Institut Universitaire de Technologie,
Aix-Marseille Université

RAPPORT DE STAGE de fin de deuxième année
Bachelor Universitaire de Technologie
Spécialité Réseaux et Télécommunications
parcours cybersécurité

Immersion dans un MSP informatique

Quentin SORAGNA

ITCOM SERVICES

Responsable entreprise : Jérôme DE GRAER

Responsable académique : Rabah IGUERNAISSI

2023

Table des matières

Introduction

Dans le cadre de ma formation B.U.T Réseaux et Télécoms (Bachelor Universitaire et Technologique), j'ai eu l'opportunité d'effectuer un stage au sein de l'entreprise ITCOM SERVICES à Marseille, plus précisément dans les services de la supervision, du développement et du réseau. Ce stage a marqué la fin de ma deuxième année de cursus et avait pour objectif principal de mettre en pratique mes connaissances théoriques et d'acquérir une expérience professionnelle concrète dans le domaine de l'informatique.

Durant ce stage, j'ai eu l'occasion de travailler sur différents projets et d'assumer diverses missions. Le premier volet était axé sur la supervision des infrastructures informatiques, où j'ai appris à comprendre et à établir des règles de supervision dans un parc informatique. J'ai également eu l'opportunité de développer des compétences en scripting (développement en programmation), en créant des programmes visant à automatiser certaines tâches complexes.

Un autre aspect important de mon apprentissage était lié aux réseaux informatiques. J'ai eu l'occasion de travailler sur des projets impliquant la segmentation de réseaux physiques à l'aide de VLAN (Virtual Local Area Network), le filtrage des connexions entrantes et sortantes, la configuration du NAT (Network Adresse Translation) et de la redirection de ports, ainsi que l'administration des firewalls et des switches.

Je présenterai l'entreprise ITCOM SERVICES, ses activités et ses projets, ainsi que les différentes missions que j'ai réalisées au cours de mon stage. Je détaillerai également les compétences techniques acquises, les défis rencontrés et les résultats obtenus dans le cadre de mes missions. Enfin, je conclurai en abordant les enseignements tirés de cette expérience et les perspectives pour mon parcours professionnel futur.

Itcom Services

Présentation de l'entreprise

Figure 1 : logo d'ITCOM SERVICES

ITCOM SERVICES (que je surnommerai ITCOM), fondé en mars 2011, est né de la volonté de Jean-Benoit CARSIN (représentant à ce jour) de créer une entreprise pouvant accompagner ses clients dans la gestion de leur infrastructure informatique.

À ces débuts, ITCOM ne proposait que des solutions téléphoniques pour les entreprises, Jean-Benoît CARSIN ayant obtenu un partenariat avec SFR Business Team, grâce à son ancien travail (Responsable de distribution chez SFR).

ITCOM se base depuis 2015 sur le modèle MSP (Managed Services Provider). C'est une société de services qui gère à distance les systèmes informatiques de ses clients, de manière proactive/réactive sous un modèle forfaitaire.

Cette dernière a connu une forte croissance, son chiffre d'affaires a augmenté de 2015 (900 000 €) à 2022 (2 000 000 €).

Aujourd'hui, les locaux d'ITCOM SERVICES sont situés 11 place du Général de Gaulle à Marseille (Vieux-Port), l'entreprise comporte 12 salariés et accueille régulièrement de nouvelles personnes (stages, formation par apprentissage, prestataires).

ITCOM se caractérise comme étant une société de conseil informatique, les prestations sont les suivantes :

- Maintenance informatique et télécom récurrente(mensuelle)
- Vente de prestations non récurrente (matériels, interventions spontanées, audit)
- Vente de prestations récurrente (messagerie, antivirus, sauvegarde...)

Le modèle MSP

Figure 2 : Activités d'un MSP

Monitoring : Surveillance, Simplified Billing : Facturation simplifiée, Scheduled Maintenance : Maintenance planifiée, Centralized Management : Gestion centralisée, Remote Support : Assistance à distance, ProActive Support : Assistance Proactive.

Notre société ITCOM SERVICES se base sur un modèle particulier et qui est en France, en pleine effervescence, c'est le modèle MSP (figure 2).

Un MSP est une société de services informatiques qui gère à distance les systèmes informatiques de ses clients, de manière proactive et sous un modèle forfaitaire.

Originaires des États-Unis, les premiers MSP sont apparus à la fin des années 1990, avant de connaître leur développement dans les années 2000, notamment grâce à l'apparition d'outils spécialisés pour ce modèle, comme un PSA (Professional Services Automation) et un RMM (Remote Monitoring and Management).
Ce modèle a été adopté par ITCOM SERVICES en 2015, il est aujourd'hui fermement implémenté, il apporte de nouvelles façons de gérer techniquement et financièrement ses clients.

Une société de type MSP se repose sur 3 piliers.

Les piliers d'un MSP

Comme dit précédemment, le modèle MSP se caractérise en trois piliers :

- La proactivité.
- L'automatisation.
- La forfaitisation.

La proactivité

D'un point de vue technique, c'est l'un des aspects les plus importants. La gérance des parcs informatiques ne peut pas s'effectuer correctement si la proactivité n'est pas à l'ordre du jour. Les clients se multiplient, les infrastructures s'additionnent, le bruit généré augmente, il n'est plus vraiment possible d'être réactif sous peine d'être noyé au premier changement/incident sur un parc. Pour s'adapter à cette notion, des outils de supervision existent sur le marché, offrant de grandes possibilités de monitoring (surveillance) des appareils dans un réseau informatique : serveurs, ordinateurs, imprimantes, commutateurs, pare-feu, Wi-Fi. Cette surveillance permet de récupérer des informations comme l'état de santé d'un appareil ou ses performances à un moment donné, mais aussi de générer des rapports dans le temps pouvant justifier, par exemple, l'acquisition d'un nouvel équipement. La proactivité se mesure aussi à l'aide de visites préventives, permettant de recenser le matériel existant, notifier tout changement, d'anticiper les problèmes d'une infrastructure et d'apporter aide au conseil au détenteur de ses équipements.

L'automatisation

L'automatisation est très souvent de pair avec la proactivité. En effet, pour une utilisation optimisée des outils de supervision, il est nécessaire d'automatiser le plus possible la récolte des informations et le traitement de celles-ci. L'opérateur humain doit uniquement s'assurer du bon fonctionnement des procédés mis en place et veiller au bon fonctionnement de ceux-ci, tout en restant vigilant aux améliorations portées à ses outils pouvant affecter son travail. La volonté d'un MSP est de standardiser les parcs clients, d'où les déploiements de nouveaux appareils. Plus le nombre d'équipements à déployer est grand, plus l'automatisation apporte de la valeur ajoutée. Le gain de temps est considérable, la libération des ressources affectées auparavant permet à celles-ci de se concentrer sur d'autres aspects de leur travail. La productivité globale en est alors affectée, elle s'améliore.

Cependant, c'est le sujet faisant le plus défaut chez les MSP. Automatiser des procédés requiert une grande connaissance des outils utilisés pour les employer à leur plein potentiel. Très souvent, l'automatisation touche plusieurs entités dans une même société (et peut parfois s'étendre au-delà) et nécessite en conséquence une connaissance globale de la structure et des services qui définissent l'entreprise.

La forfaitisation

C'est la dernière caractéristique d'un MSP, très importante, elle assure la survie des sociétés de services de ce type. Ce qui différencie les sociétés informatiques « classiques » des sociétés MSP, c'est leur source de revenus : la récurrence. En effet, la recherche de nouvelles opportunités ne devient plus obligatoire pour assurer la pérennité d'un MSP, puisque la vente de ses services est désormais forfaitisée. Il n'est plus question de facturer au temps passé, mais aux services vendus (un périmètre défini avec son client). Dans ce mode de revenu récurrent, l'on peut distinguer deux grandes familles

sur lesquelles les MSP se basent : la facturation en fonction du nombre d'équipements (ordinateurs, serveurs…) ou la facturation au nombre d'utilisateurs. La forfaitisation permet en outre des revenus mensuels stables et prédictibles dans le temps, mais nécessite une organisation à toute épreuve et une rigueur absolue dans la gestion des parcs informatiques. Effectivement, les changements d'équipements sont fréquents, de même pour les utilisateurs. L'appréhension du périmètre client vendu en est alors affectée.

Les trois piliers caractérisant les sociétés de type MSP sont liés et influent les uns sur les autres. Il est donc important de veiller régulièrement à ne pas s'écarter de l'idéologie déterminant les MSP.

