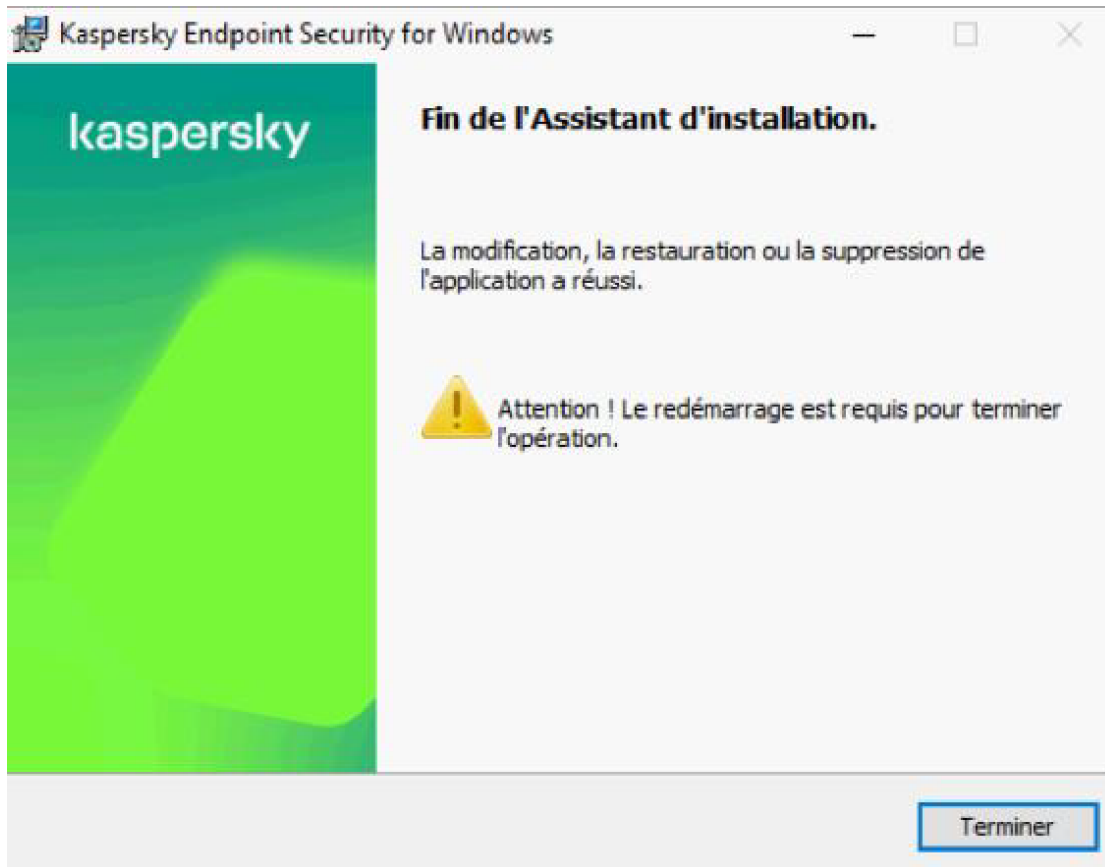




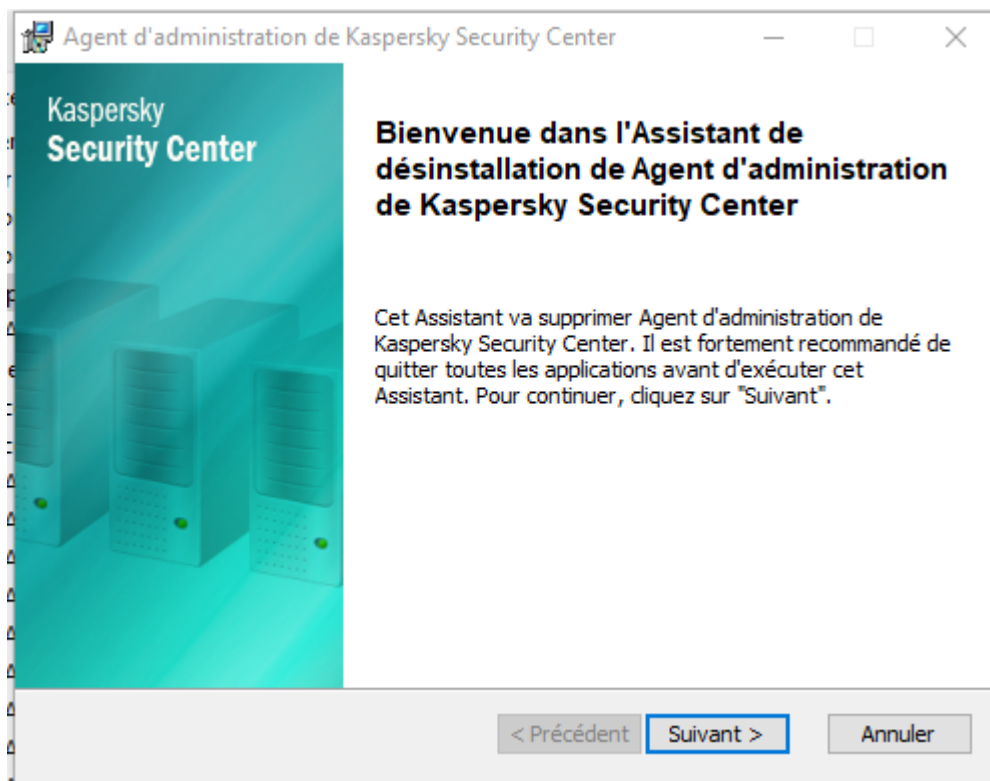
