

Titre : Mise en place et configuration de Microsoft Defender pour la protection des postes de travail et la gestion des menaces via Microsoft 365 Defender

Objectif

L'objectif de ce laboratoire est d'installer, configurer et tester **Microsoft Defender** sur un environnement Windows et Microsoft 365 afin de renforcer la sécurité des postes de travail et des communications contre les menaces cybernétiques. Nous allons :

- Installer et activer **Microsoft Defender**.
- Configurer les stratégies de sécurité via Microsoft Defender Security Center.
- Effectuer des analyses de sécurité et tester la protection en temps réel.
- Utiliser **Windows Security** pour surveiller les menaces et gérer les quarantaines.
- Explorer le portail **Microsoft 365 Defender** pour gérer les menaces et incidents de sécurité.
- Surveiller et gérer les emails bloqués via **Microsoft 365 Defender**.

Introduction

Microsoft Defender est une solution de sécurité intégrée à Windows et à Microsoft 365 permettant de protéger les systèmes contre les logiciels malveillants, les ransomwares et autres menaces. Ce laboratoire guidera pas à pas l'installation et la configuration de Microsoft Defender sur un poste Windows 10/11 ainsi que l'exploitation de ses fonctionnalités avancées pour la gestion des menaces dans un environnement Microsoft 365.

1. Prérequis

- Un poste de travail sous Windows 10 ou Windows 11.
- Une connexion Internet active.
- Accès aux paramètres de sécurité Windows et au Microsoft Defender Security Center (si utilisé en entreprise).
- Une adresse professionnelle **Microsoft 365** avec accès au portail **Microsoft Defender** et **Exchange Online Protection**.

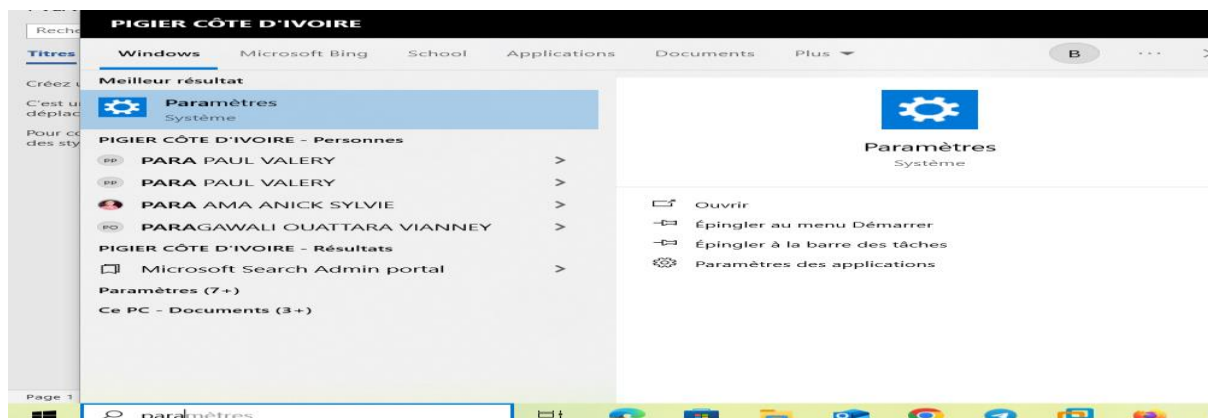
Remarque : Dans ce Lab nous utiliserons un compte client **Microsoft 365** avec accès au portail **Microsoft Defender** en version d'évaluation avec des fonctionnalités limitées.

2. Installation et Activation de Microsoft Defender

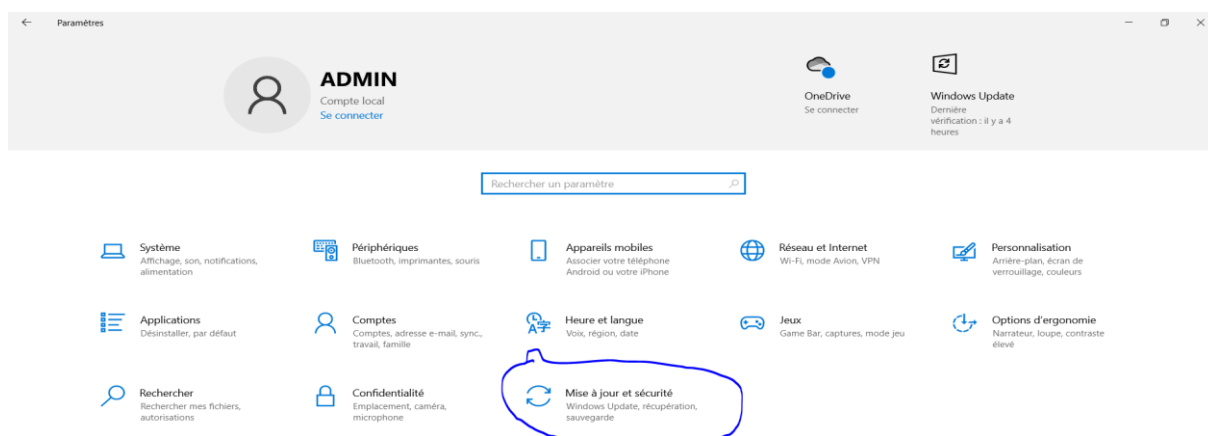
2.1 Vérifier si Microsoft Defender est activé

1. Ouvrir **Paramètres** via le menu Démarrer.

Mise en place et configuration de Microsoft Defender pour la protection des postes de travail et la gestion des menaces via Microsoft 365 Defender