Structure et services de l'entreprise

ITCOM SERVICES compte aujourd'hui 12 employés, répartis dans 3 services différents :

- Le service Opérations.
- Le service Administration des ventes.
- Le service Commercial.

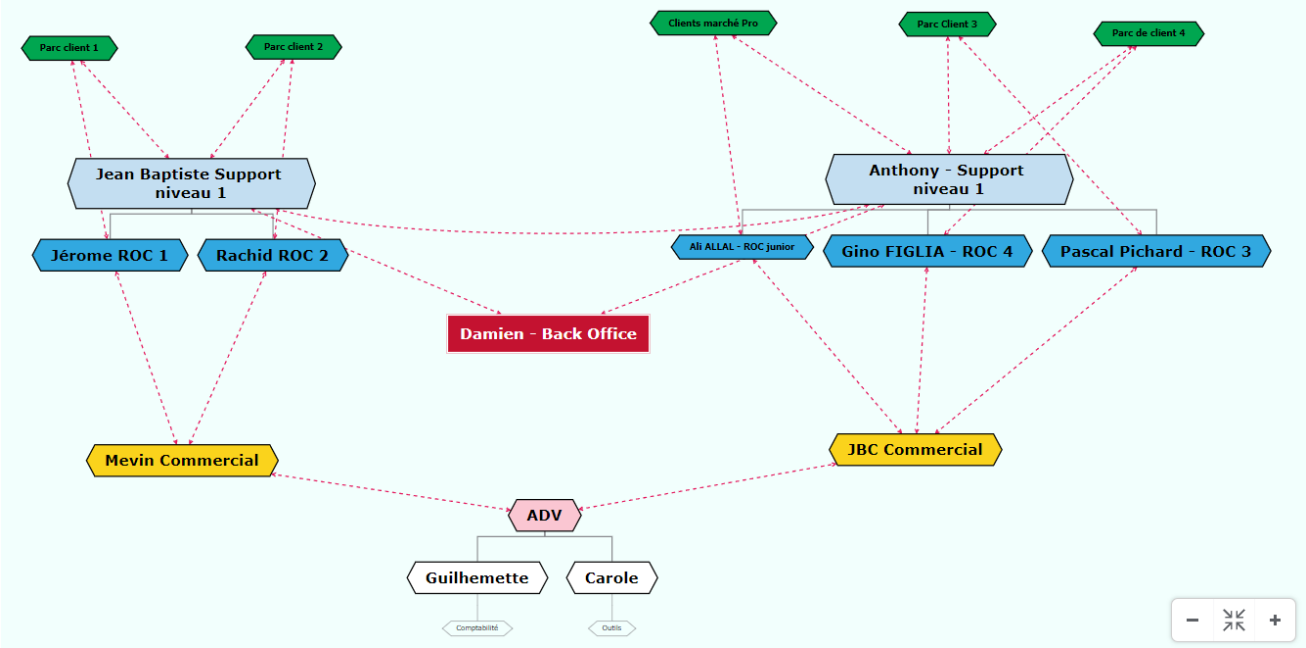

Figure 3 : Organigramme de l'entreprise

Parmi ces techniciens, 5 possèdent l'appellation de ROC (Responsable Opérationnel de Comptes), c'est-à-dire qu'ils s'occupent personnellement de parcs informatiques qui leur ont été attribués. Les tâches et responsabilités des ROC sont diverses, parmi celles-ci l'on peut noter :

- Gérer les incidents de niveau 2 (ouverture, résolution, clôture).
- Maintenir le parc informatique à jour (en accord avec l'aspect de forfaitisation, le nombre d'utilisateurs, d'ordinateurs…).
- Être l'interlocuteur privilégié du client (conseil sur l'évolution du parc, transparence au niveau des incidents et problématiques, accompagnement dans l'embarquement ou la séparation…).
- Assurer des visites préventives en lien avec le contrat sélectionné (aspect proactif et forfaitisation).

Les autres techniciens s'occupent du centre d'assistance (ou helpdesk), leur rôle consiste en :

- Réceptionner les appels et demandes entrants (qualification de la demande, priorité, retranscription).
- Résoudre les incidents de niveau 1 (et de niveau 2 lorsqu'il est accessible).
- Effectuer des déplacements brefs sur site (lors d'un dépannage non faisable à distance, ou de l'installation d'appareils ne nécessitant pas de compétences de niveau 2).

• Conseiller le client vis-à-vis de l'évolution de son matériel (changement d'ordinateur, de composants, en accord avec le ROC). Ces trois services sont liés entre eux, les différents salariés communiquent naturellement entre les services lors de problèmes et d'interrogations.

Ces trois services sont liés entre eux, les différents salariés communiquent naturellement entre les services lors de problèmes et d'interrogations (figure 3).

Cadre technique

Au cours de ce stage, j’ai eu l’opportunité de découvrir plusieurs métiers dans la structure et de comprendre de manière globale le fonctionnement des différentes professions. Pour une meilleure compréhension des tâches que j’ai pu effectuer, il apparaît approprié de traiter en premier lieu des missions et des tâches qui m’ont été confiées, puis de présenter les outils qui étaient mis à ma disposition pour effectuer des missions tout au long de mon stage.

Les objectifs du stage

L'un des objectifs majeurs de mon stage était de mettre en pratique les connaissances théoriques que j'avais acquises tout au long de mes études. Cela s'est concrétisé par ma participation à des projets concrets, me permettant ainsi de développer mes compétences dans divers domaines technologiques.

Une priorité essentielle était d'améliorer ma maîtrise de PowerShell. J'ai eu l'occasion de m'impliquer dans des tâches de scripting, d'automatisation et de gestion système en utilisant PowerShell. Cette expérience a été bénéfique pour consolider mes compétences dans la gestion des systèmes Windows.

Par ailleurs, j'avais pour objectif d'explorer différentes technologies telles que Debian, WordPress, Python, Azure, VMWare, MalwareBytes. J'ai eu l’occasion de participer à des projets centrés sur ces technologies, ce qui a contribué à développer mes compétences dans la gestion de serveurs, le développement et l’automatisation.

L’un de mes objectifs était également d'échanger mes idées et de participer activement aux différentes initiatives de l'entreprise, via des réunions et/ou ateliers pratiques.

Les outils mis à disposition

Une grande partie de mon temps a été consacrée à l'exécution de diverses missions au profit de l'entreprise. J'ai effectué ces tâches en utilisant un environnement Windows sur mon ordinateur, ce qui m'a offert une plus grande facilité d'utilisation grâce à l'utilisation de PowerShell. De plus, j'ai utilisé Visual Studio Code pour le développement de programmes en Python, ce qui m'a permis d'accomplir certains objectifs spécifiques.

Pour répondre à différents besoins et effectuer des tests, j'ai également eu accès à VMware ESXi, me permettant de changer de système d'exploitation en fonction des différentes tâches à effectuer. Par ailleurs, pour faciliter mon travail, j'ai pu connecter mon ordinateur à une station d'accueil dotée de deux écrans supplémentaires, ce qui a grandement amélioré ma productivité.

Ces outils et équipements mis à ma disposition ont été d'une grande utilité pour mener à bien mes missions et ont contribué à optimiser mon efficacité et ma qualité de travail durant mon stage.

J’ai également eu l'opportunité d'utiliser Datto RMM (Remote Monitoring and Management), un outil MSP qui m'a permis de surveiller et de prendre en charge à distance les appareils des clients. Grâce à cette solution, j'étais en mesure d'accéder et de gérer les appareils depuis n'importe quel endroit, sur n'importe quel dispositif connecté à Internet, dès lors qu'il était sous tension.

Mes projets

Déploiement d'applications via Autopilot

Descriptif

La préparation des ordinateurs est devenue un élément essentiel dans le monde de l'informatique moderne. Il s'agit d'une étape cruciale dans le processus de déploiement des postes aux utilisateurs finaux, qui permet d'automatiser la configuration de nos ordinateurs et le déploiement des logiciels. Parmi les différentes méthodes de déploiement, l'utilisation de Windows Autopilot a émergé comme une solution innovante et efficace.

Dans le cadre de ce projet, j'ai entrepris de déployer des applications en utilisant Windows Autopilot. Grâce à cette technologie, j'ai pu simplifier et accélérer considérablement le déploiement des applications, tout en garantissant une configuration cohérente et fiable (figure 4).

