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

GESTION ET ADMINISTRATION DE L'ACTIVE DIRECTORY

Maël LESAICHERRE

HelloWork

Responsable entreprise : Guénolé CARVAL

Responsable académique : Corinne HOUSSAIN

Table des matières

1 Introduction

Mon stage s'est déroulé au sein de l'entreprise HelloWork dans le service réseau. Le sujet de mon stage portait sur l'administration et l'optimisation de l'Active Directory local, le service d'annuaire utilisé pour la gestion des ressources et des identités au sein de l'entreprise.

L'objectif principal de mon stage était d'améliorer l'efficacité et la sécurité de l'Active Directory de l'entreprise. Mes missions comprenaient la configuration des stratégies de groupe, la gestion des utilisateurs et des groupes, ainsi que la mise en place de bonnes pratiques de sécurité.

Le plan de ce rapport sera structuré en plusieurs parties. Tout d'abord, je présenterai l'entreprise Hellowork et son infrastructure informatique. Je détaillerai ensuite les objectifs de mon stage et les missions qui m'ont été confiées. Par la suite, je décrirai en détail les actions que j'ai entrepris pour améliorer l'administration et la sécurité et la sécurité de l'Active Directory, tout en mettant en avant mon soutien aux différents membres de l'équipe dans leurs tâches quotidiennes. Enfin, je conclurai ce rapport en mettant en évidence les résultats obtenus et les enseignements que j'ai tiré de cette expérience enrichissante.

2 HelloWork

2.1 Son Histoire

L'entreprise HelloWork, anciennement connue sous le nom RegionsJob, a une longue histoire dans le secteur numérique dédié à l'emploi, au recrutement et à la formation en France. Fondée en 2000 à Rennes, elle a commencé son parcours sous le nom d'Ouest Job, en tant que première plateforme d'emploi de la région.

Au fil des années, l'entreprise a étendu son rayonnement à l'échelle nationale. En 2005, elle a évolué pour devenir RegionsJob, fusionnant avec une autre marque importante dans le domaine de l'emploi en ligne. Ce changement de nom a marqué une étape importante dans l'expansion de l'entreprise, lui permettant de couvrir l'ensemble du territoire français.

Depuis lors, HelloWork a continué à se développer et à se diversifier. Elle a intégré des marques renommées telles que MaFormation.fr et Diplomeo.com, élargissant ainsi ses services pour inclure la formation professionnelle. Aujourd'hui, l'entreprise propose une vaste gamme de solutions dans le domaine des ressources humaines pour les recruteurs et les candidats, ainsi que des services de médias spécialisés pour les professionnels du web et les ressources humaines.

Avec son siège social basé à Rennes en Bretagne et un effectif de plus de 420 employés, HelloWork est devenue une référence dans le domaine de l'emploi en ligne en France, attirant des millions de visiteurs sur ses différentes plateforme chaque mois. Son parcours remarquable témoigne de son engagement constant à être un acteur incontournable du marché de l'emploi en ligne en France.

Figure 1 : La Mabilais, l'immeuble où se situe le siège social de l'entreprise HelloWork, à Rennes.

2.2 Son Infrastructure Informatique

Au sein de l'entreprise HelloWork, l'environnement de travail se caractérise par une forte orientation technologique et une infrastructure informatique bien développée. L'équipe responsable des activités réseau était composée de neuf membres (dont moi), répartis en trois groupes distincts, chacun ayant des responsabilités spécifiques.

Le premier groupe est constitué de deux administrateurs systèmes et réseaux, chargés de gérer et de maintenir l'infrastructure réseau de l'entreprise. Leur objectif principal est de garantir le bon fonctionnement des serveurs, des équipements réseau et des services associés.

Le deuxième groupe est dédié au support technique, fournissant une assistance informatique aux employés de l'entreprise. Leur rôle est d'assurer la résolution des problèmes techniques, l'installation et la configuration des logiciels, ainsi que le bon fonctionnement des périphériques.

Le troisième groupe (dans lequel je faisais partie) est spécifiquement axé sur la cybersécurité. Sa mission principale est de protéger les systèmes et les données de l'entreprise contre les menaces potentielles. Ils mettent en place des mesures de sécurité, réalisent des audits réguliers et veillent à l'application des politiques de sécurité.

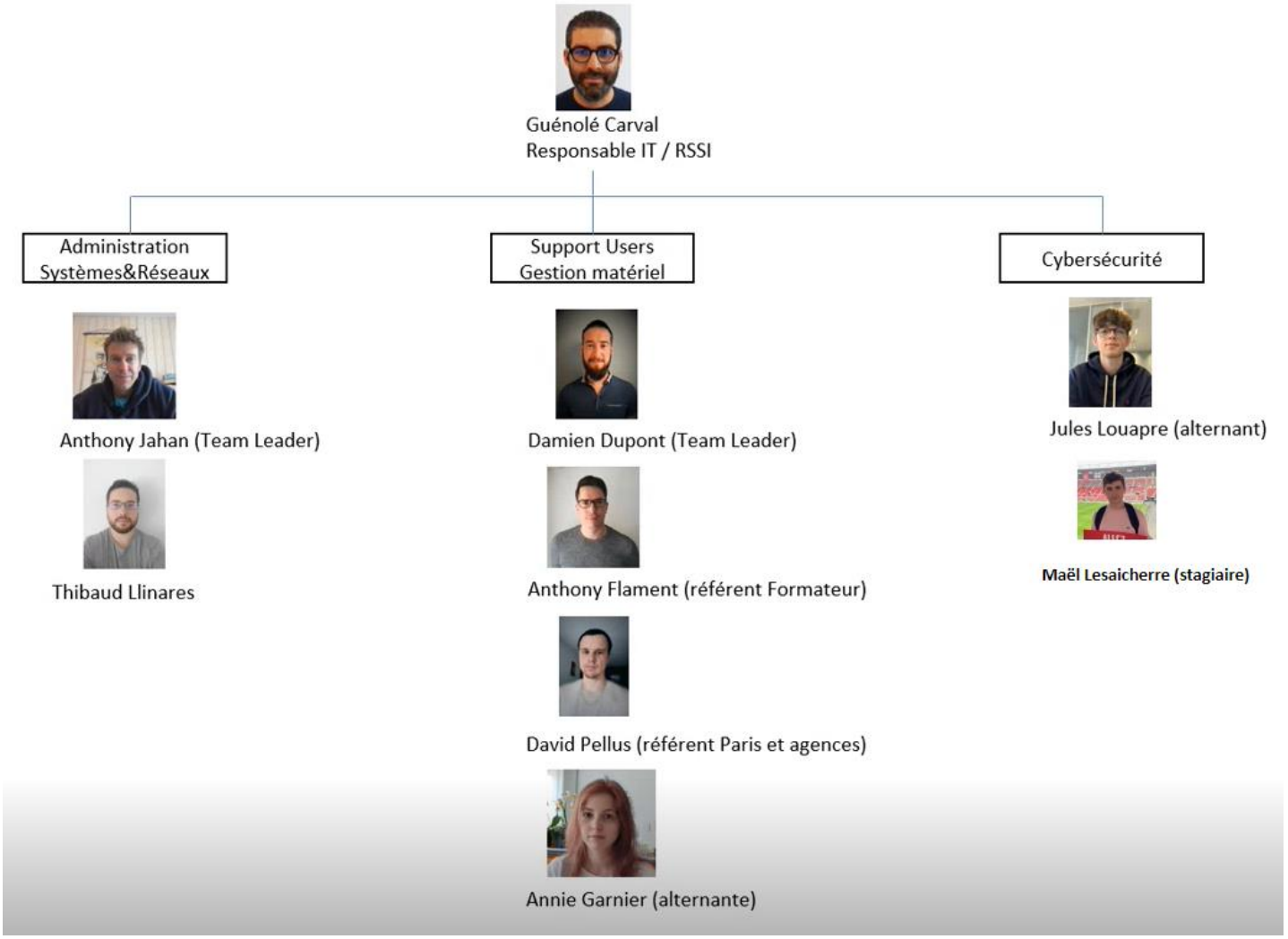

Figure 2 : organigramme de l'équipe réseau

Malgré la répartition des membres de l'équipe réseau dans des groupes distincts avec des responsabilités spécifiques, il est courant que chaque membre effectue des tâches qui ne relèvent pas exclusivement de son groupe d'origine. Par exemple, un membre de l'équipe spécialisée en cybersécurité peut être amené à traiter des tickets de support technique en plus de ses responsabilités

habituelles. Cette flexibilité et cette polyvalence témoignent de l'esprit d'équipe et de la collaboration au sein de l'équipe, où chacun est prêt à apporter son soutien dans les domaines où il est nécessaire, contribuant ainsi à l'efficacité globale de nos opérations.