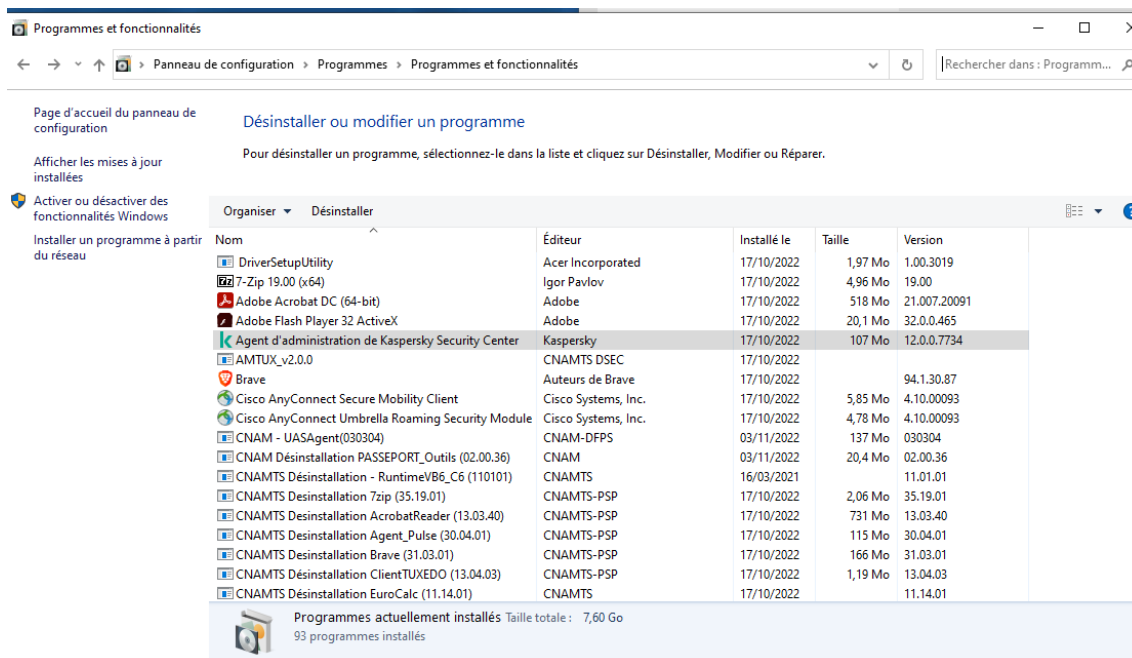
6. Cliquer sur « Supprimer »