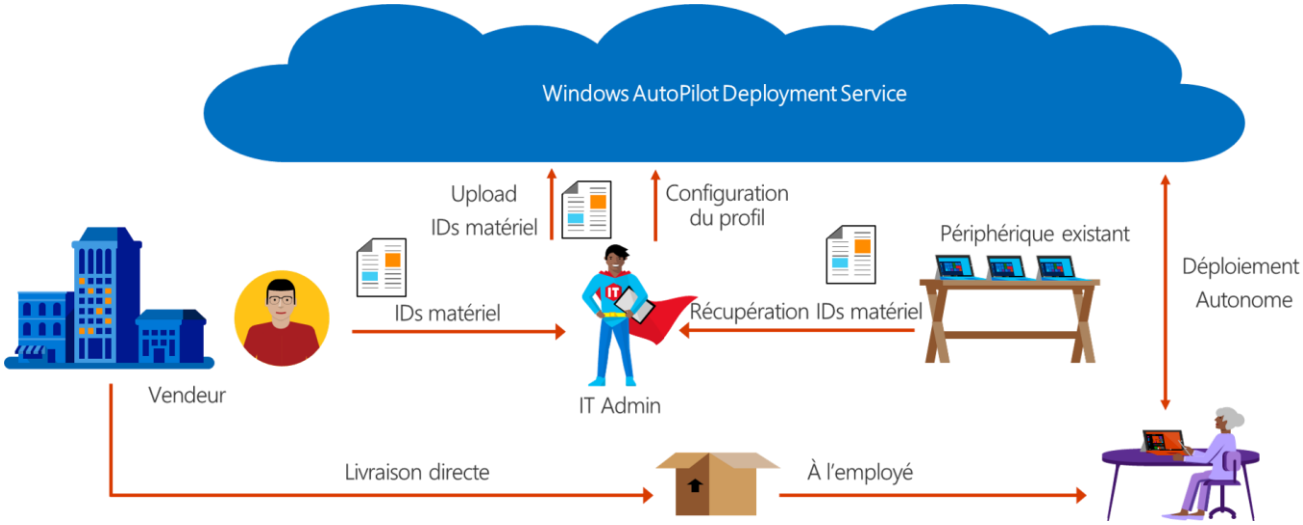

Figure 4 : Schéma Autopilot

L'IT Admin s'occupe de récupérer les différents ID qui seront nécessaires à la manipulation. Il passera par une configuration du profil et de l'appareil pour ensuite déployer des applications et logiciels de manière autonome.

La procédure complète sera disponible en Annexes.

Réalisation

Lors de la configuration de l'Autopilot, j'ai ouvert une session sur la machine cible et exécuté PowerShell en tant qu'administrateur pour obtenir les privilèges nécessaires. J'ai suivi plusieurs étapes pour préparer la machine.

La première étape consistait à créer un répertoire nommé "HWID" pour stocker les informations d'identification requises par l'Autopilot. Ensuite, j'ai modifié la stratégie d'exécution de PowerShell en utilisant la valeur "RemoteSigned" pour pouvoir exécuter les scripts sans contraintes.

J'ai vérifié la présence du fournisseur NuGet et l'ai installé si nécessaire. Ensuite, j'ai installé le script nécessaire en utilisant une commande spécifique.

Pour faciliter l'exécution future du script, j'ai modifié la variable d'environnement en ajoutant le chemin d'accès au répertoire PowerShell à sa valeur actuelle. Cela simplifie l'utilisation ultérieure du script.

Enfin, j'ai créé un fichier .csv pour stocker l'ID du PC par hash, ce qui est essentiel pour le bon fonctionnement de l'Autopilot.

Ce processus de configuration est une étape importante pour mettre en place l'Autopilot et permettre un déploiement efficace des machines. En suivant ces étapes, j'ai pu préparer la machine cible et garantir un fonctionnement optimal de l'Autopilot (figure 5).

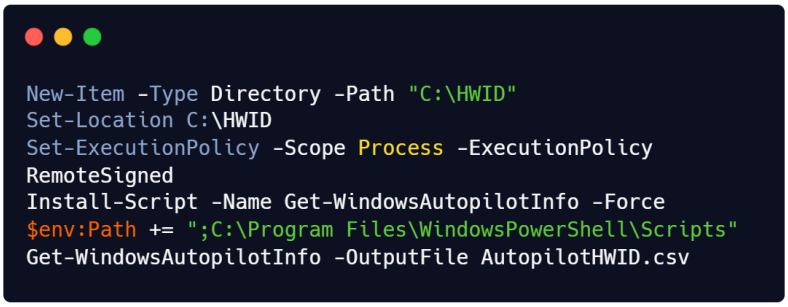

Figure 5 : Programme de capture de l'ID

Après avoir terminé mes activités sur le PC du client, je me suis connecté à mon propre poste et j'ai accédé au portail endpoint.microsoft.com (figure 6) en utilisant mes identifiants d'administrateur. J'ai utilisé la fonction d'importation disponible dans le portail et j'ai choisi le fichier CSV contenant les données de l'ordinateur pour l'importer dans le système.

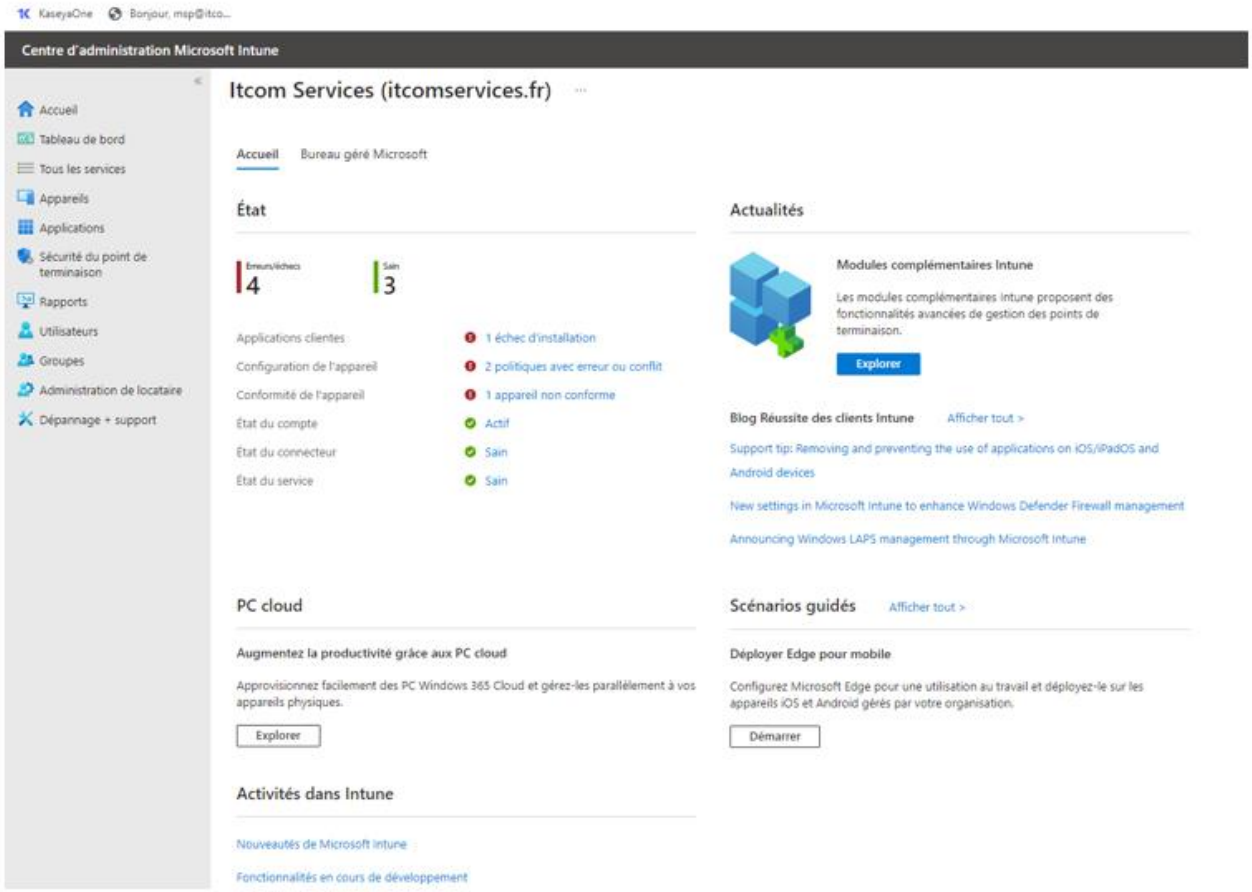

Figure 6 : Microsoft Endpoint

Une fois l'appareil importé, le PC du client sera réinitialisé en cas de refonte totale de l'ordinateur ou sinon juste éteint en cas d'ajouts d'applications.

