Mémoire de stage de fin d'études

État de l'art des systèmes de gestion des comptes à privilèges

Auteur :
Alexandre
Kervadec

Responsables :
M. Philippe Rolland
M. Damien Seiler
M. Mathieu Raffinot

2016

Remerciements

Je tiens tout particulièrement à remercier mes accompagnateurs chez SYNETIS : Damien Seiler et Philippe Rolland, qui m'ont aidé quotidiennement durant ce stage. Je remercie aussi tous les consultants de chez SYNETIS, qui ont, à des moments ponctuels, su m'enrichir de leur expertise. Il me semble aussi important d'exprimer ma reconnaissance envers Lionel Clément qui m'a suivi et aidé pour ma recherche de stage, lorsque j'avais un retard conséquent par rapport aux dates prédéfinies. Enfin mes derniers remerciements vont à mon père Albert Kervadec et ma tante Chantal Kervadec, pour m'avoir relu et corrigé, ainsi que soutenu durant mes études.

Table des matières

Table des figures

Glossaire

bastion moteur de gestion des connexions aux ressources de la solution de PAM. 19, 29, 30, 32

credential est le terme représentant les informations de connexion, comme par exemple un couple login/mot de passe ou une carte à puce. 30

from stratch démarrer un projet depuis rien, à partir de zéro. 23

PAM Privileged Account Management : gestion des comptes à privilèges. 2, 3, 7, 8, 10–12, 15–18, 24, 28–32

Introduction

Le choix de mon entreprise de stage s'est orienté vers SYNETIS, qui est une porte ouverte vers le monde de la sécurité. Monde vers lequel je souhaite m'orienter malgré, bien que je ne me sois pas spécialisé dans ce domaine pendant ma formation initiale.
SYNETIS est une PME[1] à taille humaine basée dans le centre de Paris. Une agence a été ouverte à Rennes en 2012 lors du recrutement de spécialistes en gestion des identités sur cette zone. Cette agence de Rennes compte 6 consultants et 2 managers (dont le chef d'agence). L'ambiance est très conviviale, tout le monde se connaît, des évènements de cohésion sont régulièrement organisés (afterwork, repas en groupe le vendredi midi). De même, une réunion trimestrielle est organisée sur le siège de Paris, qui regroupe tout le personnel de SYNETIS, afin de faire un bilan des projets, de rencontrer les nouveaux arrivants, et de partager les nouveaux objectifs visés par l'entreprise.
Le travail est réparti par équipes sur les différents projets en cours, chaque consultant pouvant travailler sur plusieurs projets en même temps. On peut distinguer deux types de projets : les gros projets s'étalant sur de longues périodes (plus de six mois) et les projets courts durant au maximum quatre mois. L'entreprise est spécialisée dans la gestion d'identité pour les grands groupes (conseils régionaux, grandes entreprises nationales et internationales), mais commence à développer une branche de pentest (test d'intrusion sur différentes structures, pour de plus amples informations, le guide de Rafay Baloch [2] est très complet).
J'étais considéré au même titre que les autres consultants, mais avec un tuteur qui travaillait sur des projets correspondants au sujet de mon stage, et qui me guidait au travers de mes recherches et développements.
Durant ce stage, j'ai travaillé sur les systèmes de gestion de comptes à privilèges. Les comptes à privilèges sont les comptes avec des droits élevés, comme ceux des comptes `root` des systèmes d'exploitation Linux/UNIX et `Administrateur` sur Windows. Pour ce projet, il était question de comprendre en profondeur les moyens existants et les enjeux de la gestion de comptes à privilèges. Cette compréhension avancée a permis de comparer l'ensemble des solutions disponibles sur le marché. La comparaison a mené à considérer 2 solutions à mettre en œuvre sur un environnement virtuel de test. Le test fut une mise en situation des solutions, car les spécifications des solutions sont un point clef d'un choix d'achat, mais l'ergonomie et la fonctionnalité peuvent être les critères décisifs de ce choix. Toutes les informations récoltées nous auront finalement aidé à comprendre la façon dont les solutions répondent à la problématique de la gestion des comptes à privilèges, et de déterminer quelle(s) solution(s) répond(ent) le mieux à notre problématique, afin de pouvoir proposer de l'intégration avec de futurs

1. Petite à Moyenne Entreprise

clients.

Le plan adopté pour la suite de ce mémoire consiste en une première section décrivant la problématique à résoudre, et les origines de cette problématique. Une deuxième section expliquera les moyens et les méthodes mises en œuvre pour répondre à cette problématique et enfin une dernière partie expliquera les résultats obtenus.

1 Problématique : comment pallier le manque de contrôle des comptes privilégiés

L'objectif général est de résoudre le problème de manque de contrôle et de monitoring des comptes à privilèges. Afin de parvenir à ce résultat, plusieurs solutions ont été développées par des éditeurs, le but final de ce projet étant de déterminer quelle en est, ou quelles en sont, la ou les meilleures solutions. Pour répondre à cette problématique, nous allons d'abord expliquer plus en détails ce qu'est un compte à privilèges, puis nous intéresser aux raisons pour lesquelles ces comptes sont des points clefs de la sécurité des systèmes d'information. Ensuite, nous allons expliquer un fonctionnement global et commun aux solutions du marché puis mettre en avant les limitations que peuvent avoir ces solutions de PAM.

1.1 Contexte

1.1.1 Les comptes à privilèges

Il semble important de définir clairement la différence entre un compte à privilèges et un compte d'utilisateur classique, et plus précisément les deux catégories de mot de passe qu'ils engendrent :

Les mots de passe utilisateur : basiquement, un mot de passe est un secret qui permet l'utilisation d'un compte. Un compte représente un utilisateur humain et son mot de passe justifie son identité, comme un compte Active Directory [2], qui représente digitalement un humain, et le mot de passe qui justifie l'identité de l'humain qui s'y connecte auprès du système. Ce type de mot de passe est connu par l'utilisateur humain représenté par le compte, le but étant d'avoir un minimum de comptes par entité humaine, l'idéal étant une correspondance bijective [3]

Les mots de passe de comptes à privilèges : ces mots de passe sont des mots de passe liés à un compte qui ne représente pas une entité humaine. Ce compte peut être un compte système comme `root` sur un système d'exploitation Linux ou un compte de service sur un système d'exploitation Windows. Ces mots de passe ne sont pas forcément fournis à un utilisateurs humain, et même idéalement, ne doivent pas l'être, ainsi, ils peuvent d'être d'une complexité élevée sans avoir un souci d'apprentissage de ce dernier

Le but de ce stage était de trouver la meilleure solution pour sécuriser les mots de passe de comptes à privilèges tout en supervisant les comptes

2. Système d'annuaire électronique propriétaire de Microsoft, basé sur la norme LDAP (Lightweight Directory Access Protocol).

3. Un seul utilisateur humain pour un seul compte et vice-versa.

liés à des utilisateurs.

1.1.2 La gestion de comptes à privilèges

La gestion de comptes à privilèges (PAM[4]) est une sous-section de la gestion d'identité et d'accès (IAM[5]). L'IAM est un large champ de contrôle d'accès qui se veut critique dans le domaine des technologies de l'information.
Il existe bien sûr une multitude de connexions spécifiques entre les utilisateurs et les dépendances technologiques. La PAM n'est que l'une d'entre elles.
La PAM est apparue au début des années 2000 à cause de l'impossibilité des solutions d'IAM de contrôler, gérer et faire des rapports sur les accès aux serveurs, aux bases de données, aux équipements réseau et tout autre application critique au sein d'une organisation. Cette solution entraîne une gestion d'un petit nombre d'utilisateurs, mais d'un grand nombre de dépendances technologiques ayant une importance clef dans le fonctionnement des infrastructures.
La fonctionnalité principale d'une solution de gestion d'identité privilégiée gravite autour de la sécurisation de l'accès aux ressources critiques par les administrateurs IT.
Plus précisément, des privilèges spécifiques peuvent être délivrés à des comptes d'utilisateurs. Ces privilèges sont dépendants des systèmes et des applications impliqués, mais ils peuvent inclure la capacité à écrire des données, créer des comptes, exécuter une mission, pour ne citer que quelques exemples. En plus de contrôler l'accès avec un grand niveau de finesse, beaucoup de solutions fournissent aussi un package d'actions disponibles lors de l'utilisation d'un compte privilégié. Dans le but d'assurer la sécurité de ces comptes, les solutions exploitent un large éventail de mécanismes, comme par exemple, l'utilisation de clefs SSH, la rotation de mot de passe et l'ajout de multiples authentifications (authentification multi-facteurs).
La gestion d'identités privilégiées est devenue de plus en plus importante, notamment avec la croissance des requis de sécurité et des règles de conformité (l'ISO 27001 qui est une norme de sécurité internationale sur la protection des actifs informationnels par exemple). Il est aussi important de noter que de nombreux exploits[6] compromettant des données sont liés à la compromission d'accréditations privilégiées. Avec la recrudescence des tentatives de hack et les contrecoups économiques grandissants, les entreprises commencent à porter un surcroît d'intérêt à la gestion et au contrôle des comptes à privilèges. En effet, les tentatives de piratage sont

4. Privileged Access Management
5. Identity and Access Management
6. Element permettant d'exploiter une faille de sécurité

diversifiées : du social engineering, au vol de ces accréditations par une brèche dans la sécurité en passant par des *brute force* de mot de passe n'ayant pas une complexité suffisante [7] (dont traitent Weber *et coll.* [11]).