Depuis la mise en place du confinement, l'entreprise a adapté son infrastructure pour permettre à tous les employés de travailler à distance. Chaque membre de l'entreprise dispose d'un ordinateur portable, ce qui favorise la mobilité et assure la continuité des activités, même en dehors du bureau.

Dans le cadre de ses activités, HelloWork utilise principalement Azure Active Directory (Azure AD) en tant que service d'annuaire centralisé pour la gestion des identités et des ressources au sein de l'entreprise. Parallèlement, elle maintient également un Active Directory local pour répondre aux besoins spécifiques de certaines applications ou systèmes.

Grâce à l'utilisation de ces outils informatiques, l'équipe réseau parvient à accomplir ses missions avec efficacité et professionnalisme. Elle tire parti de différentes solutions pour assurer la gestion du réseau, la sécurité des systèmes et la collaboration entre les membres. Par exemple l'entreprise fait appel à Sentinel One, une solution de sécurité avancée, afin de protéger les ressources de l'entreprise et de prévenir les risques.

De plus, pour garantir la sécurité et la gestion des appareils, l'équipe utilise des outils spécifiques adaptés aux différentes plateformes. Ainsi, pour les ordinateurs Mac, HelloWork utilise Jamf, une plateforme de gestion des appareils Apple, qui facilite le déploiement, la configuration et la protection des Macs au sein de l'entreprise. Pour les appareils Windows, l'équipe s'appuie sur Intune, une solution de gestion des appareils Microsoft, permettant un contrôle efficace des paramètres et des politiques de sécurité.

En ce qui concerne la communication, l'entreprise HelloWork utilise Aircall, une solution de téléphonie cloud, qui facilite les échanges avec les collaborateurs et les partenaires de l'entreprise.

Enfin, pour renforcer la protection contre les attaques par email, l'équipe utilise Vade Secure, un outil de filtrage des courriers électroniques malveillants, garantissant ainsi la sécurité des communications électroniques.

L'ensemble de ces outils contribue à optimiser les performances de l'équipe, à résoudre rapidement les problèmes et à garantir la sécurité des données de l'entreprises, assurant ainsi un environnement de travail fiable et sécurisé.

Au sein de l'entreprise HelloWork, la présence s'étend sur plusieurs sites à travers la France. Bien que l'entreprise possède une dizaine de sites répartis dans différentes régions, son siège principal est basé à Rennes. Cependant, deux autres sites importants se trouvent à Paris et à Bordeaux.

Cette répartition géographique représente un défi logistique pour l'équipe réseau chargé de la gestion et de la maintenance de l'infrastructure informatique. En effet, pour assurer un support efficace et une assistance technique à tous les sites, l'équipe réseau doit intervenir à distance ou se déplacer physiquement vers les différents sites.

Les déplacements sont souvent nécessaires pour les interventions qui demande une présence physique. Dans ce cas, les membres de l'équipe réseau se déplacent en utilisant des moyens de transport tels que le train pour rejoindre les sites distants. Cette approche permet une résolution rapide des problèmes et une assistance directe aux utilisateurs sur place.

Cependant, pour les tâches pouvant être effectuées à distance, l'équipe réseau utilise des outils de gestion à distance tels que TeamViewer. Ces logiciels leur permettent de prendre le contrôle des

ordinateurs à distance et de résoudre les problèmes à distance, ce qui évite des déplacements inutiles et optimise le temps et les ressources.

Par ailleurs, l'entreprise utilise également la suite Office 365, qui comprend des outils de communication et de collaboration tels que Outlook, SharePoint et Teams. Cette suite logicielle permet à l'équipe réseau de communiquer efficacement entre les différents sites, de partager des documents et des informations importantes, et de collaborer de manière transparente, facilitant ainsi la coordination et la résolution des problèmes.

Ainsi malgré la répartition géographique des sites, l'équipe réseau de HelloWork parvient à maintenir une communication fluide, à assurer un support technique adéquat et à intervenir efficacement grâce à l'utilisation d'outils de gestion à distance et de la suite Office 365. Cette approche permet de garantir la continuité des opérations et d'optimiser les performances de l'infrastructure de l'entreprise.

3 Ma mission principale

3.1 Introduction à l'Active Directory local

Au sein de l'infrastructure informatique, Hellowork utilise un Active Directory local qui joue un rôle crucial dans la gestion de nos services réseau. Cependant, contrairement à un déploiement complet de l'Active Directory, son utilisation se concentre principalement sur des fonctionnalités spécifiques telles que le DNS, le DHCP et certains serveurs.

L'active directory local est utilisé en tant que service d'annuaire pour faciliter la résolution des noms de domaine au sein du réseau. Le DNS (Domain Name System) permet de traduire les noms d'hôtes en adresses IP (Internet Protocol), ce qui est essentiel pour la communication entre les différents équipements de l'infrastructure. Grâce à l'AD local, il est possible de gérer de manière centralisée les enregistrements DNS et assurer une résolution rapide et précise des noms de domaine.

De plus, l'Active Directory local joue un rôle crucial dans la gestion des adresses IP au sein du réseau grâce au DHCP (Dynamic Host Configuration Protocol). Le DHCP permet d'attribuer dynamiquement les adresses IP aux dispositifs connectés au réseau, ce qui facilite la configuration et la gestion des équipements. L'AD local offre un contrôle centralisé sur les plages d'adresses IP, les options de configuration et les réservations, garantissant ainsi une gestion efficace du DHCP.

En outre, l'Active directory local héberge également certains serveurs essentiels à l'infrastructure. Ces serveurs peuvent inclure des services tels que la gestion des impressions, le stockage de fichiers ou d'autres applications spécifiques à l'entreprise. L'utilisation de l'AD local pour ces serveurs permet de centraliser la gestion des autorisations d'accès, de simplifier l'administration et de renforcer la sécurité de ces services.

En somme, L'Active Directory local occupe une place cruciale dans notre infrastructure en tant que support pour le DNS, le DHCP et certains serveurs clés. Cette utilisation spécifique permet de bénéficier des avantages de l'AD local tout en répondant précisément à nos besoins en matière de gestion des services réseau.

3.2 Présentation de l'outils PingCastle

PingCastle est un outil open-source spécialement conçu pour analyser la sécurité des infrastructures Active Directory. Il permet de réaliser des évaluations automatisées de l'AD et d'identifier les faiblesses susceptibles de compromettre la sécurité du système. L'outil offre une approche basée sur la gestion des risques en fournissant des indicateurs et des rapports clairs sur l'état de sécurité de l'AD.

L'une des fonctionnalités clés de PingCastle est son module d'audit. Celui-ci permet de scanner l'infrastructure Active Directory à la recherche de vulnérabilités et de configurations non sécurisés. Il analyse les différentes composantes de l'AD, telles que les contrôleurs de domaine, les relations de confiance, les stratégies de groupe, les comptes utilisateurs, les mots de passe, etc. Grâce à cette analyse approfondie, PingCastle peut détecter les erreurs de configuration, les comptes inutilisés, les permissions excessives, les mots de passe faibles et d'autres points faibles qui pourraient être exploités par des attaquants.

PingCastle fournit également des rapports détaillés sur les résultats de l'audit, qui permettent aux administrateurs de comprendre clairement les problèmes de sécurité identifiés et de prendre les mesures nécessaires pour les résoudre. Les rapports sont présentés de manière accessible, avec des explications compréhensibles et des recommandations pratiques pour améliorer la sécurité de l'AD.

En plus de l'audit, de sécurité, PingCastle propose d'autres fonctionnalités telles que la détection des comptes privilégiés, l'évaluation de l'hygiène de l'AD, la vérification des configurations de sécurité, et bien plus encore. Ces fonctionnalités fournissent une vue d'ensemble complète de l'état de sécurité de l'AD et aident les administrateurs à mettre en place des mesures correctives appropriées.