2. Aller dans **Mise à jour et sécurité > Sécurité Windows**.



3. Cliquer sur **Protection contre les virus et menaces**.

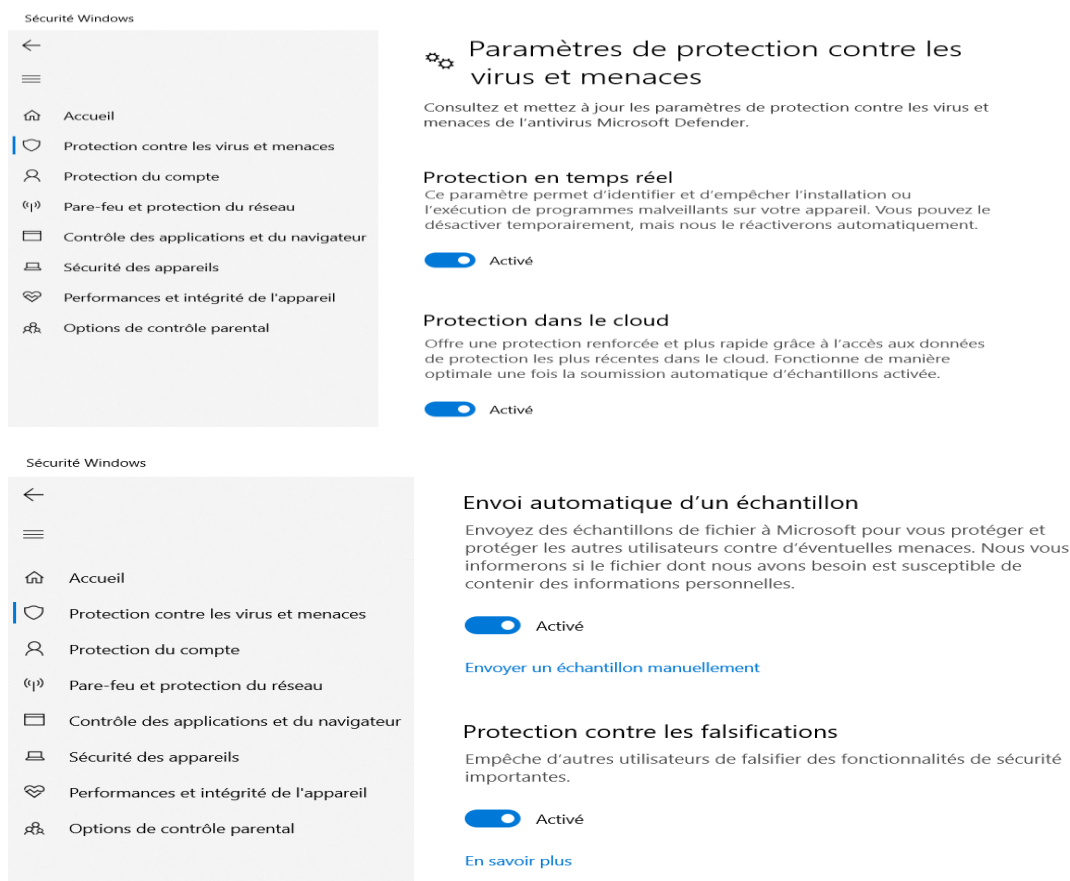


4. Vérifier que **Microsoft Defender Antivirus** est activé.

Si ce n'est pas le cas, activer la protection en cliquant sur **Gérer les paramètres** et activer les options suivantes :

- Protection en temps réel.
- Protection basée sur le cloud.
- Soumission automatique d'échantillons.
- Protection contre les falsifications.

Mise en place et configuration de Microsoft Defender pour la protection des postes de travail et la gestion des menaces via Microsoft 365 Defender



2.2 Mettre à jour Microsoft Defender

1. Ouvrir **Sécurité Windows**.
2. Aller dans **Protection contre les virus et menaces**.
3. Sous **Mises à jour de protection contre les virus et menaces**, cliquer sur **Rechercher des mises à jour**.



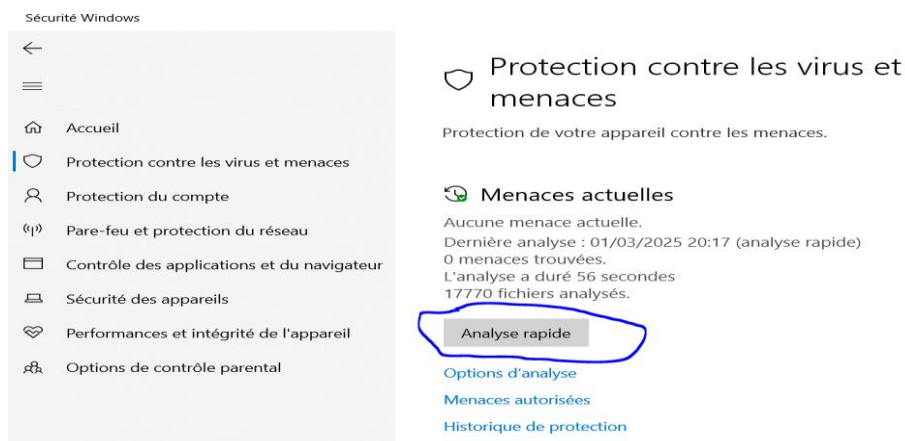
Mise en place et configuration de Microsoft Defender pour la protection des postes de travail et la gestion des menaces via Microsoft 365 Defender



4. Attendre la mise à jour et vérifier si elle est bien installée.

2.3. Analyse des menaces

1. Ouvrir **Sécurité Windows**.
2. Aller dans **Protection contre les virus et menaces**.
3. Sous **Menaces actuelles**, cliquer sur **Analyse rapide**.