1.2 Un point clef de la sécurité des systèmes d'information

1.2.1 Des prestataires de service ayant les clefs du royaume

Le principal point de sécurité posant question avec les comptes à privilèges est leurs utilisateurs.
Dans une entreprise, le personnel gérant l'infrastructure n'est pas forcément d'une dimension adaptée aux besoins. Cette dimension n'est souvent pas accessible et est comblée par l'embauche de prestataires de service. On peut prendre l'exemple d'une entreprise de taille moyenne, qui gère son infrastructure en autonomie. Seulement, l'entreprise grossit et une nouvelle infrastructure déployée en *clusters* [8] est nécessaire. Le personnel n'ayant pas les compétences pour réaliser cette mise à niveau, l'entreprise devra faire appel à une entreprise de service tierce, qui réalisera et maintiendra cette nouvelle infrastructure. Ce sont les prestataires de service.
Cependant, ces prestataires doivent intervenir avec des droits élevés d'administration. Ils ont donc ce qu'on appelle les clefs du royaume [9], sans aucune supervision par l'entreprise mandant.
Du point de vue de la sécurité, il est très risqué de recourir à de telles pratiques. C'est ici qu'une solution doit être trouvée, et c'est ici que les systèmes de gestion des comptes à privilèges ont un rôle clef.

1.2.2 Une cible de choix pour les pirates

Un compte privilégié est un compte utilisé par les administrateurs système et réseau, ainsi que par les équipes de sécurité pour accéder aux ressources réseau comme les serveurs, les pare-feux, les switches, les routeurs, les ordinateurs, les applications ou les bases de données avec des droits élevés. Ces comptes sont nécessaires à la maintenance d'une infrastructure, tout comme aux interventions de réparation, de diagnostic ou gestion de situations de crise [10]. Dans de grands groupes, il peut y avoir un grand nombre de ces comptes, de l'ordre de la centaine voire du millier d'entités, répartis

7. L'utilisation de mots de passe faibles tels que `password`, `admin`, `1234`, `azerty1234` ou `Abcd1234` reste encore très fréquente. Pour trouver ces mots de passe faibles, la technique la plus employée est le brute force avec un dictionnaire de mots de passe

8. Grappe de serveurs sur le réseau, aussi appelé ferme de calcul.

9. En anglais, littéralement *keys to the kingdom*, représente l'accès sans limite à toute l'infrastructure informatique.

10. Attaque sur un serveur par exemple

sur plusieurs sites.
Ces comptes peuvent aussi être des comptes d'application communiquant avec d'autres applications [11], comme par exemple un serveur faisant une sauvegarde régulière sur un autre serveur de récupération.
Tous ces comptes ne sont pas surveillés par les traditionnels gestionnaires d'identités, seul un mot de passe permet d'y accéder. De plus ces comptes sont très souvent partagés entre plusieurs administrateurs pour une question de facilité de gestion.
Ainsi, une personne mal intentionnée parvenant à voler les accès d'un tel compte verrait son pouvoir de destruction, voire de vol d'informations sans limites, ce qui en fait une cible privilégiée par les pirates informatiques.

1.2.3 Un manque de visibilité d'actions

Comme abordé en introduction, il existe un grand manque de visibilité sur les actions des comptes à privilèges. En effet, ces comptes aux droits élevés, ne sont ni tracés, ni surveillés. Ceci peut avoir plusieurs mauvaises incidences, certaines intentionnelles et malveillantes, d'autre involontaires, mais tout de même paralysantes.
On peut classer ces incidences en deux catégories, l'une relevant d'une erreur accidentelle, et l'autre d'une volonté de nuire à une organisation comme le décrit l'article de Shackleford [9] :

- Erreur accidentelle :
  - → Erreur de configuration, difficile à retrouver à cause du manque de supervision
- Volonté de nuire :
  - → Sabotage d'une configuration, menant à un déni de service
  - → Vol d'informations sensibles

Ce manque de visibilité crée aussi un point noir dans un audit de sécurité : il n'y a aucune détection de faille de sécurité concernant ces comptes.

1.3 Objectifs d'un système de PAM

D'après les points précédents, on peut en déduire les spécificités que nous voudrions améliorer vis-à-vis des comptes à privilèges :

- Centraliser l'accès aux données de l'entreprise
- Sécuriser les comptes à privilèges (duo identifiants et mot de passe)
- Gérer de manière forte des mots de passe et établir une politique d'authentification forte
- Journaliser et superviser les activités des comptes à privilèges

11. A2A : Application To Application, littéralement d'application à application

1.4 Fonctionnement d'un système de gestion de comptes à privilèges

1.4.1 Cas général

Le principe commun à toutes les solutions des éditeurs est la présence d'une identification sur un serveur central. On peut considérer 2 groupes : les comptes à privilèges et les ressources à protéger. Entre ces 2 entités vient s'intercaler le serveur d'identification, qui fait la passerelle entre les comptes et les ressources.
L'identification d'un utilisateur sur un compte à privilèges se fait sur le serveur central, et l'identification de ce compte à privilèges sur une ressource protégée est déléguée au serveur central. Ainsi, les utilisateurs n'ont plus à gérer et connaître les mots de passe d'accès aux ressources protégées ; c'est le serveur central qui détient tous les secrets [12].
Le serveur central a, à sa charge, de protéger les mots de passe dans un coffre-fort et de les renouveler régulièrement (il est préconisé de renouveler ses mots de passe au moins une fois par mois, ce qui est déjà peu pour une entreprise).

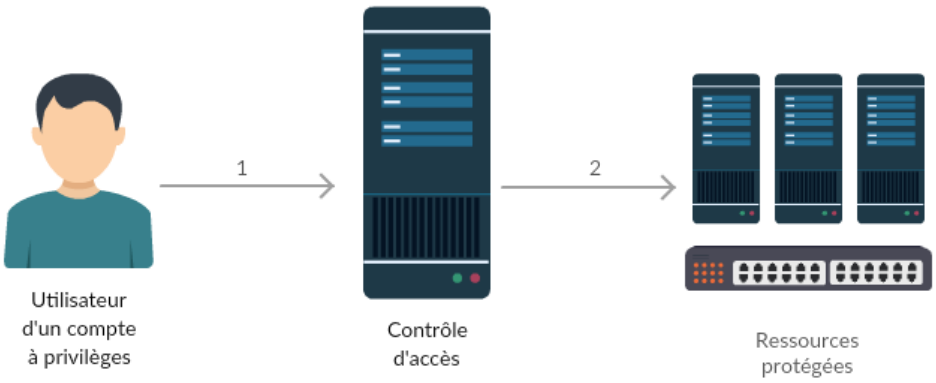

FIGURE 1 – Fonctionnement général d'un système de PAM

1.4.2 Deux types d'architecture

Malgré le principe de fonctionnement identique pour quasiment toutes les solutions de PAM, il existe cependant des différences au niveau de l'architecture de ces dernières solutions, on distingue 2 grandes familles :

— Architecture proxy [13] : les ressources et les comptes d'utilisateurs sont

12. Les logins et mot de passe, aussi appelés « credentials » en anglais.
13. Toutes les communications transitent par un point de contrôle.

séparés physiquement (ou logiquement [14]), le serveur central gère tout seul les accès aux applications

— Architecture avec agents : les accès aux ressources et la supervision sont gérés par des agents sur les ressources cibles (application installée sur la ressource)

Nous pouvons rapidement nous rendre compte qu'une architecture avec des agents est beaucoup plus intrusive et longue, ou difficile à mettre en place, qu'une architecture en proxy, où seul l'adressage est à modifier.

1.5 Les limitations des solutions PAM

1.5.1 Le facteur humain

Il faut noter que même avec un système de PAM éprouvé et efficace, nous ne pouvons pas mettre de côté le risque le plus exploitable dans le domaine de la sécurité qu'est, le facteur humain. En effet, il est souvent plus facile de tromper un élément du personnel pour réaliser une compromission de données. Il sera donc important lors d'un déploiement d'une solution de PAM, d'éduquer le personnel de l'organisation concernée, afin que ces derniers mettent correctement en œuvre les règles de base de la sécurité informatique comme par exemple :

— Totalement prohiber « l'effet *post-it* » : notation de mot de passe sur un *post-it* collé sur l'écran

— Toujours remplacer les mots de passe d'usine dans les logiciels utilisés

— Forcer le changement régulier (au minimum une fois par mois) de mot de passe des utilisateurs

1.5.2 La détection de comportements anormaux

Très peu de solutions de PAM proposent un système de détection de comportements anormaux, comme par exemple un conseiller commercial qui aurait accès aux informations des comptes clients, qui abuserait de ce droit. En effet, même avec une restriction des droits, une supervision et journalisation des activités, une solution de PAM n'est pas une intelligence artificielle qui peut détecter des comportements suspects. Cependant, il est toujours possible de détecter des comportements prédéfinis avec des successions de commandes qui lèveraient une alerte.

14. Redirection des paquet par port.

2 Méthodes et moyens mis en œuvre

Comme le titre l'indique, nous allons expliquer les méthodes et les moyens utilisés pour répondre à la problématique posée. Cette section sera séparée en 3 sous-sections : la première décrivant mon cheminement en matière de gestion de projet, la deuxième traitant de la phase de recherche d'informations, avec ses problèmes rencontrés et solutions trouvée, puis une troisième partie décrivant le travail effectué pendant la phase de test des deux produits sur un environnement de test, ainsi que les différentes technologies utilisées.

