Entreprise Proxiad, agence de Paris

Période de stage	Du 05/01/2026 au 06/02/2026
Professeur référent	Mme Sandrine LE SCANFF
Maître de stage	Mr David CHOUR, Responsable de la Sécurité des Systèmes d'Information chez Proxiad Groupe.

CAR Bilgehan

2ème année BTS SIO – Option SISR

Table des matières

Avertissement concernant la confidentialité

Ce rapport de stage contient quelques informations internes de Proxiad (procédures, outils et autres données) qui, pour l'entreprise, restent sensibles.

En respect des règles de confidentialité en vigueur chez Proxiad, ces éléments ont été manipulés avec soin. Certaines parties utiles y figurent sous forme anonymisée, d'autres ont été légèrement modifiées ou même coupées pour éviter toute exposition indésirable.

Le document est prévu uniquement pour l'équipe pédagogique et le jury du BTS SIO, afin qu'ils puissent évaluer la période de stage de manière objective.

En dehors de ce cadre, toute diffusion ou reproduction, même partielle, est interdite sans accord écrit préalable de Proxiad.

Internship Report Introduction

As part of my first-year internship for the BTS SIO (Services Informatiques aux Organisations) program, I had the opportunity to work at Proxiad, a company specializing in IT services and consulting. My role during this internship was focused on system and network administration, which allowed me to gain valuable experience in managing IT infrastructures, ensuring network security, and supporting users.

This report is structured into three main chapters. The first chapter presents the company and its IT environment, including the infrastructure and tools I worked with. The second chapter outlines the objectives of my internship, and the expectations set by my supervisor. Finally, the third chapter details the tasks I completed, the challenges I encountered, and the solutions I implemented.

This internship has been a significant step in my professional development, providing me with practical skills and a deeper understanding of the IT field.

1 Étude de l'existant

1.1 Présentation de l'entreprise, de son activité et de la DSI

Nom de l'entreprise :	Proxiad
Forme juridique :	Société par Actions Simplifées (SAS)
Date de création :	1997
Siège social :	47 Rue de Ponthieu, 75008 Paris
Effectif :	1300 collaborateurs
Secteur d'activité :	Entreprise de Services du Numérique (ESN)
Code APE :	62.02A – Conseil en systèmes et logiciels informatiques
Présence géographique :	En France avec 11 agences et à l'international avec 5 agences en Bulgarie, Macédoine, Maroc et Tunisie.

Proxiad est une ESN spécialisée dans le conseil et l'ingénierie informatique. Elle accompagne ses clients dans la transformation numérique de leurs systèmes d'information (SI), en proposant des solutions sur mesure dans :

- **L'applicatif :** conseil & audit, l'applicatif, la big data ;
- **L'infrastructure :** systèmes & réseaux, le cloud, le grid computing, les architectures ;
- **La cybersécurité :** conseil & stratégies, l'intégration, réponse aux incidents, SOC ;
- **Le DevOps :** Automatisation, Intégration continue, DevSecOps ;

Elle intervient dans de nombreux secteurs d'activité, tels que la banque, l'assurance, la santé, la distribution, l'industrie ou encore les services publics.

J'effectue mon stage au sein de la Direction des Systèmes d'Information (DSI) de Proxiad, qui a son siège à Paris. Ce service est fondamental pour l'entreprise puisqu'il gère et fait évoluer le système d'information au sein de la société. En même temps, il veille à la sécurité, disponibilité, et performance des infrastructures.

La DSI possède une équipe dotée des rôles suivants :

- **Le Directeur des Systèmes d'Information (DSI)** : Il pilote tous les projets internes et définit les orientations technologiques nécessaires pour la société tout en s'assurant que les outils informatiques de la société répondent aux besoins.
- **L'adjoint DSI, aussi nommé Responsable de la Sécurité des Systèmes d'Information (RSSI) :** Il aide le DSI dans la gestion quotidienne. Au quotidien, il gère la cybersécurité, le RGPD et les normes ISO 27001 ainsi qu'il fait le pilotage de certains projets transverses.

