Korantin Horuckowa

PRÉVISION

une vision, des valeurs, la passion d'entreprendre

Sécurisation des séquences de démarrages

Table des matières

I But du stage

A) Contexte

Le but du projet est de proposer des correctifs potentiels à l'un des problèmes soulevés dans la matrice des vulnérabilités associées à un projet d'audit cybersécurité.

Récurrence dans les attaques	Impact potentiel sur le SI	Note urgence	Statut	Catégorie	Problème	Solution	Préconisation
3	3	7	En cours	USB	Rootkits	Options BIOS / UEFI	Activation du secure boot, Trusted boot, ELAM dans le BIOS

Cellule concernant le problème relevé (ligne 5)

> J'ai ensuite posé des questions plus spécifiques sur les machines en commençant par des questions sur les accès physiques. J'ai fait plusieurs découvertes parmi lesquelles: les disques durs ne sont pas chiffrés, il n'y a pas de mot de passe sur le BIOS et certaines options ne sont pas activées comme l'early launch anti malware (ELAM).

Extrait du rapport

Quelle solution peut-être mise en place pour éliminer les risques de rootkits au démarrage des machines et comment la mettre en place de manière à gagner du temps sur le long terme?

Le but de ce projet est de pallier aux risques d'infection par Rootkits, du moins lors du boot de l'équipement.
En vue du parc informatique de l'entreprise qui est conséquent, une installation, une modification ou un paramétrage n'est pas possible à faire poste par poste. Un script peut donc être envisageable. Une solution de secure boot combinée au trust boot et à ELAM peut-être envisagée, en revanche une étude du parc informatique doit-être faite au préalable pour connaître le parc, ses caractéristiques et ainsi adapter le script en conséquence. En effet, en plus d'automatiser la tâche de configuration (si la solution citée plus haut est pertinente pour le problème rencontré) nous pouvons aussi essayer de faire en sorte de l'appliquer à tous les postes. Un déploiement à grande échelle serait donc l'issue à privilégier. Bien que la recherche du bon script et de la bonne façon de l'automatiser risque de prendre un certain temps, sur le long terme le temps passé sur sa réalisation sera amortie.

B) Définition des termes et prise en main du sujet

USB: de l'anglais "Universal Serial Bus" c'est une norme de bus informatique en série permettant de connecter des périphériques informatiques à un ordinateur ou à tout type d'appareil prévu à cet effet.

Firmware: ou micrologiciel est un programme intégré dans un matériel informatique pour que celui-ci puisse fonctionner.

BIOS: ou "Basic Input/Output System" est le programme intégré à la carte mère que le microprocesseur d'un pc utilise pour démarrer. Il permet de vérifier deux fonctions principales lors de la phase de démarrage de l'ordinateur. Premièrement vérifier le bon fonctionnement des composants à l'image de la carte mère et des périphériques (clavier, disques dur…) c'est ce que l'on appelle le test POST (Power on Self Test) et deuxièmement de lancer le système d'exploitation.
UEFI: de l'anglais "Unified Extensible Firmware Interface" ou "Interface Micrologicielle Extensible Unifiée". Il définit une interface entre le micrologiciel (firmware) et l'OS (Operating System ou système d'exploitation) d'un ordinateur. Il permet notamment l'affichage d'une interface graphique de bonne résolution.
Le BIOS ou l'UEFI servent d'interface entre le matériel de l'ordinateur et le système d'exploitation.

Secure boot: ou boot de démarrage sécurisé est une fonctionnalité du BIOS/UEFI qui permet de s'assurer qu'un ordinateur démarre uniquement en utilisant les logiciels approuvés par le fabricant de l'ordinateur, de manière à se protéger des logiciels malveillants. Il peut parfois bloquer le boot sur une clé USB, le secure boot peut donc être amené à être désactivé. Disponible depuis 2013, sur les machines compatibles Windows 8 et les serveurs depuis Windows Serveur 2012.

Trusted boot: prend le relais lorsque le démarrage sécurisé se termine. Le chargeur de démarrage vérifie la signature numérique du noyau Windows avant de le changer. Le noyau Windows examine ensuite tous les autres composants du processus de démarrage Windows, y compris les pilotes de démarrage, les fichiers de démarrage et l'ELAM. Si un fichier à été modifié, le chargeur de démarrage détecte le problème et refuse de charger le composant en question.

ELAM (Early Launch Anti-Malware): ou logiciel anti-programme malveillant à lancement anticipé. Lancé par le noyau windows, ELAM est assuré d'être lancé avant les autres programmes. Il est donc en mesure de détecter les logiciels malveillants dans le processus de démarrage et donc de les empêcher de s'initialiser. Incorporer avec Secure Boot

Measured boot: ou démarrage mesuré, il fonctionne avec le module de plateforme sécurisée TPM et les logiciels non Microsoft dans Windows. Il permet à un serveur approuvé sur le réseau de vérifier l'intégrité du processus de démarrage de Windows. Celui-ci se réalise en 4 étapes:

1. Le microprogramme UEFI du PC stock dans le module de plateforme sécurisée (TPM) un hachage du microprogramme, du chargeur de démarrage, des pilotes de démarrages et de tous les éléments qui seront chargés avant l'application ELAM.

2. A la fin du processus de démarrage, Windows démarre le client d'attestation non-Microsoft à distance. Le serveur d'attestation approuvée envoie au client une clé unique.
3. Le module de plateforme sécurisée utilise cette clé pour signer numériquement le journal enregistré par l'UEFI.
4. Le client envoie le journal au serveur , accompagné éventuellement d'autres informations de sécurité.

En fonction des données reçues, le serveur peut définir si le client est sain.

Combinaison du Secure boot, Trust boot et Measured boot: cela crée un service résistant au Bootkits et Rootkits, permettant sous windows d'éliminer des programmes malveillants au niveau du noyau.

ROM: également appelée mémoire morte, elle permet de stocker des données sur un disque dur et est non volatile. Ce qui lui permet même hors tension de ne pas effacer le contenu. Elle est présentée comme un composant de la carte mère, on parle alors de mémoire CMOS permettant de veiller à l'amorçage du système.

Bootkits: c'est un malware qui se lance au démarrage de l'ordinateur et qui se positionne dans le noyau de l'OS. Permettant le contrôle du matériel infecté. En effet, il s'injecte au moment du boot dans le MBR (Master Boot Record) qui est la partition de boot et qui ne peut être chiffrée.

Rootkits: c'est un type de malware conçu pour permettre à des pirates informatiques d'accéder à un appareil cible de manière furtive et de le contrôler. Les rootkits peuvent être un ensemble de logiciels et assurent leur furtivité via différents mécanismes de dissimulation tels que l'effacement de traces ou encore le masquage de l'activité et des communications.
Le rootkit peut être installé sur un autre logiciel, une bibliothèque ou encore dans le noyau d'un OS. Certains peuvent être conçus pour modifier l'hyperviseur (processus qui permet de créer et d'exécuter des machines virtuelles) ou bien de modifier le micrologiciels présent sur un équipement.

"*L'obtention des droits supérieurs par élévation des privilèges est également fréquemment rencontrée : cela permet notamment de désactiver les mécanismes de défense (comme un anti-virus) ou d'agir sur des objets de haut niveau de privilèges (pilotes de périphériques, noyau du système, etc.) Un rootkit va ainsi pouvoir écouter les transactions sur le réseau pour trouver des mots de passe non chiffrés (comme des connexions ftp) ou détourner une connexion ssh en interceptant l'appel système où le mot de passe n'est pas encore chiffré.*"