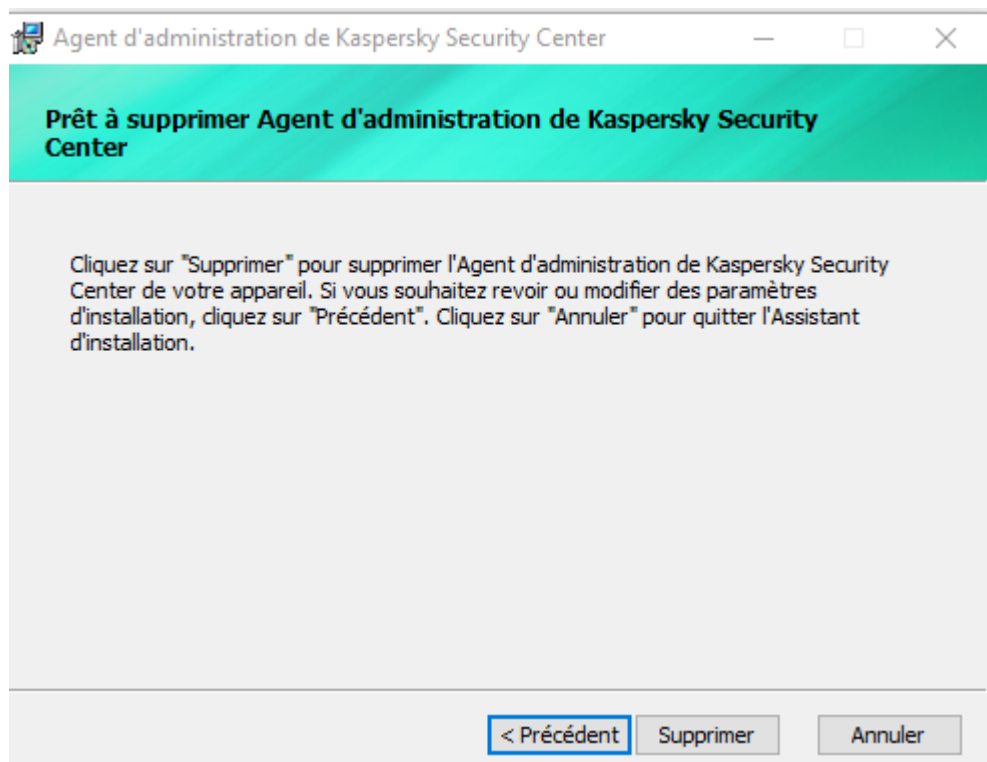


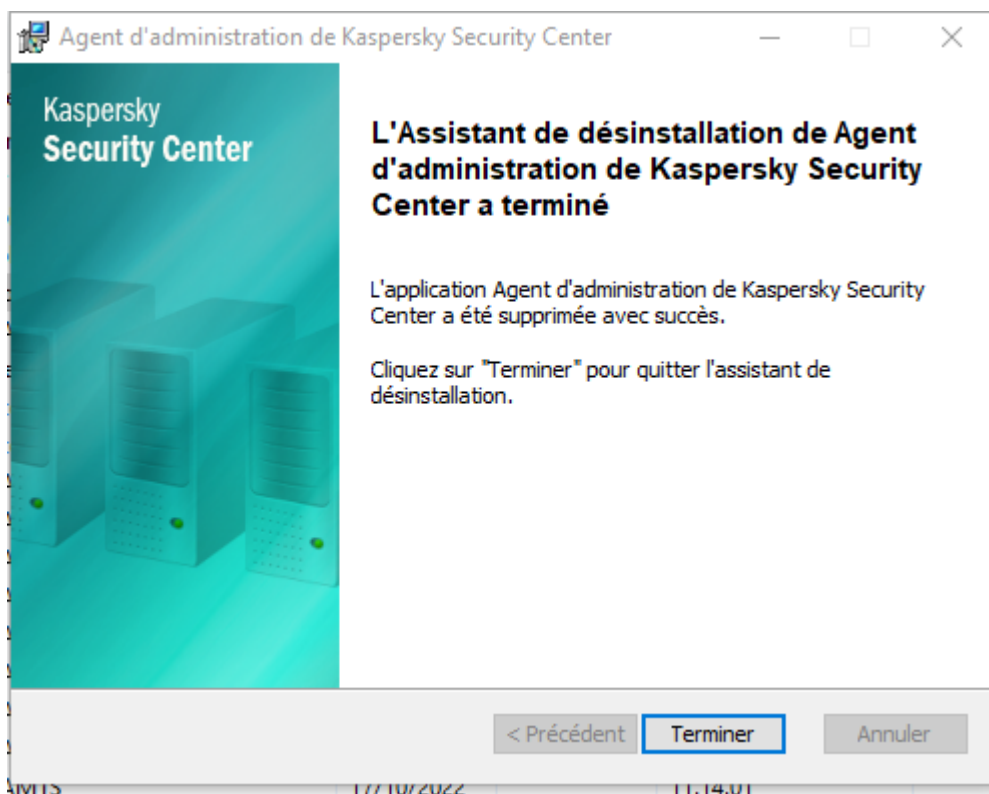
7. Cliquer sur « Terminer »



- Désinstaller l'Agent d'administration de Kaspersky : clic droit/Désinstaller







**Redémarrer le poste.**

### **INSTALLATION TEHTRIS EPP :**

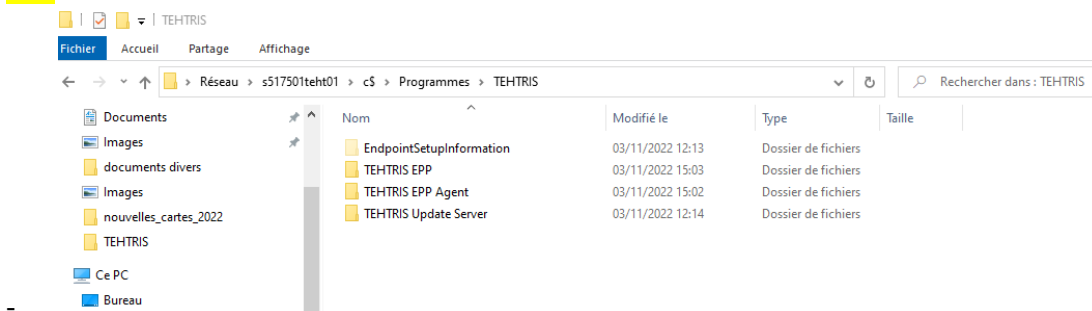
- A partir de la clé USB, copier répertoire « Tehtris » contenant (679Mo env) dans C:\PMF\Install\Cache\
- Lancer un terminal de commande :
  - o Dans Recherche taper « cmd » et l'exécuter en tant qu'administrateur :
  - o Saisir la ligne de commande suivante (ou copier-coller) et faire Entrée :

```
C:\PMF\Install\Cache\Tehtris\TEHTRIS_EPP_1.2.2_x64.exe /xenoui /q REGISTRY_SERVER="150001lty-prod.front.ramag" REGISTRY_PREFERRED_GROUP="517501_Relais" ANTIEXPLOIT="1" ANTIPHISHING="1" BEHAVIORALSCAN="1" FILESCAN="1" FIREWALL="1" NETWORKMONITOR="1" TRAFFICSCAN="1" RELAY_SERVER="1"
```

- L'installation ne dure que quelques minutes.