2.1 Gestion de projet

La première chose que j'ai dû faire en arrivant dans l'entreprise, fut ce qu'on appelle chez SYNETIS une note de cadrage. Cette note de cadrage correspond, par rapport à ce qu'on a pu faire à l'université durant divers projets, à l'analyse des besoins et les résultats attendus, l'organisation en tâches de l'intégrité du stage. Cette répartition des tâches dans le temps a permis de scinder l'ensemble du projet en de multiples étapes simples, courtes, qui m'ont permis de segmenter mon stage pour ne pas me retrouver perdu ou submergé par le travail. En dernière partie furent explicitées les contraintes et exigences de rendus pour l'entreprise ainsi que les éventuels risques à encourir.
De plus, des documents

2.1.1 Analyse des besoins

Le besoin général était de réaliser un état de l'art des solutions de gestion des comptes à privilèges, de mettre en place 2 preuves de concept sur un environnement de test virtualisé afin de pouvoir définir la ou les solutions les plus adaptées à la gestion des comptes privilégiés. Ces solutions pouvaient (à l'époque de la réalisation de l'état de l'art) et sont (à ce jour) déployées chez un gros client. Je suis notamment intégré à l'équipe travaillant sur cette intégration dans l'infrastructure, car ayant réalisé une mise en place dans un environnement de test de la solution en question, je fais partie des personnes les plus compétentes de SYNETIS pour répondre aux différents problèmes qui pourraient se présenter.
Cet état de l'art devait aboutir à un document présentant le principe de gestion de comptes à privilèges, premièrement de façon théorique, puis de façon technique. Ensuite, ce document devait déterminer une liste de solutions d'éditeurs étant des acteurs majeurs sur le marché de la gestion de comptes à privilèges. Enfin, ce document aura permis de créer un tableau comparatif de toutes les solutions étudiées, selon des critères pointus qui ont été définis comme répondant à la problématique du stage.

2.1.2 Planning prévisionnel

Afin d'avoir une vue d'ensemble du projet, un planning a été réalisé à partir d'un découpage journalier des tâches à effectuer. Ce planning a permis d'avoir une vue macroscopique du stage, et de répartir le travail sur sa durée, pour éviter d'avoir un retard qui pourrait être insurmontable à quelques semaines de la date butoir. Ce découpage a aussi permis de connaître les étapes à franchir,ainsi que de me positionner dans le temps (avance ou retard) afin d'éviter de travailler dans la précipitation pour arriver à un résultat probant.

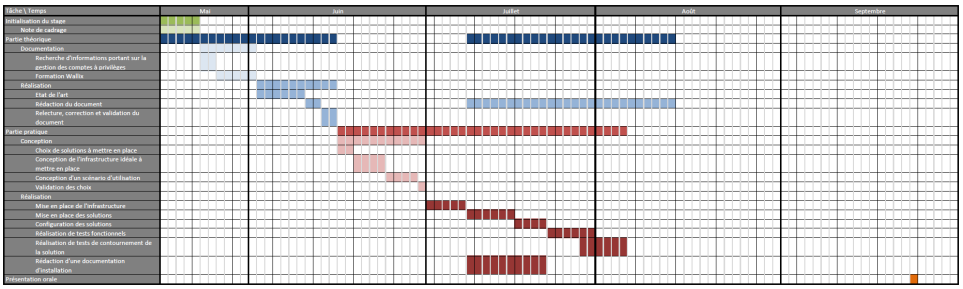

FIGURE 2 – Calendrier prévisionnel

Bien sûr, le calendrier est une estimation et la réalité s'est avérée différente : la durée de recherche sur la gestion de comptes à privilèges et sur les différentes solutions a pris presque 2 fois plus de temps que prévu, tout comme le déploiement des solutions et le test de ces dernières. Cependant, le calendrier prévisionnel étant vu avec une large marge d'erreur, le stage a tout de même pu être effectué dans la durée impartie.

2.2 Recherche

La première étape a été la recherche d'informations sur le sujet. N'ayant pas de notions sur celui-ci, j'ai d'abord commencé par me renseigner auprès des consultants de l'agence de Rennes, notamment mes tuteurs, Damien Seiler et Philippe Rolland, et aussi du manager de l'agence, David Geffroy, qui est un expert dans le domaine. Grâce à ces premières lignes directrices fournis par ceux qui sont devenus mes collègues, j'ai pu orienter mes recherches internet vers la bonne direction, et ainsi trouver un maximum de résultats.

2.2.1 Recherche du fonctionnement des solutions

La meilleure façon de trouver des informations concernant le fonctionnement d'une solution de PAM s'est d'abord avéré être la recherche

d'informations génériques, comme des tutoriels ou des articles traitant du sujet. Cependant, j'ai fini par réaliser qu'internet ne m'apportait pas suffisamment de renseignements. La solution fut donc de s'orienter directement vers les solutions des éditeurs, et de tenter de comprendre leur fonctionnement, pour en tirer moi-même un fonctionnement général des solutions. Cette étape resta tout de même laborieuse, les éditeurs ne partageant pas énormément d'informations quant à l'architecture ou le fonctionnement technique de leurs solutions, mais seulement quelques caractéristiques. Ceci ne m'empêcha pas de pouvoir trouver assez de renseignements pour pouvoir en déduire une architecture assez claire, qui me donnait une vision d'ensemble du fonctionnement [15] d'une solution de PAM.

2.2.2 Recherche des solutions existantes sur le marché

La recherche des solutions existantes sur le marché fut assez simple, compte tenu de la précédente recherche, s'appuyant sur ces solutions en question. Néanmoins, étant parti sur une base de 6 solutions trouvées pour réaliser un descriptif du fonctionnement général d'une solution de PAM, j'ai réussi à trouver plus du double de solutions par la suite, en navigant de lien en lien et en m'inscrivant à des newsletter m'envoyant des rapports tels que celui de l'éditeur FORRESTER écrit par Cser [3].

Nous avons ainsi pu nous retrouver avec une liste de solutions satisfaisante pour pouvoir commencer à faire un comparatif objectif. Nous avons alors orienté mes recherches vers les spécificités des solutions, en parcourant toute la documentation disponible, en participant à des vision-conférences avec les commerciaux et ingénieurs des maisons d'édition ou en contactant le support. Cette étape a été celle qui a été la plus longue dans la période de recherche, qui parfois s'est avérée infructueuse au vu du manque d'informations disponibles et de l'absence de réponse du support (ou plus précisément des réponses me redirigeant vers des documents en ligne ne contenant pas les réponses demandées). C'est par ailleurs une des étapes qui a complètement décalé le calendrier prévisionnel, prenant sur la marge prévue à cet effet.
Cette étape a conduit à éditer un rapport au format *docx* explicatif (en profondeur) du fonctionnement des solutions de PAM et un descriptif des fonctionnalités de chaque solution, puis à un tableau comparatif des solutions. Nous pouvons trouver un aperçu de ce tableau à la FIGURE 2.2.2. Ce tableau comparatif n'est pas disponible en annexe, en raison de sa taille impossible à imprimer ainsi que pour des raisons de confidentialité, il en est de même pour le document *docx* dont seul la table des matières a été intégré en ANNEXE B.

15. Fonctionnement décrit dans un schéma en ANNEXE 3.5.2

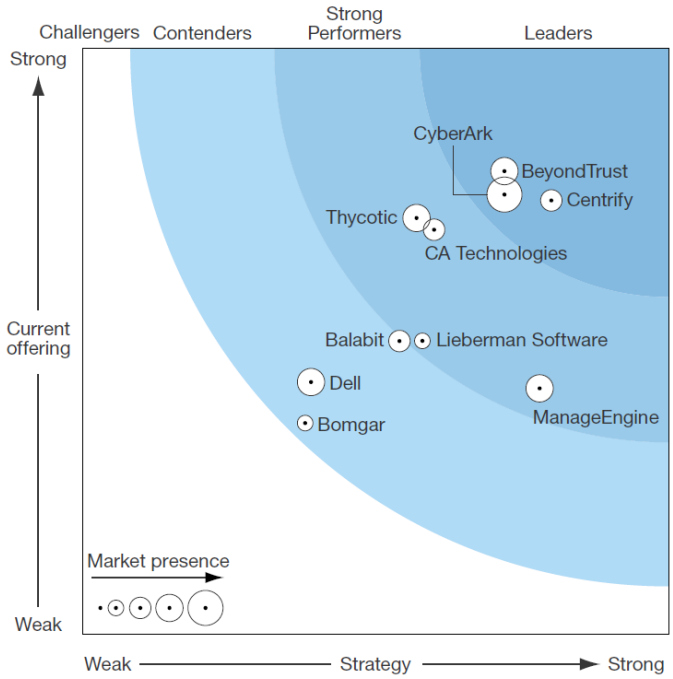

FIGURE 3 – Quadrant mettant en évidence les acteurs du marché de PAM selon le rapport offre/stratégie et l'indice de présence sur le marché

2.3 Proof of Concept

La phase de conception d'environnement de test s'est déroulée en plusieurs étapes :

— Conception architecture idéale

— Validation de l'architecture avec le tuteur, et remaniement de cette dernière pour s'adapter aux ressources matériels disponibles chez SYNETIS, ressources assez limitées car nous étions en saturation de ressources mémoire et processeur sur le serveur interne. Un nouveau serveur est arrivé en fin de stage, mais malheureusement quelques semaines trop tard

— Installation de l'infrastructure et déploiement des solutions à tester

2.3.1 Architecture

L'architecture idéale sur laquelle les solutions devaient être intégrées nous semblait être celle qui se rapprochait le plus d'une situation réelle d'entreprise, comprenant des séparations logiques pour les différents corps de métier.