Article sur les Rootkits

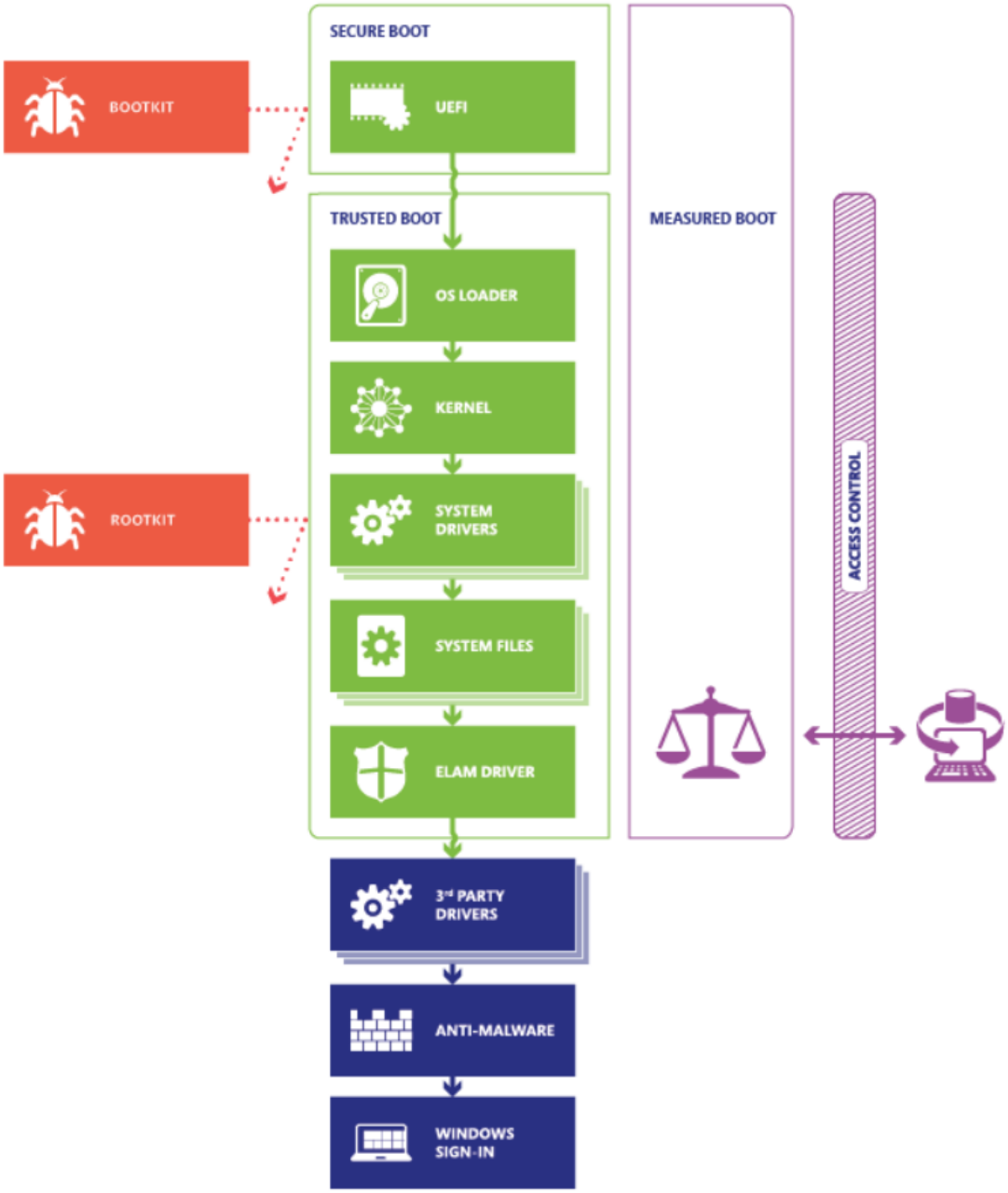


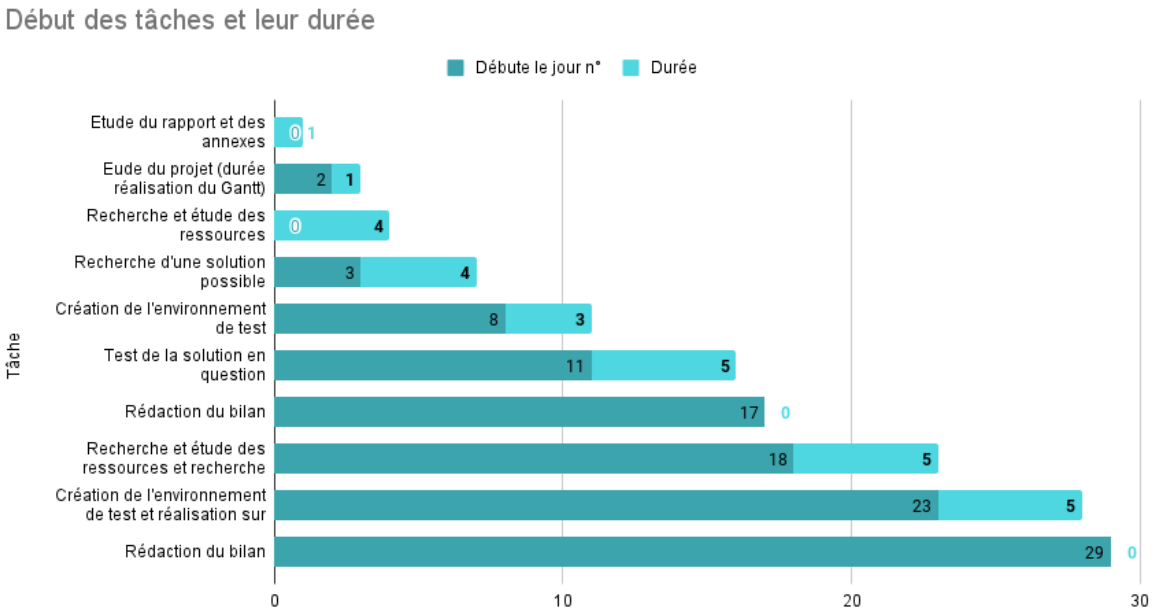
Schéma des menaces et de leurs cibles

En partant du principe que le paramétrage du BIOS/UEFI avec l'activation ou la vérification de l'activation du Secure Boot, du Trust Boot et de l'ELAM peut-être intéressant, des questions se posent.
Comment modifier un BIOS sur des postes DELL ?
Y a- t-il un anti-virus ? ELAM fonctionnera t-il avec celui-ci ?
Est-ce que tous les postes peuvent recevoir un script ? Comment le vérifier ? S'ils ne le peuvent pas comment faire ?
Si la solution fonctionne comment l'automatiser et la lancer à grande échelle ?
Comment le faire de manière sécurisée ?

Bien que différentes solutions existent tels que des antivirus, anti-rootkit, réinstaller le système d'exploitation ou encore l'utilisation d'une sauvegarde après avoir formaté l'appareil, ce ne

sont en général que des solutions après coup. Le plus sage est de trouver une solution fiable à mettre en place en prévention. D'où l'utilisation des outils rendus disponibles via Windows et grâce aux différents constructeurs.

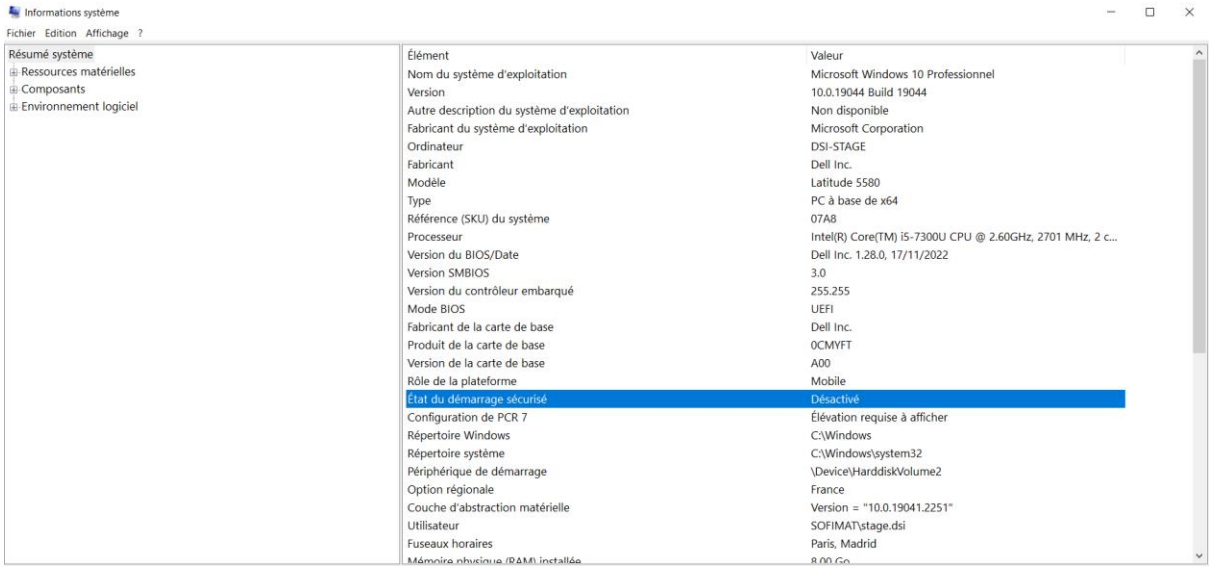
C) Planning projet



II Le Secure Boot

A) Vérification et activation

Premièrement, intéressons-nous au Secure Boot. Nous nous devons de vérifier s'il est activé ou non sur l'appareil. Et pour cela nous n'avons pas forcément besoin de nous rendre sur le BIOS/UEFI. En effet, il suffit de se rendre dans les informations du système pour en prendre connaissance.



Vérification de l'état du démarrage sécurisé

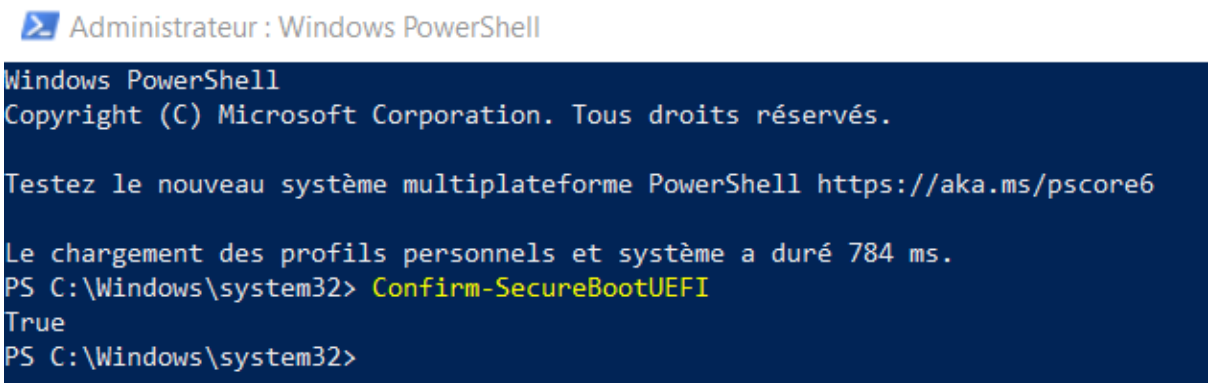
Sur cette machine, le secure boot est désactivé. La question est, est-ce le cas pour toutes les machines du parc informatique? Sachant que celui-ci est présent sur toutes les machines depuis Windows 8 et Windows Server 2012, le parc doit en être munis.

Options de l'écran Démarrage sécurisé

Option	Description
Secure Boot Enable	Permet d'activer ou de désactiver l'option **Secure Boot (Démarrage sécurisé)**. • Disabled (Désactivé) • Enabled (Activé) Paramètre par défaut : activé.
Expert Key Management	Permet de manipuler les bases de données de clés de sécurité uniquement si le système est en mode personnalisé. L'option **Enable Custom Mode (Activer le mode personnalisé)** est désactivée par défaut. Les options disponibles sont les suivantes : • PK • KEK • db • dbx Si vous activez le **Custom Mode (Mode personnalisé)**, les options applicables à **PK, KEK, db et dbx** apparaissent. Les options disponibles sont les suivantes : • **Save to File (Enregistrer dans un fichier)** : enregistre la clé dans un fichier sélectionné par l'utilisateur • **Replace from File (Remplacer depuis un fichier)** : remplace la clé actuelle par une clé obtenue à partir d'un fichier utilisateur sélectionné • **Append from File (Ajouter depuis un fichier)** : ajoute une clé à la base de données actuelle à partir d'un fichier sélectionné par l'utilisateur • **Delete (Supprimer)** : supprime la clé sélectionnée • **Reset All Keys (Réinitialiser toutes les clés)** : réinitialise les clés selon les paramètres par défaut • **Delete All Keys (Supprimer toutes les clés)** : supprime toutes les clés **REMARQUE :** Si vous désactivez le **Custom Mode (Mode personnalisé)**, toutes les modifications effectuées seront effacées et les clés seront restaurées selon les paramètres par défaut.