- **Le Référent Technique :** Il apporte une expertise technique pour les outils qui sont en place et les choix techniques qui ont été faits. Il aide l'équipe sur les enjeux difficiles et participe à la conception des architectures des nouvelles solutions.
- **Un Administrateur Systèmes & Réseaux :** C'est un spécialiste qui gère l'infrastructure : serveurs, réseaux, virtualisation, sauvegardes et supervision. Il intervient également sur les projets informatiques du service.
- **Le Technicien Support :** assiste les utilisateurs avec des problèmes matériels et logiciels, configure des postes de travail, gère les tickets d'incidents et aide à gérer l'inventaire des équipements informatiques.

Au-delà de son périmètre local, la DSI du siège centralise également la gestion et la coordination des services informatiques des agences régionales de Proxiad (Lyon, Nantes, Aix-en-Provence, Strasbourg, etc.…).

Afin d'assurer une cohérence technique et organisationnelle entre tous les sites, une réunion hebdomadaire est organisée avec les équipes informatiques des agences. Ces échanges permettent de :

- Suivre et rendre compte des progrès sur les projets ;
- Coordonner les interventions techniques ;
- Résoudre les besoins particuliers des agences ;
- Standardiser les configurations et les pratiques.

1.2 Présentation du contexte informatique

La DSI de Proxiad gère un parc d'ordinateurs portables fonctionnant sous Windows 11 Professionnel et reliés au domaine Active Directory et gère avec des stratégies de groupe (GPO).

L'infrastructure est virtualisée avec VMware ESXi, les services majeurs étant hébergés dans des Machines Virtuelles (VM) : Active Directory, serveur de fichiers, serveur d'impression et serveur de rebond. Un serveur NAS Synology permet la sauvegarde quotidienne des machines via Veeam selon une rotation définie.

Un pare-feu en Haute Disponibilité (HA) de type Sophos et des VLANs pour le filtrage des flux (utilisateurs, invités, serveurs) segmentent le réseau interne. L'accès distant s'effectue de manière sécurisée via VPN. Des réseaux Wi-Fi professionnels avec authentification différenciée sont également disponibles aux collaborateurs et aux invités.

La DSI gère ses projets et support via un système de ticketing interne Redmine. Microsoft 365 (Pack Office, Teams, SharePoint, OneDrive) est utilisé au quotidien. Des bases de données internes comme Microsoft SQL Server ou MariaDB alimentent les applications métiers. La protection est gérée par l'outil ESET, tandis que la supervision des ressources critiques est réalisée par Centreon.

2 Cahier des charges

2.1 Descriptions des objectifs du stage

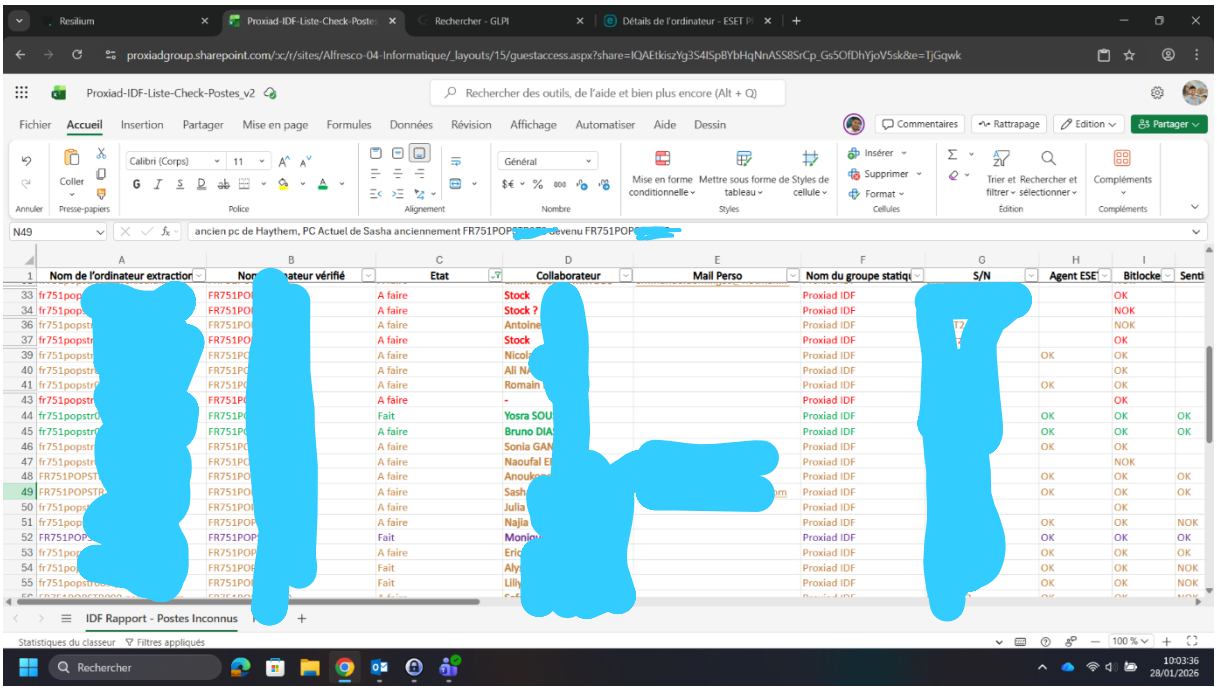
L'objectif central de cette mission est la refonte complète de la gestion du parc informatique, avec un accent particulier mis sur la cybersécurité et la protection des données. Mes responsabilités s'articulent autour de quatre axes majeurs :

