

PROCEDURE NETTOYAGE LOGIQUE

OBJECTIF :

- Supprimer les applications inutiles, les infections éventuelles, réparer le système d'exploitation, le mettre à jour et le sécuriser.

MATERIELS :

- Clef USB de nettoyage

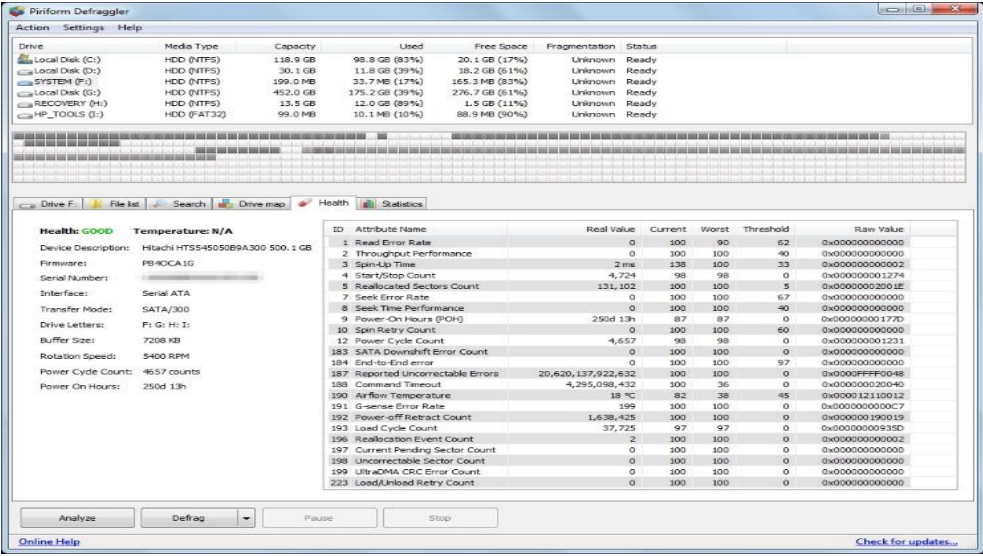
DEMARRAGE	1
NETTOYAGE OFFLINE	2
NETTOYAGE ONLINE	4
SECURITE	11
REPARATION	13
VERIFICATION	14
RESULTATS ATTENDUS	15



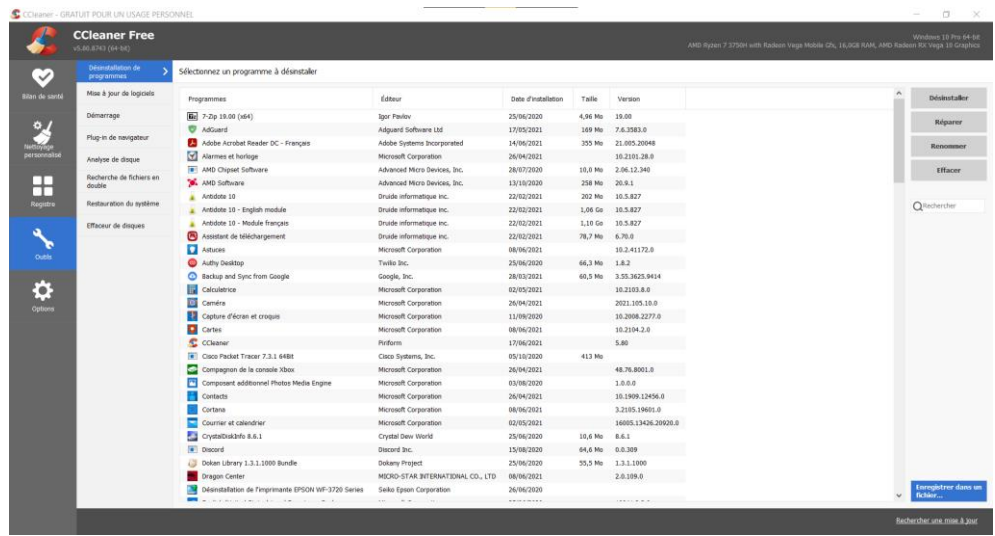
Activité	NETTOYAGE LOGIQUE	Version	1.0
Date de création / Auteur	16 juin 2021 / Florent SPRING (Technicien informatique en apprentissage)	Date de dernière mise à jour	
Acteurs concernés	Techniciens informatiques de l'atelier	Approbateur	