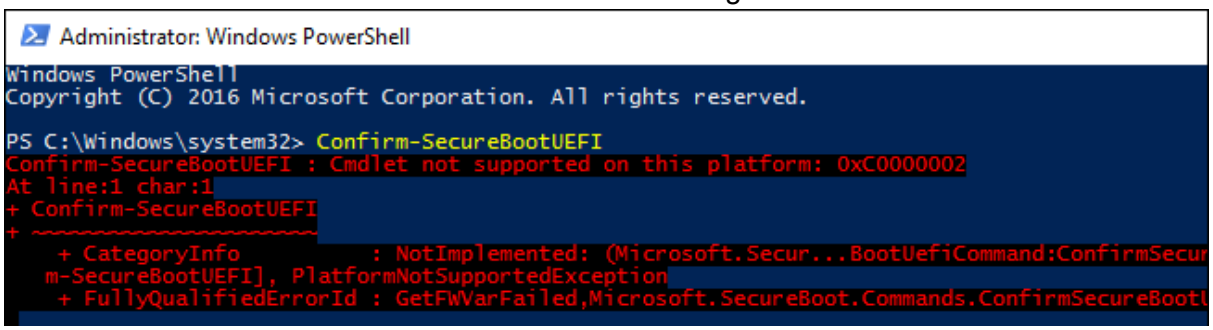
Dell Latitude 5580 Manuel du propriétaire (page 76)

Il est aussi possible de vérifier l'état du Secure boot via une commande Windows Powershell. Pour cela il faut lancer Powershell en tant qu'administrateur et utiliser la commande "Confirm-SecureBootUEFI". Si Secure Boot est activé alors la réponse True sera renvoyée sinon ce sera la réponse False.



Exécution de Confirm-SecureBootUEFI dans powershell

Il est possible que le matériel ne supporte pas Secure boot principalement par raison d'ancienneté du matériel. Si c'est le cas alors un message d'erreur sera retourné.



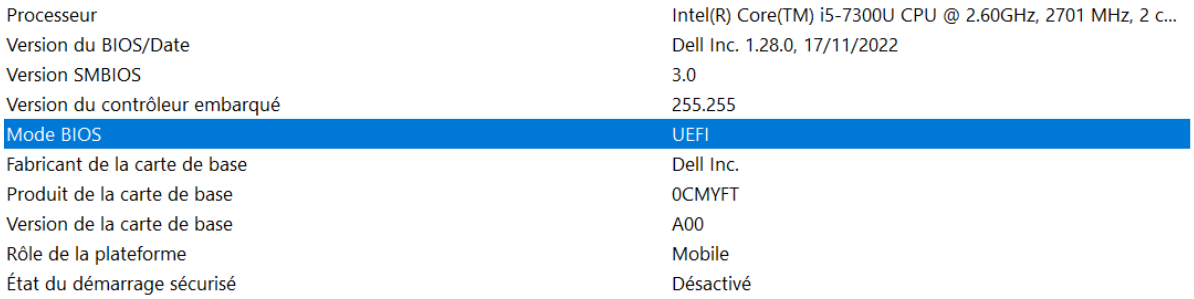
Message d'erreur lors de l'exécution de Confirm-SecureBootUEFI

Enfin, Secure boot peut-être activé via le BIOS/UEFI mais cela va dépendre du modèle du poste ou de la marque. Dans le cas présent, la majeure partie du parc provient du distributeur Dell.

Marque	Game	Touche 1	Touche 2
Dell	Alienware, Inspiron, Latitude, Precision, XPS, Vostro	F2	F12

Touche pour accéder au BIOS chez Dell

Dans le but d'activer secure boot sur un appareil DELL nous devons d'abord contrôler que le mode BIOS est sur UEFI comme sur la figure ci dessous. Si le mode BIOS est sur "hérité", il faut alors le passer sur UEFI.



Vérification du paramétrage du mode BIOS sur UEFI et non Hérité (ou Legacy)

En revanche, il faut faire attention lors de la manipulation puisque passer du mode Hérité à UEFI nécessiterait selon le support DELL, la réinstallation de Windows.

> ⓘ **Remarque :** lorsque vous passez du mode **Hérité** au mode **UEFI**, vous ne pouvez plus démarrer l'installation actuelle de Windows. Cette modification nécessite donc une réinstallation de Windows. Veillez à sauvegarder vos données personnelles avant de poursuivre cette procédure.

(Après une discussion avec l'un des techniciens, j'ai pu conclure que leur logiciel de clonage et les appareils récents règle ce problème automatiquement. Il n'y a donc plus de réelle crainte à devoir réinstaller l'OS et tous ses logiciels, ou cas exceptionnels.)

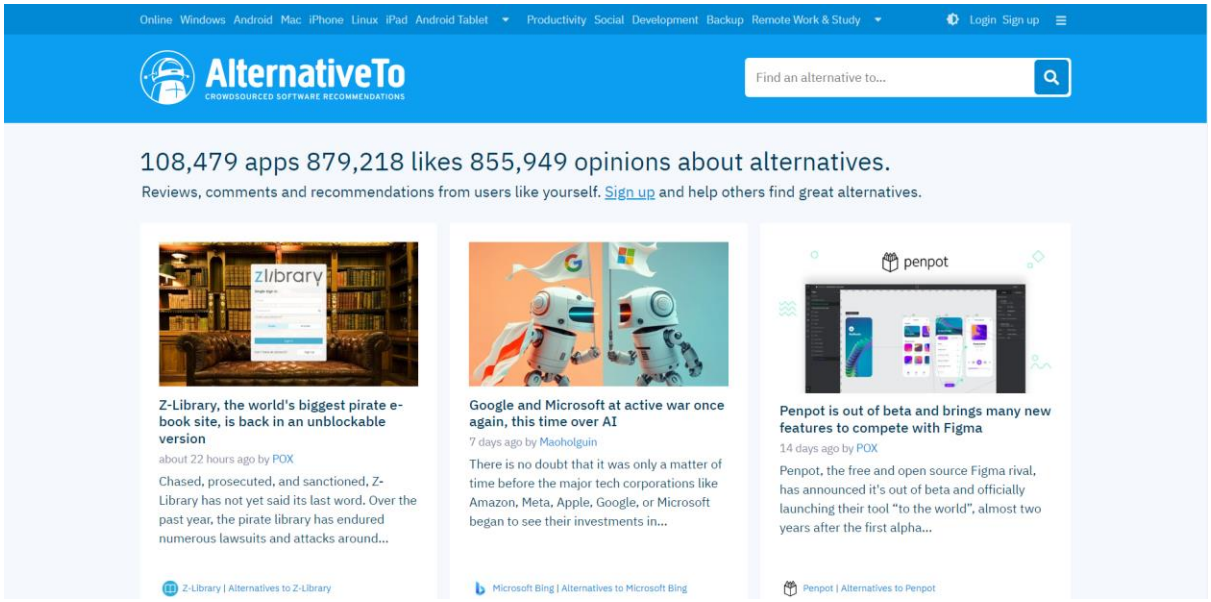
B) BIOS et UEFI

Le fait de passer du mode BIOS Hérité à UEFI donne accès à plus de paramètres de sécurité, une interface plus ergonomique et une gestion de disques plus importants, il est donc plus adapté dans le cas d'une entreprise aussi importante.
Sur la majeure partie des équipements le BIOS est directement paramétré sur UEFI, puisque bien qu'il ne soit pas une norme, c'est un standard technique.

La fonction Secure boot est contrôlée par le firmware de l'ordinateur. Les plates-formes UEFI sécurisées chargent donc uniquement les fichiers logiciels binaires, tels que les pilotes d'options ROM, les programmes de démarrage et les pilotes de chargement du système d'exploitation, non modifiés et considérés comme fiables par la plate-forme.

C) Changer le logiciel de clonage ?

Après avoir parlé avec les techniciens à propos du parc informatique et de l'objectif de mon stage, j'ai appris que les environnements sont cloner sur les postes de travail ce qui apporte un gain de temps. Or, le logiciel de clonage étant trop ancien, il ne supporte pas le Secure Boot et sa désactivation est nécessaire pour que les PC configurés démarrent correctement.
Une autre solution que le script peut donc être envisagée, car un script modifiant directement le BIOS/UEFI n'est pas aisé à faire. Il n'en reste pas moins une bonne solution. En revanche, la configuration des postes avec le Secure Boot activé reste l'option la plus simple à mettre en place. En effet, la désactivation résulte de la configuration de la machine. Or, puisque les ordinateurs sont clonés de cette manière, il peut être intéressant de chercher un nouveau moyen de clonage, plus récent ou du moins qui prend en compte Secure Boot lors du clonage d'environnement.



(via Alternative To par exemple qui permet de trouver des alternative à un logiciel)

Après un test sur le PC portable nommé “Test Cybersécurité” qui est un Dell 5580, nous avons pu constater sur le BIOS/UEFI que le Secure Boot était désactivé. Nous l’avons activé et le PC à démarrer correctement.
De plus, le logiciel de clonage ne prenait pas en compte le secure boot, mais le prends désormais. Les nouveaux postes possèdes donc théoriquement le secure boot activé et les postes futurs l’auront aussi. Sachant que les postes sont changés à la fin de leurs garanties, qui pour les appareils Dell est de 5 ans, alors la majeure partie du parc est théoriquement compatible avec le Secure Boot.
Il resterait ≈ 50 postes dénués du Secure boot, se trouvant probablement sur les services de comptabilité. En partant du principe que tout le parc est remplacé tous les 5 ans ou à date d’expiration de la garantie, la machine la plus ancienne daterait de 2017 ou 2018. Sachant que windows 10 est sorti depuis juillet 2015 alors la quasi totalité des ordinateurs devraient se trouver sous Windows 10. De plus les nouveaux PC bien que sortit sous Windows 11 se trouvent sous Windows 10 pour des raisons de licences et de logiciels. Sous Windows 10 le Secure Boot est activé par défaut. Le clonage étant récent sur ces machines, il en est de même. Les seules potentiels ordinateurs n’ayant pas le Secure Boot activé sont des machines anciennes.
Le remplacement du logiciel de clonage n’est donc plus forcément nécessaire.
D’autres questions se posent désormais, sachant qu’il en va de la sécurité de l’entreprise, il est nécessaire que le Secure Boot soit activé. Or doit-on prendre le risque comme soulevé par le support Dell de rendre un PC inutilisable à moins de réinstaller Windows en changeant les paramètres BIOS ? Et comment contourner cela

Le Secure Boot est donc présent sur les ordinateurs de nos jours, certains paramétrage et/ou manipulations peuvent nécessiter de le désactiver ou le désactivent en suivant une logique. Il est nécessaire de la garder activé puisque d’une part il est efficace et représente le seul réel moyen de se prémunir avant attaque contre les rootkits.

