Rapport de stage

Intégration de la sécurité dans les projets

CHOUIPE Thibault

Période de stage : de Mars 2019 à Septembre 2019

Tuteur de stage : M. Fréderic HOUNGUE

Superviseur académique / Enseignant référant : M. Louis GOUBIN

Etablissement / Formation : Université de Versailles Saint-Quentin-En-Yvelines – Master SeCReTS

Entreprise d'accueil : Davidson Consulting (Paris)

Table des matières

Remerciement

Un grand merci à toute l'équipe pédagogique de l'université de Versailles Saint-Quentin-En-Yvelines pour l'enseignement dispensé pendant ces deux ans de Master de sécurité des contenus, des réseaux, des télécommunications et des systèmes.

Je tiens à remercier tout particulièrement mon tuteur Fréderic HOUNGUE, pour sa disponibilité, sa compréhension et ses conseils, qui ont pu faire de ce stage au sein de Davidson Consulting, une expérience à la fois épanouissante et enrichissante.

Je remercie également toute l'équipe NSA (Network Security Architecture) pour leur accueil et leur esprit d'équipe qui m'ont permis de comprendre de nombreuses problématiques liées à notre activité.

Enfin je tiens à remercier Lucas PEREZ de m'avoir fait confiance et permis d'intégrer Davidson Consulting.

Glossaire

AD	Active Directory
CDR	Cahier De Raccordement
CPM	Central Policy Manager
GDH	Gestion Des Habilitations
GPO	Global Policy
GPL	General Public Licence
HW	Hardware
IAS	Ingénieur Accompagnement Projet
ISP	Intégration de la Sécurité dans les Projet
LPM	Loi de Programmation Militaire
MOA	Maitrise d'Ouvrage
MOE	Maitrise d'œuvre
NSA	Network Security Architecture
OIV	Organisme d'Importance Vitale
RFQ	Request For Quotation
RGPD	Règlement Générale sur la Protection des Données
SIIV	Système d'Information d'Importance Vitale
SI	Système d'information
SIEM	Security Information and Event Management
SOC	Security Operations Center
SW	Software
SSR	Spécifications Sécurité Réseaux
TMA	Tierce Maintenance Applicative
TTI	Transport Technique IP
VBA	Visual Basic for Application

Liste des figures

Liste des Tableaux

Introduction

Notre société subit une révolution numérique depuis maintenant de nombreuses années. La place de l'informatique dans notre société augmente chaque jour et rares sont les domaines qui ne sont pas impactés par cette révolution. Plus de la moitié de la population est connectée à internet, cela implique une augmentation considérable des objets connectés avec des utilisateurs souvent peu documentés sur leurs fonctionnements et les risques liés à leurs utilisations. Dans un même temps, la quantité de données sensibles circulant sur Internet croit fortement. Cette transformation numérique augmentant la surface d'attaque disponible, le nombre d'attaques informatiques n'a par conséquent, cessé de croitre durant les 20 dernières années.

Dans le cadre de mon master SeCReTS (Sécurité de Contenus, des Réseaux, des Télécommunications et des Systèmes) à l'Université de Versailles St-Quentin-En-Yvelines, j'ai souhaité réaliser mon stage dans une entreprise qui répond à ce besoin grandissant de sécuriser les systèmes informatiques. La mission proposée par Davidson m'a particulièrement attirée car le rôle transversal qui nous est confié nous permet de voir sous différents angles la cybersécurité appliquée en entreprise. De plus, le client est Bouygues Télécom, ce stage m'a donc permis d'appliquer mes connaissances à un contexte centré sur le réseau et les télécommunications.

Ce rapport de stage se divisera en plusieurs parties : dans un premier temps, je décrirai l'entreprise Davidson Consulting ainsi que le contexte du stage. Dans un second temps, je présenterai l'activité d'un Ingénieur Accompagnement Sécurité (IAS), c'est-à-dire l'intégration de la sécurité dans les projets, puis je présenterai un outil développé pour faciliter le travail du consultant cybersécurité dans la réalisation de certaines tâches.

I _ Description du cadre de travail

I-1 _ Présentation de l'entreprise : DAVIDSON CONSULTING

Davidson Consulting est une société créée en 2005 qui regroupe des jeunes entreprises à taille humaine qui sont spécialisées dans le conseil en management de projet et l'expertise technologique. Elle est présente sur différents secteurs d'activités qui peuvent être regroupés en deux grands pôles : Télécommunications-Multimédia et Industrie. Elle est aujourd'hui présente dans 8 pays différents et regroupe 25 sociétés pour un effectif total de 2600 consultants. Elle agit sur les cinq domaines d'activités suivants : big data, cloud et virtualisation, business intelligence, software factory et cybersécurité.

Cette entreprise a décidé de centrer son expansion autour de valeurs fortes comme le développement personnel de ses employés afin de se différencier de ses concurrents. Elle est arrivée 3 fois première au classement GPTW (Great Place To Work) de 2014 à 2018. Elle a également obtenu la certification ISO 9001 ainsi que la certification B-Corp (qui garantit un engagement environnemental et sociétale).