En effet, les ressources limitées ont réduit notre infrastructure de test au

	A	L	M	N
1	Solutions / Caractéristiques	Secret Server	Vormetric Data Security Platform	AdminBastion
26	Condition de montée en privilèges	- Autorisations basées sur les rôles (role-based) - Approbation d'un supérieur (ou autre personne désignée)	Role LDAP	Basée sur un ensemble de règles prédéfinies
27	Check-out et check-in	- OTP		N/A
28	Session limitée dans le temps			+ plage horaire
29	**Monitoring**			
30	Enregistrement vidéo	Uniquement pour l'édition Enterprise plus		
31	Reconnaissance OCR			
32	Enregistrement des logs			
33	Contenu des logs	N/A	Protocole Syslog RFC5424	L'ensemble des sessions
34	Monitoring en direct			
35	Remonté d'alerte en direct			
36	Edition de rapports	- via un SIEM	- via compatibilité avec un SIEM	
37	**Aspect Financier**			
38	Modes de licensing	3 modes de licences : - Professional - Enterprise - Enterprise Plus - Version d'essai (Enterprise Plus) de 30 jours L'achat de la licence Professional se fait en ligne, les deux autres licences sont juste des upgrades de clef qui permettent l'accès à la licence supérieure. Chaque utilisateur doit avoir une adresse email liée à une clef de licence valide.	3 appliances : - VM (machine virtuelle) : le client doit fournir le serveur dédié - V6000 : serveur hébergeant l'application fourni - V6100 : serveur avec HSM hébergeant l'application fourni	5 Appliances physiques disponibles : - **WAP 50** : CPU : Pentium 1403 (2,6 GHz) - Dual Core RAM : 4 Go SAS : RAID 1 - 500 Go utile - Hot-plug Alim : Rendondante - Hot-plug - **WAP 200** : CPU : Xeon E5-2620 (2,4 GHz) - Hexa Core RAM : 8 Go SAS : RAID 1 - 1,2 To utile - Hot-plug Alim : Rendondante - Hot-plug - **WAP 600** : CPU : Xeon E5-2640 (2,6 GHz) - Octo Core RAM : 16 Go SAS : RAID 1 - 2,4 To utile - Hot-plug Alim : Rendondante - Hot-plug - **WAP 1000** : CPU : 2 * Xeon E5-2640 (2,6 GHz) - Octo Core RAM : 32 Go SAS : RAID 1 - 3,6 To utile - Hot-plug Alim : Rendondante - Hot-plug - **WAP 2000** : CPU : 2 * Xeon E5-2667 (3,2 Ghz) - Octo Core RAM : 64 Go SAS : RAID 1 - 1,8 To utile - Hot-plug Alim : Rendondante - Hot-plug
39	Coût des licences	Contacter les revendeurs (Thycotic n'est pas en France) : Vendeurs certifiés : - ADINES - Acternet - Nellsoft Revendeurs autorisés : - Atlantis		N/A
40	Légende :			
41	Condition remplie			
42	Condition non-remplie			

FIGURE 4 – Extrait du tableau comparatif de solutions édité au terme de la phase de recherche

strict minimum, donc une machine de chaque type :

— MS WINDOWS SERVER 2012 R2 : serveur de test de connexion RDP [16], de configuration des solutions de PAM (base de données *MySQL* et *SQL Server*), de mail (avec le logiciel *hMailServer* [5] et contrôleur de domaine *Active Directory*

— MS WINDOWS SERVER 2012 : serveur TSE [17] permettant de tester une connexion sur une application distante (*VMWare vSphere Client* [18] dans notre cas)

— LINUX DEBIAN 8.4.0 JESSIE : serveur Linux permettant de tester une

16. Remote Desktop Protocol : contrôle à distance d'un serveur.

17. Terminal SErvice : permet d'utiliser le serveur pour faire tourner des applications utilisées en bureau distant.

18. Programme Windows permettant de configurer un hôte de virtualisation et de faire tourner des machines virtuelles.

connexion SSH [19]

Cette architecture limitée nous a permis de tester et d'éprouver 2 des solutions choisies, tout en respectant les contraintes de ressources établies. Bien plus que les solutions en elles-même, le déploiement de l'infrastructure de base a nécessité d'autres technologies, que l'on peut lister en tâches suivantes :

— Sur Microsoft Windows Server 2012 et 2012 R2 :
  → Installation du rôle contrôleur de domaine [20]
  → Création et configuration d'un domaine, d'une forêt et de toutes ses dépendances assurant le bon fonctionnement de l'infrastructure
  → Création d'utilisateurs de domaine [21] avec les droits nécessaires et suffisants à leur fonctionnement, grâce aux groupes de sécurité Windows (consulter le livre de Minasi *et al.* [7] pour plus d'informations sur Active Directory et la sécurité de Windows Server 2012 R2)
  → Création de comptes de service de domaine (MSA [22]) sous *Powershell* [23]
  → Installation de systèmes de gestion de base de données relationnelles *MySQL* et *SqlServer* et création de bases de données pour les solutions de PAM
  → Installation et configuration d'un serveur de mail local *hMailServer* pour récupérer les mails envoyés par les solutions de PAM
  → Installation du rôle TSE et configuration de ce dernier avec l'application *VMWare vSphere Client*
— Sur Debian 8.4.0 :
  → Installation du serveur SSH
  → Configuration réseau

2.3.2 Choix des solutions de PAM à tester

Nous avions fait, au terme de la phase de recherche, une sélection de 3 solutions potentielles à déployer sur nos environnements de test. Ce choix s'était fait en prenant en compte les données présentées dans le tableau

19. Secure SHell : protocole de connexion à distance à une machine Linux/Unix.
20. gestionnaire d'un domaine sous le système d'exploitation Windows.
21. Utilisateurs créés dans un annuaire Active Directory, disponible pour toute machine du domaine.
22. Managed Service Account : compte Active Directory dédié aux service, le système gère lui-même les mots de passe.
23. Interface en ligne de commande et langage de scripting dédié à Windows.

comparatif des solutions dont on a un aperçu dans la FIGURE 2.2.2. Ces 3 solutions étaient :

— WALLIX ADMINBASTION

— CYBERARK PRIVILEGED ACCOUNT SECURITY SUITE

— THYCOTIC SECRETSERVER

Nous étions déjà en contact avec *Wallix*, car partenaires et mon tuteur était en formation avec eux, pour la solution en question. Nous avons donc pu avoir facilement une installation de leur solution. En revanche, *CyberArk* a refusé de nous fournir une version d'évaluation tant que nous n'abandonnions pas notre partenariat avec *Wallix*, pour devenir le partenaire exclusif *CyberArk*. Ce choix de *CyberArk* venant du fait que *Wallix* est leur plus gros concurrent en France, car *Wallix* est une entreprise Française et que beaucoup d'entreprises jouent le jeu de la préférence locale[24]. Nous avons donc décliné la solution de *CyberArk* et sommes entrés en contact avec *Thycotic*, avec qui nous n'avons eu aucun soucis et qui nous ont offert un suivi remarquable (une communication omniprésente à toutes les étapes de test).

2.3.3 Déploiement : Wallix AdminBastion

La version d'essai de *Wallix AdminBastion* se présente sous forme d'une machine virtuelle (fichier `vmdk`[25]). L'hyperviseur[26] hébergé sur le serveur local étant *VMWare ESXi*,
Cette machine virtuelle est un Debian 8 personnalisé par Wallix, avec leur propre configuration d'usine. Elle doit utiliser une base de données *MySQL* externe afin de stocker ses données (logs et accréditations). Nous avons donc créé une base de données sur le serveur *MySQL* présent sur la machine Windows Server 2012 R2. On avait donc l'architecture présentée sur la FIGURE 2.3.3

Nous avons, suite à l'installation de la solution et à sa configuration, pu tirer des points techniques importants sur son fonctionnement. Le produit présente deux interfaces différentes, l'une hébergée sur le moteur même de la solution, que l'on appellera WAB et qui correspond au bastion, l'autre beaucoup plus axée sur le design que l'on appellera WABAM[27], est hébergée sur un serveur parallèle. Les utilisateurs de comptes à privilèges se connectent sur cette interface.

24. Information fournie par le troisième éditeur, *Thycotic* durant des échanges de mails.
25. VMWare Virtual Disk : format de disque virtuel créé par *VMWare*
26. Plate-forme de virtualisation permettant de faire fonctionner plusieurs systèmes d'exploitation (dits virtualisés) sur une même machine physique.
27. Wallix AdminBastion Administration Manager

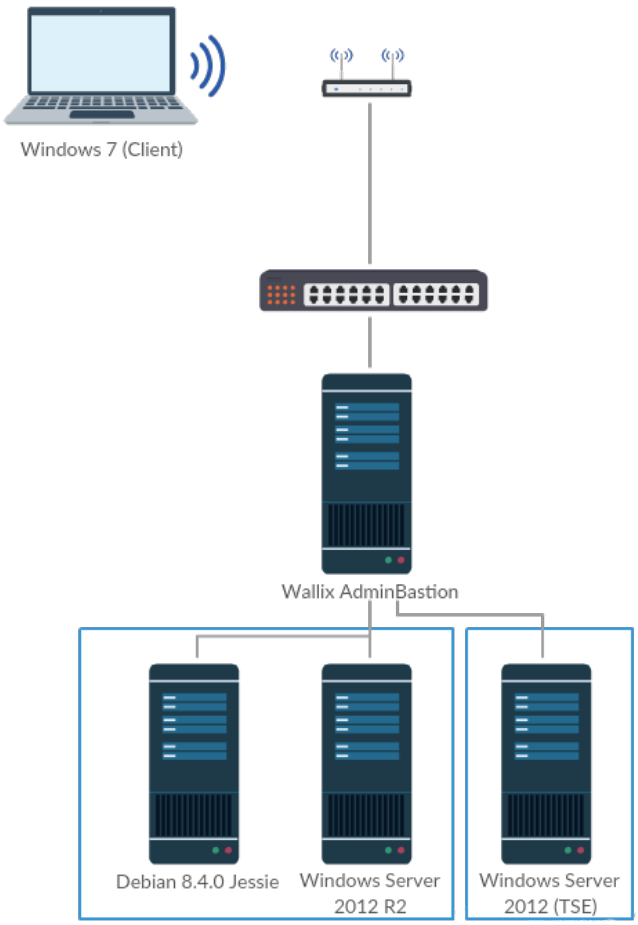

FIGURE 5 – Architecture mise à l'échelle des ressources disponibles chez SYNETIS

WAB Le WAB est le moteur central de gestion des connexions entre les ressources et les utilisateurs. C'est à partir de cette interface que sont gérés (ajout/suppression/modification) les utilisateurs de comptes à privilèges. Le principe de fonctionnement du WAB peut être décomposé en 4 parties :

1. Les comptes utilisateurs, ils peuvent être locaux ou directement importés d'un annuaire LDAP, ce que nous avons fait pour le PoC, avec notre domaine Active Directory.
2. Les ressources, qui fournissent des informations sur la localisation (adresse IP ou FQDN[28]) de cette dernière.
3. Les comptes de ressource, avec les mots de passe qui peuvent être modifiés automatiquement grâce à une extension native ou programmable

28. Fully Qualified Domain Name : nom de domaine complet permettant de cibler une machine ou un équipement

manuellement, qui sont les comptes des ressources précédemment citées.