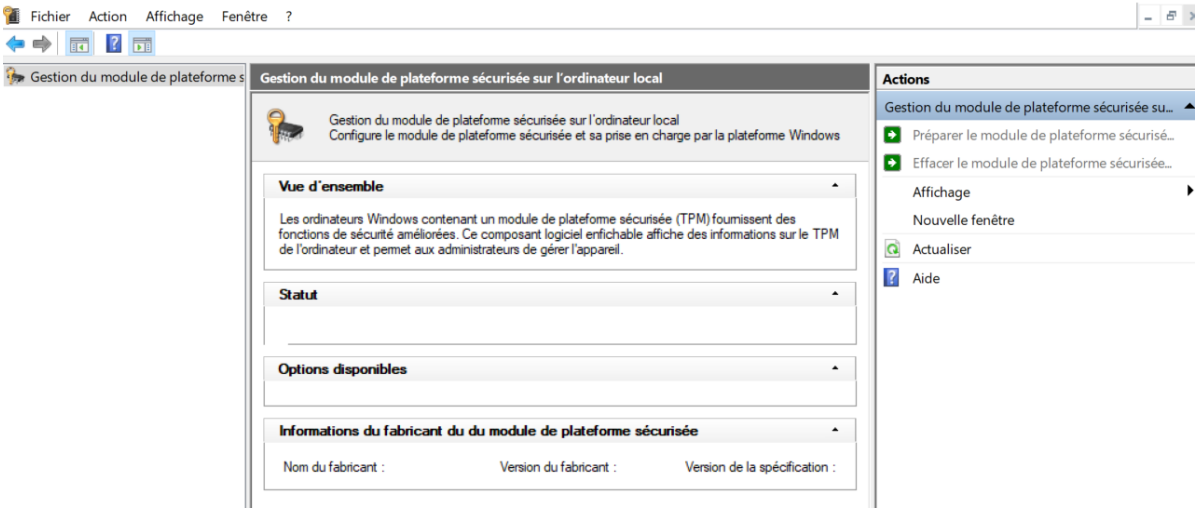
III Trusted Boot

A) Fonction

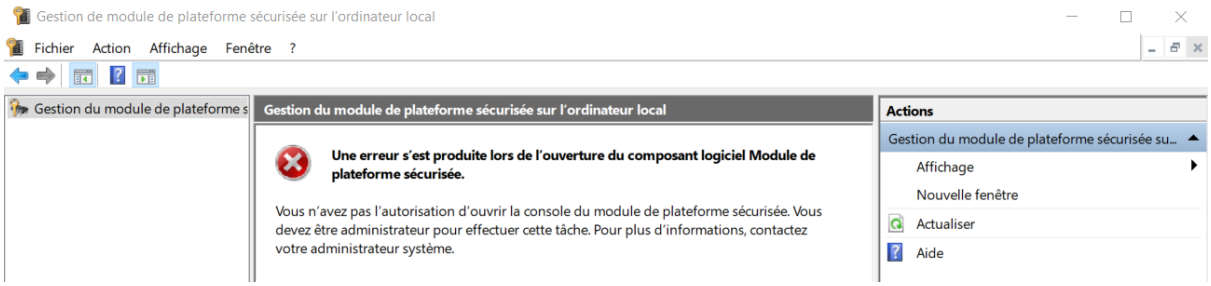
Deuxièmement TPM 2.0 (Trusted Platform Module) ou trusted boot. La fonction de Trusted boot utilise le module VTPM (Virtual Platform Module), c'est une instance virtuelle de Trusted Computing Group (le Trusted Computing Group est un consortium d'entreprises d'informatiques visant à sécuriser les équipement et communications informatiques) Il permet de stocker de manière sécurisée les mesures du système d'amorçage à des fins de vérifications.

B) Vérification et activation

Pour savoir si TPM est actif sur la machine, nous pouvons taper '*tpm.msc*' dans la barre de recherche Windows. A cet instant une fenêtre s'ouvre et donne accès au TPM, mais faisant partie intégrante du système de sécurité, la fenêtre demande dès le premier clic une autorisation administrateur.



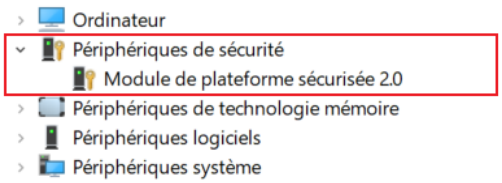
TPM tpm.msc 1



TPM tpm.msc 2

Chez le constructeur Dell, il est aussi possible de vérifier que le module TPM est détecté grâce aux étapes suivantes:

1. Ouvrez une session Windows
2. Cliquez avec le bouton droit de la souris sur le bouton démarrer
3. Cliquez sur le "Gestionnaire de périphériques"
4. Développez la section "Périphérique de sécurité"
5. Vous devriez voir le "Module de plate-forme sécurisée 2.0



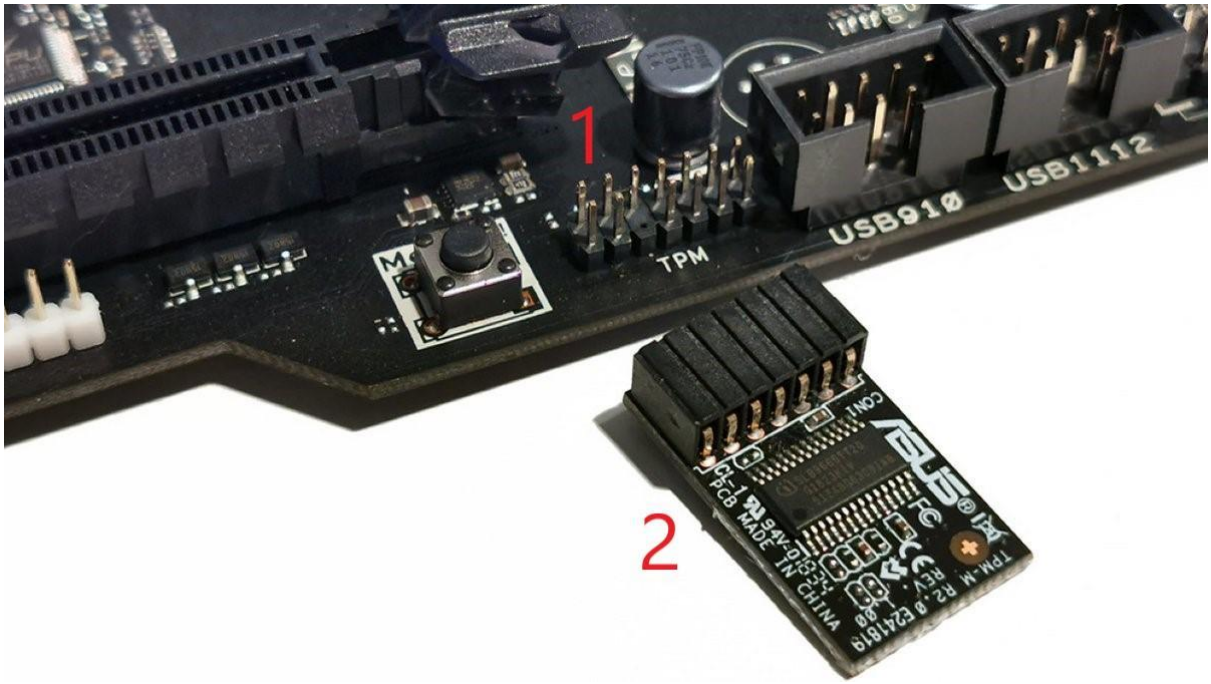
TPM gestionnaire de périphériques

Par ailleurs, il est aussi possible de vérifier si TPM est activé via powershell grâce à la commande Get-Tpm, des informations sont données en plus. En revanche, l'exécution de la commande nécessite un privilège administrateur.

```
Get-Tpm

TpmPresent                 : True
TpmReady                   : True
TpmEnabled                 : True
TpmActivated               : True
TpmOwned                   : True
RestartPending             : True
ManufacturerId             : 1229870147
ManufacturerIdTxt          : INTC
ManufacturerVersion        : 402.1.0.0
ManufacturerVersionFull20 : 402.1.0.0

ManagedAuthLevel           : Full
OwnerAuth                  :
OwnerClearDisabled         : False
AutoProvisioning           : Enabled
LockedOut                  : False
LockoutHealTime            : 10 minutes
LockoutCount               : 0
LockoutMax                 : 31
SelfTest                   : {}
```

Exemple du résultat de l'exécution de Get-Tpm sous Windows Powershell

TPM est en général présent sur la plupart des machines récentes, via le firmware ou bien via un plug TPM directement connecté à la carte mère. La version et le nom du TPM peuvent changer en fonction du processeur de la machine mais respecte en tous points les exigences TPM Microsoft. Chez Intel PTT (Platform Trust Technology) et chez AMD fTPM (Firmware TPM).



*Exemple de connecteur TPM **1** et d'un module TPM à plugger **2***

Dans le cas où TPM n'est pas activé il faudra se rendre sur le BIOS/UEFI et faire en fonction du BIOS de la machine paramétrée. Dans le cas présent, le parc provient majoritairement de chez DELL.
Selon le support Dell traitant ce sujet:

Pour activer le module TPM sur votre ordinateur Dell dans le BIOS, procédez comme suit.