La suite du projet s'effectue sur l'Azure Active Directory (Azure AD). Azure AD fonctionne comme un annuaire de gestion des identités, permettant aux administrateurs informatiques de créer, gérer et supprimer des utilisateurs et des groupes, ainsi que de définir des politiques de sécurité pour contrôler l'accès aux ressources. Il prend en charge l'authentification unique (Single Sign-On) pour permettre aux utilisateurs de se connecter à plusieurs applications cloud et locales à l'aide d'un seul ensemble d'identifiants. Dans notre cas, il va nous fournir des fonctionnalités de gestion des accès et des identités, telles que la gestion des appareils, la gestion des applications et la gestion des rôles. Il offre des intégrations étroites avec d'autres services Azure, tels qu'Azure Information Protection et Azure Multi-Factor Authentication, pour renforcer la sécurité des identités et des données.

À l'aide de Microsoft Intune, je configure les paramètres nécessaires pour le bon fonctionnement du processus comme la portée de l'utilisateur GDR ou l'étendue utilisateur GAM (jointure des appareils à Azure AD gérés par Intune).

La création d'un groupe que j'ai appelé « Autopilot » est obligatoire pour renseigner l'utilisateur en question (le PC du client) ainsi que l'administrateur du compte. Par suite de cela, je devais configurer un profile pour le déploiement d'Autopilot en renseignant le groupe et effectuer une jointure.

Figure 7 : Profil Autopilot

On synchronisera par la suite l'appareil du client pour que la connexion soit établie (figure 7).

Pour installer une application, il y avait un large éventail de choix. On pouvait installer Microsoft ou des applications bien précises. Ce qui nous intéresse donc ici est l'installation d'applications Windows (Win32). Cela est très utilisé si je veux télécharger ou installer l'application que je veux déployer, car le service sur Azure AD est assez limité en termes de diversité d'installation.
L'installateur de notre application sera un package .msi. Cela dit, je vais faire face à un problème. Le package doit être un fichier .intunewin,

Après une recherche sur la documentation Microsoft, j'ai trouvé un exécutable qui permet de convertir un .msi en un .intunewin. Cette application se nomme IntuneWinAppUtil.exe (figure 8). Je vais donc créer un dossier, mettre le .msi et le .exe dans le même répertoire pour effectuer la conversion.

Les données à rentrer pour faire marcher le processus sont les suivantes :

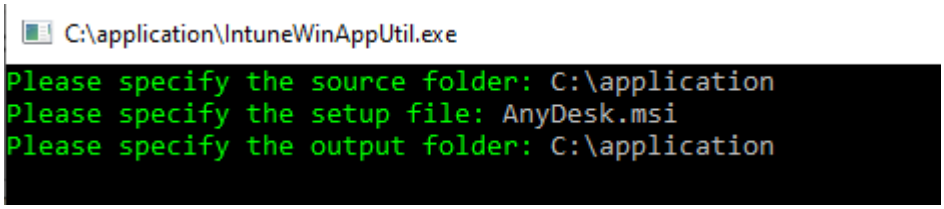

Figure 8 : IntuneWinAppUtil.exe

The source folder : le chemin où le fichier se trouve
The setup file : le nom de l'installateur
The output folder : le chemin dans lequel on exporte le fichier .intunewin

Sur Microsoft Intune, je sélectionne le package et j'arriverai sur la page d'information sur l'application. À ce moment-là, je dois spécifier un nom d'éditeur, les deux commandes d'installation et de désinstallation sont automatiquement rentrées, car nous avons un fichier en .msi. Nous mettons l'architecture du système d'exploitation sur 64 bits. Pour le système d'exploitation minimal, cela peut-être au choix, mais nous pouvons mettre Windows 10 20H2.
Des règles seront aussi à formater, mais cela est fait automatiquement par l'application. J'ajoute enfin le groupe « Autopilot » créé avant pour raccorder l'application au PC du client.

Après validation, notre application est enfin prête à être déployée.

Malheureusement, beaucoup d'applications ou logiciels ne sont pas disponibles avec le package .msi. Nous trouvons de nos jours majoritairement des fichiers en .exe pour le téléchargement et l'installation de nos besoins informatiques. Une solution pour pallier ce problème est l'utilisateur d'un convertisseur MSI pour nos applications (figure 9).

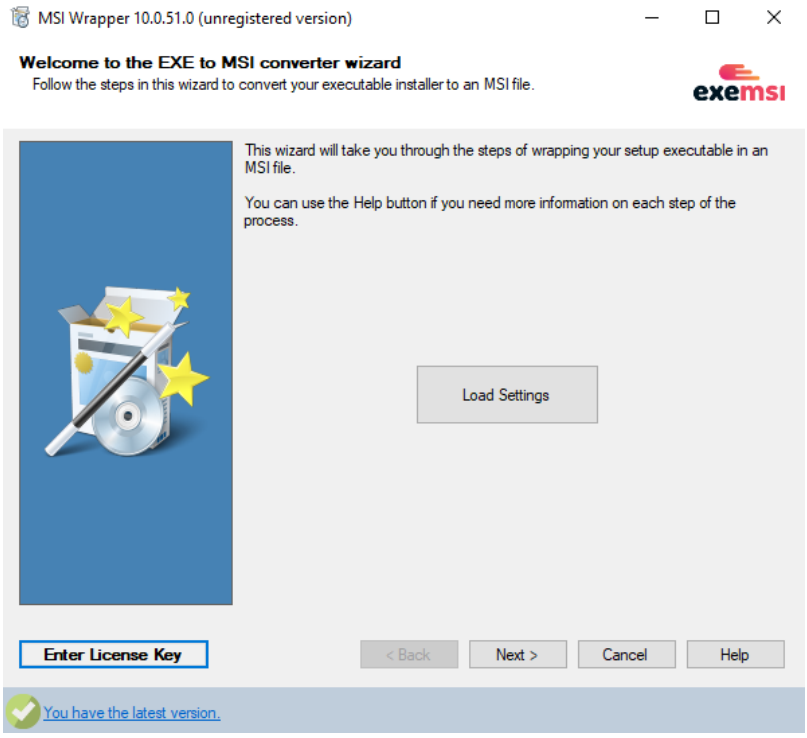

Figure 9 : MSI Wrapper

Cette application a été facilement trouvée sur internet en plus d'être gratuite pour le grand public. L'utilisation est simple, en suivant les étapes d'installation, j'ai juste eu à sélectionner le chemin de mon fichier .exe. Le nom du fichier en .msi est automatiquement ressorti. Je dois aussi générer un code d'authentification que je garderais pour les futures mises à jour. Le reste des informations sont par défaut vu que l'application arrive à reconnaitre notre fichier d'installation, je dois juste vérifier si elles sont correctes et je peux convertir mon fichier (figure 10).

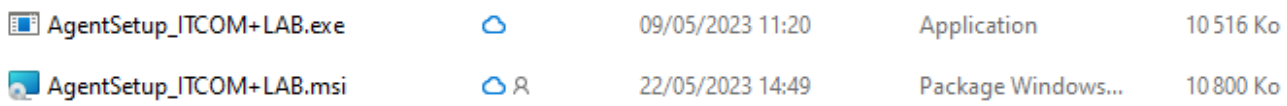

Figure 10 : Résultat de la conversion

Conclusion du projet

À travers le processus de Windows Autopilot, j'ai pu simplifier de manière considérable le processus de déploiement des nouveaux PC. La configuration et le provisionnement des appareils à distance ont pu se mettre en place sans intervention physique sur site. Cela permet de gagner du temps et de réduire les coûts liés au déploiement traditionnel (figure 11).