4. Attendre la fin de l'analyse.



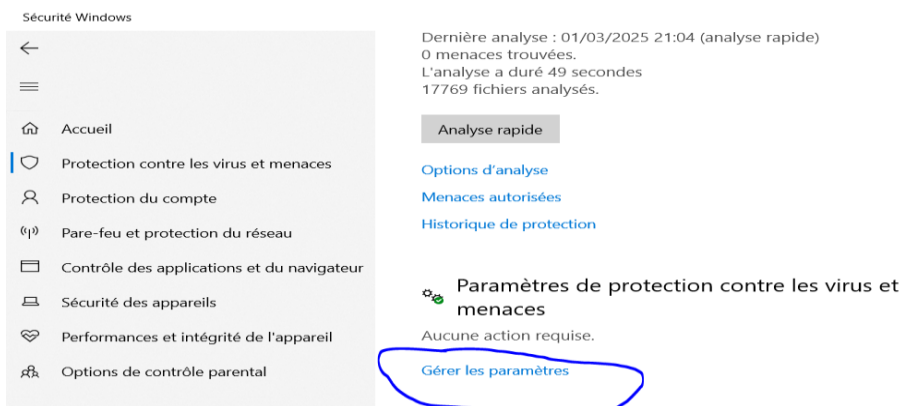
3. Configuration avancée de Microsoft Defender

3.1 Configuration des exclusions

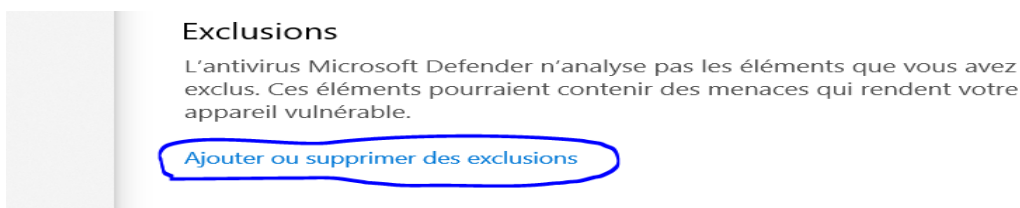
Si certaines applications sûres sont détectées comme malveillantes, vous pouvez ajouter une exclusion :

Mise en place et configuration de Microsoft Defender pour la protection des postes de travail et la gestion des menaces via Microsoft 365 Defender

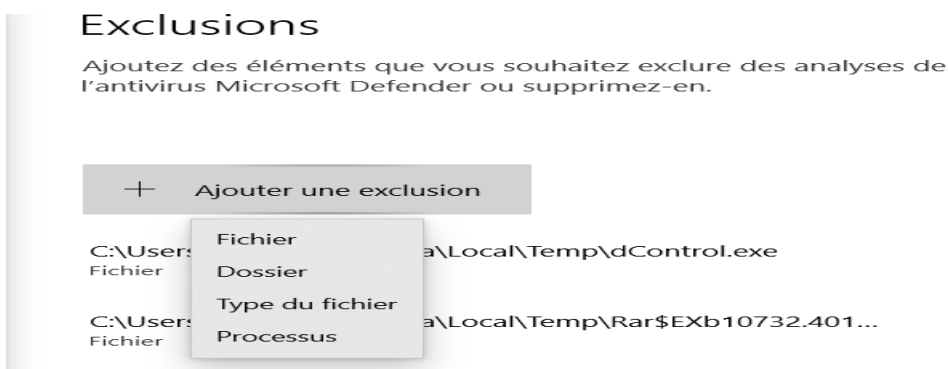
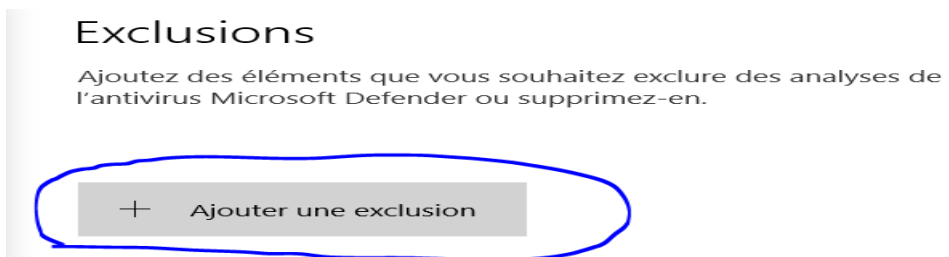
1. Ouvrir **Sécurité Windows**.
2. Aller dans **Protection contre les virus et menaces**.
3. Cliquer sur **Gérer les paramètres** sous **Paramètres de protection contre les virus et menaces**.