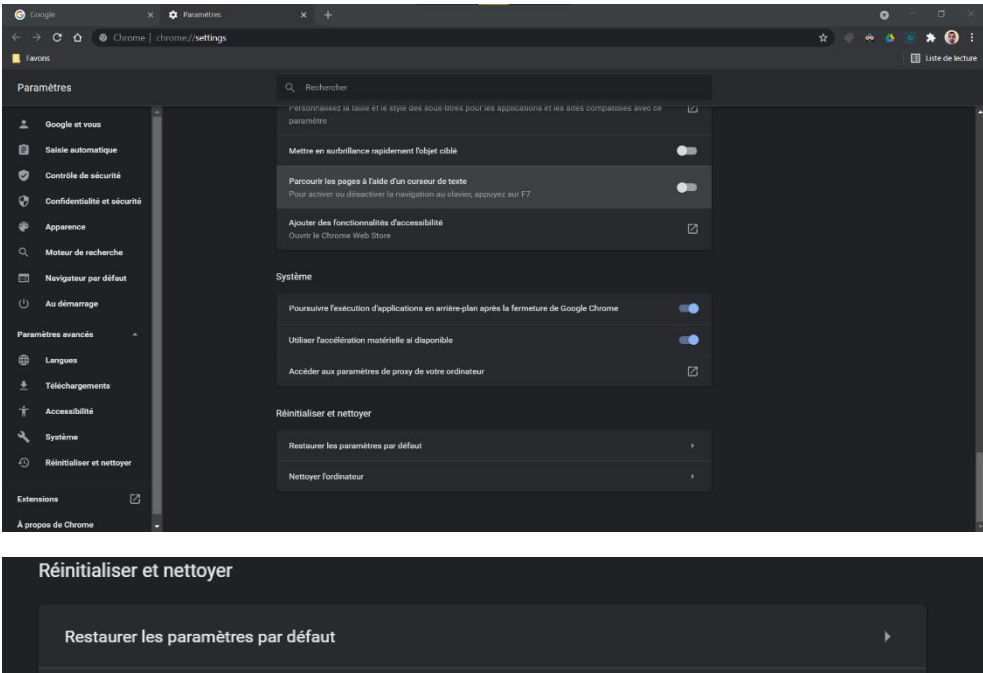
Version	Modifié par	Approbateur	Modifications

DEMARRAGE

N°	Description	Points de vigilance	Moyens	Captures
1 - Réseau	- Le matériel ne doit pas être connecté au réseau.	- Bien vérifier que le wifi ne soit pas activé et que le câble Ethernet soit débranché.	° Cable Ethernet débranché et wifi non connecté	
2 - Stockage	- Vérifier la santé du disque dur.		° Defragger	 <p>The screenshot shows the Piriform Defraggler interface. The top section lists drives with their media type, capacity, used space, free space, fragmentation, and status. The bottom section shows the 'Health' and 'Statistics' for the selected drive (C:). The health is 'GOOD' and the temperature is 'N/A'. The statistics table includes various attributes like Read Error Rate, Throughput Performance, Spin-Up Time, Start/Stop Count, Reallocated Sectors Count, Seek Error Rate, Seek Time Performance, Power-On Hours (POH), Spin Retry Count, Power Cycle Count, SATA Downshift Error Count, End-to-End error, Reported Uncorrectable Errors, Command Timeout, Airflow Temperature, 0-sense Error Rate, Power-off Retract Count, Load Cycle Count, Reallocation Event Count, Current Pending Sector Count, Uncorrectable Sector Count, and Load/Unload Retry Count.</p>