Lorsque PingCastle est exécuté, l'utilisateur est accueilli par un menu d'options permettant de choisir le type d'analyse que l'utilisateur souhaite effectuer sur son domaine Active Directory local. Au total sept choix sont proposés, chacun ayant un objectif spécifique.

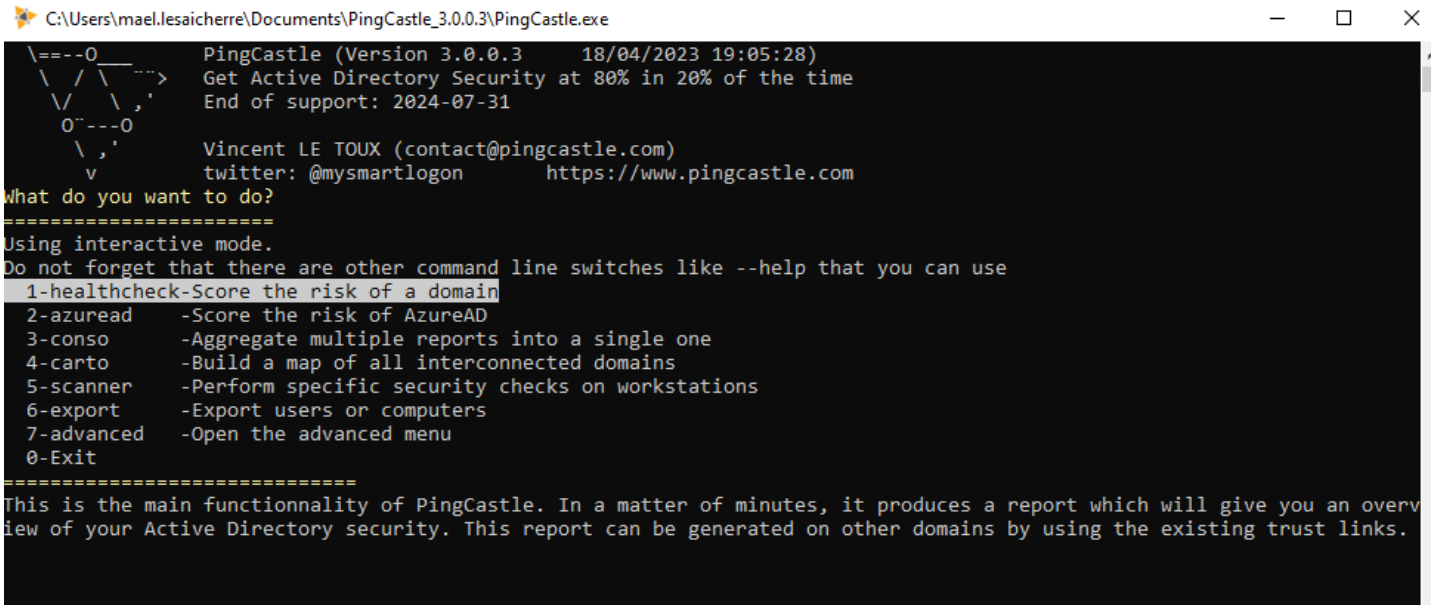

Figure 3 : Le menu d'option de PingCastle

Afin d'établir une analyse approfondie du domaine, l'option "1-healthcheck-Score the risk of a domain" est la plus intéressante. PingCastle effectue une série de test automatisés qui portent sur différents aspects de la sécurité de l'AD.

PingCastle utilise des algorithmes sophistiqués pour évaluer les risques associés à chaque aspect analysé. Il attribue des scores aux différentes vulnérabilités détectées, en fonction de leur gravité et de leur impact potentiel sur la sécurité de l'infrastructure.

Une fois l'analyse terminée PingCastle génère un rapport détaillé qui récapitule les résultats obtenus. Ce rapport fournit une vue d'ensemble claire des risques identifiés, en les classant par ordre de priorité. Chaque vulnérabilité est accompagnée d'une explication détaillée, permettant aux administrateurs de comprendre les problèmes rencontrés.

3.3 Méthodologie d'analyse des vulnérabilités

Dans le cadre de l'analyse des vulnérabilités de l'Active Directory local, j'ai suivi une méthodologie précise pour identifier les risques potentiels.

J'ai utilisé VMware, un logiciel de virtualisation, pour créer un environnement isolé sur mon ordinateur. J'ai configuré une machine virtuelles Windows 10 que j'ai relié au domaine

“regionsjob.dom”, le domaine sur lequel j’ai effectué mes analyses. Cette approche m’a permis de réaliser les tests en toute sécurité, sans impacter l’environnement de production.

J’ai téléchargé PingCastle sur cette machine virtuelle. Après l’installation, j’ai procédé à la configuration de l’outil en spécifiant les paramètres nécessaires pour analyser l’Active Directory local. Puis, j’ai lancé une première analyse.

Une fois l’analyse terminée, PingCastle a généré un rapport complet contenant les résultats détaillés de l’audit. Ce rapport est fourni sous la forme d’une page HTML (Hypertexte Markup Language) interactive.

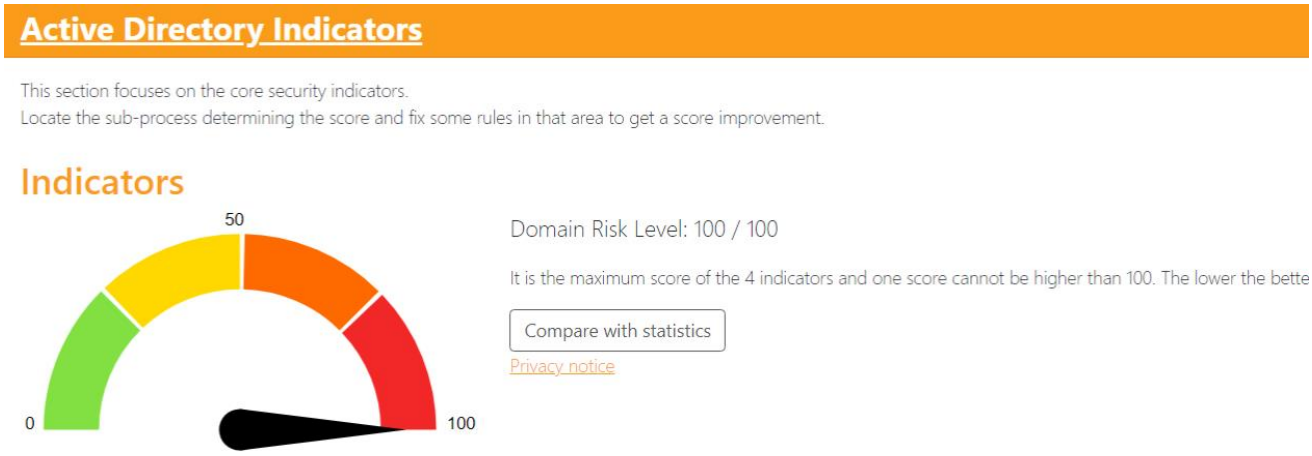

Figure 4 : Note de sécurité attribué par PingCastle à la suite de la première analyse

Il est apparu que l’Active Directory local présentait un nombre significatif de vulnérabilités. En examinant les résultats, nous avons constatés que notre note de sécurité était au niveau maximal, révélant ainsi l’importance des mesures correctives nécessaires.

Figure 5 : Vue d’ensemble des vulnérabilités : Évaluation des 4 groupes et identification des 35 vulnérabilités

La note de sécurité attribué par PingCastle repose sur l’évaluation de quatre groupes de vulnérabilités clés. Après avoir effectué l’analyse, j’ai pu recenser l’intégralité des vulnérabilités détectées et les ai répertoriées dans un document Word. J’ai classé ces vulnérabilités par ordre de priorité, en y incluant des consignes permettant de résoudre chaque problème identifié. Dans certains cas, j’ai fourni des commandes PowerShell spécifiques, tandis que dans d’autres cas, j’ai inclus des liens vers les recommandations de l’ANSSI pour une résolution adéquate.