- **Gestion de la relation utilisateur et support à distance :**
    - Établir un contact direct avec les collaborateurs pour planifier les interventions techniques.
    - Assurer la prise en main des postes de travail via l'outil **TeamViewer** pour effectuer les configurations nécessaires sans interrompre durablement l'activité des utilisateurs.
- **Optimisation de la sécurité Endpoint (EDR/AV) :**
    - **SentinelOne :** Déploiement de l'agent sur les postes de travail performants (minimum 16 Go de RAM) pour assurer une détection et une réponse aux menaces en temps réel.
    - **ESET :** Mise à jour et homogénéisation de l'antivirus sur les postes ne répondant pas aux critères de l'EDR, garantissant ainsi une protection de base à jour sur l'ensemble du parc.
- **Protection des données (Chiffrement) :**
    - Vérifier l'activation du chiffrement **BitLocker** sur tous les postes mobiles et fixes.
    - Garantir la sécurité de l'organisation en automatisant la remontée des clés de récupération dans l'**Active Directory** pour prévenir toute perte d'accès aux données.

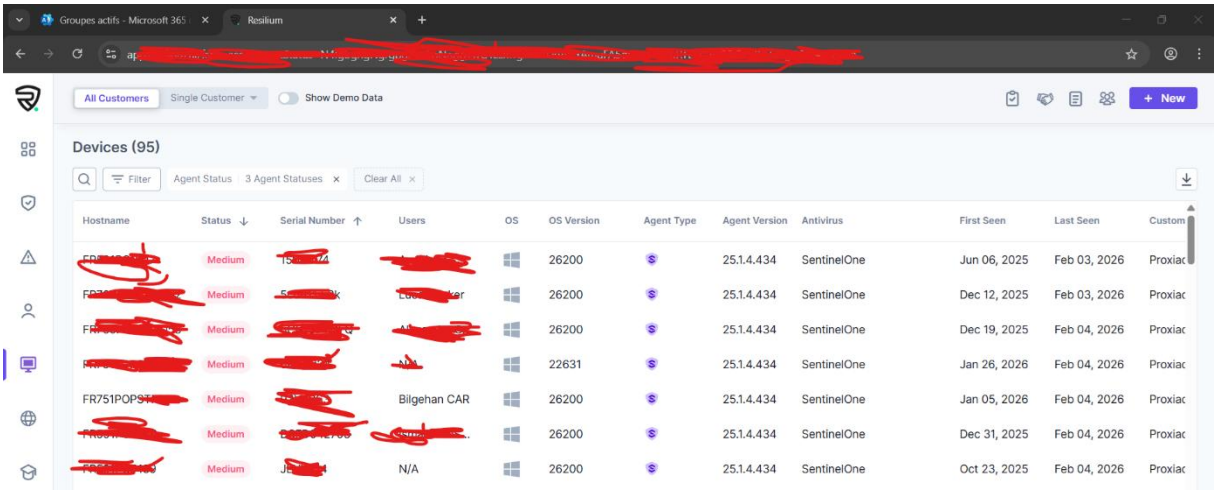
2.2 Schémas / Images explicatifs du cahier des charges