1. Redémarrez votre ordinateur
2. Appuyez sur la touche **F2** ou **F12** du clavier une fois pendant une seconde lorsque le logo Dell s'affiche
3. Une fois dans le BIOS, reportez-vous à la section correspondant à la marque de votre ordinateur

Pour les PC des gammes: Latitudes, OptiPlex, Precision, Vostro et certains XPS:

1. Développez la section "**Security**"
2. Sélectionnez "**TPM 2.0 Security**"
3. Sélectionnez "**TPM On**"
4. Sélectionnez "**Appliquer**"
5. Sélectionnez "**Exit**"

Pour les PC de la gamme: Inspiron

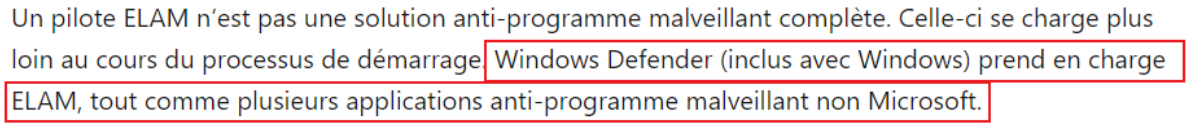
1. Sélectionnez "**Security**"
2. Basculez le bouton sous "**Intel Platform Trust Technology**" sur "**On**"
3. Sélectionnez "**Apply Changes**"
4. Sélectionnez "**Exit**" (si possible)

Pour conclure sur le Trusted Boot, il est en général activé par défaut et au moins présent s'il n'est pas activer. Pour vérifier sa présence et son état nous pouvons utiliser le tpm.msc ou le gestionnaire de périphérique. Dans le cas où TPM n'est pas activer au niveau firmware cela

est réglable dans le BIOS ou via une mise à jour du pilote TPM . Si le problème est matériel, une puce peut régler le problème.
TPM permet d'utiliser des services Microsoft en lien avec la sécurité tels que le chiffrement de lecteur Bitlocker, Windows Hello (depuis Windows 10 cela concerne le PIN, la reconnaissance faciale et digitale entre les appareils Microsoft d'un utilisateur), etc. Le service permet aussi de générer et stocker des clés cryptographiques et surtout de vérifier que le système d'exploitation et le microprogramme du BIOS/UEFI de l'appareil ne sont pas modifiés ou piratés. De plus, sa présence est nécessaire pour passer de Windows 10 à Windows 11 depuis sa sortie.

IV ELAM

Troisièmement ELAM, cet anti-malware se lance avant la 3ème partie du processus de démarrage de la machine et permet de vérifier qu'aucun pilote inconnu non Microsoft ne soit lancé.
Un rootkits peut donc se déguiser en pilote de manière à se lancer pendant ce lapse de temps.
Le logiciel ELAM (anti-programme malveillant à lancement anticipé) charge un pilote anti-programme malveillant d'origine Microsoft ou non avant tous les autres pilotes de démarrage et d'applications non Microsoft. Il examine donc chaque pilote de démarrage et détermine s'il figure sur la liste des pilotes approuvés. Dans le cas où un pilote n'est pas approuvé, Windows ne le charge pas. ELAM est pris en charge par Windows Defender et est un élément à part entière du processus de démarrage sécurisé.


Un pilote ELAM n'est pas une solution anti-programme malveillant complète. Celle-ci se charge plus loin au cours du processus de démarrage. Windows Defender (inclus avec Windows) prend en charge ELAM, tout comme plusieurs applications anti-programme malveillant non Microsoft.

Article sur le démarrage sécurisé sous Windows

V Mot de passe BIOS

Quatrièmement, le mots de passe BIOS
Le BIOS/UEFI peut prendre en charge différents types de mots de passe BIOS. Ceux-ci fournissent différents niveaux de sécurité aux ordinateurs Dell. Les mots de passe administrateur (configuration) et le mot de passe système (utilisateur) sont majoritairement utilisés et ont tous deux un objectif distinct.

Récurrence dans les attaques	Impact potentiel dans le SI	Note urgence (sur 10)	Statut	Problème	Préconisations
4	3	8	A faire	Accès BIOS/UEFI	Mettre des mots de passe admin/setup et système

Cellule concernant le problème relevé (ligne 2)

A) Différents type de mots de passe

Le mot de passe administrateur:
Celui-ci assure la sécurité en verrouillant toutes les fonctionnalités et les paramètres du BIOS. L'utilisateur peut démarrer le BIOS et voir ses paramètres mais ne peut les modifier à moins de renseigner le mot de passe approprié.

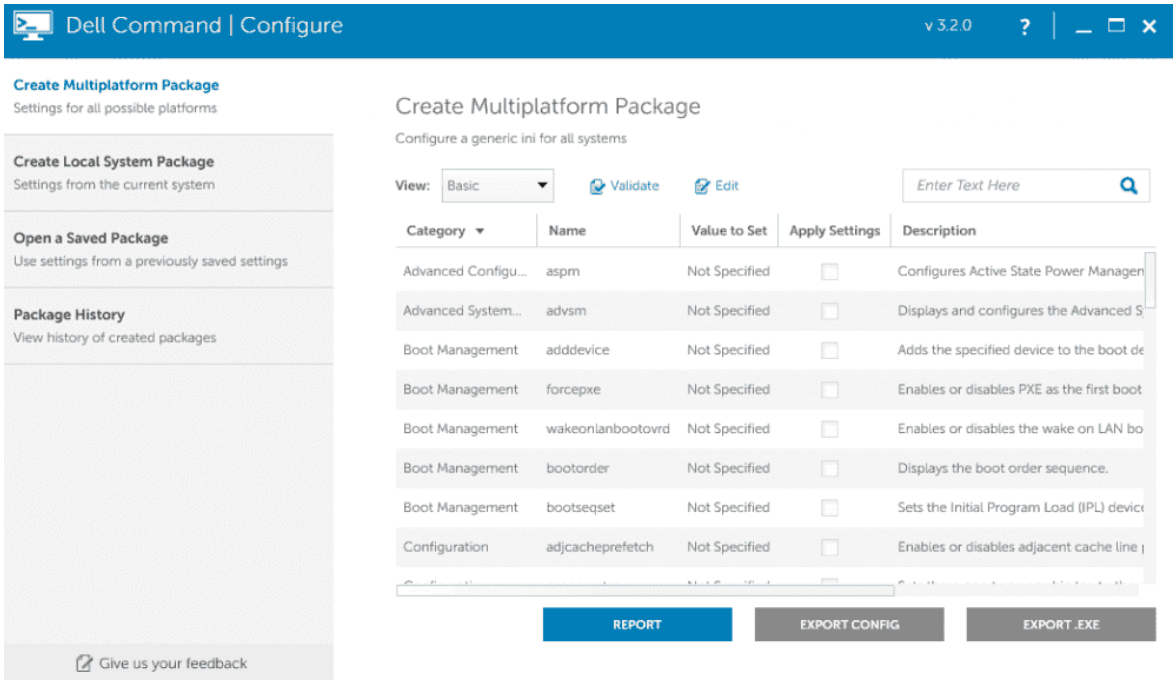
Le mot de passe système:
Il assure la sécurité en empêchant l'utilisateur de démarrer l'ordinateur. Il ne peut pas voir le BIOS (avec F2 ou F12). Le mot de passe système doit donc être renseigné. Dans le cas où le mot de passe administrateur est aussi activé, il doit aussi être renseigné pour modifier les paramètres du BIOS, ce qui ajoute une touche de sécurité.

Il est possible de définir les mots de passe via Dell Command | Configure en interface graphique via les règles :

"**setuppwd**" pour le mot de passe de configuration (mot de passe du BIOS)
"**syspwd**" pour le mot de passe système
"**hddpwd**" mot de passe du disque dur

Sécurité	--SetupPwd	Non spécifié	☐	Définit le mot de passe de configuration.
Sécurité	--SysPwd	Non spécifié	☐	Définit le mot de passe du système.
Sécurité	--HddPwd	Non spécifié	☐	Définit, modifie et supprime le mot de passe du disque dur (HDD).