Sur la page HTML, on trouve également un tableau de notation des vulnérabilités selon le modèle de risques. Ce tableau met en évidence chaque groupe de vulnérabilités en l’associant à une liste spécifique, et chaque élément de cette liste est représenté par une couleur. Cette approche permet une identification rapide et efficace des différents niveaux de risque. En un coup d’oeil, il est possible de repérer les vulnérabilités spécifiques associées à chaque groupe, grâce à leur code couleur correspondant. Cette méthode visuelle facilite la compréhension et l’analyse des risques, en permettant une évaluation précise et ciblée des vulnérabilités de l’Active directory local.

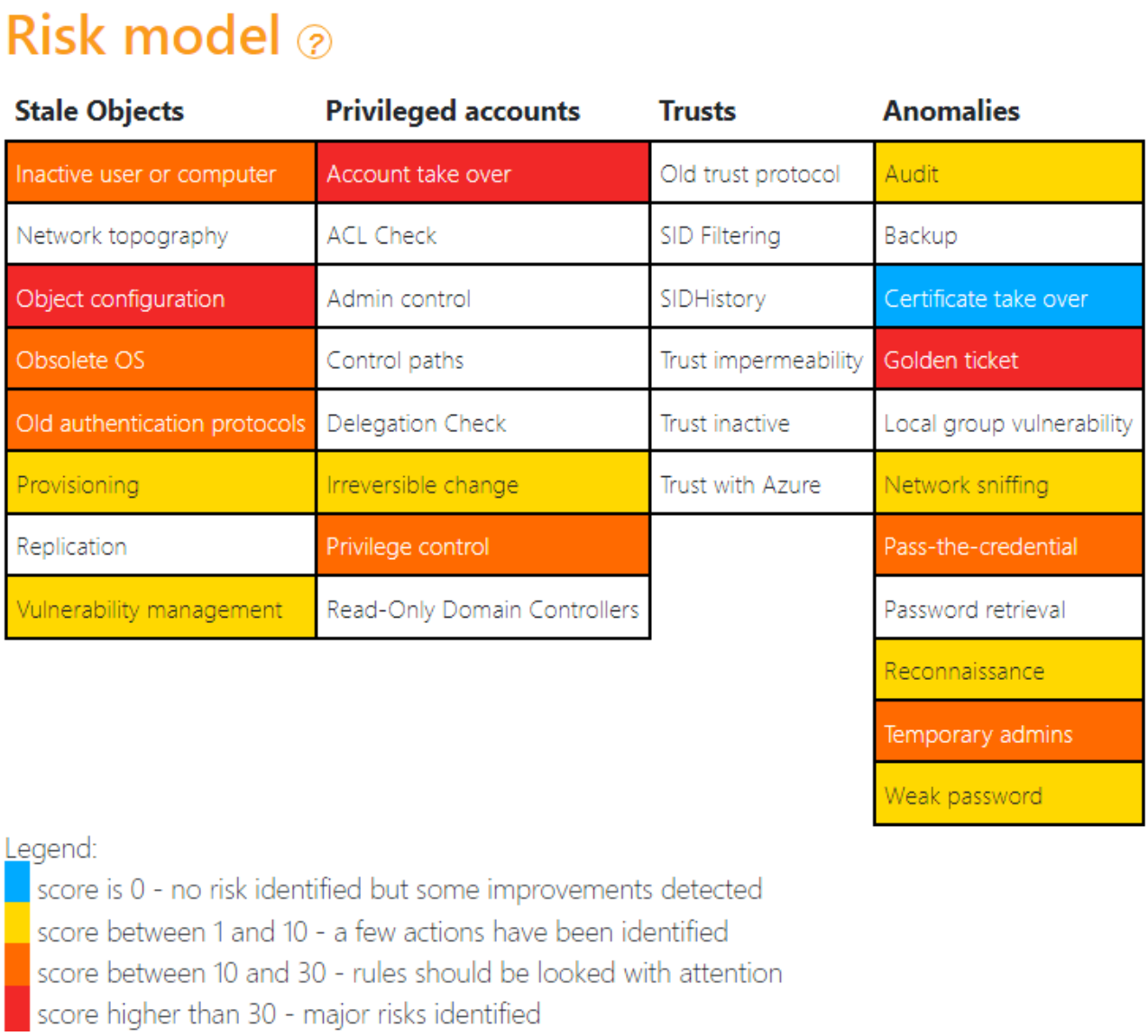

Figure 6 : Tableau d'identification et de notation des vulnérabilités selon le modèle de risques

3.4 Actions de remédiation des vulnérabilités

Pour remédier aux vulnérabilités détectées dans l'Active Directory local, j'ai mis en place plusieurs mesures spécifiques en utilisant la fonctionnalité de Bureau à distance pour effectuer ces manipulations. Voici en détail les actions que j'ai entrepris :

Tout d'abord j'ai revu les autorisations accordées aux comptes non-administrateurs et j'ai restreint leurs privilèges, en révoquant certains droits d'accès.

J'ai renforcé la sécurité des mots de passe en modifiant la politique de mot de passe pour exiger une longueur minimale de 8 caractères, conformément aux recommandations de l'ANSSI qui préconise une taille de 20 caractères pour une meilleure sécurité.

J'ai procédé à la suppression des utilisateurs du groupe "Pre-Windows 2000" et du groupe administrateur "schema", afin de limiter l'accès aux ressources sensibles et de garantir une gestion plus rigoureuse des droits.

J'ai effectué une réorganisation des groupes d'administrateurs en les rendant plus sécurisés. J'ai créé des groupes dédiés et j'ai assigné les administrateurs uniquement à ces groupes, en évitant les droits administratifs directs pour réduire les risques de compromission des comptes.

J’ai procédé au changement du mode d’encryptions des mots de passe de plusieurs dizaines d’utilisateurs, en utilisant des algorithmes plus robustes pour garantir une meilleure protection

J’ai apporté des modifications au mode d’authentification utilisé sur le réseau local. Auparavant, le réseau utilisait une version obsolète de NTLM qui présentait des vulnérabilités. J’ai mis à jour le mode d’authentification, passant donc de NTLMv1 à NTLMv2 et j'ai également ajouté une règle qui refuse les réponses LM et NTLMv1. Cette mise à jour permet de limiter la quantité d’informations sensibles transmises lors de l’authentification, renforçant ainsi la sécurité du réseau local.

J’ai revu les droits d’accès accordés aux utilisateurs ne nécessitant pas de privilèges d’administration et j’ai révoqué certains accès inutiles, limitant ainsi les risques potentiels liés à des autorisations excessives.

Pour mener à bien les actions de remédiations, j’ai utilisé la fonctionnalité de Bureau à distance, qui m’a donné accès à distance à l’ensemble des répertoires contenant les règles de groupe, ainsi qu’aux informations sur les utilisateurs et les groupes présents sur l’Active Directory local. Cette connexion à distance m’a permis de travailler efficacement tout en ayant une vue complète et détaillée de l’infrastructure.

3.5 Suivi et évaluation des actions de remédiation

J’ai adopté une approche proactive pour mesurer l’efficacité des mesures mises en place afin d’améliorer la sécurité de l’Active Directory local. Après chaque modification apportée à l’AD local, j’ai effectué des analyses supplémentaires à l’aide de PingCastle pour évaluer l’impact des changements et vérifier la réduction des vulnérabilités.