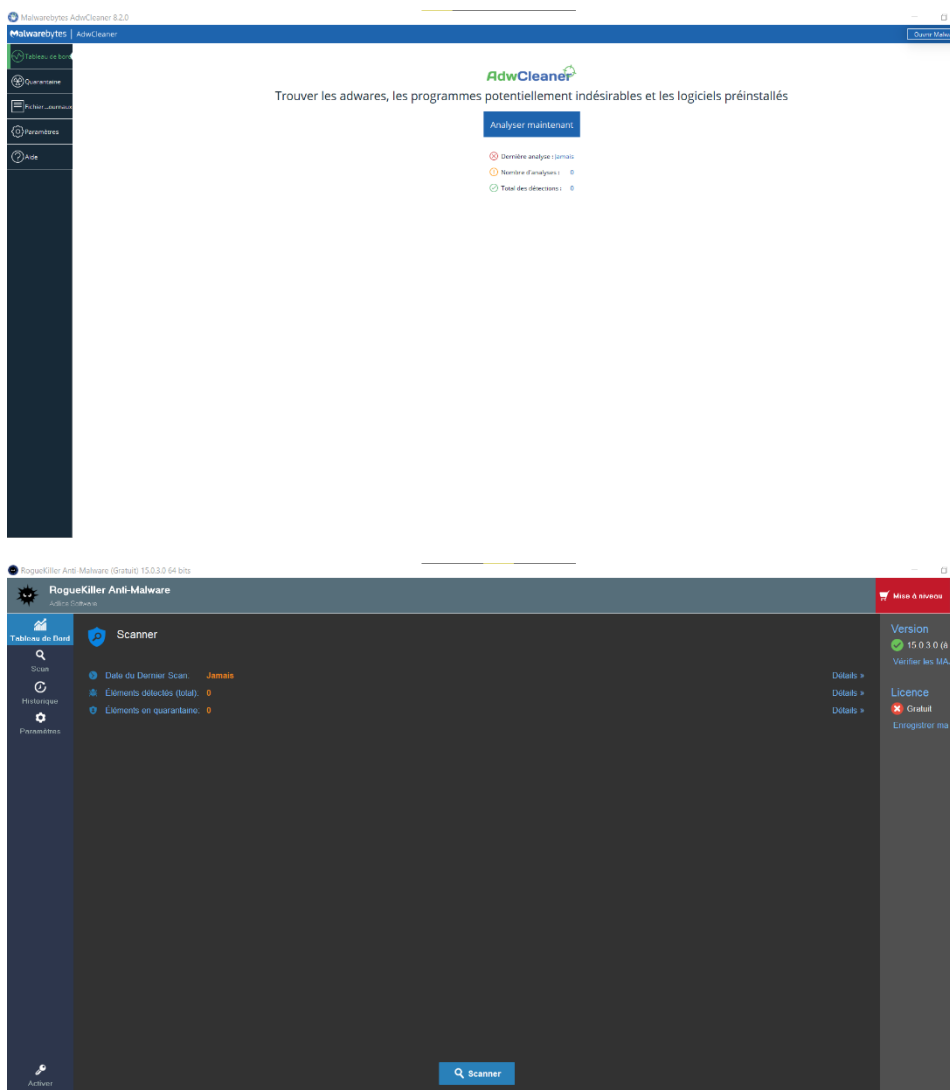
NETTOYAGE OFFLINE

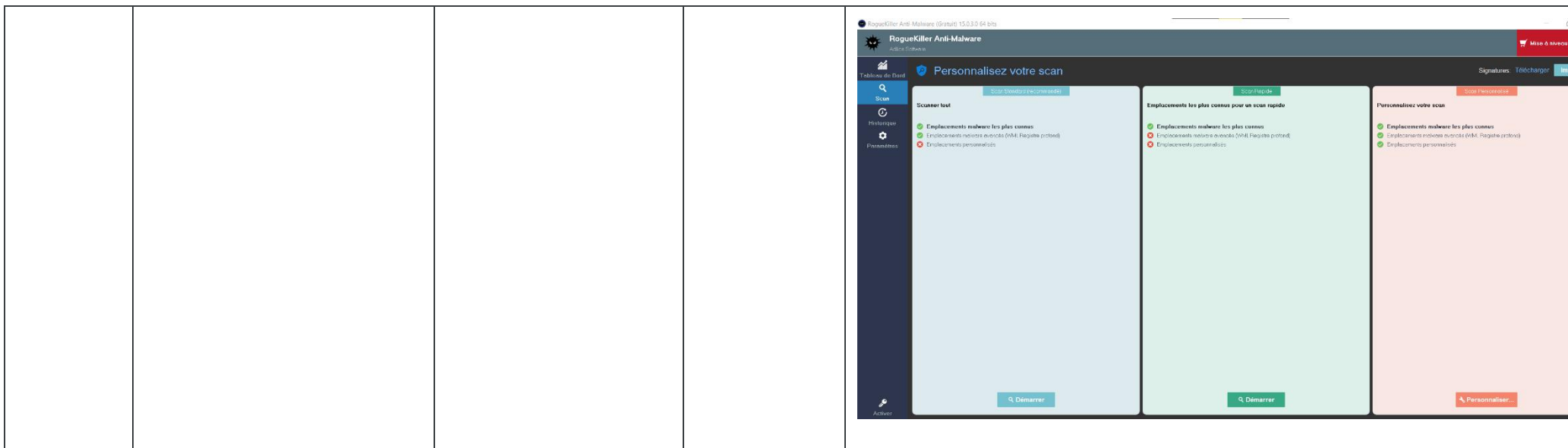
N°	Description	Points de vigilance	Moyens	Captures
1 - Applications-Logiciels installés	- Vérifier qu'il n'y a pas de logiciels malveillants/néfastes d'installés.	- Faire attention aux logiciels qui ne s'installent pas mais qui sont en version portable exécutable (dans le dossier téléchargement par exemple).	<ul style="list-style-type: none"> ° CCleaner ° Outils spécifiques, par exemple, un exécutable de nettoyage d'un logiciel antivirus en particulier (Avastclear.exe, ...) 	 <p>The screenshot shows the CCleaner Free application window. The 'Programs' tab is selected, displaying a list of installed programs. The list includes columns for Programmes, Éditeur, Date d'installation, Taille, and Version. Programs listed include 7-Zip, AdGuard, Adobe Acrobat Reader DC, Alarms and Hurlage, AMD Chipset Software, AMD Software, Autodesk 10, Autodesk 10 - English module, Autodesk 10 - Module Français, Assistant de téléchargement, Audacity, Audacity Desktop, Backup and Sync from Google, Calculatrice, Caméra, Capture d'écran et croquis, Cartes, CCleaner, Cisco Packet Tracer 7.3.1 64Bit, Campaigne de la console Xbox, Composant additionnel Photos Media Engine, Contacts, Cortana, Courrier et calendrier, CrystalDiskInfo 8.6.1, Discord, Vulkan Library 1.3.1.1000 Bundle, Dragon Center, and Désinstallation de l'imprimante EPSON WF-3720 Series.</p>