4. Les autorisations, qui font le lien entre les utilisateurs et les ressources (via leurs compte de ressource).

WABAM Le WABAM est simplement une interface web qui récupère les informations que lui fournit le WAB. C'est une interface complètement personnalisable, sur laquelle se connectent les utilisateurs finaux. Beaucoup plus élégante et destinée aux utilisateurs finaux, elle est en fait une vitrine du WAB. Elle embarque des extensions permettant d'ouvrir une connexion RDP, SSH ou tout autre connexion disponible avec le WAB directement dans le navigateur web. Nous ne nous intéresserons pas plus à cette interface qui n'a pas beaucoup de valeur, autre que son design et la séparation de l'administration des utilisateurs finaux.

2.3.4 Test : Wallix AdminBastion

Une série de tests fonctionnels ont été effectués, des scénarios d'utilisation ont été joués : des connexions d'utilisateurs à des ressources, de toute origine possible et sur un maximum de ressources disponibles (soit du RDP sur Windows, du SSH sur une machine Linux et une application sur un serveur TSE). Seule une anomalie a été relevée : une erreur générée lors de la synchronisation des utilisateurs avec un annuaire Active Directory, le mot de passe pour l'accès à cet annuaire ne peut pas contenir de caractères spéciaux, car l'encodage de la requête ne parvient pas à traiter lesdits caractères. Cependant, l'erreur reste minime et a été signalée au support pour une correction dans une version future.
Par la suite, nous avons recherché des points de faiblesse qui permettraient de mettre la solution en porte-à-faux. Certains points ont été trouvés, mais ces points nécessitent un non-respect des conseils de sécurité proposés par Wallix. Les points de faiblesse sont les suivants :

— Single Point Of Failure [29] : toutes les connexions passent par le WAB, on peut donc imaginer une attaque de type DDoS [30] bloquant le fonctionnement du WAB. Cependant, Wallix conseille d'éviter de mettre en place un système de haute disponibilité (deux machines WAB en parallèle qui traitent les requêtes), mais de plutôt monter un plan de reprise d'activité, qui consiste à conserver un serveur clone inactif en parallèle du premier, qui prendrait le relais en cas de panne et/ou attaque de

29. SPOF : point unique de défaillance, c'est un point unique dont tout le système d'information est dépendant.

30. Distributed Denial of Service : déni de service réparti (ou distribué), est une déni de service entraîné par une énorme masse d'information créant une congestion (le célèbre `ping flood` lancé depuis plusieurs machines est un DDoS).

ce type. Il reste aussi difficile de tenir une telle attaque dans la durée compte tenu de la quantité de ressources nécessaires. Enfin, le WAB ne devant être autorisé de l'extérieur du réseau (pour des prestataires par exemple) que depuis des adresses IP spécifiques, cette nécessité de ressources pour monter une attaque est encore moins envisageable.

— Contournement des routes : nous avons imaginé qu'un utilisateur modifie manuellement sa table de routage pour accéder directement aux ressources. Cependant, cette action nécessite deux prérequis :

  1. Les ressources sont dans le même sous-réseau que les utilisateurs, ce qui est une très mauvaise pratique en terme de sécurité, car il est important de cloisonner les différents types de machines (serveurs/utilisateurs).
  2. Les mots de passe ne sont pas gérés automatiquement par le WAB, mais par des administrateurs, ce qui est totalement à l'opposé du but de l'utilisation d'une solution de PAM.

— Le vol d'une session d'un utilisateur, s'il part, par exemple, en pause et oublie de bloquer sa session. Mais cette faille est une faille humaine à laquelle on ne peut pallier uniquement en sensibilisant le personnel.

2.3.5 Déploiement : Thycotic Secret Server

Encore une fois, l'architecture de l'infrastructure de test a été limitée par les ressources internes. La solution de PAM a dû être déployée sur le contrôleur de domaine Active Directory, ce qui n'est pas conseillé, car Windows Server gère très mal la cohabitation avec le rôle contrôleur de domaine et le rôle Internet Information Services (IIS).
La première tentative d'installation fut infructueuse, sûrement à cause de la machine qui avait déjà été utilisée pour un projet portant sur une autre problématique. Toute l'installation s'est bien déroulée (installation des rôles et sur SQL Server), mais une fois l'installation terminée, il était impossible de joindre le serveur "Secret Server" dans les pools d'application IIS (piscine d'applications). Le problème ne pouvant être résolu, même avec l'aide du support Thycotic, nous avons décidé de repartir de zéro et de formater notre serveur, pour y ré-installer un serveur neuf, sans paramétrage possible générant des erreurs.
Cette seconde installation posa juste un souci avec l'attribution des droits d'exécution, ne fonctionnant pas avec un compte de service[31]. Ce problème

31. A partir de Windows Server 2008 R2, Microsoft à mis en place les MSA (Managed Service Account) afin de déléguer la gestion d'un compte de service à un domaine Active Directory. Ces compte n'ont pas de mot de passe attribué par un administrateur, mais ils sont tout simplement assigné à des machines qui ont le droit de récupérer ce mot de passe d'accès auprès du contrôleur de domaine. Ainsi il peut être modifié régulièrement sans affecter l'utilisation.

était sûrement dû à la cohabitation des rôles de contrôleur de domaine en même temps que le rôle IIS.
Du point de vue du routage, le Secret Server doit être positionné en proxy pour capturer les connexions et pouvoir les surveiller. En étant configuré dans ce mode, il permet d'établir toutes les connexions disponibles (SSH, RDP, Citrix, etc) directement dans le navigateur web.
Cependant, toutes ces configurations sont laborieuses à mettre en place, surtout si l'on a installé le logiciel en français (c'est peut-être aussi le cas pour les autres langues), il est donc plus raisonnable de migrer vers la langue d'origine, l'anglais. La version française est très mal faite car les traductions sont très souvent fausses, il est donc compliqué de retrouver les configurations décrites dans le manuel. Par exemple, « Edit Discovery Sources » traduit en « Editer les Domaines » au lieu de « Editer les sources de découverte », sans parler des erreurs d'orthographe comme « Déconnection » au lieu de « Deconnexion », qui n'influe pas sur la fonctionnalité, mais donne une très mauvaise image du sérieux de l'entreprise.

2.3.6 Test : Thycotic Secret Server

Les tests effectués sur Thycotic Secret Server se sont limités aux tests fonctionnels, qui ont été concluants (lancement d'une session SSH et RDP, visualisation des sessions enregistrées, limitation d'accès, etc). Le gros point négatif que l'on peut noter sur cette solution est le manque d'ergonomie de l'interface : la configuration des *secrets* (autorisations) est simple mais lier ces secrets aux ressources cibles et aux utilisateurs nécessite beaucoup de modifications dans l'interface d'administration, pas forcément faciles à trouver compte tenu du manque d'informations dans les manuels d'utilisateurs et des erreurs de traduction.
On notera aussi le manque de liberté dans l'identification des ressources cibles : celles-ci sont gérées en masse, avec des plages d'IP ou sur des domaines entiers, mais l'on ne peut pas configurer une ressource cible individuellement.

3 Résultats et discussion

Dans cette partie, nous allons discuter des résultats obtenus, pour déterminer s'il y a une solution plus à même de répondre aux besoins d'une entreprise avec laquelle SYNETIS pourrait envisager travailler.

3.1 Des solutions se démarquant par des spécificités

Après avoir travaillé avec les deux différentes solutions (*Wallix* et *Thycotic*), il s'est clairement imposé que celles-ci apportent une approche similaire de la gestion des comptes à privilèges. Cette ressemblance d'utilisation a aussi été pointée lorsque je réalisais les PoC par l'étude de marché produite par l'entreprise de conseil Gartner[32] [4]. Les seuls gros points notables les différenciant sont la haute disponibilité qui n'est pas présente chez *Thycotic*, la gestion des interactions d'application à application absente chez *Wallix* et les formats de licences ne se recoupant que sur la disponibilité en mode « cloud ».
Nous pouvons aussi noter une différence majeure entre ces deux solutions, au niveau des choix technologiques : *Wallix* a choisi de développer sa solution sous Linux, tandis que *Thycotic* s'appuie sur un système Windows Server. Ceci implique une facilité d'installation non-négligeable pour *Wallix*, ne nécessitant pas de configuration préalable car l'ensemble du moteur du bastion est contenu dans la machine virtuelle (ou serveur physique, selon la licence choisie). Cette solution est complète, pour ainsi dire « prête à l'emploi » car il ne reste que la configuration des ressources et utilisateurs à gérer. A l'opposé, *Thycotic* fournit un exécutable à installer sur un serveur Windows, avec plusieurs solutions lourdes[33] à installer au préalable. Cette configuration n'a en l'occurrence pas fonctionné dans notre cas avec un serveur de test, il nous a fallu reprendre une installation from stratch.
Il faut aussi ajouter à cela que l'ensemble de la sécurité de *Secret Server* s'appuie sur la sécurité du système d'exploitation Windows. Etant le plus touché par les attaques et donc le plus susceptible de connaître des failles de sécurité, comme l'ont démontré Sundar ET COLL.[10] sur une faiblesse de Windows Server 2012 R2 (soit la dernière version de Windows Server) face à une attaque de type DDoS (Syn flood[34]).