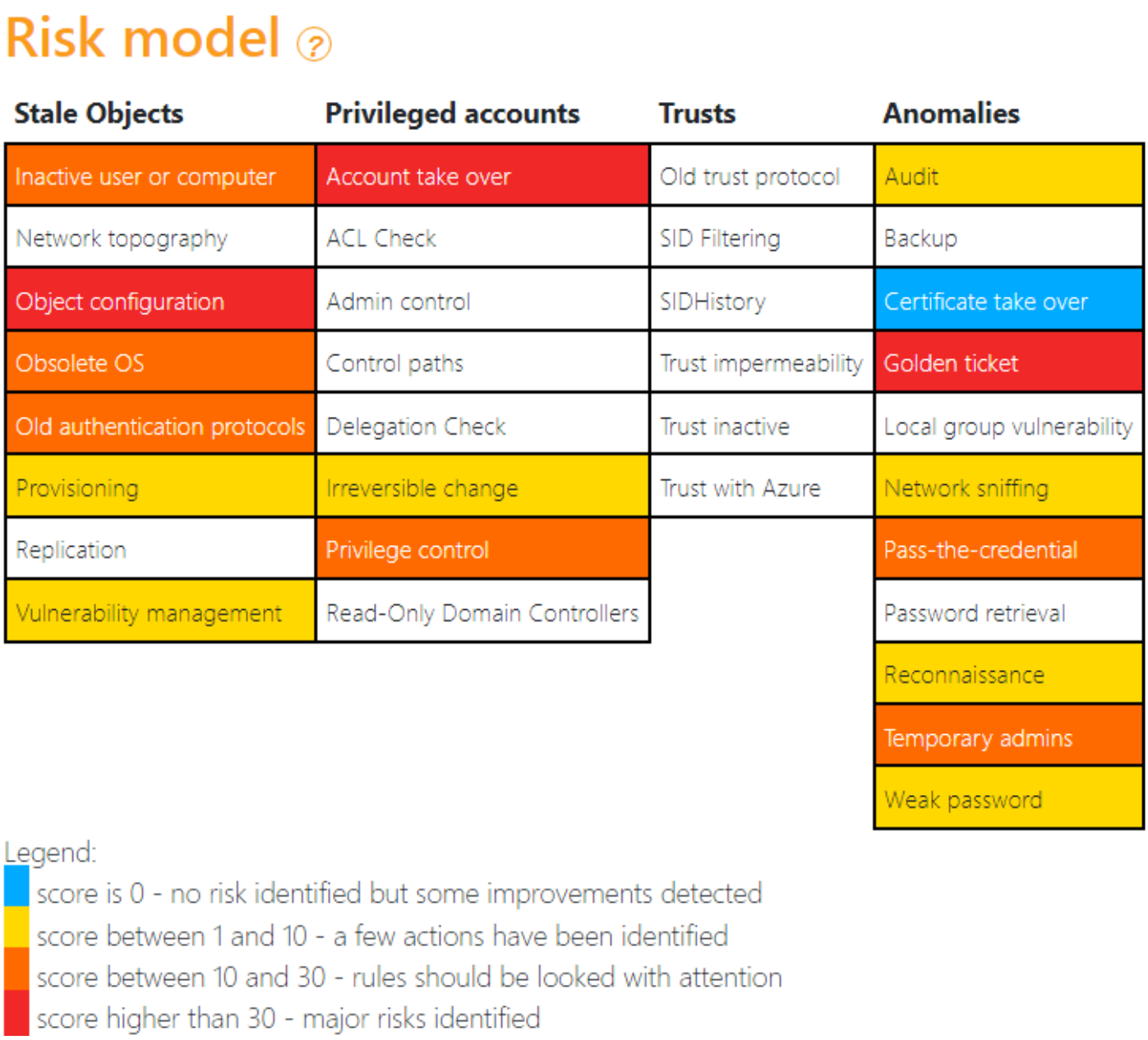

Figure 7 : Tableau d'identification et de notation des vulnérabilités après la première analyse

Les résultats obtenus ont été très encourageants, avec une quasi-totalité des vulnérabilités initialement identifiées qui ont été supprimées. Les actions de remédiation, telles que la configuration des stratégies de groupe, la gestion des mots de passe et la restriction des privilèges, ont contribué de manière significative à renforcer la sécurité de l'AD local

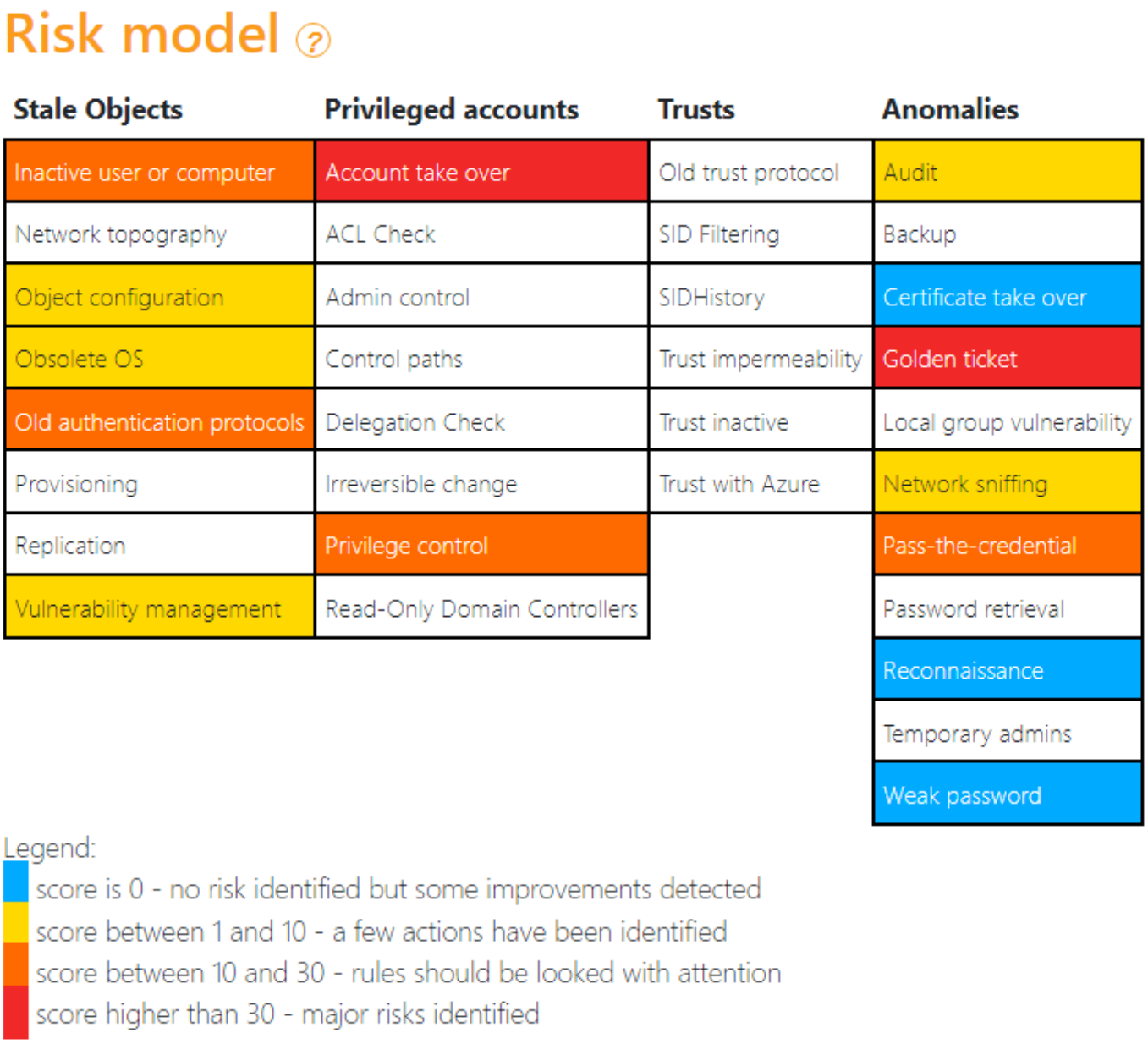

Figure 8 : Tableau d'identification et de notation des vulnérabilités après la dernière analyse

Il convient de noter que certaines vulnérabilités ont été identifiées, notamment la nécessité de modifier les mots de passes des comptes administratifs inchangés depuis plusieurs années, et de renforcer la sécurité des comptes administratifs des prestataires externes chargés de tests réguliers sur les sauvegardes de l'AD. Cependant, il est important de souligner que ces tâches ne relèvent pas de ma responsabilité directe.

Dans le cadre de mon travail, j'ai pu identifier ces vulnérabilités et les rapporter à l'équipe ou aux personnes concernées. Il leur incombe de prendre les mesures nécessaires pour résoudre ces problèmes spécifiques.

Il est important de souligner que la sécurisation de l'Active Directory est un processus continu, et qu'une surveillance constante est nécessaire pour s'assurer que de nouvelles vulnérabilités ne surgissent pas et que les mesures de sécurité restent adéquates. Cependant, grâce aux actions de remédiation entreprises et à leur suivi attentif, l'AD local a connu une nette amélioration de sa posture de sécurité.

4 Autres Missions et Contributions

4.1 Soutien à l'équipe support

Pour assister l'équipe de support, j'ai entrepris différentes actions visant à résoudre les problèmes informatiques et à fournir une assistance efficace aux utilisateurs. Voici quelques exemples concrets des tâches que j'ai accomplies.