<p>2 - Nettoyage des navigateurs</p>	<ul style="list-style-type: none"> - Reset des différents navigateurs installés. - Vérifier les extensions des navigateurs. 	<ul style="list-style-type: none"> - Aller dans chaque navigateur et restaurer les paramètres par défaut sans suppression des favoris ni des mots de passe enregistrés. - Supprimer toutes les extensions inutiles. 	<p>° Voir dans les paramètres de chaque navigateur</p>	 <p>The screenshot shows the Chrome settings page in French. The left sidebar lists various settings categories. The main content area is titled 'Paramètres' and includes sections for 'Google et vous', 'Système', and 'Réinitialiser et nettoyer'. The 'Réinitialiser et nettoyer' section is highlighted, showing options to 'Restaurer les paramètres par défaut' (Restore default settings) and 'Nettoyer l'ordinateur' (Clean up computer). Below the screenshot, there is a dark grey box with the title 'Réinitialiser et nettoyer' and a button labeled 'Restaurer les paramètres par défaut' with a right-pointing arrow.</p>
--	---	---	--	---

NETTOYAGE ONLINE

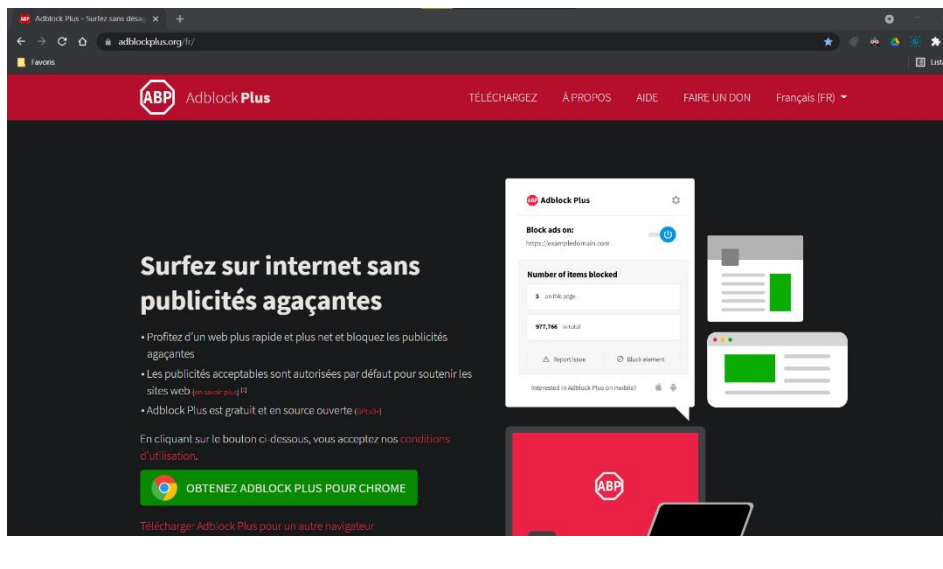
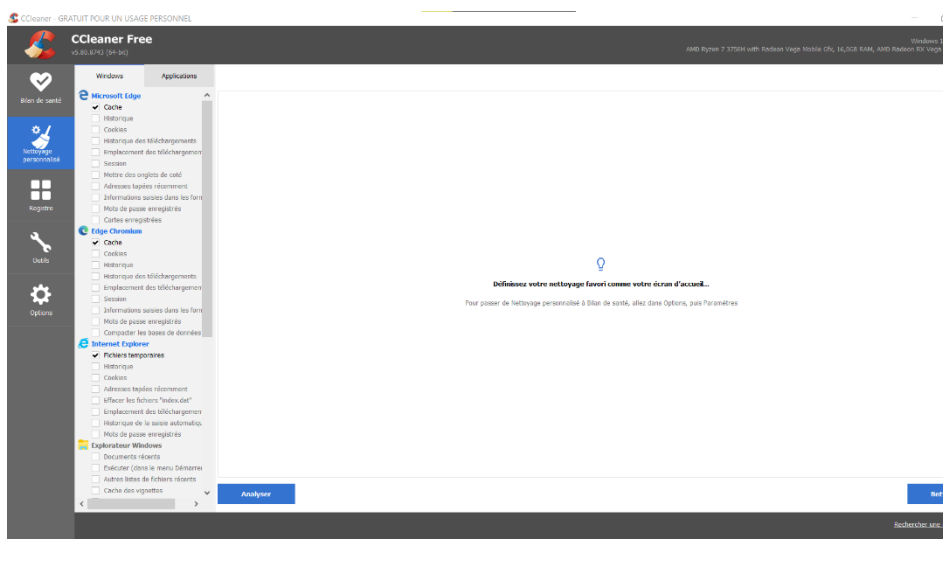
<i>N°</i>	<i>Description</i>	<i>Points de vigilance</i>	<i>Moyens</i>	<i>Captures</i>
1 - Réseau	- Connecter le matériel au réseau.		° Cable Ethernet branché ou Wifi connecté	