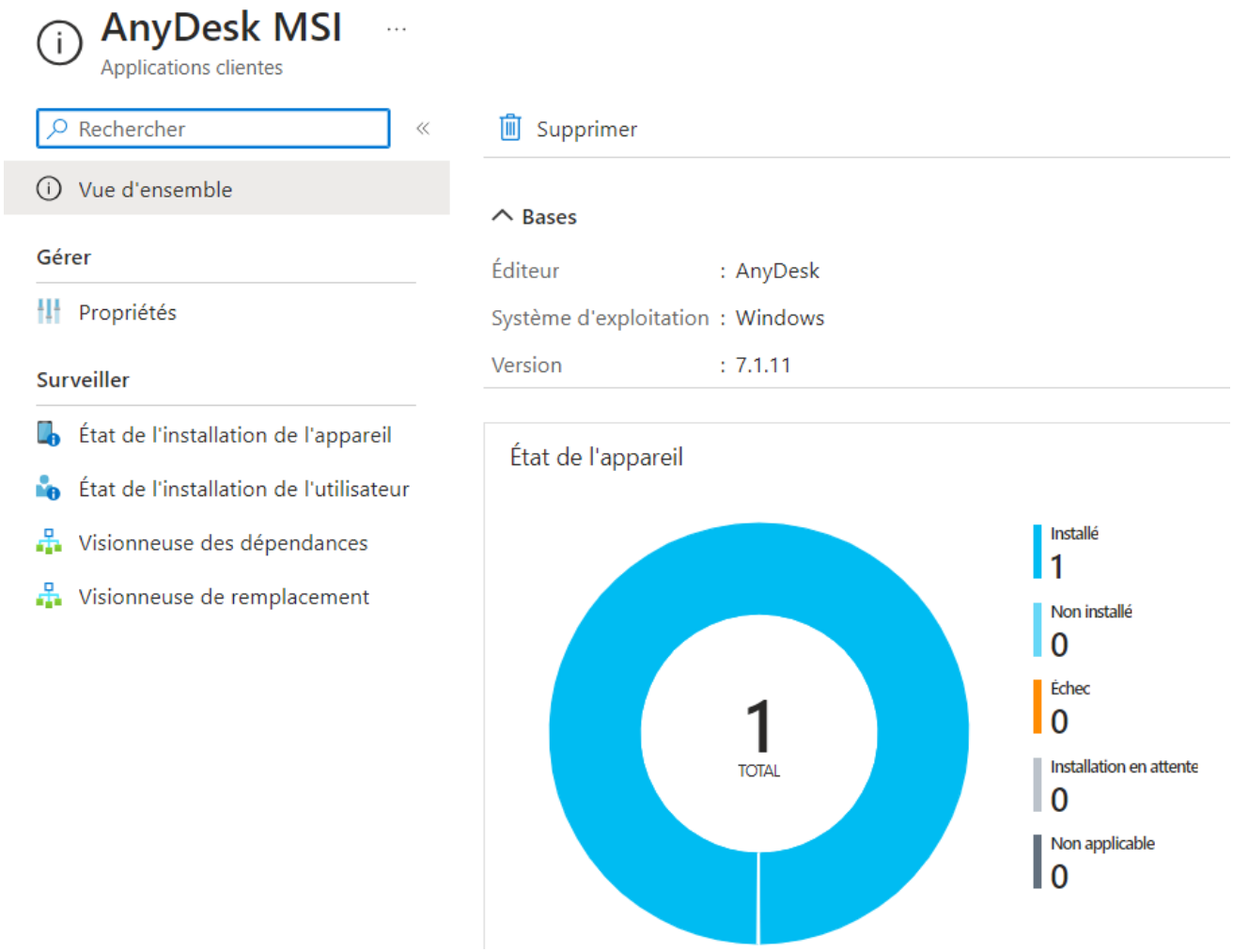

Figure 11 : Etat de l'application

MalwareBytes EDR

Descriptif

La sécurité informatique est un enjeu majeur dans le monde numérique d'aujourd'hui, où les cybermenaces sont de plus en plus sophistiquées et omniprésentes. Les attaques malveillantes peuvent causer d'importants dégâts aux entreprises, allant de la perte de données à des interruptions de service critiques. Dans ce contexte, les solutions de détection et de réponse aux incidents (EDR - Endpoint Detection and Response) jouent un rôle crucial pour protéger les systèmes et les réseaux contre les attaques.

Malwarebytes EDR est une solution EDR de pointe développée par Malwarebytes, une entreprise leader en matière de cybersécurité et connue du grand public pour sa version gratuite. Conçu pour fournir une protection avancée contre les menaces émergentes, Malwarebytes EDR offre une visibilité étendue sur les endpoints (points d'accès) d'un réseau et permet une détection proactive des activités suspectes.

L'approche d'EDR adoptée par Malwarebytes repose sur une surveillance continue et en temps réel des endpoints, ainsi que sur l'analyse des comportements et des modèles d'activité. L'objectif principal de Malwarebytes EDR est d'identifier rapidement les comportements anormaux et les indicateurs de compromission (IOC) pour une réponse proactive aux attaques avant qu'elles ne causent des dommages significatifs.

Les fonctionnalités clés de Malwarebytes EDR comprennent la détection en temps réel des menaces, l'analyse comportementale avancée, la remédiation automatisée des incidents, la collecte de données forensiques et la génération de rapports détaillés sur les événements de sécurité. Grâce à son architecture évolutive et à sa capacité à s'intégrer avec d'autres solutions de sécurité, Malwarebytes EDR offre une approche holistique de la défense des endpoints (figure 12).

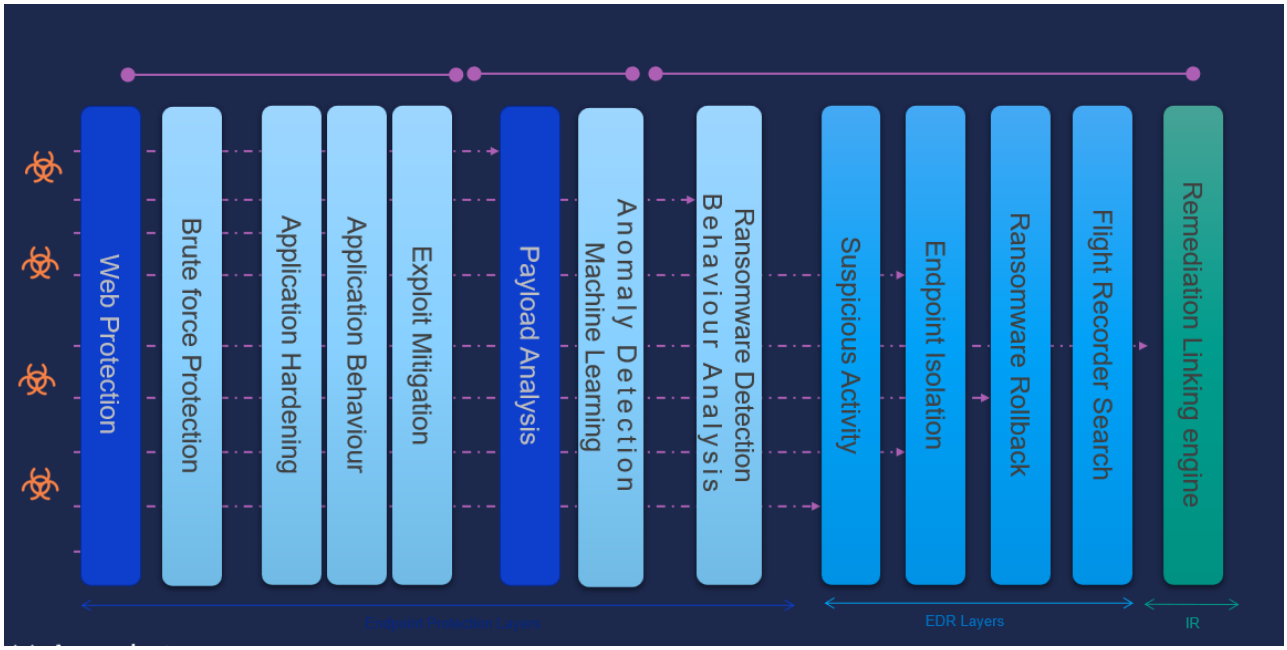

Figure 12 : Les différentes couches

Les détails des couches seront disponibles en Annexes.

Réalisation

J'ai commencé par créer une machine virtuelle (VM) Windows et installer le système d'exploitation requis. J'ai configuré les paramètres de la VM en fonction des besoins du projet, notamment les ressources allouées et la connectivité réseau. La création de celle-ci s'est faite avec l'aide de L'ESXi de l'entreprise.

Grâce aux accès à la console fournis par l'entreprise sur Malwarebytes, j'ai pu accéder à la console de gestion MSP. C'est une interface centralisée qui permet aux administrateurs informatiques de gérer et de surveiller les produits Malwarebytes déployés sur leurs systèmes. J'ai procédé à l'installation de Malwarebytes sur la VM et j'ai configuré la console en créant une stratégie personnalisée (figure 13). J'ai ajusté les règles de sécurité pour permettre le passage du virus dans le cadre de mes tests. J'ai également associé mon adresse électronique au groupe, de sorte que je puisse recevoir une notification en cas de détection d'une intrusion grave.