J'ai pris en charge des tickets signalés par des utilisateurs, que ce soit par le biais du système de ticketing interne ou par des communications directes. La grande partie des tickets que j'ai traité concernait des problèmes informatiques courants, telles que le remplacement de casques et de souris cassés, mais aussi des problèmes de mots de passe oubliés, des difficultés liées à des mises à jour logicielles, et bien d'autres encore.

ID	TITRE	STATUT	DERNIÈRE MODIFICATION	DATE D'OUVERTURE
18 081	Message changement de nom machine sur le réseau	Nouveau	20-06-2023 14:40	20-06-2023 14:40
18 059	2FA pour le login sur nos postes	En cours (Attribué)	20-06-2023 14:33	19-06-2023 10:15
18 079	Mute off mute on casque dell 100	Nouveau	20-06-2023 11:10	20-06-2023 11:10
18 071	[redacted]	En cours (Attribué)	20-06-2023 10:08	19-06-2023 16:50
18 052	qualité réseau	Nouveau	20-06-2023 09:18	16-06-2023 14:10
18 053	Badge	Nouveau	20-06-2023 09:11	16-06-2023 16:05
18 037	PC salariée sortie - [redacted]	En cours (Attribué)	19-06-2023 16:13	14-06-2023 12:15
18 007	Authenticator [redacted]	En cours (Attribué)	19-06-2023 11:13	12-06-2023 10:35
18 049	RE: visite technique pour pose fibre Optique	En cours (Attribué)	16-06-2023 15:22	16-06-2023 11:00
18 038	Problème de PC [redacted]	En attente	14-06-2023 17:51	14-06-2023 12:25
18 041	Mac - impossible de [redacted]	En cours (Attribué)	14-06-2023 16:55	14-06-2023 15:35
17 984	Problème de clavier - Lettres qui se détachent	En attente	14-06-2023 16:44	07-06-2023 17:15
18 042	Touche E qui s'est décollée sur le poste de Maxence	En cours (Attribué)	14-06-2023 15:58	14-06-2023 15:57
17 927	Bordeaux + Aix - Déménagements	En cours (Attribué)	14-06-2023 15:19	02-06-2023 16:55
17 970	Premier ticket !	En attente	13-06-2023 12:05	07-06-2023 11:05
17 873	Ordinateur toujours à la peine	En cours (Attribué)	13-06-2023 12:04	26-05-2023 09:10
17 997	Web cam qui ne fonctionne plus	En attente	12-06-2023 10:04	09-06-2023 12:20
17 860	Serveur [redacted]	En cours (Attribué)	08-06-2023 11:35	25-05-2023 09:20
17 978	problème ordinateur	En cours (Attribué)	08-06-2023 10:16	07-06-2023 15:15
17 963	Lenteur ordinateur	En cours (Attribué)	07-06-2023 14:24	06-06-2023 17:55
17 940	[redacted]	En cours (Attribué)	05-06-2023 13:17	05-06-2023 11:55
17 920	[redacted]	En cours (Attribué)	02-06-2023 12:01	02-06-2023 11:20
17 894	Gestion accès outils Google	En cours (Attribué)	31-05-2023 08:54	30-05-2023 18:00
17 857	Webcam via Teams	En attente	24-05-2023 16:43	24-05-2023 15:45
17 844	Reset Mac	En attente	23-05-2023 13:56	23-05-2023 11:55

Figure 9 : Vu d'ensemble de GLPI, l'outils utilisé pour le ticketing

Lorsque des problèmes matériels nécessitaient une assistance supplémentaire, j'ai utilisé la plateforme Aircall pour passer des appels et contacter les techniciens compétents. J'ai expliqué les problèmes rencontrés et coordonné les interventions sur site pour réparer ou remplacer le matériel défectueux.

J'ai été chargé de configurer différents types d'ordinateurs pour les employés de l'entreprise. Cela comprenait des systèmes d'exploitation variés tels qu'Ubuntu et Windows. J'ai pris en compte les besoins spécifiques de chaque utilisateur et j'ai effectué les paramétrages appropriés, y compris l'installation et la configuration des logiciels requis, comme l'antivirus, ou la suite office 365.

J’ai été chargé de présenter l’équipe réseau et les différentes applications utilisées dans l’entreprise aux nouveaux employés, lors d’une session d’introduction appelé ‘Point Réseau’. J’ai expliqué les rôles et les responsabilités de l’équipe réseau, ainsi que l’utilisation des applications clés. De plus, j’ai distribué les ordinateurs préalablement configurés aux nouveaux employés, en m’assurant qu’ils disposaient des logiciels nécessaires et des paramètres adaptés à leurs besoins.

J’ai apporté mon aide lors de divers déménagements au sein de l’entreprise. Par exemple, lors de travaux effectués au septième étage, nous avons dû déplacer plusieurs dizaines de postes de travail vers le deuxième, quatrième et cinquième étage. Cela impliquait le démontage et le déplacement des claviers, des écrans, des docks, ainsi que tous les câbles d’alimentation et câbles Ethernet avec les commutateurs réseau. J’ai veillé à ce que tous les équipements soient correctement déplacés, reconnectés et testés

4.2 Utilisation de Sentinel One sur l’Azure AD

Dans le cadre de l’analyse d’applications sur les ordinateurs de l’Azure AD avec Sentinel One, j’ai mis en évidence le rôle essentiel de cette pratique dans la détection et la prévention des menaces potentielles qui pourraient compromettre la sécurité des systèmes informatiques. L’utilisation de Sentinel One, un outil de sécurité avancé, permet de bénéficier de fonctionnalités puissantes pour mener cette analyse.

Grâce à la capacité de Sentinel One à surveiller en temps réel les activités des applications, HelloWork est en mesure d’identifier les comportements anormaux, les fichiers malveillants et les vulnérabilités potentielles. Cette surveillance proactive nous permet de prendre des mesures rapides et précises pour protéger nos systèmes contre les menaces émergentes.
L’une des actions que j’ai entrepris grâce à Sentinel One a été de recenser toutes les applications installées sur l’ensemble des ordinateurs de l’entreprise. Cette démarche permet d’avoir une vue d’ensemble des applications utilisées, ce qui est essentiel pour une gestion efficace de la sécurité. En connaissant les applications présentes sur nos systèmes, l'entreprise en mesure d’agir rapidement en cas de vulnérabilité publiée sur l’une de ces applications, en appliquant les correctifs nécessaires ou en prenant d’autres mesures préventives appropriées.