Afin de mener à bien la sécurisation du parc, j'ai utilisé un fichier de suivi précis répertoriant l'ensemble des postes de travail et les collaborateurs associés. Ce document m'a servi de base pour auditer l'état logiciel de chaque machine et planifier les actions correctives.

Ça m'a servi également dans le fichier de consolidation de l'entreprise pour savoir si un collab est toujours affecter à un des pcs renseignés.



CAR	BILGEHAN		IDF	H	Stage	PROXIAD UP	47 rue de Ponthieu Paris 8	INFRA / DEVOPS	Technicien infrastructure		
CAR	BILGEHAN	25000089	IDF	H	Salarié·e	PROXIAD UP	47 rue de Ponthieu Paris 8	INFRA / DEVOPS	Technicien infrastructure	Technicien informatique	



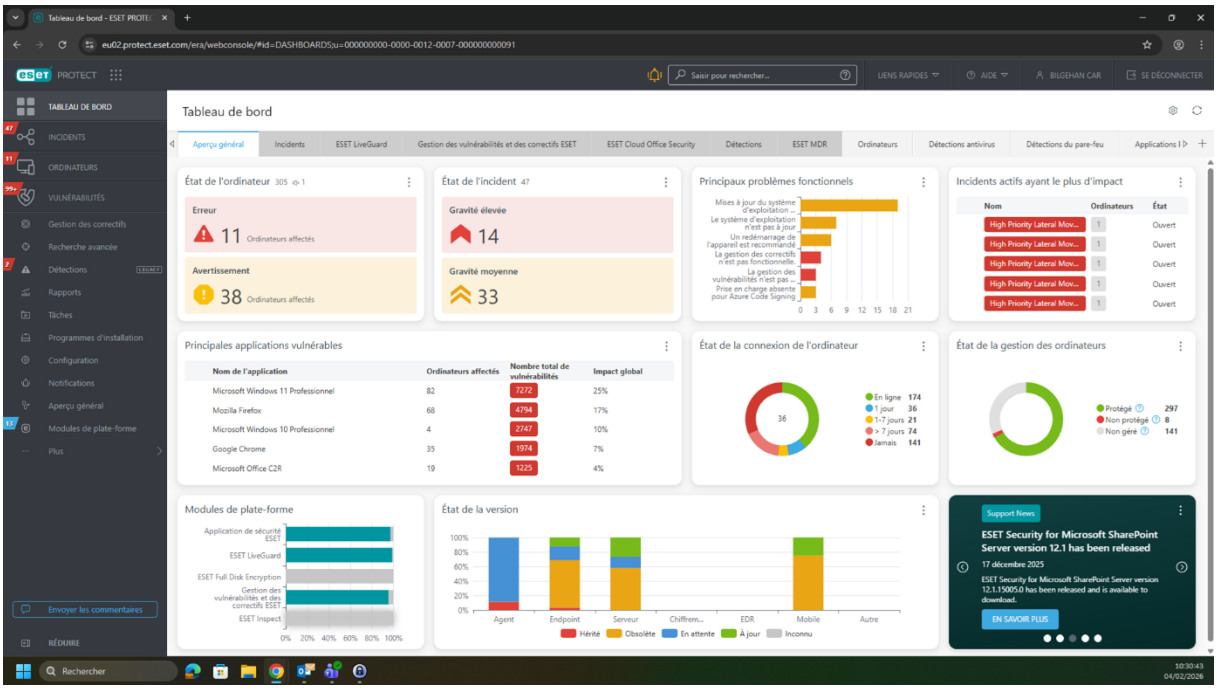
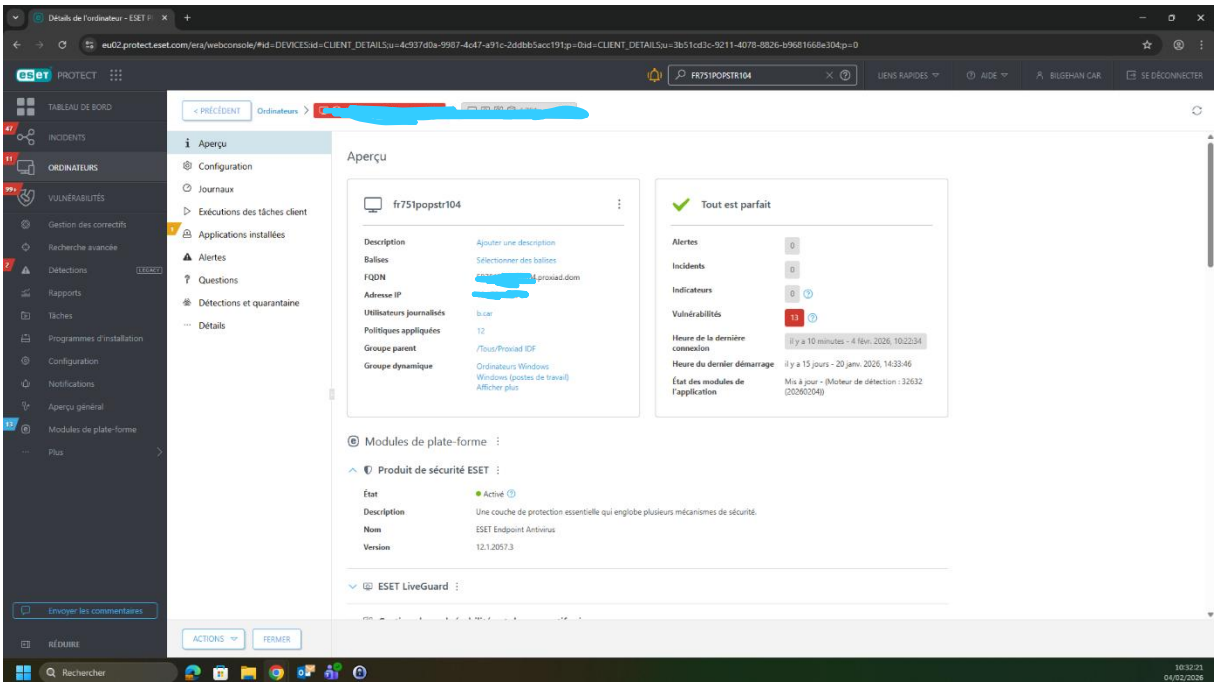