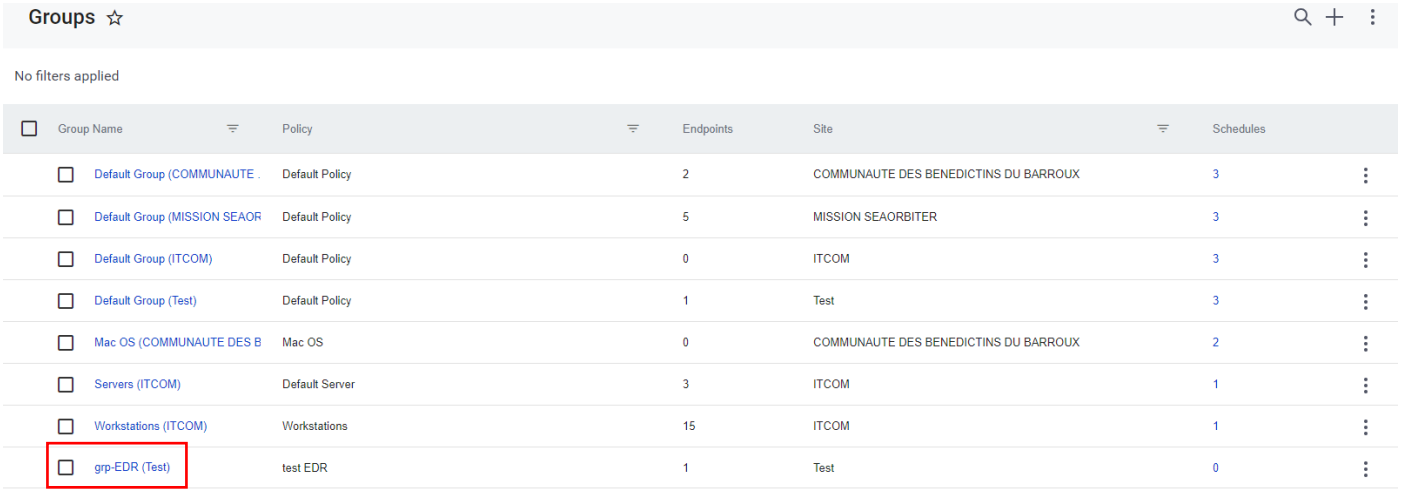

Figure 13 : Liste de stratégies

Avant d'exécuter les tests, j'ai effectué quelques préparatifs sur la VM. Tout d'abord, j'ai installé un paquet permettant de configurer le clavier en français, car cette option n'était pas disponible par défaut. J'ai téléchargé le paquet requis et l'ai placé dans un répertoire que j'avais créé, sur le stockage de données de la VM. Ensuite, j'ai établi une connexion SSH avec la VM et me suis déplacé vers le répertoire approprié. J'ai exécuté la commande nécessaire pour installer le paquet et configurer le clavier en français.

Une fois la préparation terminée, j'ai utilisé Malwarebytes EDR Tester (figure 14), un outil fourni par Malwarebytes, pour effectuer les tests sur l'antivirus. Tout d'abord, j'ai vérifié l'état des plugins et agents dans la console de gestion afin de m'assurer qu'ils étaient à jour. Ensuite, j'ai téléchargé le payload de test spécifique à mes scénarios d'intrusion.

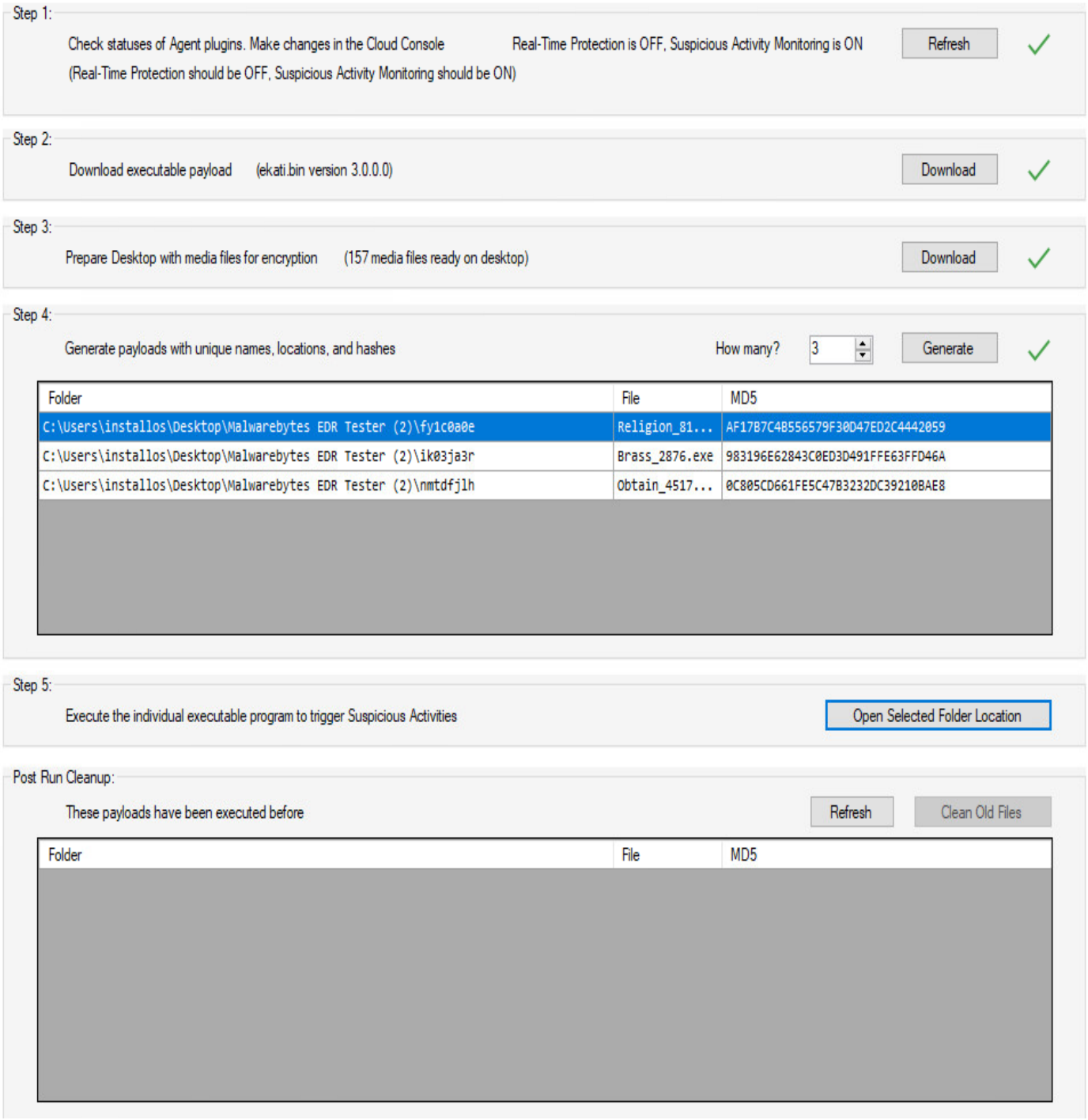

Figure 14 : EDR Tester

Après avoir téléchargé le payload, l'EDR Tester a préparé mon bureau en ajoutant des fichiers média qui seraient ensuite chiffrés par le virus. J'ai généré des payloads avec des noms uniques, des emplacements spécifiques et des hash associés. Ensuite, je me suis rendu dans le dossier approprié sur la VM et j'ai lancé l'exécution du virus en cliquant dessus.

Le ransomware va se dérouler sous plusieurs étapes. Il va pénétrer le système informatique par suite du fonctionnement de l'exécutable. Il va s'activer en s'installant de manière discrète sur l'ordinateur ciblé. Il peut se dissimuler dans des fichiers exécutables ou exploiter des failles de sécurité pour obtenir les privilèges nécessaires. Le ransomware identifie et sélectionne les fichiers à chiffrer. Il utilise généralement des algorithmes de chiffrement forts pour rendre les fichiers illisibles sans la clé de

déchiffrement appropriée. Les types de fichiers couramment ciblés sont les documents, les images, les vidéos, les bases de données, etc (voir figure 15).