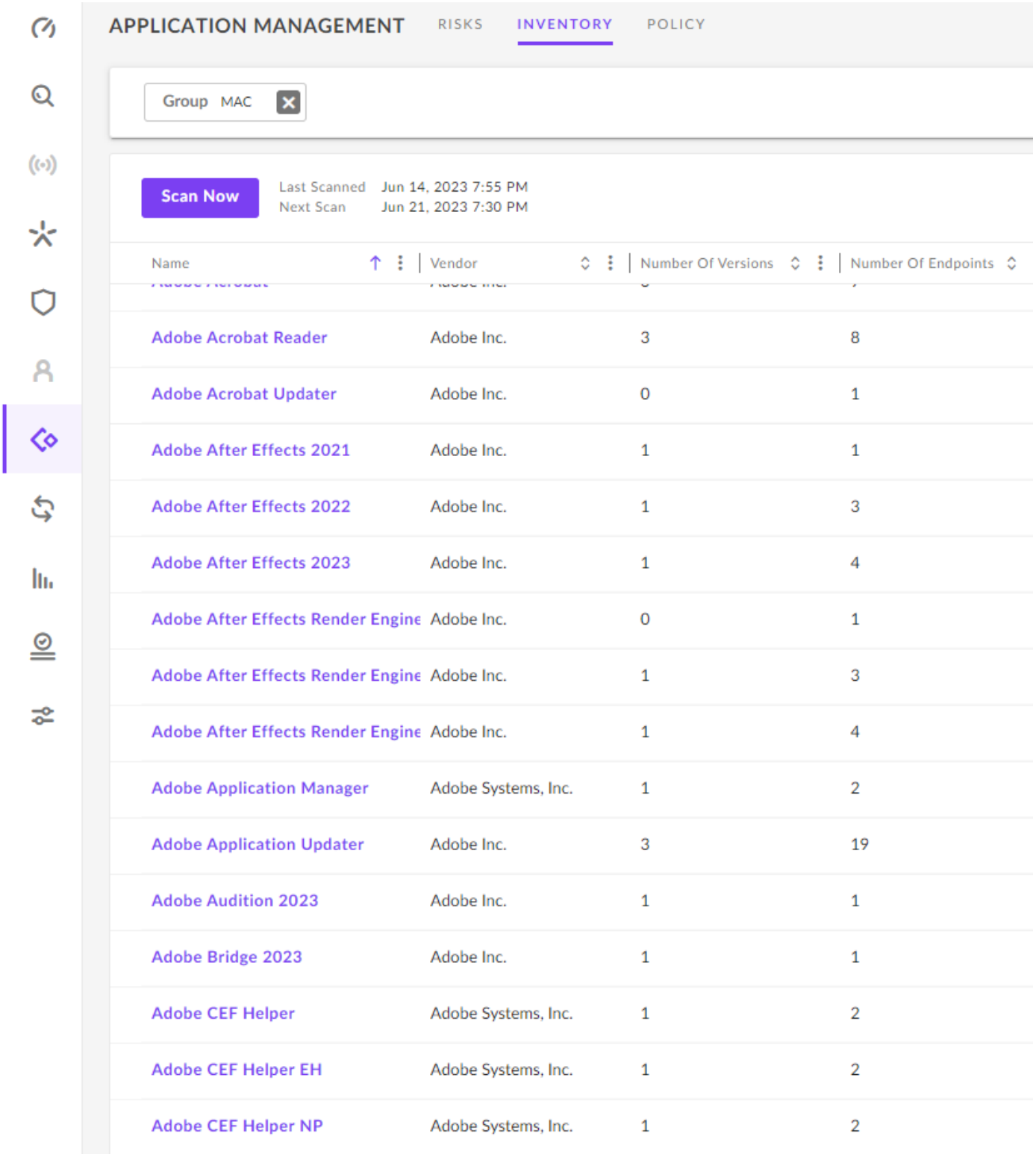

Figure 10 : Inventaire des applications présentes sur les MAC de l'entreprise

Sentinel One offre également une vision détaillée des vulnérabilités potentielles présentes dans notre environnement informatique.

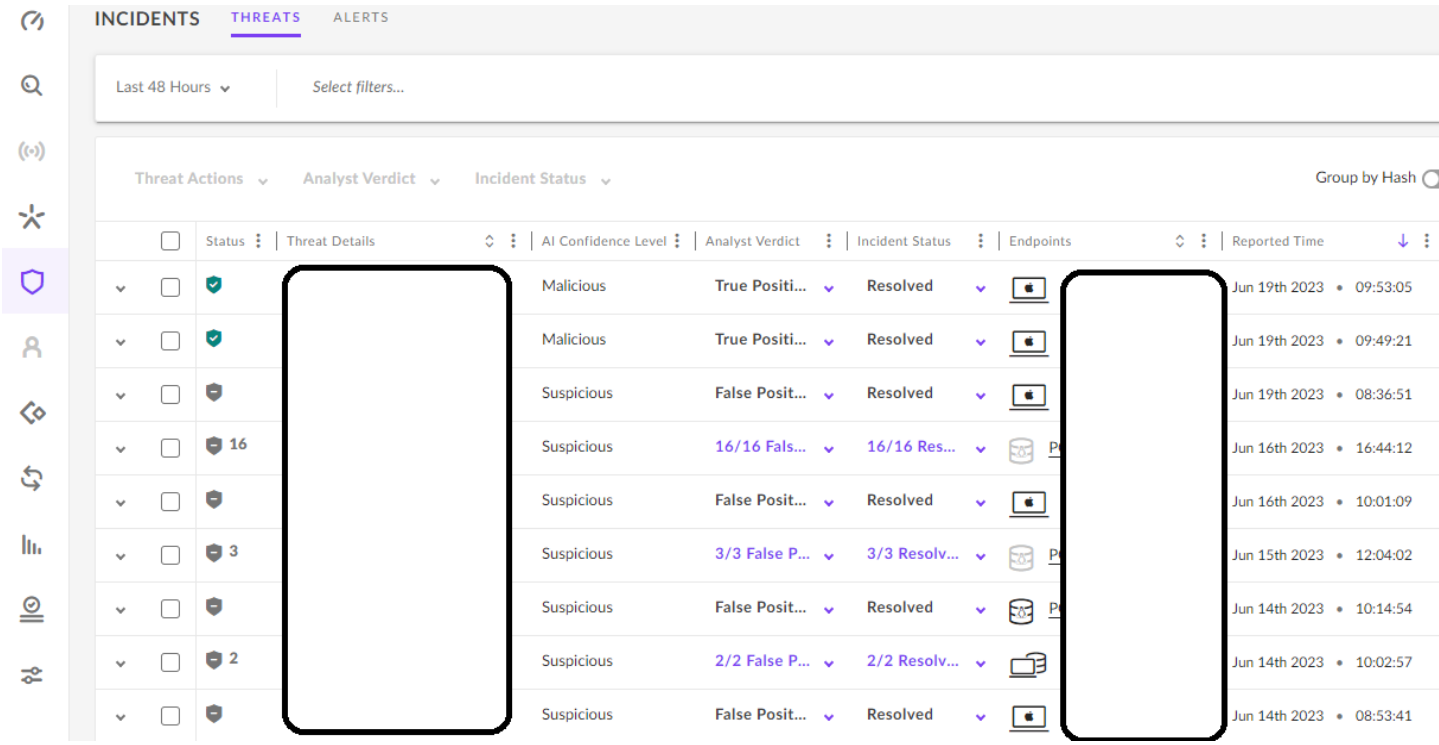

Figure 8 : Vision des incidents recensés par Sentinel One

4.3 Puits de logs sur l'Azure AD

J'ai été chargé de mettre en place la récupération des logs d'authentification des utilisateurs sur l'Azure AD. J'ai bénéficié d'une liberté de choix quant aux outils à utiliser pour cette tâche, ce qui m'a permis d'explorer plusieurs options et de les tester afin de sélectionner la solution la plus adaptée. Après plusieurs séries d'essais et de comparaisons, j'ai finalement opté pour l'utilisation de Grafana.

En plus de la récupération des logs, il était également nécessaire de mettre en place des scripts PowerShell pour détecter et alerter en cas de connexion à partir d'une adresse IP située en dehors de la France. Cette mesure de sécurité supplémentaire visait à renforcer la protection de notre environnement en identifiant toute activité suspecte et potentiellement malveillante.

La mise en place de Grafana et des scripts PowerShell a nécessité une analyse approfondie des besoins et des contraintes spécifiques de notre environnement. J'ai travaillé en étroite collaboration avec l'équipe de sécurité pour garantir que les alertes étaient configurées de manière adéquate et qu'elles répondaient aux critères de détection définis.

Cependant, après avoir exploré ses fonctionnalités, il est devenu évident que Grafana ne fournissait pas les capacités requises pour répondre à nos besoins spécifiques.

Conscient de l'importance de cette tâche et de la nécessité d'une solution plus robuste, j'ai entrepris d'évaluer d'autres options, C'est ainsi que j'ai découvert Graylog, un outil de gestion des logs offrant des fonctionnalités avancées et une meilleure compatibilité avec nos exigences. J'ai effectué des tests approfondis avec Graylog et j'ai constaté qu'il répondait mieux à nos besoins en termes de récupération, d'analyse et de visualisation des logs d'authentification.

Toutefois, compte tenu de la complexité et de l'ampleur de cette mission, mon responsable a décidé de confier ce service à des employés disposant d'une expertise avancée. Afin de bénéficier d'un niveau de compétence supplémentaire et d'une expérience spécialisée, l'idée de faire appel à un prestataire externe a également été abordé.

Aujourd'hui, l'opération de mise en place de récupération des logs d'authentification est en stand-by car des missions prioritaires nécessitent plus d'attention. Une fois ces missions prioritaires achevées, les travaux sur la mise en place de la solution de récupération des logs d'authentification reprendront.