## VERIFICATION INSTALLATION :

Pour vérifier l'installation, on peut checker la présence du répertoire c:\Program Files\TEHTRIS :



- Ou sinon Processus en cours d'exécution - *Statut : En cours d'exécution* (taskmgr.exe => Détails)

▪ Produit de sécurité :

▪ epconsole.exe

▪ epintegrationservice.exe

▪ epprotectedservice.exe

▪ epsecurityservice.exe

▪ epupdateservice.exe

▪ Agent de communication

▪ TehtrisEPP.exe

- Vérification des services - 'sc query ...' => *STATE : 4 RUNNING*

▪ Produit de sécurité

▪ TEHTRIS Endpoint Redline Service => 'sc query EPRedline'

▪ TEHTRIS Endpoint Integration Service => 'sc query EPIntegrationService'

▪ TEHTRIS Endpoint Protected Service => 'sc query EPProtectedService'

▪ TEHTRIS Endpoint Security Service => 'sc query EPSecurityService'

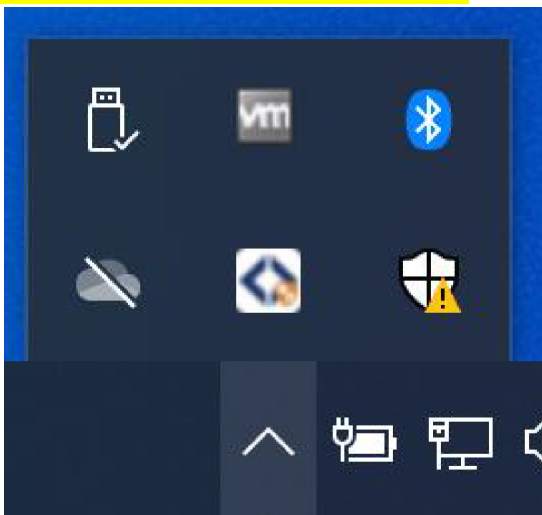
- TEHTRIS Endpoint Update Service => 'sc query EPUUpdateService'
- Agent de communication
- TehtrisEPP.exe => 'sc query TehtrisEPP'



□ Vérification des clés de registre

- `HKEY_LOCAL_MACHINE\SOFTWARE\TEHTRIS\TEHTRIS EPP`
- `HKEY_LOCAL_MACHINE\SOFTWARE\TEHTRIS\TEHTRIS EPP Agent`
- Cette clé contient les informations pour la connexion à l'appliance EPP (nom de server, uid de la machine, etc)

□ Interface graphique / Console locale :



- Message 'You are at risk' car le Full scan n'a pas encore eu lieu sur la machine. Vous en aurez aussi un en rouge car le module Firewall est désactivé par défaut. **A ignorer dans un premier temps.**

17

Pour vérifier si le mode relais est installé sur un PMF/Serveur Windows, vous pouvez vérifier localement si le répertoire TEHTRIS UPDATE SERVER est présent :

Ce PC > Windows (C:) > Programmes > TEHTRIS > TEHTRIS Update Server >				
	Nom	Modifié le	Type	Taille
le	bin	21/10/2022 10:17	Dossier de fichiers	
	data	19/10/2022 12:41	Dossier de fichiers	
ement:	etc	21/10/2022 10:19	Dossier de fichiers	
ts	tmp	19/10/2022 12:41	Dossier de fichiers	
	var	21/10/2022 10:13	Dossier de fichiers	

## 6. Désinstallation de l'EPP TEHTRIS

### 5.1 Procédure de désinstallation de l'EPP

CLI -> /x // /q

Vous pouvez utiliser cette option pour une désinstallation silencieuse.

Usage: C:\PMF\Install\Cache\Tehtris\ TEHTRIS\_EPP\_1.2.2\_x64.exe/x // /q

A noter qu'il est nécessaire de rebooter la machine pour que la désinstallation soit effective suite à la désinstallation silencieuse.