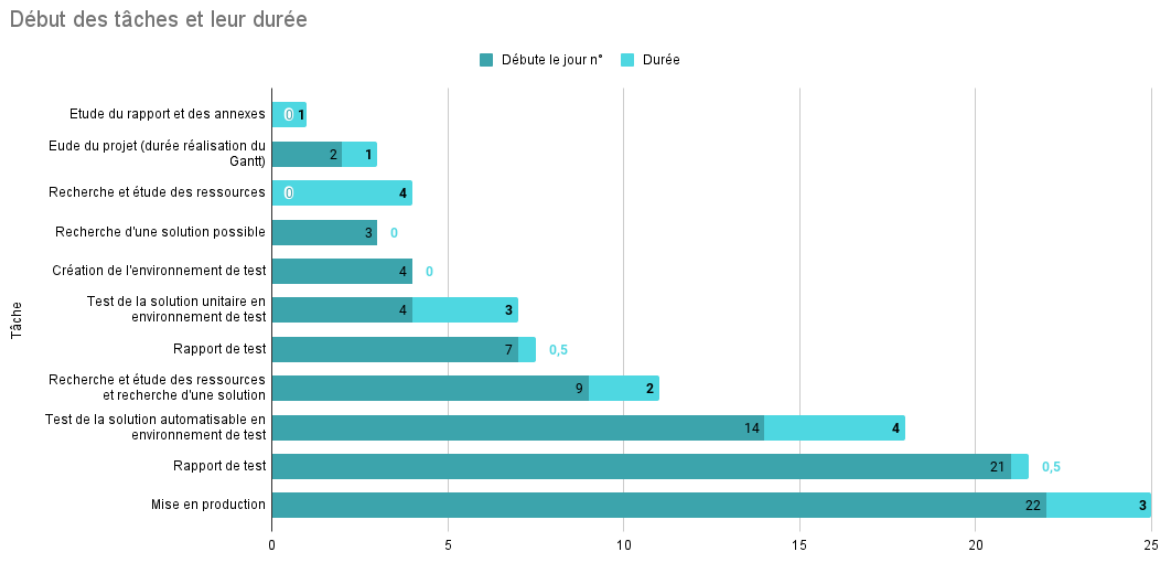
Screenshot de Dell CC



Interface de Dell Command | Configure

B) Dell Command | Configure

Un certain nombre de solutions peuvent être pertinentes. Une a retenu mon attention. Comme demandé, la solution doit-être en mesure de modifier un certain nombre de postes en simultanés si possible ou du moins en limitant les interactions. Dell Command | Configure peut être une bonne solution.
Selon l'article du support Dell, Dell Command | Configure est une application logicielle packagée qui fournit des fonctionnalités de configuration aux plateformes clientes d'entreprises. Ce produit se compose d'une interface de ligne de commande (CLI) et d'une interface utilisateur (UI) pour configurer diverses fonctionnalités du BIOS. Un site regroupant des commandes et fonctionnalités est mis en source.
Par ailleurs, avec cette interface il est possible de créer un exécutable (.exe) qui modifie les caractéristiques BIOS une fois lancer. Dans notre cas nous cherchons l'activation du Secure Boot ce qui créera une continuité avec TPM (qui peut aussi être activé via Dell CC) et ELAM. Il n'est pas dans le cadre de cette mission de trouver comment activer un mot de passe BIOS mais via cette solution il est possible de le faire donc pourquoi ne pas en profiter.
La question est désormais comment envoyer cet exécutable aux différentes machines du parc.



Mise à jour du diagramme

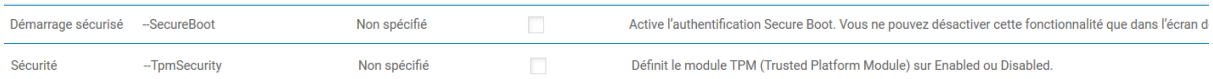
VI Test en environnement de test

A) Test unitaire

Pour tester cette solution nous pourrions reconfigurer le pc TESTCYBERSECURITE en Secure Boot Disabled, TPM Disabled et essayer le script manuellement puis refaire la manipulation et essayer de le faire parvenir via un intermédiaire dont je n'ai pas encore idée pour le moment. Il est peut-être possible de déployer un .exe via GPO. Or en général il n'y a

que les .msi qui sont pris en charge par celles-ci, à voir s'il est possible de contourner cela via une conversion ou un script par exemple.

Pour le test, nous avons donc paramétré le Secure Boot sur Enabled ainsi que la puce TPM pour le trust boot.

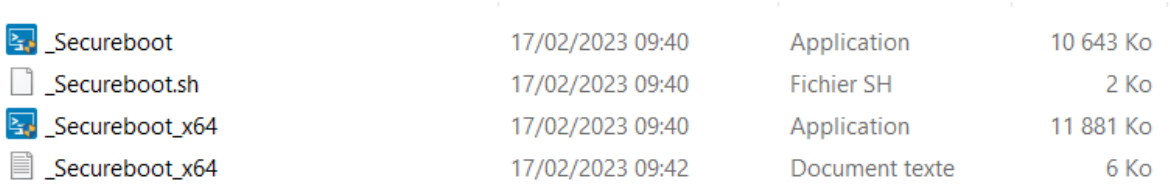


Screenshot de Dell CC

Nous avons exporter la configuration au format .exe sur une clé pour un test en environnement local.

Interface d'exportation DELL CC

Les fichiers suivants ont été générés. Après exécution un rapport est automatiquement généré et donne le détail sur l'exécution du script et sa réussite ou non.



Screenshot des documents générés

```
[Fri Feb 17 09:42:25 2023]    Self Contained Executable(SCE) Execution Start
[Fri Feb 17 09:42:25 2023]    Original command line: "D:\Dell Command
Configure\_Secureboot_x64.exe"
[Fri Feb 17 09:42:25 2023]    SCE Framework Version: 4.6.0.0
[Fri Feb 17 09:42:25 2023]    SCE Release: R309560
[Fri Feb 17 09:42:25 2023]    Initializing framework...
[Fri Feb 17 09:42:25 2023]    Data in smbios table is (hex)value = a , Chasis type
(hex)value = a , System type is : Client
[Fri Feb 17 09:42:25 2023]    User Command: attended
[Fri Feb 17 09:42:25 2023]    SCE Capabilities Value: 1042284543 (0x3E1FFFFF)
[Fri Feb 17 09:42:25 2023]    SCE Vendor Software Version: 4.6.0
[Fri Feb 17 09:42:25 2023]    Local System/Model Compatible with this Package? Yes
[Fri Feb 17 09:42:25 2023]    Local System OS Version: 10.0.19045
[Fri Feb 17 09:42:25 2023]    OS Compatible with this Package? Yes
[Fri Feb 17 09:42:25 2023]    Local System OS Language: FR
[Fri Feb 17 09:42:25 2023]    Language Compatible with this Package? Yes
[Fri Feb 17 09:42:25 2023]    Extraction-miniunz path:
C:\PROGRA~3\dell\drivers\2261D0~1\miniunz.exe
[Fri Feb 17 09:42:25 2023]    Extraction-arguments:  -x D:\DELLCO~1\_SECUR~2.EXE -o
-d C:\PROGRA~3\dell\drivers\2261D0~1
[Fri Feb 17 09:42:25 2023]    Extraction-GetExitCode: 0
[Fri Feb 17 09:42:25 2023]    Identified Behavior : attended
```

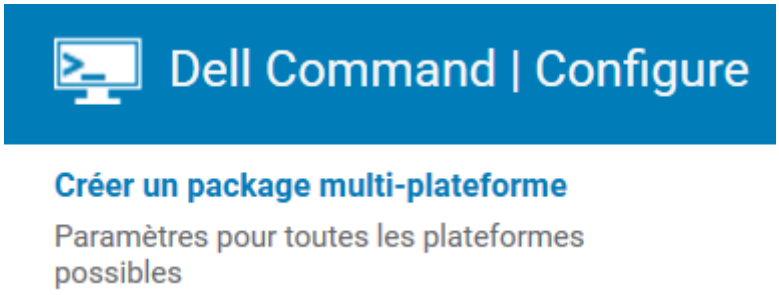
```
[Fri Feb 17 09:42:25 2023]    Temporary payload log file name:
C:\ProgramData\dell\drivers\2261d055-48c7-4aa0-ab7c-2aef56bb98d2\SCE8ECF.tmp
[Fri Feb 17 09:42:25 2023]    Translated Command Line : applyconfig.bat -
l="C:\ProgramData\dell\drivers\2261d055-48c7-4aa0-ab7c-2aef56bb98d2\SCE8ECF.tmp"
[Fri Feb 17 09:42:25 2023]    Path : C:\ProgramData\dell\drivers\2261d055-48c7-4aa0-
ab7c-2aef56bb98d2
[Fri Feb 17 09:42:25 2023]    Working Directory: C:\ProgramData\dell\drivers\2261d055-
48c7-4aa0-ab7c-2aef56bb98d2
[Fri Feb 17 09:42:35 2023]    Append Vendor Software Log:
C:\ProgramData\dell\drivers\2261d055-48c7-4aa0-ab7c-2aef56bb98d2\SCE8ECF.tmp
[Fri Feb 17 09:42:35 2023]
--- Start of Vendor Software Log ---

[Fri Feb 17 09:42:35 2023]    ASCII payload log file detected.
[Fri Feb 17 09:42:35 2023]    2023/02/17 09:42:35 cctk - CCTKAppEngVer=4.6.0.277
2023/02/17 09:42:35 cctk - SecureBoot=Enabled
2023/02/17 09:42:35 cctk - TpmSecurity=Enabled
CCTK STATUS CODE : SUCCESS
[Fri Feb 17 09:42:35 2023]
--- End of Vendor Software Log ---

[Fri Feb 17 09:42:35 2023]    Get name of the Folder file: D:\Dell Command Configure
[Fri Feb 17 09:42:35 2023]    Vendor Software Return Code: 0
[Fri Feb 17 09:42:35 2023]    Name of Exit Code: SUCCESS
[Fri Feb 17 09:42:35 2023]    Exit Code set to: 0 (0x0)
[Fri Feb 17 09:42:35 2023]    Result: SUCCESS
[Fri Feb 17 09:42:35 2023]    Name of Exit Code: SUCCESS
[Fri Feb 17 09:42:35 2023]    Execution terminated at date-time Fri Feb 17 09:42:35 2023
[Fri Feb 17 09:42:35 2023]    ######
```

Résultat contenus dans _Secureboot_x64

Après avoir tester la solution en question sur le PC TESTCYBERSECURITE, tout est fonctionnel. Après un redémarrage et un tour sur le BIOS nous pouvons voir que TPM 2.0 et Secure Boot qui originellement n'étaient pas activé le sont désormais.

Est-ce que le script activer sur un PC en legacy (Secure Boot Off) fait passer le pc en UEFI (Secure Boot On)?
Pour cela nous changeons les paramètres du BIOS et appliquons le script sur un PC de test. Le pc test passe bien en mode UEFI avec Secure Boot on mais le TPM lui ne s'active pas. C'est peut-être due à une mise à jour Windows non installée ou bien des pilotes trop anciens. Grâce à ce test j'ai pu observer qu'il manquait un paramètre au script, pour activer le TPM il faut aussi mettre TPM Activation sur Enabled.
En revanche, bien que le pc passe de Legacy en UEFI, avec Secure Boot et TPM sur Enabled sans réel problème, c'est après un redémarrage qu'il est impossible de reboot.

La question est désormais: est-*ce que tous les postes vont réagir correctement?*
En théorie oui puisque l'exécutable en question est multiplateforme c'est-à-dire que toute la gamme Dell devrait être prise en compte.



Interface Dell CC

B) Test d'automatisation

Il est donc nécessaire de tester ce correctif à distance puisque l'expérience n'a été pour le moment faite qu'en local et à plus grande échelle sur un environnement de test adapté.
Nous pourrions rassembler un ordinateur ou un petit groupe et lui/leurs faire passer le .exe via une GPO et forcer le l'utilisation via un .BAT ou d'un script PowerShell.
Il reste donc à trouver le bon script pour installer l'exécutable et tester s'il est déjà installé ou non pour qu'à chaque démarrage l'exe ne soit pas réinstaller. Plusieurs .exe ont déjà été installés auparavant via un script adapté.