32. Gartner est une entreprise américaine de conseil et de recherche fondée en 1979. Elle vend des recherches et des analyses dans le domaine des technologies de l'information.
33. Le serveur Windows d'une part, puis Microsoft SQL Server, Microsoft Internet Information Services et .NET Framework pour faire tourner l'interface de la solution.
34. Bombardement de requête TCP SYN

3.2 L'avenir dans le cloud

Selon l'étude de Gartner[4], les besoins de solution de PAM dans le cloud représentent seulement 3% des parts de marché, pour, selon leur estimation, 30% en 2019. Ces chiffres ne sont pas surprenants compte tenu de l'évolution des infrastructures décentralisées, comme le proposent les grands éditeurs comme Microsoft avec la suite *365*, le géant du net Google avec son *Google Enterprise*, Amazon avec l'ensemble de ses solutions qui vont du stockage de données (*Amazon EC2*) au cluster de calcul (*Amazon S3*).
Il est important de noter que cette gestion des comptes à privilèges dans le cloud représente un certain défi, sachant que ces infrastructures ne sont pas maintenues par les entreprises concernées (client final) mais par ces grands éditeurs. On peut alors se poser des questions sur la responsabilité des comptes à privilèges : relève-t-elle du client ou de l'éditeur ?

3.3 Une synergie entre solution de PAM et une fédération d'identité

Un des leaders du marché des solutions de PAM, *Centrify* (voir l'étude de marché menée par Cser [3] pour plus d'informations), propose un produit apportant une synergie entre la gestion des comptes à privilèges et la fédération d'identité[35]. En effet, il semble logique d'intégrer une solution de gestion des comptes à privilèges avec une solution de fédération d'identités, la gestion des utilisateurs en sera facilitée, et l'homogénéité du système offrira une assurance de qualité de service. Cependant, *Centrify* est pour le moment le seul à proposer une telle solution, avec Microsoft et sa solution MIM (Microsoft Identity Manager) qui inclut l'extension PIM (Privileged Identity Manager) gérant les comptes à privilèges avec des groupes Active Directory de sécurité à usage limité dans le temps (*shadow group*, voir l'article de Microsoft Technet [6] pour pus d'informations).

3.4 CamStudio 2.7.4 : expérience personnelle d'attaque par escalade de privilèges

Le poste de travail, qui m'a été fourni durant ce stage, était un ordinateur de dépannage servant pour les nouveaux arrivants à Synetis Rennes. Au bout de quelques mois de stage, j'ai eu une notification douteuse me demandant de mettre à jour un logiciel (Yahoo ! Search) qui n'étais pas installé sur le poste. Avec l'aide de plusieurs collègues, nous avons donc cherché à comprendre d'où venait cette notification, ce qui l'exécutait et quelles actions elle générait.

35. Gestion des accès et supervision des utilisateurs communs, par exemple la gestion des comptes des étudiants à l'université.

Nous avons commencé par suivre le processus avec le gestionnaire de tâches de Windows. Le processus était déclenché par un fichier présent dans le répertoire `AppData`, qui est le répertoire de stockages de données des applications s'exécutant sur Windows. Le fichier ayant lancé le processus (fichier avec une extension .dat) n'existait plus, mais il restait cependant un fichier de logs conséquent (plus de 1000 lignes de logs). Ce fichier nous a donné des informations sur les tentatives d'exécution de code sur la machine, en l'occurrence beaucoup d'ouvertures de shell, infructueuses avec le compte local. Un tel accès pourrait mener à une compromission complète du poste de travail, pouvant se traduire par une destruction du système, ou pire encore, un vol de données. Le vol de données serait le pire des scénario, si l'on tient compte que SYNETIS est un sous-traitant/intégrateur de solution de fédération d'identités pour des grands groupes tels que EDF ou encore des conseils régionaux, détenant ainsi les accès à l'administration de leur infrastructure.
Par la suite, nous avons trouvé comment était exécuté la fenêtre qui apparaissait : c'était une ancienne technologie, un fichier hta exécuté par un moteur de Windows. Ce moteur permet de convertir n'importe quel fichier binaire en page html dans une fenêtre embarquée. Nous avons réussi à trouver où menait le lien présent sur cette fenêtre : vers deux domaines qui ne répondaient pas lorsque l'on essayait de les joindre via un navigateur web. Ceci était sûrement dû à des paramètres traitant la requête sur le serveur n'acceptant que un certain type de requête, par exemple un `user-agent` [36] spécifique.
Après une recherche sur le net, nous avons trouvé un sujet ouvert sur le forum *Reddit* discutant de ce malware, qui s'avère être présent dans une installation du logiciel CamStudio 2.7.4 compromis.
Finalement, la désinstallation de ce logiciel a empêché le malware de nuire. Toutefois, c'est une situation dans laquelle une solution de PAM aurait bloqué le problème à la source, en limitant l'installation d'un tel logiciel, si l'on considère que même l'installation de logiciel sur un poste est géré par les administrateurs de l'entreprise.

3.5 Les bonnes pratiques à intégrer

Même avec une infrastructure sécurisée au plus proche de la perfection, les plus grosses failles restent l'humain. Il est donc important, lors d'un déploiement de solution de PAM de sensibiliser le personnel à certaines bonnes pratiques de sécurité incontournables. Ces pratiques sont détaillées dans une publication faite par le NIST [37] [8].

36. Dans une requête HTML, l'`user-agent` est le type de client lançant la requête, dans notre cas, notre navigateur web, par exemple Mozilla Firefox.

37. National Institute of Standards and Technology : institut national des standards et de la technologie des USA.

3.5.1 Renforcer l'authentification

Comme il a été vu en introduction, l'utilisation de mots de passe faibles, devinables par ingénierie sociale [38], d'algorithmes de hachage faibles, ou un faible chiffrement d'un mot de passe qui serait recouvrable par une *rainbow table* [39].
Pour éviter de rencontrer des infiltrations par ces failles, il est important de mettre en place une politique de renforcement de l'authentification avec :

— Une authentification forte : multi-facteur, au minimum double-facteur, par exemple l'utilisation du couple login/mot de passe et d'une validation avec envoi de SMS sur le téléphone personnel de l'employé. Plusieurs solutions déjà implémentées sont utilisables, comme par exemple *Google Authenticator* ou le MFA de *Microsoft*. Il est aussi possible de mettre en place un système PIV (Personnal Identity Verification, souvent une carte à puce à insérer dans un lecteur).

— Une augmentation des couches de sécurité dans le chiffrement des mots de passe : utilisation d'un algorithme de hachage fort comme le SHA-256 ou AES-256 doublé d'un salage (comme l'explique durant la conférence Blackhat US 2013 Aumasson [1]) de ce hash avec une chaîne aléatoire.

— La mise en place d'une politique de mot de passe forte qui force l'utilisateur à utiliser un mot de passe d'une longueur minimale, avec un nombre minimal de caractères spéciaux, lettres minuscules et majuscules et chiffres. Il est même recommandé d'utiliser un passphrase, qui augmente la taille de la chaîne de caractères, en remplaçant les lettres par des chiffres et des symboles [40].

3.5.2 Minimiser les accès privilégiés

Le but de ce stage étant la gestion des comptes à privilèges, nous avons clairement pu comprendre que le meilleur moyen de limiter les compromissions de système était de limiter au maximum les accès privilégiés. La pratique est donc de commencer par :

— Supprimer les accès des comptes à privilèges qui ne nécessitent plus ce type d'accès (par exemple l'administration de système, réseau ou base de données qui sont des tâches ponctuelles).

— Supprimer ou désactiver tous les comptes à privilèges qui ne sont plus nécessaires (y compris les comptes natifs du système).

38. Deviner le mot de passe d'une personne en se renseignant sur ses habitudes, sa vie et ses relations sociales.
39. Table de correspondance de mots et de leur hash, disponible et utilisable en ligne.
40. Par exemple "4" pour "A", "$" pour "s", etc.

— Supprimer l'excès de privilèges d'un compte en tenant compte du contexte de l'entreprise, plus que celui applicatif.

— Supprimer toutes les permissions inutiles des comptes à privilèges, notamment les commandes non-relatives à l'utilisation de ces comptes.

— Réduire au minimum la durée d'une session privilégiée unique.

— Exiger une re-connexion lorsque cette dernière a expiré.