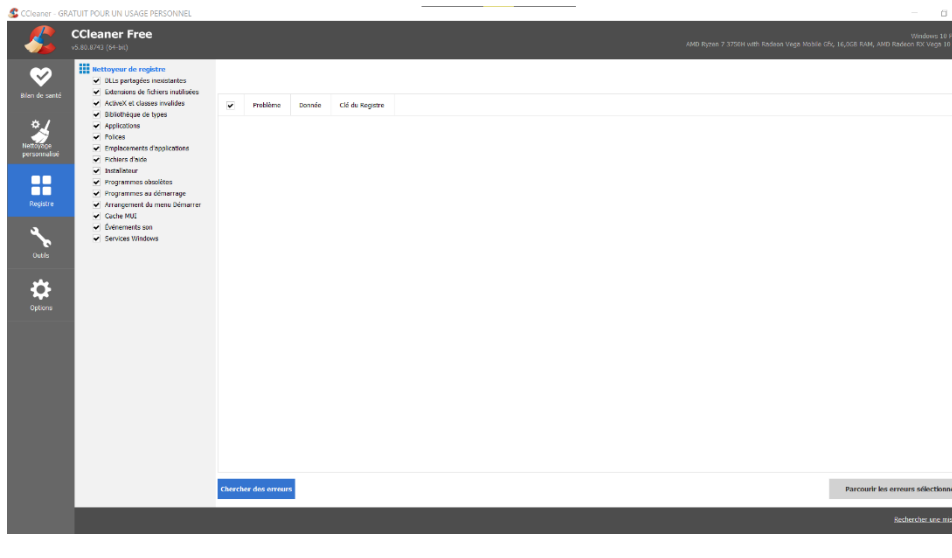
2 - Logiciels de désinfection	- Lancer un scan grâce aux différents outils, mettre en quarantaine/supprimer les menaces.	<p>- A faire dans l'ordre :</p> <ul style="list-style-type: none"> • Adwcleaner • RogueKiller (faire un scan standard) • Mbar (penser à cliquer sur « update » avant de scanner) 	° Dans le dossier « Nettoyage logique » de la clef USB de nettoyage	 <p>The image shows two screenshots of malware removal software. The top screenshot is the AdwCleaner 8.2.0 interface, which is a web-based application. It has a blue header with the title 'Malwarebytes AdwCleaner 8.2.0'. The main area is white and contains the text 'Trouver les adwares, les programmes potentiellement indésirables et les logiciels préinstallés'. There is a blue button labeled 'Analyser maintenant'. Below this, there are three status indicators: 'Dernière analyse : Jamais', 'Nombre d'analyses : 0', and 'Total des détecteurs : 0'. The bottom screenshot is the RogueKiller Anti-Malware (v15.0.3.0) interface. It has a dark blue header with the title 'RogueKiller Anti-Malware (Gratuit) 15.0.3.0 64 bits'. The main area is dark grey and contains a 'Scanner' button. Below this, there are three status indicators: 'Date du Dernier Scan : Jamais', 'Éléments détectés (total) : 0', and 'Éléments en quarantaine : 0'. On the right side, there is a sidebar with 'Version 15.0.3.0 (64 bits)', 'Licence Gratuit', and 'Créé par Florent Spring'.</p>
-------------------------------	--	---	---	---