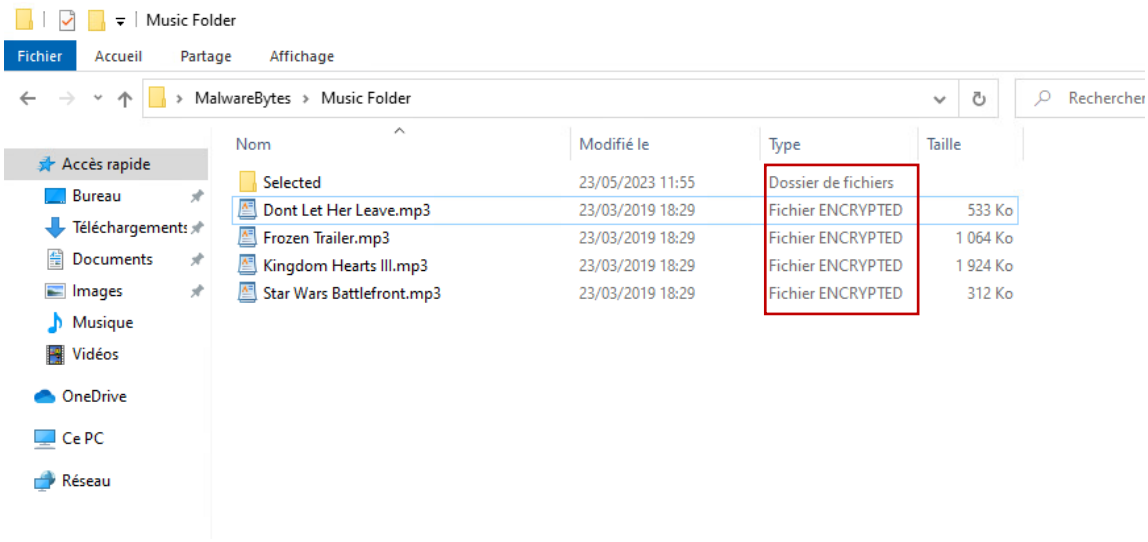

Figure 15 : Fichiers encryptés

Une fois les fichiers chiffrés, le ransomware affiche un message à l'utilisateur, informant que ses fichiers ont été pris en otage et qu'il doit payer une rançon pour obtenir la clé de déchiffrement. Les instructions détaillées sur la manière de procéder au paiement sont fournies, souvent avec un délai limite. Le ransomware peut mettre en place des mécanismes de persistance pour assurer sa survie sur le système infecté, tels que la création de nouvelles entrées de registre ou la modification des paramètres du système.

Dans les cas les plus graves, il peut se propager à travers le réseau de l'organisation, infectant d'autres systèmes connectés. Cela peut se produire en exploitant des vulnérabilités ou en utilisant des techniques d'ingénierie sociale pour inciter les utilisateurs à ouvrir des pièces jointes ou des liens malveillants.

Conclusion du projet

L’objectif principal était de faire une vidéo à but explicatif sur le fonctionnement de l’EDR sur la console Malwarebytes et présenter son environnement à l’entreprise. À la fin du projet, nous avons observé qu'EDR Tester, l'outil utilisé, semblait être après discussion avec Malwarebytes, whitelisté par l'éditeur, car nous n'avons reçu aucune notification indiquant une intrusion. Il n'a donc pas été détecté comme une menace et a pu passer inaperçu.

Le système d’alerte n’a donc pas fonctionné, un ticket a été généré à l’éditeur. Entre-temps, j’ai eu la possibilité de vérifier si le fichier en question (figure 16) est malveillant avec l’utilisation de la Sandbox Malwarebytes.

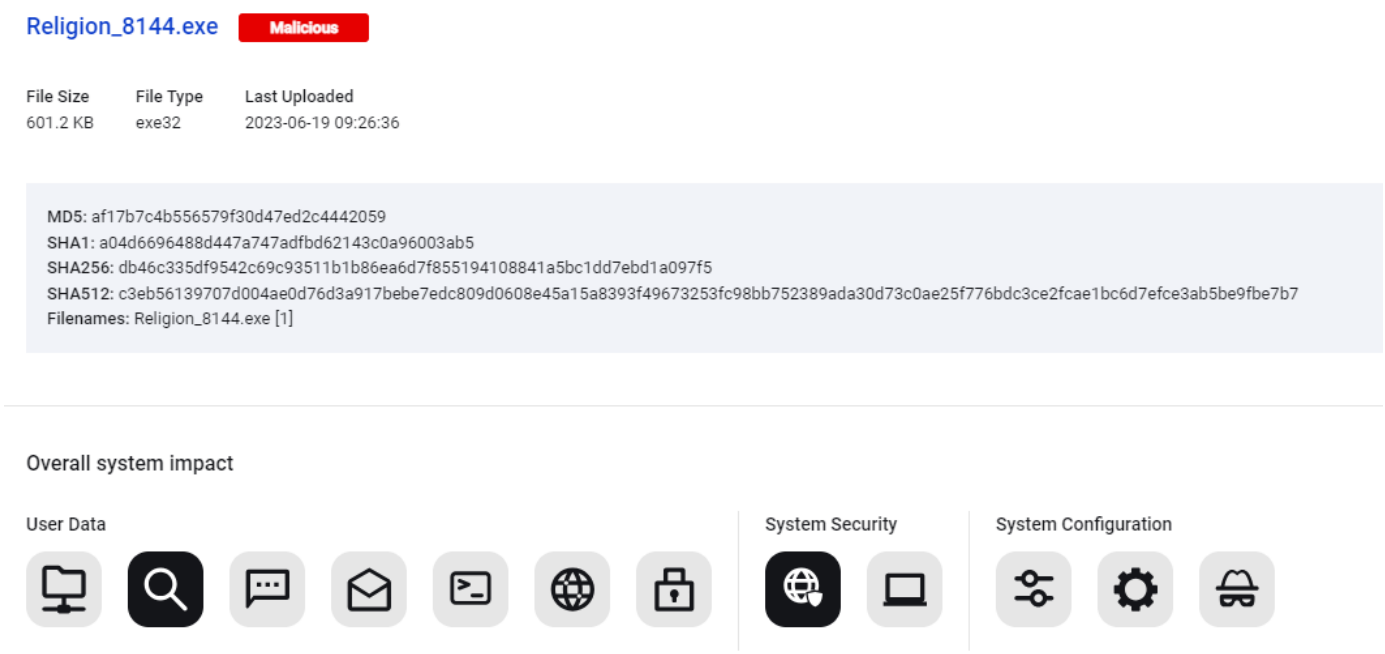

Figure 16 : Description du virus

L’entreprise propose une fonctionnalité appelée "Sandbox" (bac à sable) qui permet d'exécuter des fichiers suspects dans un environnement isolé et sécurisé. Je peux choisir de l’exécuter pour l’analyser en toute sécurité sans risquer d’infection dans mon système. Il sera confiné dans l’environnement lors de l’analyse des actions du fichier telles que les tentatives de modification des fichiers système, l’accès au réseau, les modifications du registre, etc. Si le fichier exécuté dans la Sandbox est identifié comme malveillant, Malwarebytes le détectera et prendra les mesures nécessaires pour le supprimer. Cela permet de prévenir les infections potentielles et de protéger le système principal. Une fois l'analyse terminée, Malwarebytes fournit des rapports détaillés sur le comportement du fichier dans la Sandbox. Ces rapports peuvent inclure des informations sur les activités malveillantes détectées, les fichiers ou processus impactés, ainsi que les mesures prises pour protéger votre système.