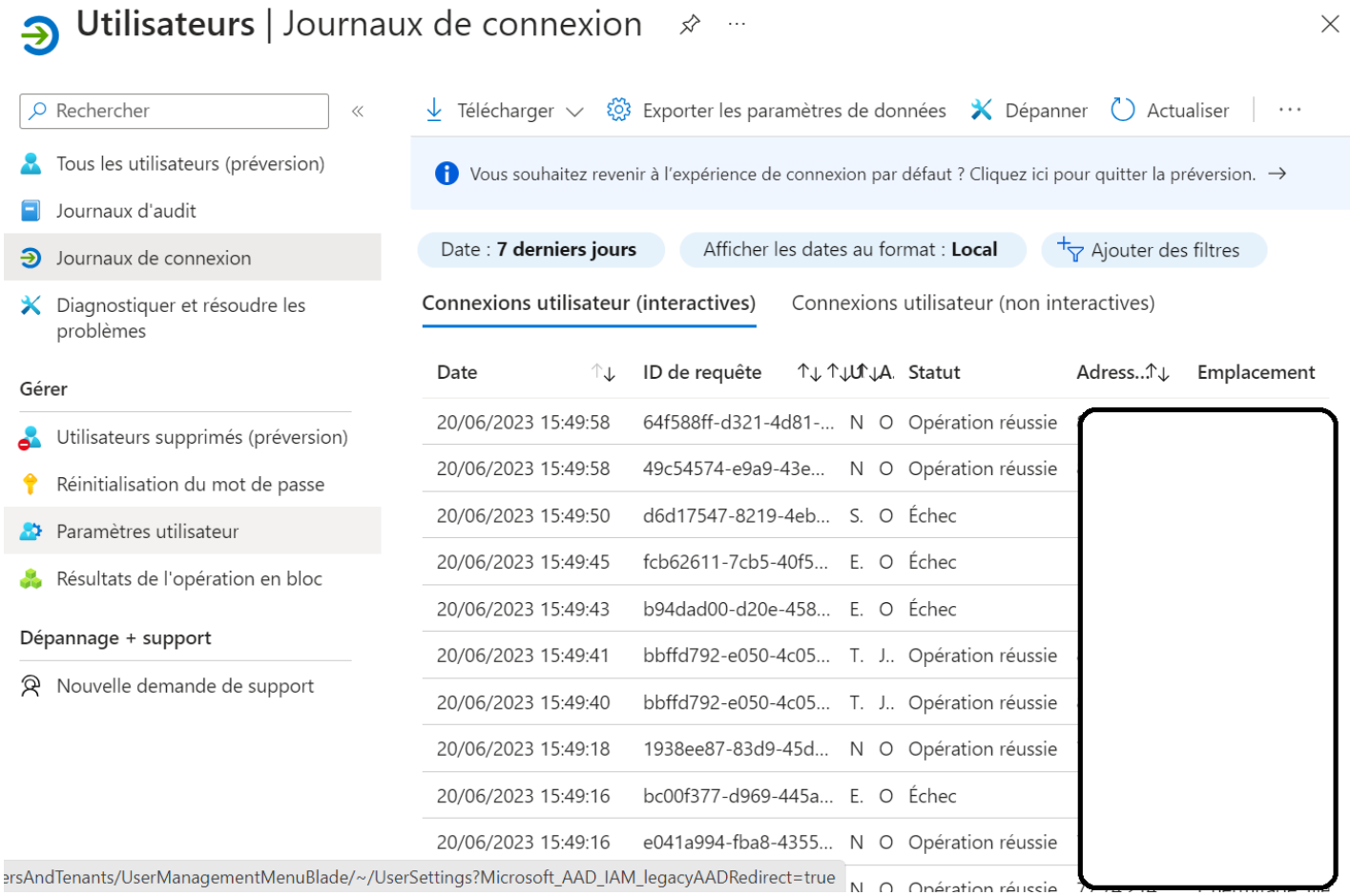

Figure 11 : centre d'administration de l'Azure AD, vue d'ensemble sur la gestion des logs de connexion

5 Conclusion

Cette expérience enrichissante m'a permis d'obtenir des résultats concrets dans le renforcement de la sécurité de l'Active Directory local. A travers ces différentes actions, j'ai tiré des enseignements essentiels sur la sécurité informatique et son importance dans notre environnement professionnel.

En analysant les vulnérabilités avec des outils tels que PingCastle, j'ai pu identifier et remédier à un grand nombre de failles, ce qui a considérablement amélioré la robustesse de l'infrastructure. De plus, l'utilisation de Sentinel One pour l'analyse des applications a renforcé la capacité à détecter les menaces potentielles et à prendre des mesures appropriées pour protéger nos systèmes.

Parallèlement, j'ai apporté un soutien précieux à l'équipe support en les aidant dans leurs tâches hebdomadaires. Cela m'a permis de développer mes compétences en communication et ma capacité à résoudre efficacement les problèmes rencontrés par les utilisateurs du quotidien.

Bien que la mise en place de la récupération des logs d'authentification ait été mise en attente en raison de priorités plus importantes, cette expérience m'a permis de comprendre l'importance cruciale de la sécurité des données et de l'authentification dans un environnement informatique.

Ce stage m'a apporté une précieuse expérience professionnelle, une opportunité que je n'avais jamais eue auparavant. J'ai acquis une solide compréhension des enjeux de sécurité et développé des compétences pratiques en résolution de problèmes et en soutien aux utilisateurs. Cette expérience a renforcé ma confiance dans ma capacité à relever des défis complexes et à trouver des solutions efficaces.

6 Remerciements

Je tiens à exprimer ma profonde gratitude envers toutes les personnes qui m'ont accompagné tout au long de mon stage et de mon parcours académique. Leur soutien, leurs conseils et leur encouragement ont été essentiels pour mon développement professionnel et personnel. Je souhaite adresser mes remerciements spéciaux à mon tuteur de stage, ma tutrice académique et mon équipe en général.

Tout d'abord, je voudrais remercier chaleureusement mon tuteur de stage, M. CARVAL, pour sa guidance précieuse et son expertise inestimable. Grâce à sa disponibilité, sa patience et sa bienveillance, j'ai pu acquérir des connaissances approfondies dans le domaine de l'Active Directory. Ses conseils éclairés et ses encouragements constants m'ont permis de progresser et de relever de nouveaux défis. Je suis reconnaissant pour l'opportunité qui m'a été offerte de travailler sous sa supervision.

Ensuite, je souhaite exprimer ma reconnaissance envers ma tutrice académique, Mme. HOUSSAIN. Sa supervision attentive, ses retours constructifs et ses précieux conseils ont été d'une grande valeur pour moi. Je suis reconnaissant pour son investissement et son soutien continu tout au long de mon parcours académique.

Enfin, j'aimerais adresser mes remerciements sincères à toute l'équipe avec laquelle j'ai eu le privilège de travailler. Leur accueil chaleureux, leur esprit d'équipe et leur collaboration ont créé un environnement de travail agréable et stimulant. Chacun des membres de l'équipe a contribué à ma formation en partageant ses connaissances et en m'offrant des opportunités d'apprentissage. Leur soutien indéfectible et leur encouragement ont été d'une importance capitale pour moi.

7 Glossaire

BUT, Bachelor Universitaire de Technologie

AD, Active Directory

DNS, Domain Name System

IP, Internet Protocol

DHCP, Dynamic Host Configuration Protocol

8 Bibliographie

Documentation de l'ANSSI sur les différents points de contrôle de l'Active directory:
https://www.cert.ssi.gouv.fr/uploads/guide-ad.html
https://www.cert.ssi.gouv.fr/uploads/ad_checklist.html

Documentation sur l'utilisation de PingCastle:

https://www.pingcastle.com/documentation

Liste complète de tous les sites que j'ai utilisé afin d'acheminer mes tâches avec succès:

https://adsecurity.org/?p=3299

https://adsecurity.org/?p=4056

https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#compatible_2000_not_default

https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#dont_expire_priv

https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#password_change_inactive_servers

https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#kerberos_properties_deskey

https://www.ssi.gouv.fr/uploads/IMG/pdf/NP_ActiveDirectory_NoteTech.pdf#subsection.3.6

https://github.com/microsoft/New-KrbtgtKeys.ps1/blob/master/New-KrbtgtKeys.ps1

https://www.microsoft.com/en-us/download/details.aspx?id=46899

https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/deploy/2-configure-wsus#23-secure-wsus-with-the-secure-sockets-layer-protocol

https://www.cert.ssi.gouv.fr/uploads/guide-ad.html#dont_expire