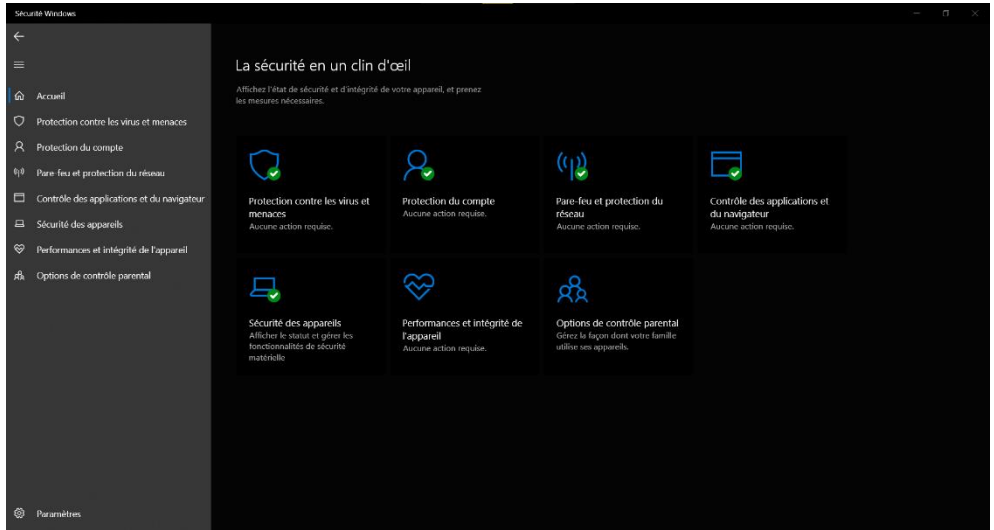
				
--	--	--	--	--

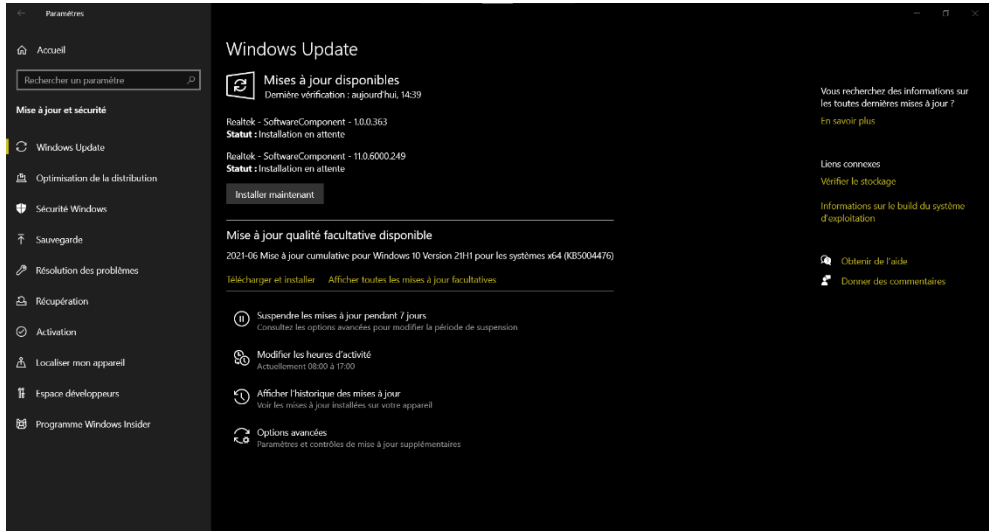


3 - Adblockplus	- Ajouter l'extension dans chaque navigateur.	- Bien installer l'extension du site : « https://adblockplus.org/fr/ ».	° Par les navigateurs directement	
4 - Nettoyage fichiers inutiles	- Suppression des fichiers temporaires, cookies, etc...	- Laisser par défaut les paramètres pour le nettoyage.	° CCleaner	