Tableau de bord
Aperçu général
Incidents
ESET LiveGuard
Gestion des vulnérabilités et des correctifs ESET
ESET Cloud Office Security
Détections
ESET MDR
Ordinateurs
Détections antivirus
Détections du pare-feu
État de l'ordinateur
Erreur
11 Ordinateurs affectés
Avertissement
38 Ordinateurs affectés
État de l'incident
Gravité élevée
14
Gravité moyenne
33
Principaux problèmes fonctionnels
Incidents actifs ayant le plus d'impact
Principales applications vulnérables
Nom de l'application
Ordinateurs affectés
Nombre total de vulnérabilités
Impact global
Microsoft Windows 11 Professionnel 82 7272 25%
Mozilla Firefox 68 4794 17%
Microsoft Windows 10 Professionnel 4 2747 10%
Google Chrome 35 1974 7%
Microsoft Office C2R 19 1225 4%
État de la connexion de l'ordinateur
État de la gestion des ordinateurs
Modules de plate-forme
État de la version
Support News
ESET Security for Microsoft SharePoint Server version 12.1 has been released
17 décembre 2025
EN SAVOIR PLUS


Aperçu
fr751popstr104
Tout est parfait
Description
Balises
FQDN
Adresse IP
Utilisateurs journalisés
Politiques appliquées
Groupe parent
Groupe dynamique
Alertes
Incidents
Indicateurs
Vulnérabilités
Heure de la dernière connexion
Heure du dernier démarrage
État des modules de l'application
Modules de plate-forme
Produit de sécurité ESET
ESET LiveGuard
ACTIONS
FERMER

3 Travail accompli

3.1 Présentation approfondie des tâches effectuées

Dans le cadre du projet de déploiement EDR, j'ai pris en charge la mise en conformité logicielle et sécuritaire du parc. Cette mission a nécessité une organisation rigoureuse pour traiter chaque poste individuellement tout en assurant un suivi précis de l'avancement.