4. Faire défiler vers le bas et cliquer sur **Ajouter ou supprimer des exclusions**.



5. Ajouter un fichier, dossier ou processus à exclure.



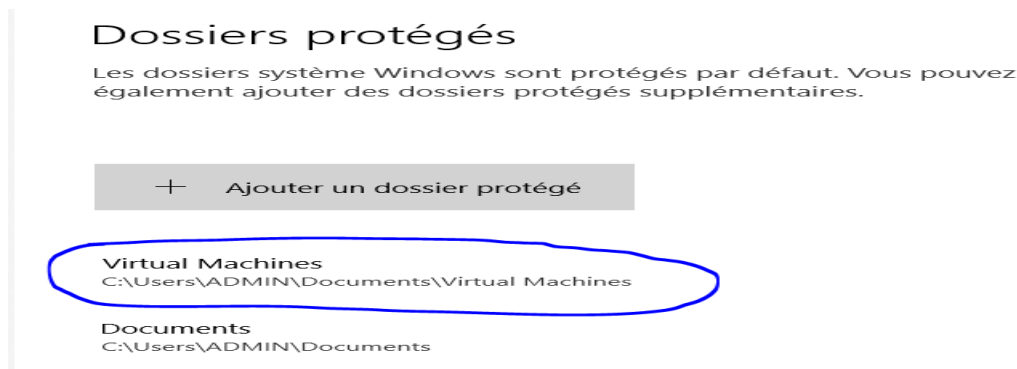
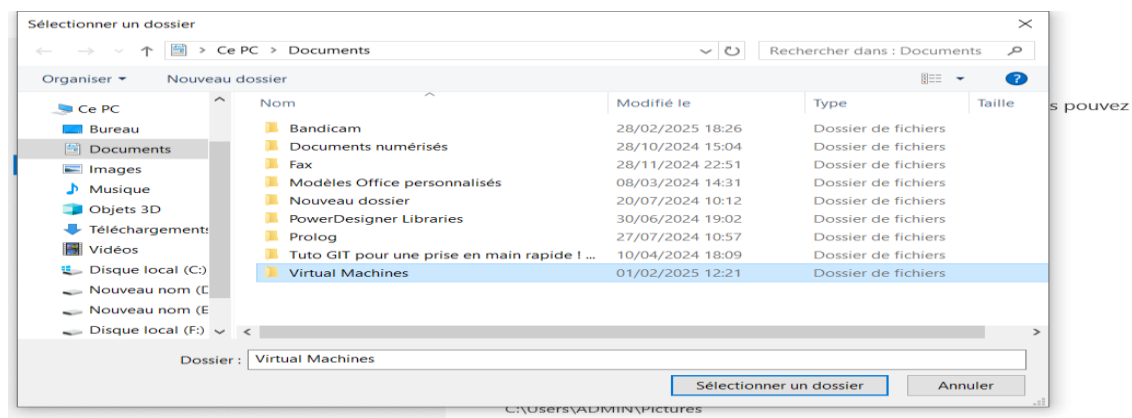
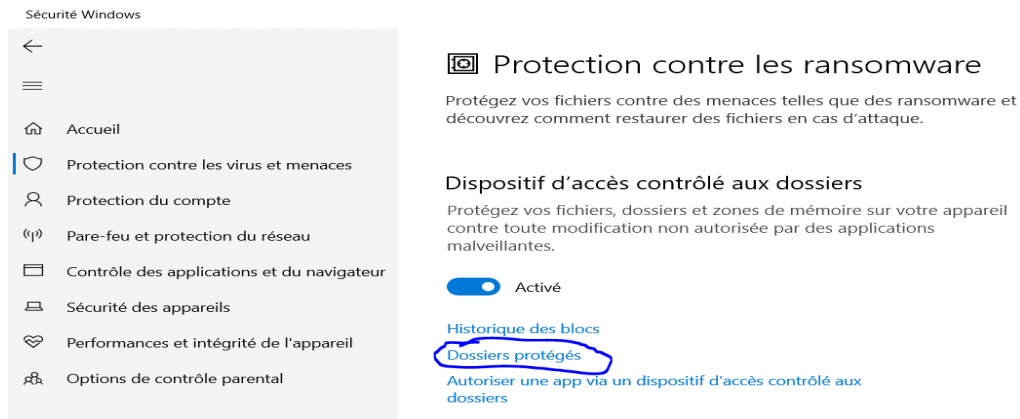
3.2 Activer la protection contre les ransomwares

1. Aller dans **Sécurité Windows > Protection contre les virus et menaces**.
2. Sous **Protection contre les ransomwares**, cliquer sur **Gérer la protection contre les ransomwares**.

Mise en place et configuration de Microsoft Defender pour la protection des postes de travail et la gestion des menaces via Microsoft 365 Defender



3. Activer **Accès contrôlé aux dossiers** et ajouter les dossiers critiques à protéger en allant dans **Dossiers protégés > Ajouter un dossier partagé**.



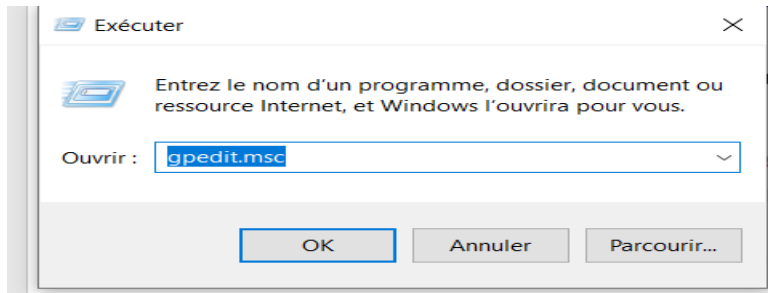
Remarque : On constate que notre dossier **Virtual Machines** a bien été ajouté avec succès.

3.3 Configurer les notifications et rapports

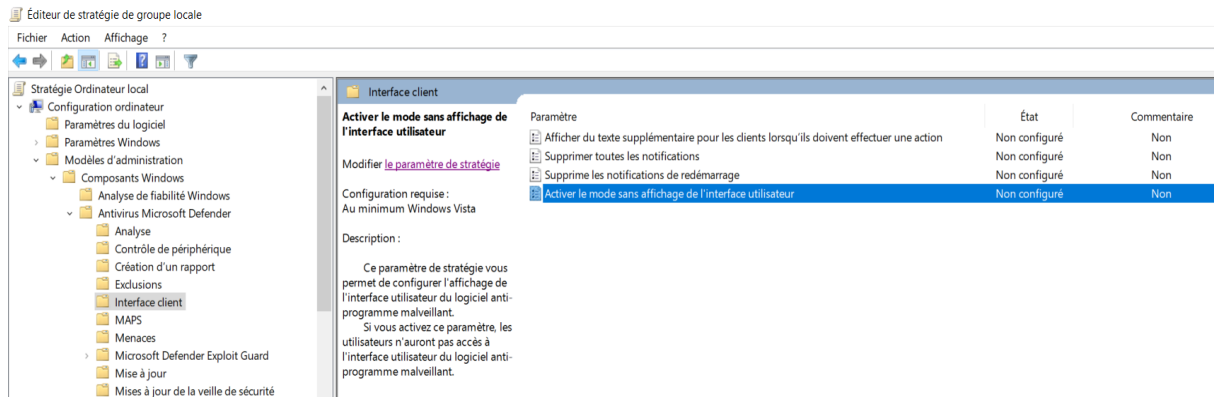
1. Ouvrir **Stratégies de groupe (gpedit.msc)**.

Appuyez sur **Windows + R**, tapez **gpedit.msc**, puis appuyez sur **Entrée**.

