Comment effacer manuellement l'historique de Windows Defender avec Windows 10

Remerciements et crédits à Monsieur André Carrier, membre du CIVBDL

L'historique de protection affiche les détections effectuées par Windows Defender et fournit des informations détaillées et plus faciles à comprendre sur les menaces et les actions disponibles.

À partir de la version 18305 de Windows 10, cet historique inclut les blocs d'accès aux dossiers contrôlés, ainsi que tous les blocs qui ont été créés par la configuration.
Dans cet article, nous vous montrerons comment effacer manuellement l'historique de protection dans Windows Defender sur Windows 10.

Si vous utilisez l'outil d'analyse hors ligne de Windows Defender, toutes les détections qu'il effectue apparaîtront désormais également dans cet historique.
De plus, vous verrez toutes les recommandations en attente (états rouges ou jaunes dans toute l'application) dans la liste de l'historique.

Supprimer l'historique de la protection de Windows Defender

Cet historique précise le nombre de jours pendant lesquels les éléments sont stockés dans le journal.
Après ce délai, Windows Defender supprime les éléments.
Si vous spécifiez une valeur nulle, Windows Defender ne supprime pas les éléments.
Si vous ne spécifiez pas de valeur, Windows Defender supprimera les éléments du dossier du journal d'analyse par défaut, c'est-à-dire 30 jours.

Cependant, si vous souhaitez effacer l'historique de protection manuellement, vous pouvez le faire de l'une des trois manières suivantes ;

- En utilisant le cmdlet Set-MpPreference de PowerShell.
- En supprimant le dossier Windows Defender Service du disque dur local.
- En utilisant l'Observateur d'évènements.

Cmdlet Set-MpPreference de PowerShell

Le **cmdlet Set-MpPreference** configure les préférences pour les analyses et les mises à jour de Windows Defender.
Vous pouvez modifier les extensions des noms de fichiers d'exclusion, les chemins d'accès ou les processus, et spécifier l'action par défaut pour les niveaux de menace élevés, modérés et faibles.

Vous pouvez spécifier une période de délai différente (en jours) en exécutant le cmdlet ci-dessous en mode administrateur de PowerShell (appuyez sur **Win + X**, puis sur **A** du clavier) :

```
Set-MpPreference -ScanPurgeItemsAfterDelay 1
```

La valeur **1** indiquée représente le nombre de jours après lequel le journal de l'historique de la protection et les éléments du dossier de journal seront effacés.

Supprimez le dossier Windows Defender Service du disque dur local

Pour effacer manuellement l'historique de protection, cette méthode nécessite de supprimer le dossier **Service** sous le dossier **Windows Defender** sur le disque dur local.

- Appuyez sur la combinaison de touches **Windows + R** pour ouvrir la boîte de dialogue **Exécuter.**
- Dans la boîte de dialogue **Exécuter**, copiez et collez le chemin d'accès ci-dessous et appuyez sur **Entrée** (si vous y êtes invité, cliquez sur **Continuer**).

```
C:\ProgramData\Microsoft\Windows Defender\Scans\History
```

- Cliquez avec le bouton droit de la souris sur le dossier **Service** et sélectionnez **Supprimer.**
- Fermez l'**Explorateur de fichiers**.
- Ensuite, ouvrez **Sécurité Windows > Protection contre les virus et menaces > Gérer les paramètres.**
- Basculez le bouton sur **Désactivé** puis sur **Activé** pour la **Protection en temps réel** et la Protection dans le cloud.

Utilisez l'Observateur d'évènements

Pour effacer manuellement l'historique de protection de Windows Defender à l'aide de l'observateur d'évènements (eventvwr), procédez comme suit :

- Appuyez sur la combinaison de touches **Windows + R** pour ouvrir la boîte de dialogue **Exécuter.**

- Dans la boîte de dialogue **Exécuter**, tapez **eventvwr** et appuyez sur la touche **Entrée** pour ouvrir l'**Observateur d'évènements.**
- Dans la section de l'**Observateur d'évènements (local)** située sur le côté gauche du volet, développez la branche **Journaux des applications et des services.**
- Sous cette section, développez l'option **Microsoft.**
- Cliquez sur **Windows** pour ouvrir la liste de tous ses fichiers dans le volet central.
- Dans le volet central, faites défiler la liste des fichiers vers le bas pour trouver **Windows Defender.**
- Cliquez avec le bouton droit de la souris sur **Windows Defender**, puis cliquez sur **Ouvrir.**
- Parmi les deux options du panneau central, cliquez avec le bouton droit de la souris sur **Operational**, et cliquez sur **Ouvrir** pour voir tous les journaux.
- Sous le dossier **Windows Defender** dans le panneau de gauche, cliquez avec le bouton droit de la souris sur **Operational**.
- Cliquez sur **Effacer le journal…** dans le menu.
- Sélectionnez **Effacer** ou **Enregistrer et effacer** en fonction de votre besoin d'effacer l'historique de protection.

Vous connaissez maintenant les trois méthodes connues pour effacer manuellement l'historique de protection de Windows Defender avec Windows 10.

Recherches et mise en page:
Michel Cloutier
CIVBDL
20230125
"C'est ensemble qu'on avance en cybersécurité"