Conclusion

La gestion des comptes à privilèges, qui ne représentait pas un intérêt énorme il y'a encore quelques années, est aujourd'hui un des piliers centraux de la sécurité des systèmes d'information.
Cette intérêt pour ces comptes vient majoritairement du fait que 80% des failles de sécurité impliquent des credentials privilégiés selon une estimation de Forrester [3]. A cette volonté de combler des failles de sécurité s'ajoute la volonté de valider les audits de sécurité en consultant les activités des comptes à privilèges.
Ce stage m'aura permis de répondre à ce besoin, avec des solutions d'éditeurs, sur lesquelles il ne faut pas entièrement se reposer. Il est important de poser des règles de sécurité à faire respecter pour chacun, afin de limiter les risques, car le risque zéro n'existe jamais. Il est aussi important de noter que ces solutions devront évoluer avec les systèmes d'informations, qui tendent à être de plus en plus délocalisés (dans le cloud), ou bien à réfléchir à la nécessité pour une entreprise de délocaliser son infrastructure, afin de trouver un équilibre entre sécurité et facilité d'utilisation et d'accès.
Ce stage m'aura par ailleurs enrichi au niveau technique en découvrant et me formant sur de nouvelles technologies, tout autant qu'au niveau humain, avec la découverte du travail en équipe dans le monde du service informatique. Il a par la même occasion parachevé ma formation, en mettant en application mes compétences acquises au cours de celle-ci.
J'ai pu découvrir le monde de la sécurité, et la quantité de domaines qu'il comprenait, ce qui me pousse à continuer dans cette voie afin de pouvoir en avoir une vue d'ensemble tout en le maîtrisant.

Références

[1] J-P. Aumasson *Password Hashing : the Future is Now*, Blackhat US 2013, page 2, 2013.

[2] R.Baloch *Ethical Hacking Penetration Testing Guide*, Auerbach Publications ; 1 edition, 531 pages, 2014.

[3] Andreas Cser *The Forrester Wave^{TM} : Privileged Identity Management*, Forrester®, Q3 2016.

[4] Gartner. Consulté le : 10/08/2016. *Market Guide for Privileged Access Management.* Site web. URL : https ://www.gartner.com/technology/media-products/newsletters/beyondtrust/1-3B8FB2Z/gartner.html

[5] hMailServer. Consulté le : 02/08/2016. *Functionality - hMailServer - Free open source email server for Microsoft Windows.* Site web. URL : https ://www.hmailserver.com/functionality

[6] Microsoft Technet. Consulté le : 18/08/2016. *Privileged Access Management pour les services de domaine Active Directory.* Site web. URL : https ://docs.microsoft.com/fr-fr/microsoft-identity-manager/pam/privileged-identity-management-for-active-directory-domain-services

[7] Minasi, Mark, et al. *Mastering Windows Server 2012 R2*, John Wiley & Sons, 2013.

[8] NIST *Best Practices for Privileged User PIV Authentication*, NIST Cybersecurity White Paper, 2016.

[9] Dave Shackleford *Keys to the Kingdom : Monitoring Privileged User Actions for Security and Compliance*, SANS Whitepaper, 2010.

[10] Sundar, Koushicaa and Kumar, Sanjeev *Blue Screen of Death Observed for Microsoft Windows Server 2012 R2 under DDoS Security Attack*, Journal of Information Security, Volume 7, numéro 4, 2016.

[11] James E. Weber, Dennis Guster, Paul Safonov & Mark B. Schmidt, *Weak Password Security : An Empirical Study*, Information Security Journal : A Global Perspective, 17 :1, 45-54, DOI :10.1080/10658980701824432, 2008.

Annexe A : Fonctionnement détaillé des solutions de PAM

Nous détaillerons dans cette annexe, le fonctionnement détaillé d'une solution de PAM. Afin d'illustrer les propos tenus, nous nous appuierons sur des schémas et digrammes de séquences.
Avant d'expliquer le fonctionnement d'une solution de PAM, nous allons voir comment les systèmes fonctionnent en temps normal.

1.6 Sans solution de PAM

Dans ce scénario, les utilisateurs finaux possèdent le mot de passe d'accès direct à la ressource protégée, comme on peut le voir sur la FIGURE 6.

FIGURE 6 – Connexion à une ressource protégée sans solution de PAM

On remarque qu'ici, les utilisateurs accèdent directement aux ressources protégées avec des mots de passe dédiés à chaque service/application/matériel. Il est donc très fréquent car inévitable que des utilisateurs partagent le même mot de passe. De plus, n'ayant aucune fédération (pas de supervision, ni de traçage), l'utilisateur est apte à effacer ses traces, par exemple en vidant les logs des applications et de ses actions [41].
On ne peut donc pas savoir ce que l'utilisateur a fait, ni quel utilisateur a fait des actions sur la ressource cible.
Le diagramme de séquence en FIGURE 7 décrit en détail les action qui se déroulent lors d'une telle connexion. Il permet de aussi de mettre en évidence l'absence de contrôle des utilisateurs : aucun registre d'événements ne prend en compte les actions des utilisateurs. Les utilisateurs se partageant le même mot de passe pour chaque ressource cible, le contrôle n'est ainsi plus mis sur

41. Par exemple sous Debian 8, la commande `cat /dev/null > /.bash_history && history -c && exit` supprime toute action effectuée sur la machine avec le compte courant.

les utilisateurs, mais sur les ressources cibles, ce qui est l'opposé de ce que nous cherchons à faire. La FIGURE 8 schématise cette inversion du contrôle.

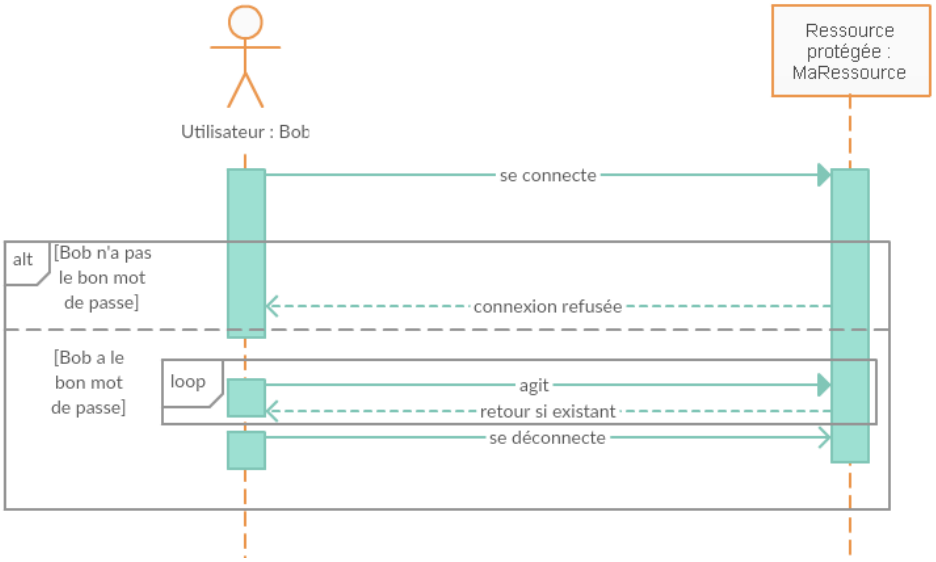

FIGURE 7 – Diagramme de séquence détaillant les actions effectuées lors d'une connexion à une ressource sans solution de PAM

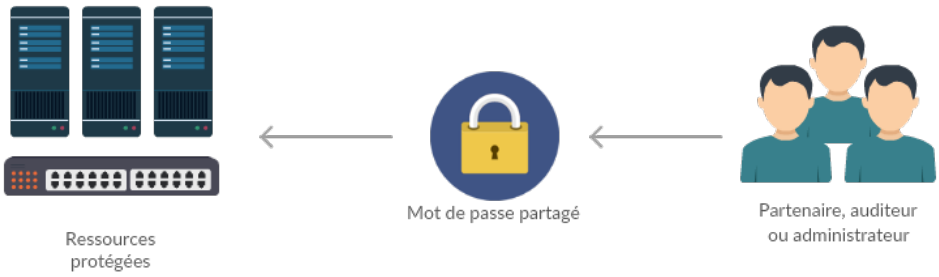

FIGURE 8 – Schéma mettant en évidence l'inversion du contrôle de sécurité, mis sur les ressources plutôt que sur les utilisateurs

1.7 Avec solution de PAM

Dans ce scénario, une solution de PAM est en place. Ainsi les utilisateurs n'ont pas d'accès direct aux ressources cible. Toute l'architecture s'articule autour d'un composant central : le contrôleur d'accès appelé bastion. Tout accès à une ressource cible se fait via ce bastion. Cette architecture centralisée est schématisée dans la FIGURE 9. Nous allons reprendre point par point un

scénarion de connexion réussie à une ressource cible (en correspondance avec les étapes de la FIGURE 9).