Mise en place et configuration de Microsoft Defender pour la protection des postes de travail et la gestion des menaces via Microsoft 365 Defender

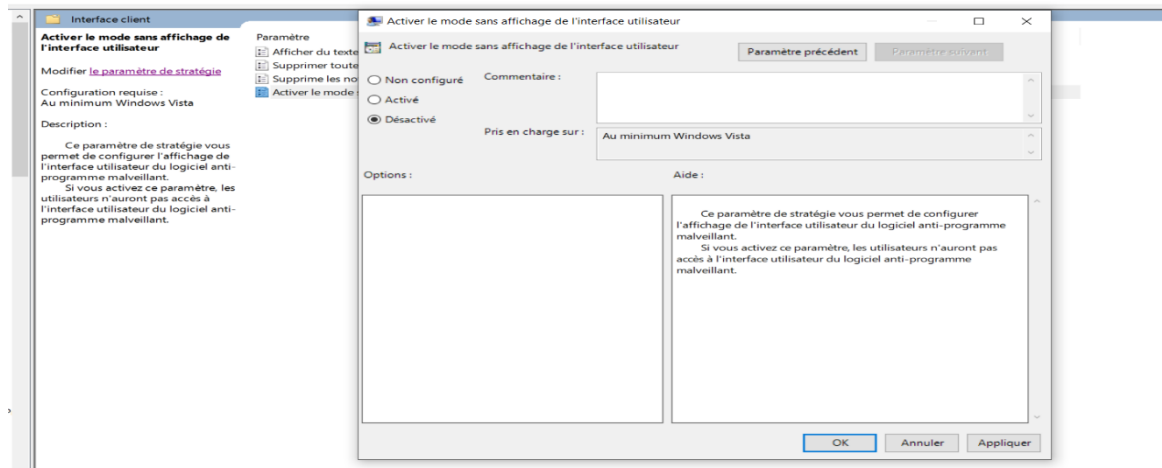


2. Aller dans **Configuration ordinateur > Modèles d'administration > Antivirus Microsoft Defender > Interface client.**



3. Activer les notifications pour obtenir des alertes en cas de menace.

Double-cliquez sur **Activer le mode sans affichage de l'Interface utilisateur**. Si elle est activée, désactivez-la (en choisissant "**Non configuré**" ou "**Désactivé**"). Cela permet à Windows Defender d'afficher l'interface utilisateur et les notifications.

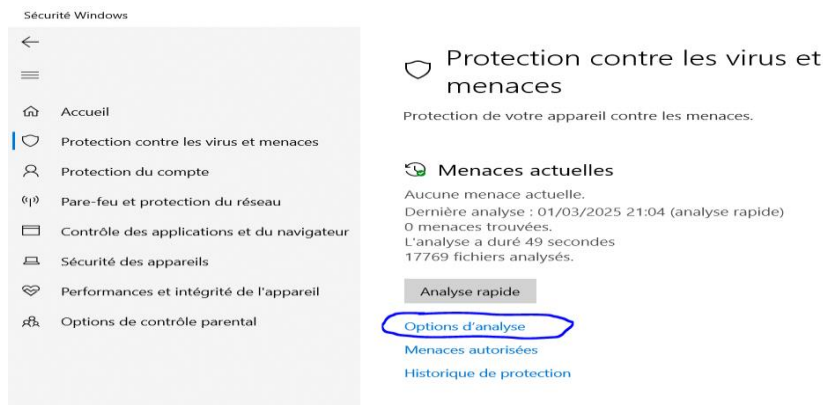


4. Test et Validation de la Sécurité

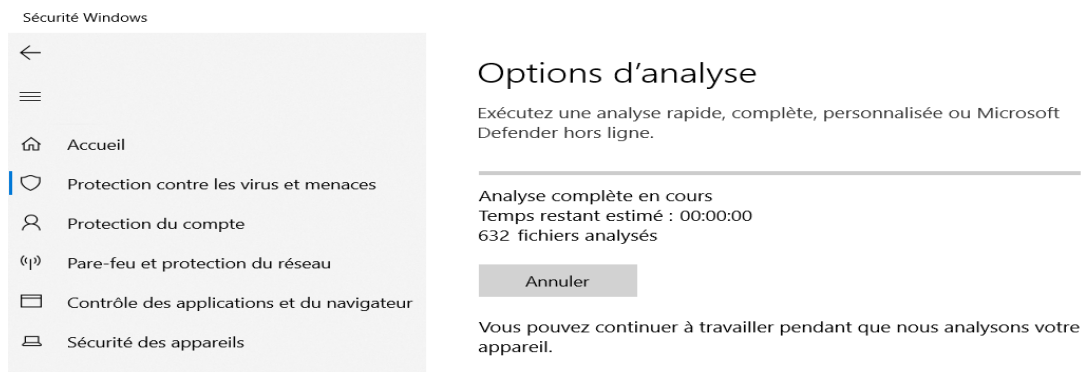
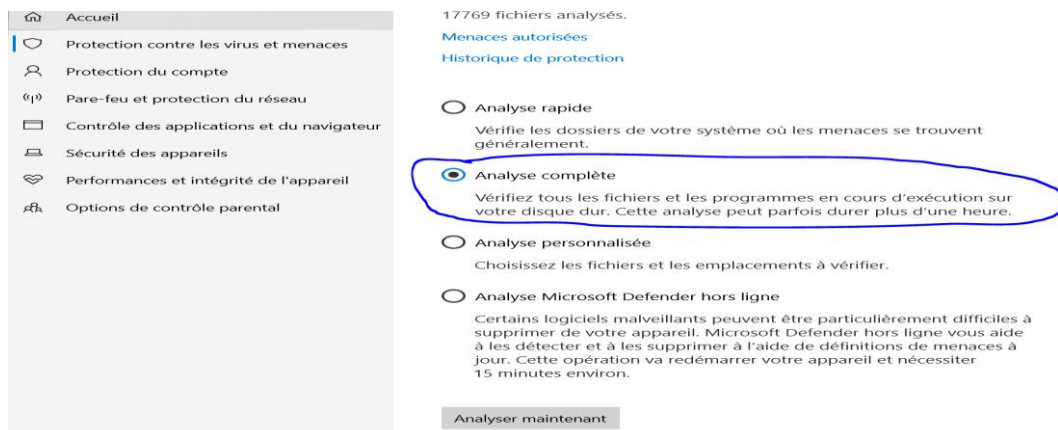
4.1 Exécuter une analyse complète du système