A. Pilotage via l'inventaire dynamique

Pour organiser mes interventions, je me suis appuyé sur une liste détaillée au format Excel regroupant les informations critiques de chaque poste :

- **Identification :** Nom de l'ordinateur, numéro de série (S/N) et collaborateur associé.
- **Suivi de l'état :** Utilisation de colonnes de statut ("À faire" / "Fait") pour piloter le déploiement en temps réel.
- **Audit logiciel :** Vérification de la présence et de la conformité de l'agent **ESET**, de l'agent **SentinelOne** et du chiffrement **BitLocker**.

B. Interventions à distance et remédiation

Une fois les besoins identifiés dans le fichier de suivi, j'ai contacté les collaborateurs pour planifier une prise en main à distance. L'utilisation de **TeamViewer** a été indispensable pour agir sur les postes sans immobiliser physiquement les utilisateurs :

- **Segmentation par performance :** J'ai installé l'EDR **SentinelOne** sur les machines disposant de 16 Go de RAM minimum, tandis que les autres postes ont reçu la dernière mise à jour de l'antivirus **ESET**.
- **Sécurisation des données :** J'ai systématiquement vérifié l'activation de **BitLocker** et forcé la remontée des clés de récupération dans l'**Active Directory** pour prévenir tout risque de perte d'accès.

C. Résultat et reporting

Chaque intervention se concluait par la mise à jour du fichier Excel, permettant à la DSI d'avoir une vision claire et immédiate de la couverture sécuritaire du parc. Cette méthode a permis de réduire considérablement les vulnérabilités logicielles tout en garantissant une homogénéité des solutions de protection.

3.2 Description des problèmes rencontrés et démarches de résolution

Tout au long du projet, j'ai été confronté à divers obstacles techniques et organisationnels. Voici les principaux défis et les solutions mises en œuvre pour les surmonter :

1. Indisponibilité ou mobilité des collaborateurs

- **Problème :** De nombreux collaborateurs étaient en déplacement ou en réunion, rendant la planification des interventions difficile sur une période courte de 5 semaines.
- **Résolution :** J'ai utilisé le fichier de suivi pour marquer les priorités et j'ai instauré une communication proactive via messagerie interne. L'utilisation de **TeamViewer** a permis d'intervenir dès qu'une fenêtre de disponibilité se présentait, sans contrainte géographique.