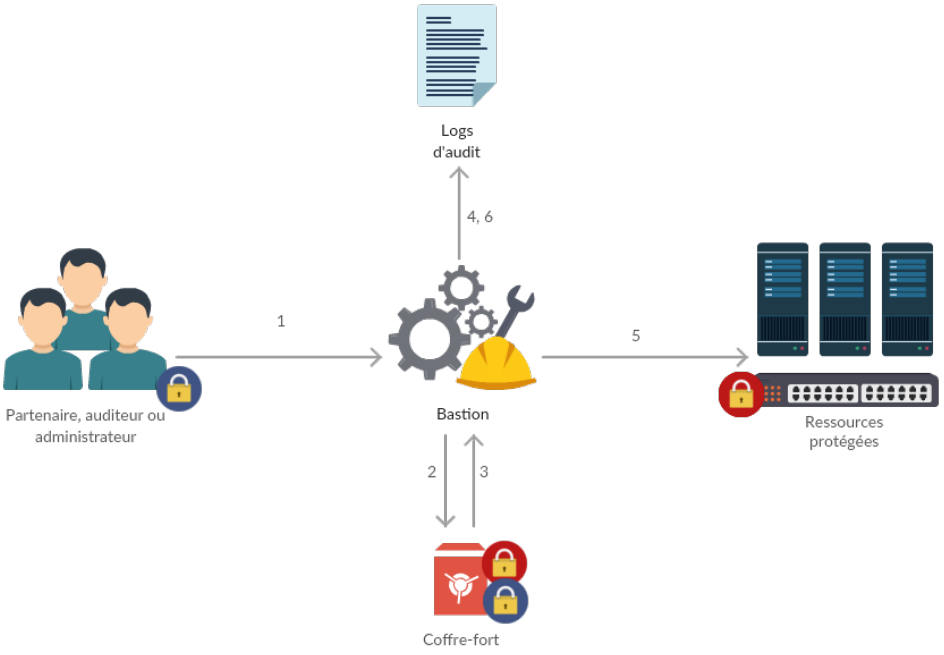

FIGURE 9 – Schéma décrivant l'architecture d'une solution de PAM intégrée dans une infrastructure

1. L'utilisateur se connecte au bastion avec ses credentials, que l'on appellera ses accès primaires (cadenas bleu)
2. Le bastion vérifie l'identité de l'utilisateur en interrogeant le base de données du coffre-fort
3. Le coffre-fort retourne un jeton, qu'on appellera accès secondaire (cadenas rouge), pour se connecter à la ressource cible si l'identification primaire est bonne
4. Le bastion génère des logs de connexion
5. L'utilisateur se connecte à la ressource protégée via la bastion qui lui fournit les accès secondaires
6. Chaque action de l'utilisateur est logué par le bastion, tout comportement interdit alerté voir coupe la connexion à la ressource

Afin de détailler toutes les actions effectuées, nous allons décrire chaque étape, pour tous les cas d'utilisation, dans le diagramme de séquence en FIGURE 1.7.

Pour ne pas nous égarer dans les explications, les diagramme sera expliqué dans son fonctionnement intrinsèque.

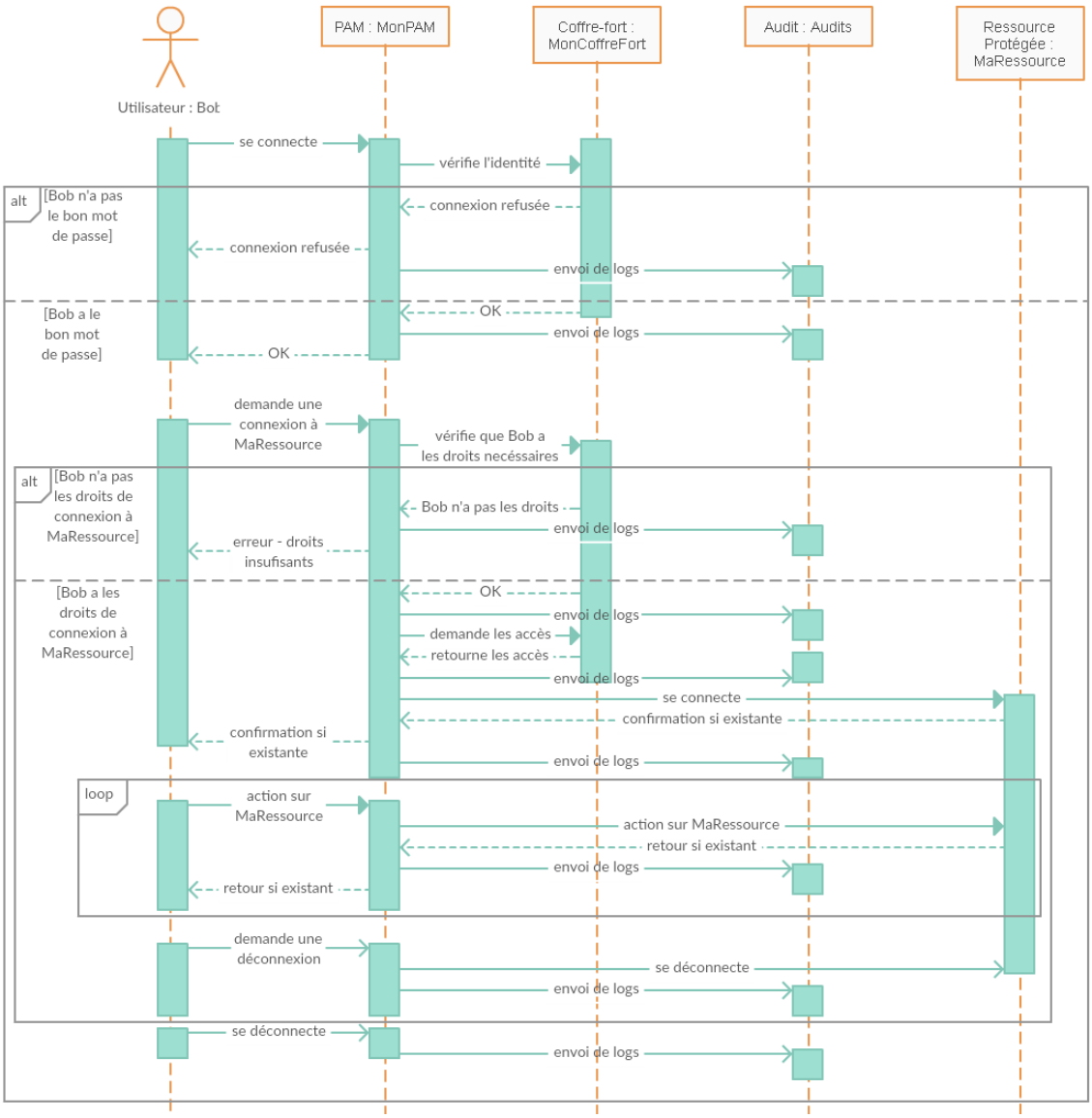

FIGURE 10 – Diagramme de séquence détaillant les actions effectuées lors d'une connexion à une ressource avec une solution de PAM

— Chaque ligne verticale représente un objet ou un utilisateur. Les utilisateurs sont représentés par un bonhomme, les objet par des cases

— Plus l'on descend sur ces lignes verticales, plus l'on avance dans le temps

— Les cadres représentent des boucles ou des conditions :

→ `alt` : condition "si", la condition est explicitée en haut à gauche, les deux possibilités sont séparées par une ligne discontinue

→ `loop` : boucle qui tourne de 0 à N fois, N étant un entier naturel

— Chaque rectangle sur une ligne de temps (ligne verticale) représente une séquence d'actions

— Les flèches représentent des messages qui peuvent être :

→ Asynchrones (n'attendent pas de retour) : flèches simples

→ Synchrone (requête et réponse) : pour la requête, flèche simple avec le bout plein (triangle), pour la réponse, flèche en pointillés

On peut alors voir 4 étapes :

1. Une étape de connexion de l'utilisateur au bastion avec ses accès primaires (qui aboutit ou pas selon la légitimité de l'utilisateur)
2. Une étape de connexion de l'utilisateur à le ressource cible avec des accès secondaires fournis par le bastion (via le coffre-fort)
3. Une étape d'actions sur le ressource cible
4. Une dernière étape de déconnexion

Durant toute ces étapes, des logs sont envoyés par le bastion, afin de conserver toutes les traces des actions effectuées par l'utilisateur. On peut alors clairement faire la différence avec la présence d'une solution de PAM :

— Les utilisateurs sont suivis individuellement

— Chaque utilisateur est identifiable

— L'accès aux ressources cibles n'est pas direct, ce qui ajoute une couche de sécurité

— L'utilisateur utilisant un jeton (accès secondaire) pour se connecter aux ressources cibles, il n'a donc plus besoin de connaître ces mots de passe secondaires. Ils peuvent donc être changés périodiquement pour rendre la connexion sans solution de PAM impossible

Annexe B : Extrait de l'état de l'art au format docx produit pour Synetis

Table des matières

Résumé La gestion des comptes à privilèges est un domaine clef de la gestion d'accès et d'identité. Elle permet de suivre et journaliser les activités des comptes ayant des droits élevés comme `root` sur Linux/UNIX ou `Administrateur` sur Windows. Cette gestion permet ainsi de retrouver une erreur de configuration ayant entrainé une perturbation des services, de prévenir les intrusions par escalade de privilèges sur les système et de suivre d'éventuels prestataires de service dans un grand groupe (sous-traitance de la maintenance d'un service). Les solutions commerciales offrent différentes approches de la problématique des comptes à privilèges. Ce stage a donc fait l'objet d'une étude de ces différentes solutions, de leurs fonctionnalités et de leur fonctionnement. Cette étude a permis de faire ressortir 3 produits, Wallix AdminBastion, CyberArk Privileged Access Security Solution et Thycotic Secret Server, pour finalement en déployer 2 dans un environnement de test virtualisé. Cette mise en situation nous a permis d'aller plus en profondeur dans la compréhension du fonctionnement de la gestion des comptes à privilèges, des points traités et des points nécessitant des traitement supplémentaires à la diminution des risques des comptes à privilèges.

Mots-clefs :

sécurité, privilèges, compte, supervision, gestion

Abstract The management of privileged accounts is a key area of access and identity management. It can track and log activity of accounts with elevated privileges such as `root` on Linux/UNIX or Windows `Administrator`. This allows to recover a misconfiguration that caused a disruption of services, prevent intrusions by escalating privileges on the system, and monitor potential service providers in a large groups (outsourcing of maintenance service). Commercial solutions offer different approaches to the problem of privileged accounts. This internship has been the subject of a study of these different solutions, their functionalities and operation. This study allowed us to highlight three products : Wallix AdminBastion, CyberArk Privileged Access Security Solution and Thycotic Secret Server, to finally deploy in 2 proof of concept. This development has allowed us to go further in understanding the operation of the management of privileged accounts, treaties points and points requiring additional treatment to lower risk on privileges accounts.

Keywords :

security, privileges, account, monitoring, management