Le but de ce script serait de :

- forcer l'exécution du script
- faire un test pour voir s'il est déjà installé
- s'il l'est alors ne pas réinstaller

cela de manière à optimiser le démarrage et à ne pas le rendre trop lourd.

Après des tests en local, le but est de tester cette solution en global. Or, nous devons, pour faire passer cette installation en GPO, faire un script pour automatiser l'installation et tester si les paramètres sont appliqués.

Cela donnerait :

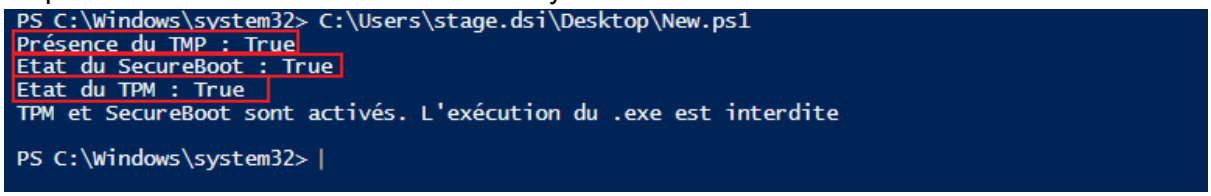
```
$DossierPartager = \\CheminVersLeFichier\
$DossierLocal = "C:\Temporaire"
$NomDeL'exe = "_SecureBoot_x64.exe"
$ExeArgument = "/S"
$TPMEnabled= Status TPM
$SecureBootEnabled= Status SecureBoot

If (Secure Boot Enabled && TPM Enabled){
        return True
}else{ return false
        execute $DossierLocal\$NomDel'exe}
```

Ce qui devrait donner à peu près :

```
### Variables
#Chemin UNC vers le partage qui contient l'exécutable
$SharedFolder = "\\server\folder"
#Chemin vers le dossier temporaire local sur le poste
$LocalFolder = "C:\TEMP"

#Nom de l'exécutable
$ExeName = "SecureBootTPM_x64.exe"

#Argument(s) à associer à l'exécutable
$ExeArgument = "/S"

#Test pour TPM
$TpmActivated = (Get-Tpm).TpmReady
$TpmPresent = (Get-WmiObject -class Win32_Tpm -namespace
"root\CIMV2\Security\MicrosoftTpm").IsActivated_InitialValue
#Test pour SecureBoot
$SecureBootEnabled = Confirm-SecureBootUEFI

Write-Host "Présence du TMP : $TpmPresent"
Write-Host "Etat du TPM : $TpmActivated"
Write-Host "Etat du SecureBoot : $SecureBootEnabled"

if ($TpmActivated -eq $True -and $SecureBootEnabled -eq $True) {
   Write-Host "TPM et SecureBoot sont activés. L'exécution du .exe est interdite"
   Exit
}else{
   Write-Host "TPM et/ou SecureBoot ne sont pas activés. L'exécution du fichier exécutable peut
commencer."
   #Commande de lancement du .exe

   #Si le chemin réseau vers l'exécutable est valide, on continue
   if(Test-Path "$SharedFolder\$ExeName"){

      #Créer le dossier temporaire en local et copier l'exécutable sur le poste
      New-Item -ItemType Directory -Path "$LocalFolder" -ErrorAction SilentlyContinue
      Copy-Item "$SharedFolder\$ExeName" "$LocalFolder" -Force

      #Si l'on trouve bien l'exécutable en local, on lance l'exécution
      if(Test-Path "$LocalFolder\$ExeName"){
         Start-Process -Wait -FilePath "$LocalFolder\$ExeName" -ArgumentList "$ExeArgument"
      }

      #On supprime l'exécutable à la fin de l'installation
      Remove-Item "$LocalFolder\$ExeName"

   }else{
      Write-Warning "L'exécutable ($ExeName) est introuvable sur le partage!"
   }
}
```

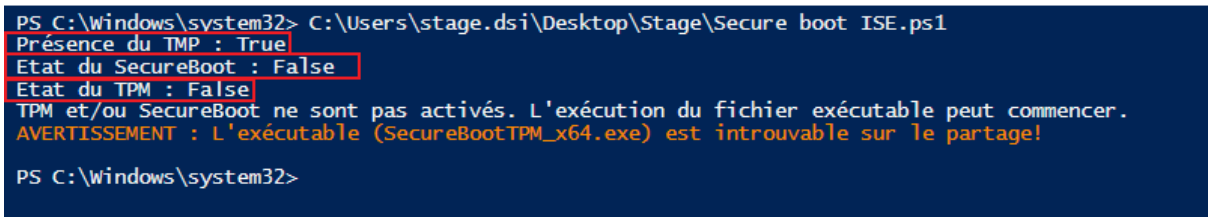
Test du script dans l’environnement PowerShell ISE

Le premier test à été effectué sur un PC ayant Secure Boot et TPM d'activé.



Test 1 sous PowerShell ISE

Le second test à été effectué sur le même PC ayant subi des modifications, en effet le TPM et Secure Boot on tous deux étés désactivés manuellement. Le retour console est encourageant.



Test 2 sous PowerShell ISE

Nous pouvons voir que le test est bien fonctionnel et que lorsque l'un des résultats est faux alors le script est appelé.

Le principe est maintenant de déployer cet exécutable et ce script via GPO.
Pour éviter toute erreur, nous faisons d'abord un test sur un PC présent dans le domaine, le PC Formation 01 sera notre cobaye.
Après de multiples tests, le script a finalement été bien incorporé à la GPO par le responsable technique sur le pc cobaye.

"En soit, le script fonctionne pour le test mais il n'est pas effectif avec une GPO ordinateur. Il doit donc être déployé avec une GPO user ce qui amène donc de la difficulté.
De plus, une sécurisation du BIOS est la nouvelle tâche, un mot de passe admin doit donc être paramétré ainsi qu'une sécurisation de la procédure de boot."

L'objectif est donc d'apporter des paramètres aux script, notamment un mot de passe pour la modification du BIOS, et une sécurisation de la procédure de boot qui doit uniquement boot sur le hdd de l'ordinateur a part si le mots de passe BIOS (admin) est renseigné.

Après l'ajout des paramètres:
cctk --SetupPwd=motdepasse

cctk --UefiBootPathSecurity=AlwaysExceptInternalHdd --ValSetupPwd=motdepasse
cctk --SecureBoot=Enabled --ValSetupPwd=motdepasse
cctk --TpmSecurity=Enabled --ValSetupPwd=motdepasse
cctk --TpmActivation=Enabled --ValSetupPwd=motdepasse

Le mot de passe bios est activé et demande avant toutes configurations d'un paramètre BIOS le mot de passe administrateur.

Lors des tests un problème est survenu. En effet, les pc bootant en Legacy (Hérité) ne peuvent plus démarrer une fois le script appliquer, cela suite à l'activation du Secure Boot qui passe automatiquement le paramètre en UEFI. Nous devons donc tester le BIOS à boot sur UEFI ou Legacy.

Le script donnerais donc cela :

```
$BootMode = bcdedit | Select-String "path.*efi"
if ($null -eq $BootMode) {
    # I think non-uefi is \Windows\System32\winload.exe
    $BootMode = "Legacy"
}else {
    # UEFI is:
    #path                \EFI\MICROSOFT\BOOT\BOOTMGFW.EFI
    #path                \Windows\system32\winload.efi
    $BootMode = "UEFI"
}

Write-Host "Computer is running in $BootMode boot mode."
```

Ce script teste la présence des fichiers EFI qui atteste que le pc à démarrer en mode UEFI.

C) Mise en production et acceptation du service

L'objectif final est donc la mise en place de la solution sur un environnement large. L'environnement choisi est celui de la DSI. Une étude du parc informatique de la DSI à donc été nécessaire avant toute chose. Cette analyse à été faite via GLPI puisqu'il permet via Fusioninventory de centraliser les données du parc (pour plus de détails sur GLPI un document lui est adressé) et un fichier CSV à été généré à partir des résultats.

Nom	Entité	Statut	Numéro de série	Type	Modèle	Lieu	Utilisateur	Réseau - IP	Système d'exploitati	Informations financié	Plugins - Fusinv - Dei	Usager
DSI-STAGE	Entité racine > Sofin	Spare	B2D6XF2	Laptop	Latitude 5580	Sofimat Pencran > C	Stage DSI	fe80::c9 10.0.0.6 10.254.: fe80::99	8XBTB-N3KJM-8378	17-06-2022	2023-03-07 9:39:01	Matthieu
DSI01	Entité racine > Sofin	Production	51HR593	Notebook	Latitude 9510		Julien	10.200.: fe80::a5 fe80::ee 2001:86 192.168 2001:86 10.254.(fe80::81	3NVHR-3KBYT-VGJ1	11-01-2026	2023-03-07 9:20:21	julier @SOFIMA
DSI02	Entité racine > Sofin	Production	44G96S2	Notebook	Latitude 5590		Olivier	fe80::2(10.200. 10.13.0 fe80::d6 fe80::a1 192.16 2a01:cb 2a01:cb	K8KFN-QWH2B-X49	03-12-2023	2023-03-07 9:05:34	olivier @SOFI
DSI03	Entité racine > Sofin	Production	7FCLST2	Notebook	Latitude 5590		Norman	10.200. fe80::61 fe80::e(10.254. fe80::b5 192.16	NF6HC-QH89W-F8W	16-01-2024	2023-03-06 16:23:42	norman @SC
DSI04	Entité racine > Sofin	Production	9N18K12	Laptop	Latitude E5540	Sofimat Pencran > D	Stephane	fe80::5c 10.200.: fe80::ec 10.18.2(10.13.0	VK7JG-NPHTM-C97-	16-03-2018	2023-02-28 11:48:16	stephane @SOF
DSI05	Entité racine > Sofin	Production	CJV9JM2	Notebook	Latitude 5580		Mickael	10.200.: 10.18.0 10.254.: 10.0.0.6 fe80::56	NQF6F-C4MVH-6V8	01-02-2023	2023-03-07 9:54:05	mickael@SOFIMAT
DSI07	Entité racine > Sofin	Production	33Z79C3	Notebook	Latitude 5510		Loic	10.200. 192.16 fe80::3 2a01:cb fe80::e fe80::a 2a01:cb 192.16 2a01:cb	CY9NQ-8FP2C-YVY2	07-03-2026	2023-03-07 9:19:34	loic @SOFIM
DSI11	Entité racine > Sofin	Production	5ZDK5S1	Laptop	Latitude E5520	Sofimat Pencran > D	CSE Sofimat	fe80:: fe80:: 10.0.0 10.0.2	VK7JG-NPHTM-C97-	10-12-2014	2022-11-18 10:40:12	cse@SOFIMAT
								192. fe80 fe80				

GLPI à donc permis d'éviter d'aller chercher les informations postes par postes, ce qui permet un gain de temps considérable.