2. Conflits logiciels lors de l'installation des agents de sécurité

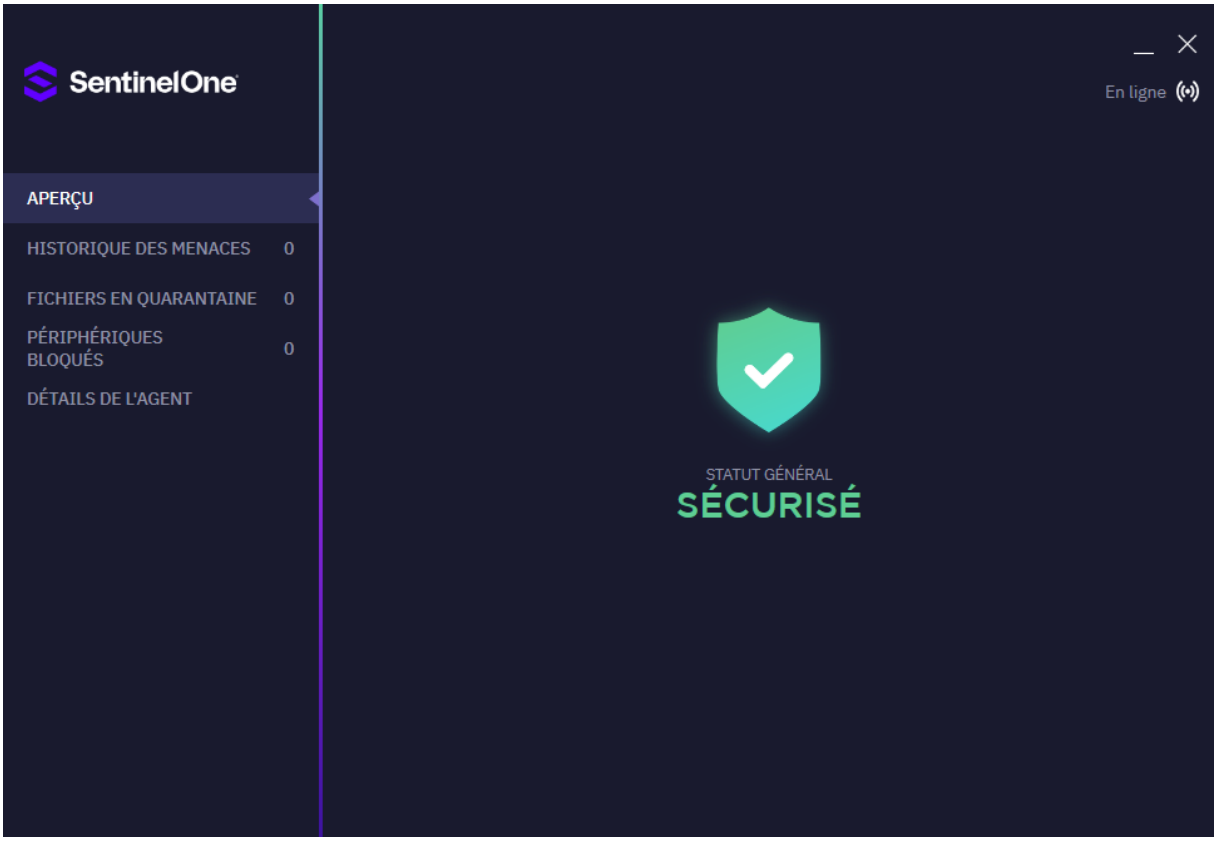
- Problème : Sur certains postes, d'anciennes solutions antivirus ou des versions obsolètes d'ESET empêchaient l'installation propre de SentinelOne.
- Résolution : J'ai dû effectuer un nettoyage manuel des registres et utiliser des outils de désinstallation spécifiques (Uninstaller) avant de procéder au déploiement de la nouvelle solution.

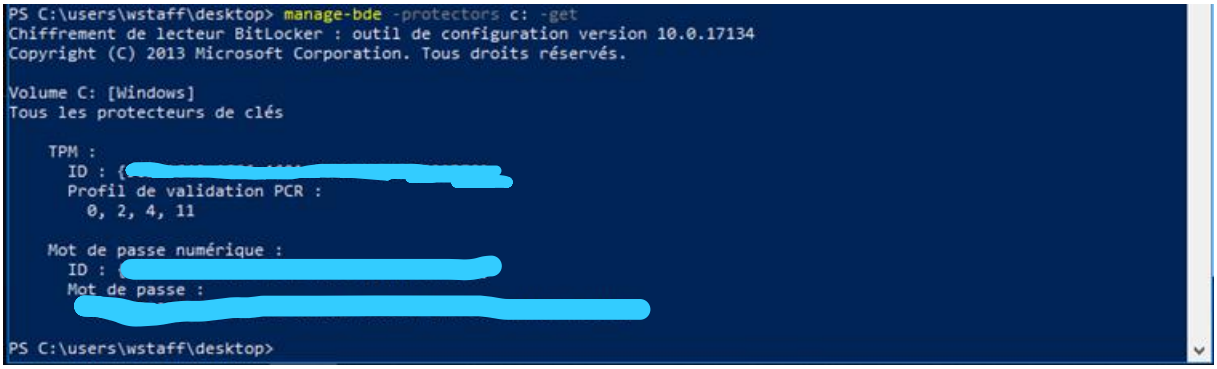
3. Clés BitLocker manquantes dans l'Active Directory

- **Problème :** Bien que le chiffrement soit actif sur certains postes, la clé de récupération ne remontait pas automatiquement dans l'AD, créant un risque de perte de données.
- **Résolution :** J'ai exécuté des commandes PowerShell (manage-bde -protectors c: -adbackup -id {ID du TPM}) pour forcer manuellement la sauvegarde de la clé dans l'Active Directory et j'ai vérifié la validation du statut dans la console d'administration.