1. Ouvrir **Sécurité Windows > Protection contre les virus et menaces.**
2. Cliquer sur **Options d'analyse.**

Mise en place et configuration de Microsoft Defender pour la protection des postes de travail et la gestion des menaces via Microsoft 365 Defender



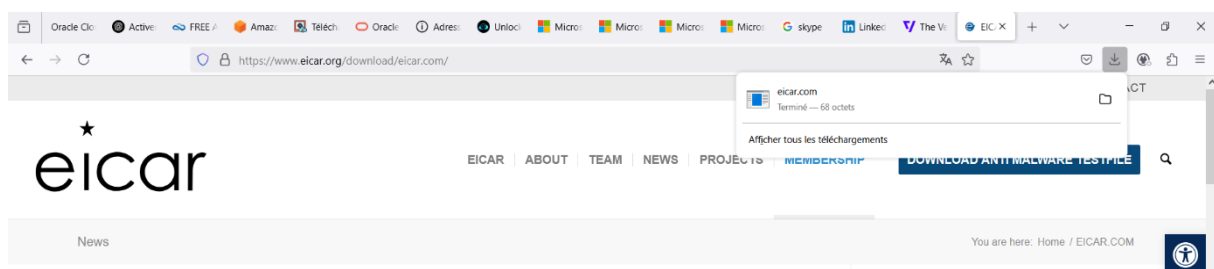
3. Sélectionner **Analyse complète** et lancer l'analyse.



4.2 Simuler une attaque avec un fichier de test EICAR

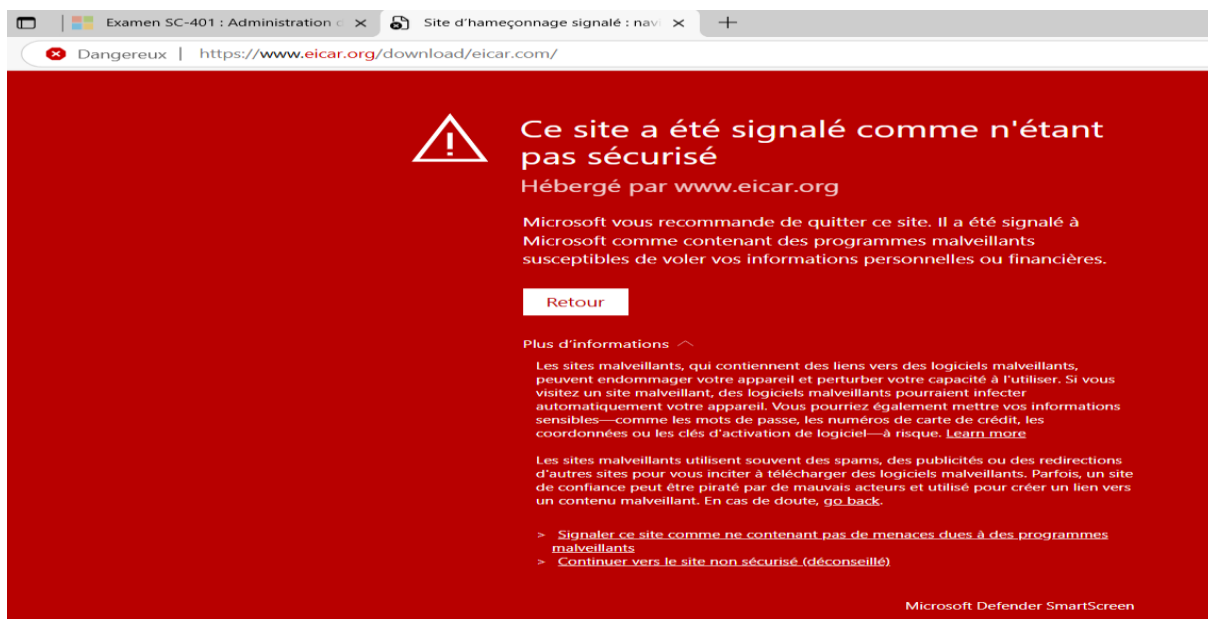
1. Télécharger un fichier de test EICAR (simulation d'un virus inoffensif) depuis :

<https://www.eicar.org/download/eicar.com>



Mise en place et configuration de Microsoft Defender pour la protection des postes de travail et la gestion des menaces via Microsoft 365 Defender

Remarque : L'accès au site via le navigateur **Microsoft Edge** sera bloqué automatiquement par **Microsoft Defender** comme le montre l'image ci-dessous.



2. Microsoft Defender devrait immédiatement détecter et bloquer le fichier.



3. Vérifier les logs dans **Protection contre les virus et menaces > Historique de protection**.



 **Historique de protection**

Consultez les dernières actions de protection et les recommandations de Sécurité Windows.

Tous les éléments récents Filtres ▾



Menace supprimée ou restaurée
02/03/2025 01:37 Grave ^





Détecté : Virus:DOS/EICAR_Test_File
État : Supprimé ou restauré
Cette menace ou application a été supprimée de la quarantaine ou restaurée sur l'appareil.


Date : 02/03/2025 01:38
Détails : Ce programme est dangereux et il se réplique en infectant d'autres fichiers.


Éléments affectés :
file: C:\Users\ADMIN\Downloads\eicar.com


[En savoir plus](#)

En cliquant sur **En savoir plus**, on est redirigé sur la page web ci-dessous :

← → ↺  https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?name=Virus%3ADOS%2FEICAR_Test_File&threatid=2   

 Maximiser vos points avec l'extension Microsoft Rewards
Accès rapide à vos points et offres quotidiens Non merci Ajoutez-le maintenant

 | [Microsoft Security Intelligence](#) Menaces Blogs Téléchargements Soumissions Aide Ensemble de Microsoft Recherche Chariot Se connecter

 Nous mettons progressivement à jour les noms d'acteurs de menaces dans nos rapports pour s'aligner sur la nouvelle taxonomie sur le thème des météorologies.
[En savoir plus sur les noms d'acteurs de la menace de Microsoft](#)

Publiée le 10 janvier 2005 - Mis à jour le 05 septembre 2017 [Renseignez-vous sur d'autres menaces >](#)

Virus:DOS/EICAR-Test-File

[Détecté par Microsoft Defender Antivirus](#)

Alias : EICAR (ORG de la liste des feuilles de commerce), EICAR-Test-File (et non un virus) (BitDefender), Échelle d'essai, EICAR (AC), Eicar-test (ESET), Eicar-test-file (Frisik (F-Pro)), EICAR-Test-File (Kaspersky), EICAR-AV-Etest (Sophos), Eicar-test-file (Trend Micro)

Résumé

Ce fichier n'est pas malveillant.