Le script à du recevoir des modifications avant de pouvoir être déployé par GPO, en effet des parties de script notamment celle qui teste si le pc à boot sous UEFI ou bien sous Legacy qui sont juste mais lors d'un déploiement ne fonctionne pas, retournant des test erroné qui pousse le script à ne pas activer les paramètres voulus.

Le script final donne donc cela (le mot de passe n'a été renseigné dans le script mais à été mis en paramètre lors de la création de la GPO):

```
param ($SetupPwd)

Function LogWrite
{
   Param ([string]$logstring)

   Add-content $Logfile -value $logstring
}

### Variables
#Chemin UNC vers le partage qui contient l'exécutable
$SharedFolder = "\\sofimat.fr\netlogon\ConfigBIOS"

#Chemin vers le dossier temporaire local sur le poste
$LocalFolder = "C:\INSTALL"

#Nom de l'exécutable
$PathCCTK = "cctk"

#Argument(s) à associer à l'exécutable
$ExeArgument = "--logfile=$LocalFolder\cctk.log"

$LogFile = "$LocalFolder\Check_Secure_Boot_Tpm.log"

#Check Windows en UEFI
$BootMode = $env:firmware_type
LogWrite("$BootMode")

#Check si l'outil cctk est présent sur l'ordinateur
if((Test-Path "$LocalFolder\$PathCCTK\cctk.exe") -eq $False){
Write-Host "Le fichier $LocalFolder\$PathCCTK\cctk.exe n'existe pas."
LogWrite("Le fichier $LocalFolder\$PathCCTK\cctk.exe n'existe pas.")

#Check si le partage source est disponible
if(Test-Path "$SharedFolder\$PathCCTK"){
Write-Host "Copie du dossier $SharedFolder\$PathCCTK vers $LocalFolder\$PathCCTK."
LogWrite("Copie du dossier $SharedFolder\$PathCCTK vers $LocalFolder\$PathCCTK.")

#Création du dossier temporaire en local et copie l'exécutable sur le poste
LogWrite("Creation du dossier $LocalFolder")
      New-Item -ItemType Directory -Path "$LocalFolder" -ErrorAction SilentlyContinue

LogWrite("Copie de $SharedFolder\$PathCCTK vers $LocalFolder")
```

```
        Copy-Item -Path "$SharedFolder\$PathCCTK" -Destination
"$LocalFolder\$PathCCTK" -Force -Recurse
}else{
Write-Warning "Le partage $SharedFolder\$PathCCTK est introuvable sur le réseau!"
LogWrite("Le partage $SharedFolder\$PathCCTK est introuvable sur le réseau!")
}
}

#Re-check si l'outil cctk est présent sur l'ordinateur
if(Test-Path "$LocalFolder\$PathCCTK\cctk.exe"){

    $TpmActivated = & $LocalFolder\cctk\cctk.exe --TpmActivation
    $TpmPresent = & $LocalFolder\cctk\cctk.exe --TpmSecurity
    $SecureBootEnabled = & $LocalFolder\cctk\cctk.exe --SecureBoot

    LogWrite("Exécution de $LocalFolder\cctk\cctk.exe --SetupPwd=***")
    Start-Process -Wait -FilePath "$LocalFolder\cctk\cctk.exe" -ArgumentList "--
SetupPwd=$SetupPwd $ExeArgument"

    LogWrite("BootMode=$BootMode")
    if($BootMode -eq "UEFI") {
        if ($TpmActivated -eq "TpmActivation=Enabled" -and $SecureBootEnabled -eq
"SecureBoot=Enabled") {
            #Write-Host "TPM et SecureBoot sont activés. L'exécution du .exe est interdite"
       LogWrite("TPM et SecureBoot sont activés. L'exécution du .exe est interdite")
        } else {
            LogWrite("Tpm et SecureBoot Disabled,BootMode=$BootMode")
            LogWrite("Exécution de $LocalFolder\cctk\cctk.exe --SecureBoot=Enabled --
ValSetupPwd=*** $ExeArgument")
       Start-Process -Wait -FilePath "$LocalFolder\cctk\cctk.exe" -ArgumentList "--
SecureBoot=Enabled --ValSetupPwd=$SetupPwd $ExeArgument"

            LogWrite("Exécution de $LocalFolder\cctk\cctk.exe --TpmSecurity=Enabled --
ValSetupPwd=*** $ExeArgument")
       Start-Process -Wait -FilePath "$LocalFolder\cctk\cctk.exe" -ArgumentList "--
TpmSecurity=Enabled --ValSetupPwd=$SetupPwd $ExeArgument"

            LogWrite("Exécution de $LocalFolder\cctk\cctk.exe --TpmActivation=Enabled --
ValSetupPwd=*** $ExeArgument")
       Start-Process -Wait -FilePath "$LocalFolder\cctk\cctk.exe" -ArgumentList "--
TpmActivation=Enabled --ValSetupPwd=$SetupPwd $ExeArgument"
        }
        LogWrite("Exécution de $LocalFolder\cctk\cctk.exe --
UefiBootPathSecurity=AlwaysExceptInternalHdd --ValSetupPwd=*** $ExeArgument")
    Start-Process -Wait -FilePath "$LocalFolder\cctk\cctk.exe" -ArgumentList "--
UefiBootPathSecurity=AlwaysExceptInternalHdd --ValSetupPwd=$SetupPwd
$ExeArgument"
    }
}
```

Script final pour l'activation du Secure Boot, du TPM, mettre un mots de passe sur le BIOS et forcer le démarrage sur le hdd de la machine

Pour ce qui de l'acceptation du service, après un entretien avec le Directeur du système d'information, la solution mise en place répond à l'objectif du stage et corrige plusieurs problèmes relevés sur la matrice à savoir la séquence de boot et la sécurisation du BIOS.

Du point de vue des différents techniciens, il n'y a pas de problème avec la mise en place de la solution, bien que la mise en place du mot de passe BIOS ajoute une manipulation de plus lors de la configuration des machines et puisse ajouter des contraintes. Le service proposé est donc bien accepté tant par la direction que par les techniciens.

Conclusion

Cette mission à demandé un gros travail de recherche, ne connaissant que les bases du BIOS, n'ayant jamais entendu parler de Secure Boot et encore moins de TPM tout était nouveau. Le fait de devoir chercher et de devoir proposer une solution au bout de la première semaine de stage m'a donné une certaine motivation à trouver les informations les plus pertinentes possible, à documenter et croiser mes recherches avec des ressources fiables. De plus, le fait de pouvoir échanger avec des professionnels m'a permis de ne pas rester dans une zone de flou et par ailleurs de tester les solutions que je proposais sur du matériel dédié à des tests, ce qui m'a mis en confiance et m'a donné envie d'essayer des choses sans avoir trop peur des conséquences.
De plus, cette mission à été très complète et m'a permis de voir plusieurs notions vus en cours passant de la stratégie de groupe à la création de script.
Mais surtout, ce stage m'a conforté dans l'idée de continuer dans le domaine de l'informatique et pourquoi pas dans la cyber sécurité, l'étude de rapport, d'audit de sécurité m'a donné un point de vue très concret sur ce qui m'intrigue depuis le début de mon BTS. Par ailleurs, j'ai pu voir que le monde professionnel est très rythmé et qu'on y apprends plus vite et des choses beaucoup plus concrètes, sans forcément tout oublier de la formation initiale qui m'a apporté ses bases sans lesquelles je n'aurait pas pu faire grand chose. Cette expérience était donc très intéressante, enrichissante et formatrice malgré une aussi courte durée.

Bibliographie et sources:

Les documents, citations, légendes présents dans ce compte rendu comportent un lien retournant soit sur le document, la vidéo ou bien le site qui traite du sujet. Ce n'est pas le cas pour tous les screenshots.

Les rapport d'audit de sécurité étudiés sont trop sensibles pour être divulgués.

Article Wikipédia
USB
Firmware
BIOS
UEFI

Article DELL support
Secure boot
Accéder, naviguer, mettre à jour le BIOS ou l'UEFI
Présentation du démarrage sécurisé
Activation du module TPM (Trusted Platform Module)
Dell Command | Configure

Article IBM
Trusted Boot

Article Learn Microsoft
ELAM
Rootkit
Démarrage en mode UEFI ou en mode BIOS
Sécuriser le processus de démarrage de Windows
Comment activer le TPM
Get-TPM
Magasin Système BDC paramètres

Article NordVPN
Rootkit

Vidéo
Security expert explains TPM 2.0 and Secure Boot
Dell Command Configure as a Command Line Tool
Dell Command COnfigure as an UI
Playlist Dell
Tutoriel Dell Command Configure (fr)
Comment déployer un .exe via GPO

Outils
Dell
Dell Command Configure suite video

Dell Command Configure guide d'installation
Dell Command PowerShell Provider
Comment naviguer dans le BIOS/UEFI selon le modèle
Dell Command | Configure version 4.3 Command Line Interface Reference Guide
Manuel Dell Latitude 5580
Pistes
Package PowerShell
Script Secure boot

Documentation produit
DELL Latitude 5580

Source pour le script
GitHub
Confirm-SecureBootUEFI
TPM Ready