4 Annexes

4.1 Annexe 1





5 Conclusion

5.1 Bilan du travail accompli pour l'entreprise

Le stage a permis à l'entreprise de bénéficier d'une contribution majeure dans le cadre d'un projet de sécurisation et d'optimisation du parc informatique. Au cours d'une période de cinq semaines, plusieurs travaux techniques ont été accomplis, ce qui a contribué à l'amélioration de la sécurité, de la fiabilité et de la gestion du système d'information.

L'une des premières contributions a été la remise en conformité de la baie de brassage de la salle serveur. Cette intervention a permis une nette amélioration de l'infrastructure réseau et de la maintenance. Les risques d'erreurs humaines lors des manipulations ont été réduits grâce à un branchement méthodique, un étiquetage normalisé des câbles et une documentation détaillée du plan de câblage.

La deuxième contribution majeure a été la mise en conformité sécuritaire de l'ensemble du parc informatique via le déploiement de l'EDR SentinelOne et la mise à jour des solutions ESET. Cela a permis à l'entreprise :

- D'homogénéiser la protection de ses postes de travail en fonction de leurs performances matérielles (RAM).
- De sécuriser les données critiques en généralisant le chiffrement BitLocker et en assurant la remontée systématique des clés de récupération dans l'Active Directory.
- D'identifier et de corriger les vulnérabilités logicielles grâce à une gestion rigoureuse des interventions à distance via TeamViewer.

Tous les travaux ont été achevés dans les délais, respectant la qualité de travail demandée et le cahier des charges. Le stage a ainsi permis à la DSI :

- D'économiser du temps sur un projet de cybersécurité prioritaire.
- D'optimiser la visibilité sur son parc grâce à la création d'un inventaire dynamique et précis.
- De bénéficier d'un parc informatique à jour et protégé contre les menaces modernes.

5.2 Bilan de mon expérience

Ce stage de **cinq semaines** m’a permis d’appréhender le métier d’administrateur systèmes et réseaux dans un environnement professionnel exigeant. J’ai eu l’opportunité de piloter un projet majeur de **déploiement EDR (SentinelOne)** et de mise en conformité globale du parc informatique. Cette mission a été déterminante pour le renforcement de mes compétences techniques, mon autonomie ainsi que mon sens de l’organisation.

Cette période m’a également appris à gérer mon temps de manière efficace et à hiérarchiser les tâches en fonction des impératifs techniques et des disponibilités des utilisateurs. Ma mission principale a consisté à sécuriser les postes de travail via le déploiement de **SentinelOne**, la mise à jour des solutions **ESET** et la vérification du chiffrement **BitLocker**. Pour ce faire, j'ai dû assurer un support de proximité et une gestion rigoureuse des interventions à distance.

Je voudrais remercier particulièrement M. David CHOUR, mon tuteur de stage, pour sa disponibilité, ses conseils et la bienveillance qu’il m’a manifesté tout au long de mon parcours.

Cela me donne également l'occasion d'exprimer mes sincères remerciements à :

- M. Philippe RENOUF, le Directeur des Systèmes d'Information.
- M. Tony HANNON, le Référent Technique.
- M. Aviel CHEMLA, le Technicien Support Informatique.

Pour leur accueil chaleureux, leurs conseils et m’avoir fait confiance en m’accueillant dans leur équipe. Leurs idées m'ont offert des connaissances et des approches inestimables qui seront cruciales dans mes futures entreprises.

De plus, j'ai appris des choses très importantes durant ce stage qui m'aideront dans ma carrière professionnelle. Cela a été utile sur le plan personnel et professionnel et m'aidera à mettre en valeur mes compétences auprès d'autres entreprises et à renforcer ma position dans le domaine des systèmes et des réseaux.