Il est utilisé pour vérifier que votre logiciel de sécurité fonctionne correctement.

Si vous avez téléchargé ce fichier et continuez à recevoir des avertissements à partir de votre logiciel de sécurité à ce sujet, vous pouvez le supprimer manuellement ou le supprimer.

4.3 Vérifier la protection en temps réel

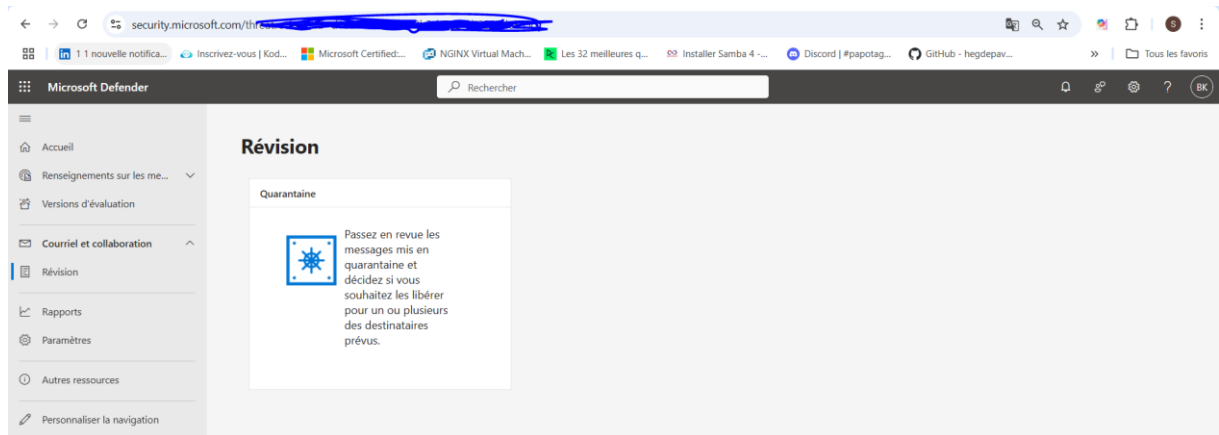
1. Tenter de désactiver Microsoft Defender via les paramètres.
2. Il doit refuser la désactivation en raison de la **protection contre les falsifications**.
3. S'assurer que la protection est bien activée.

5. Surveillance et gestion des menaces avec Microsoft 365 Defender

5.1 Accéder au portail Microsoft Defender

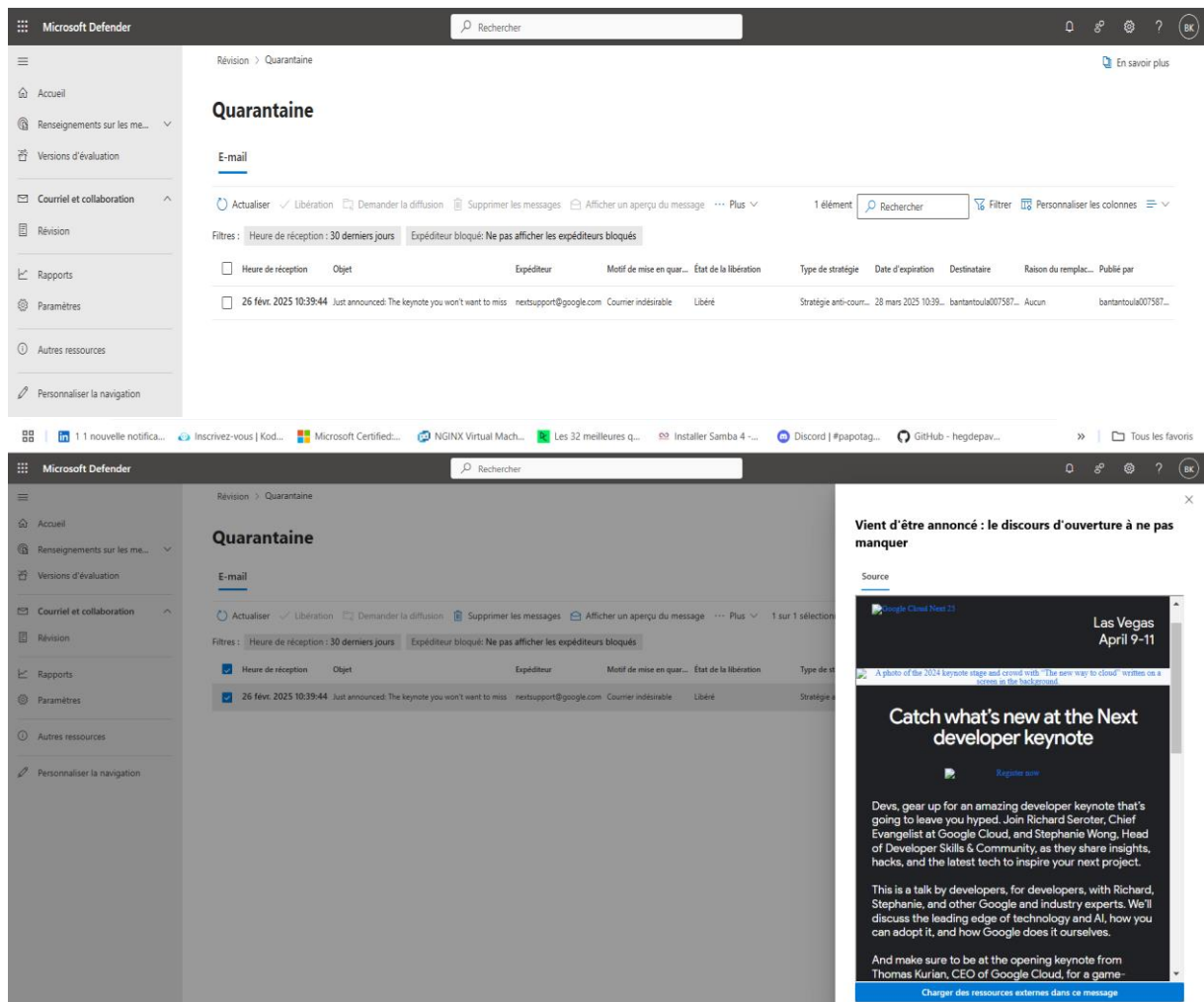
1. Aller sur <https://security.microsoft.com>.
2. Se connecter avec votre compte Microsoft 365.
3. Explorer le tableau de bord pour voir les menaces et incidents signalés.