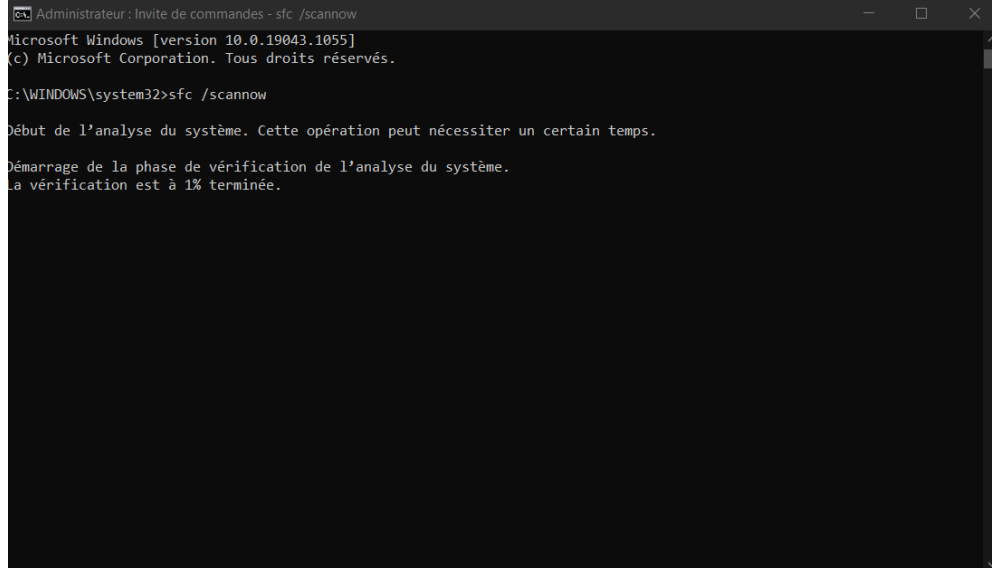
5 - Nettoyage du registre	- Supprimer les entrées de registre manquantes/défectueuses.	- Pas besoin d'enregistrer un fichier backup des entrées qu'on va supprimer.	° CCleaner	
---------------------------------	--	---	------------	---

SECURITE

N°	Description	Points de vigilance	Moyens	Captures
1 - Vérifier la sécurité de l'ordinateur	- Vérifier que l'antivirus installé soit bien activé (Kaspersky, Defender, ...)	<p>- Si le client a une suite de sécurité payante et que l'abonnement est en cours, lui laissé cette protection. Sinon remettre Windows Defender.</p> <p>- Pas plus d'un logiciel de sécurité à la fois.</p>	<p>° Logiciel de sécurité tiers ou dans la sécurité de Windows</p> <p>Onglet « Mise à jour et sécurité / Sécurité Windows »</p>	

2 - Vérifier les mises à jour	- Vérifier si l'ordinateur est bien à jour.		° Dans les paramètres Windows et dans l'application fournie par le fabricant du matériel (Lenovo Vantage, HP Support Assistant, ...)	
-------------------------------	---	--	--	---

REPARATION

N°	Description	Points de vigilance	Moyens	Captures
1 - Système d'exploitation	- Réparer les problèmes éventuels du système d'exploitation.		- Invite de commande : « sfc /scannow »	 <pre> Administrateur : Invite de commandes - sfc /scannow Microsoft Windows [version 10.0.19043.1055] (c) Microsoft Corporation. Tous droits réservés. C:\WINDOWS\system32>sfc /scannow Début de l'analyse du système. Cette opération peut nécessiter un certain temps. Démarrage de la phase de vérification de l'analyse du système. La vérification est à 1% terminée. </pre>

VERIFICATION

N°	Description	Points de vigilance	Moyens	Captures
1 - Vérifier le réseau	- Vérifier que le PC à bien internet.		° En lançant une recherche internet par exemple.	
2 - Redémarrage	- Vérifier que le PC redémarre correctement.			

Résultats attendus

- Le PC ne doit plus avoir d'infections et doit fonctionner de façon optimale. Il doit être à jour et sécurisé.