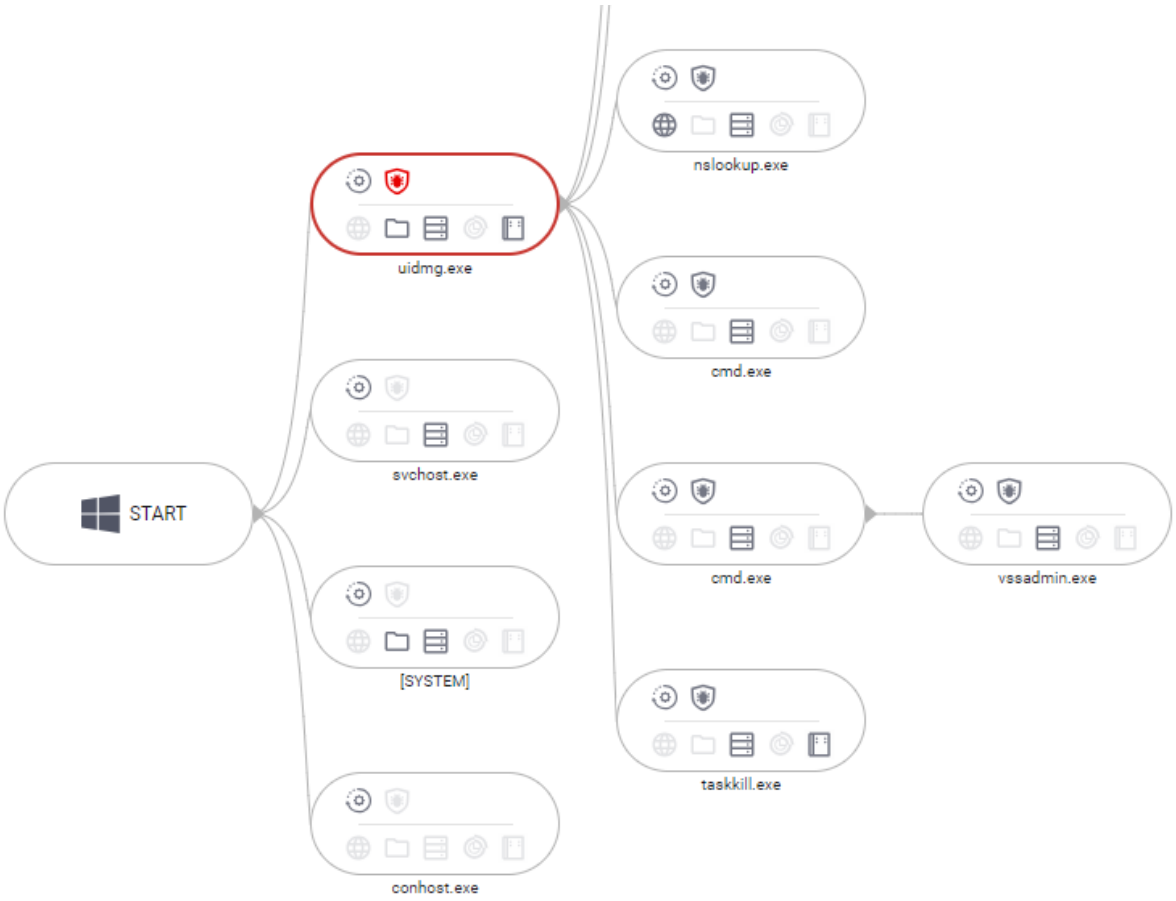

Figure 17 : Segment du virus

Nous pouvons voir le flux d'exécution du fichier en indiquant les différentes étapes et les actions effectuées sur notre système.

Le graphique illustre les relations entre le fichier malveillant et d'autres processus ou applications présents dans la Sandbox. Cela peut inclure les processus initiés par le fichier, les dépendances ou les interactions avec d'autres fichiers ou programmes. Les analystes de sécurité peuvent identifier les schémas d'activité malveillante, les points de vulnérabilité du système et les indicateurs de compromission potentiels.

Le process graph (graphique) de la Sandbox de Malwarebytes permet de comprendre visuellement le comportement d'un fichier malveillant lors de son exécution. Il offre une représentation détaillée des actions effectuées par le fichier dans un environnement isolé, ce qui permet de détecter les activités suspectes et de prendre les mesures nécessaires pour protéger le système contre les menaces.

Conclusion

Au cours de mon stage chez ITCOM SERVICES, j'ai pu mettre en pratique mes connaissances théoriques et développer mes compétences dans plusieurs domaines technologiques. J'ai eu l'opportunité de participer à des tâches concrètes, ce qui m'a permis d'appliquer les concepts et les compétences appris en cours.

J'ai particulièrement travaillé sur deux projets durant mon stage. Le premier projet consistait à mettre en place Windows Autopilot, une solution de déploiement à distance des PC pour faciliter la gestion informatique. J'ai effectué les configurations nécessaires et réalisé des tests pour évaluer son efficacité et sa facilité d'utilisation.

Le deuxième projet portait sur le test d'EDR (Endpoint Detection and Response) de Malwarebytes en utilisant un virus spécifique. J'ai utilisé la console de gestion de Malwarebytes pour configurer les paramètres de test, exécuter le virus dans un environnement sécurisé (sandbox) et évaluer la capacité d'EDR à détecter et à répondre à cette menace.

Ce stage m'a permis de développer mes compétences techniques, de découvrir de nouvelles technologies et de m'immerger dans un environnement professionnel. J'ai acquis une expérience précieuse dans la gestion des systèmes, la collaboration en équipe et la résolution de problèmes concrets.

Je tire de cette expérience des enseignements importants qui vont orienter mes choix de carrière. Je suis désormais mieux préparé pour relever de nouveaux défis et je suis enthousiaste à l'idée d'explorer davantage les opportunités dans le domaine de la programmation et de la sécurité informatique.

Les démarches effectuées sur les anti-virus m’intéressent de plus en plus, en passant par tout type de procédés pour sécuriser et protéger les clients. Cet environnement qui est assez grand et intéressant pourrait être un choix d’étude ou de travail envisageable.

En conclusion, ce stage chez ITCOM SERVICES a été une expérience enrichissante qui m'a permis de développer mes compétences, d'acquérir une expérience pratique et de confirmer mon intérêt pour ces domaines.

Remerciements

En premier lieu, je tiens à remercier le dirigeant de la société, M. Jean-Benoît CARSIN, représentant de l'entreprise ITCOM SERVICES. Un grand merci pour son accueil chaleureux au sein de l'entreprise qu'il dirige, ainsi que pour sa patience et ses précieux conseils. Il m'a beaucoup appris sur sa société et les défis qu'un directeur d'entreprise doit relever au quotidien.

Je remercie également mon tuteur professionnel, M. Jérôme DE GRAER, qui a toujours été à mon écoute et a su m'apporter un soutien sans faille.

Je désire aussi remercier mon directeur de formation, M. Jean-Luc DAMOISEAUX, ainsi que l'équipe pédagogique de l'I.U.T R&T Marseille qui m'ont tous deux fourni les outils nécessaires au bon déroulement de mon apprentissage.

Je tiens particulièrement à remercier M. Rabah IGUERNAISSI, mon tuteur académique, qui fut le premier à m'apporter des précisions dans la réalisation de mon projet, aussi bien dans l'approche méthodologique que technique.

J'adresse également mes sincères salutations à l'équipe ITCOM SERVICES, mais aussi aux autres collaborateurs de la société, qui m'ont accueilli, guider et aider tout au long de mon apprentissage.

Glossaire

VLAN : c'est un réseau LAN virtuel et indépendant. Le VLAN a pour but d'améliorer la gestion d'un réseau, d'optimiser la bande passante, de séparer les flux et de renforcer la sécurité.

NAT : La NAT (Network Address Translation) permet à des serveurs, des hôtes et des consoles se trouvant sur différents réseaux de communiquer entre eux via un réseau interne commun.

VMware ESXi : VMware ESXi est un hyperviseur de type 1 indépendant des systèmes d'exploitation. Il repose lui-même sur le système d'exploitation VMkernel qui assure l'interface avec les agents dont il soutient l'exécution.

Windows Autopilot : Windows Autopilot est un ensemble de technologies utilisées pour configurer et reconfigurer de nouveaux appareils de manière à les préparer à une utilisation productive.

RemoteSigned : Stratégie d'exécution par défaut pour les ordinateurs serveur Windows où les scripts peuvent être exécutés.

Fournisseur NuGet : NuGet est le gestionnaire de paquets de la plateforme de développement Microsoft .NET.

Hash : Le terme hash fait référence à un type de fichier utilisé dans le monde de l'informatique et celui de la cryptographie.

Package : Ensemble de prestations constituant un programme complet, et assuré pour un prix forfaitaire.

Payload : Partie fonctionnelle d'un programme.

Single Sign-On : Avec l'authentification unique fédérée, Azure AD authentifie l'utilisateur dans l'application en se servant de son compte Azure AD.

Bibliographie

https://www.microsoft.com/fr-fr/microsoft-365/windows/windows-autopilot

https://learn.microsoft.com/fr-fr/mem/autopilot/configuration-requirements

https://www.starwindsoftware.com/blog/vmware/replace-default-esxi-ssl-certificate-self-signed-certificate-101-introduction/

https://www.dell.com/support/home/fr-fr/drivers/driversdetails?driverid=vmrgg

https://www.windowscentral.com/how-create-scheduled-tasks-powershell-windows-10