Mise en place et configuration de Microsoft Defender pour la protection des postes de travail et la gestion des menaces via Microsoft 365 Defender

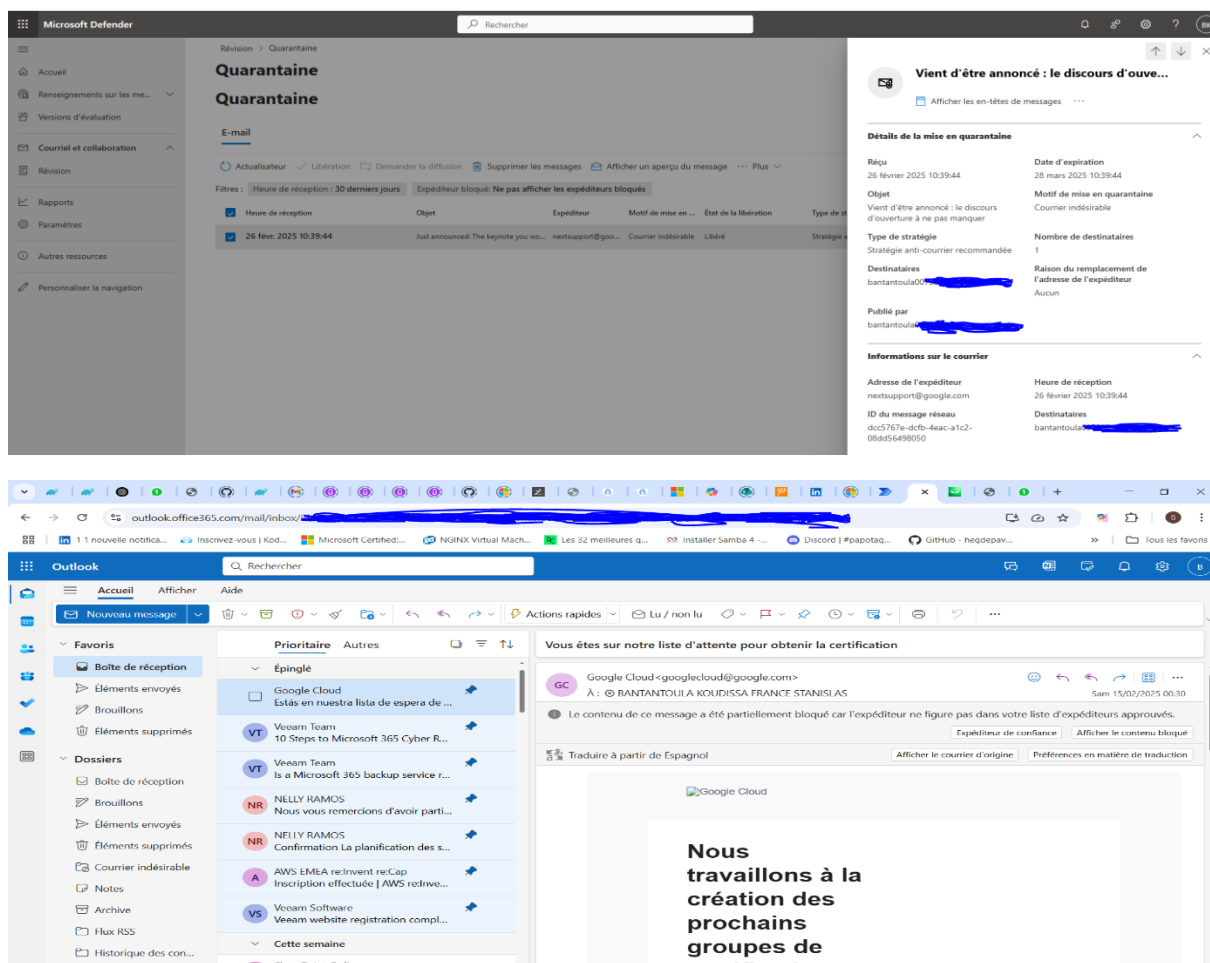


5.2 Gestion des emails bloqués via Microsoft 365 Defender

1. Aller dans **Courriels et collaboration**.
2. Vérifier les emails placés quarantaine dans **Révision > Quarantaine**.
3. Restaurer, afficher ou supprimer des emails en fonction de l'analyse.
4. Configurer des règles anti-phishing et anti-spam.



Mise en place et configuration de Microsoft Defender pour la protection des postes de travail et la gestion des menaces via Microsoft 365 Defender



5.3 Générer des rapports de sécurité

1. Aller dans **Rapports**.
2. Générer un rapport sur les menaces détectées.
3. Analyser les tendances et améliorer la protection en fonction des résultats.



Conclusion

Ce laboratoire nous a permis de configurer et tester Microsoft Defender de manière approfondie, tout en intégrant **Microsoft 365 Defender** pour la gestion centralisée des menaces. Nous avons renforcé la protection de notre système contre les cyberattaques et appris à exploiter les outils avancés de surveillance et de protection des emails.