I-2 _ Contexte du stage

Dans le cadre de ce stage, j'ai occupé un poste d'Ingénieur Accompagnateur Sécurité (IAS) pour le compte du client Bouygues Telecom au sein de l'équipe NSA (Network Security Architecture). Cette entité est constituée de 6 consultants en cybersécurité. Ces consultants travaillent au sein du Département TTI (technique du service IP et transport) de Bouygues Télécom et sont chargés de l'Intégration de la Sécurité dans les Projets (ISP). L'objectif de l'ISP dans ce département est de s'assurer que tous les actifs (équipements, applications, ...) qui doivent entrer dans le réseau de Bouygues Télécom sont conformes à sa politique de sécurité réseau. De plus, le consultant s'assure que toutes les données manipulées respectent les lois et réglementations définies par les autorités compétentes (ANSSI, CNIL, ...), notamment la LPM, les réglementations sur les OIV (Organisme d'Importance Vitale), SIIV (Système d'Information d'Importance Vitale) et la RGPD (Régulation Générale sur la Protection des Données).

I-3 _ Objectifs du stage

Dans le cadre de ce stage, différentes missions sur l'accompagnement projet en sécurité étaient à ma charge :

- Garantir la conformité avec la Politique de Sécurité Réseau du client ;
- Formuler des recommandations et des préconisations de sécurité et s'assurer de leurs prises en compte ;

- Raccorder les actifs aux servitudes de sécurité (SIEM, coffre-fort, authentification unifiée, rebond, ...) ;
- Identifier et gérer les non-conformités, ainsi que les risques inhérents à celles-ci ;
- Piloter la mise en place des accès distants dans les cas TMA (Tierce Maintenance Applicative) ;
- Sensibiliser les parties prenantes aux enjeux de la sécurité du réseau ;
- Analyser les rapports du scanneur de vulnérabilités ;
- Automatiser les tâches et processus.

II _ Intégration de la Sécurité dans les Projets (ISP)

Tout actif, équipement ou application, qui doit rentrer dans le réseau du client doit être conforme à la Politique de Sécurité Réseau définie au préalable afin de répondre aux objectifs techniques de sécurité suivants :

Figure 1 : Objectifs de sécurité exigés dans chaque projet

Ainsi, l'Ingénieur Accompagnement Sécurité (IAS) a la charge d'intégrer la sécurité tout au long des projets, depuis leur conception jusqu'à la mise en service. Il s'assure que les contraintes techniques de disponibilité, d'intégrité, de confidentialité et de traçabilité sont garanties par les actifs de chaque projet.

Dans cette démarche, l'IAS a la responsabilité de :

- Définir les exigences de sécurité à inclure dans les appels d'offre ou dans les documents de spécifications dans le cas de développements internes ou encore pour les paliers logiciels ;
- Réaliser les analyses de risques sécurité pour les projets sensibles ;
- Effectuer les revues de conformité des réponses des fournisseurs ou des contributeurs internes ;
- Contribuer à la matrice de flux globale du projet ;
- Rédiger le cahier de tests et de raccordements et contribuer au cahier de durcissement ;
- Réaliser les livrables de sécurité devant être produits dans le cadre de la démarche ISP 2.0

II-1 _ Définir les exigences de sécurité à inclure dans les appels d'offre ou les développements internes

L'ingénieur Accompagnement Sécurité a pour fonction de définir toutes les exigences sécurité que doivent remplir tous les équipements ou toutes les applications qui vont intégrer le réseau. Ces exigences sont alors consignées dans un document appelé Spécifications Sécurité Réseau (SSR) qui définit un cadre contractuel avec les partenaires. Ainsi, toutes les exigences sur les protocoles de communication autorisés ou non y sont consignées, ainsi que l'ensemble des exigences sur la gestion des comptes et privilèges.

De même, les exigences relatives à la gestion et le traitement des données sensibles sont définies en s'appuyant sur un document interne de Bouygues Télécom appelé Politique Générale sur la Sécurité des Données (PGSD). Par conséquent, l'Ingénieur Accompagnement Sécurité s'assure que :

- Aucune donnée secrète (clé, mot de passe, etc.), personnelle (secrets clients, données privées clients telles que les données bancaires), sensible ou privée ne peut transiter sur un canal non chiffré.
- Aucune donnée secrète (clé, mot de passe, etc.), sensible (données de communication) ou privée ne peut être transmise ni stockée en clair.
- Toute manipulation des données est tracée.
- En fin de vie, ou en cas de réutilisation de matériels et/ou logiciels d'un fournisseur ayant hébergé des données sensibles du client, celles-ci doivent être effacées avec des moyens garantissant un effacement logique non réversible ou bien par la destruction physique desdits matériels et/ou logiciels.

Ce document de Spécification de Sécurité Réseau est transmis à tout fournisseur afin d'évaluer son niveau de conformité aux exigences de sécurité.

II-2 _ Réaliser les analyses de risques sécurité pour les projets sensibles

En fonction de la sensibilité du projet une analyse de risque peut être requise. L'objectif de ces analyses de risques est de s'assurer que les principales fonctions de sécurité sont garanties : disponibilité, intégrité, confidentialité et traçabilité. Ainsi, ces analyses permettent d'identifier les menaces qui pourraient peser sur les actifs afin de déterminer l'impact et la vraisemblance de ces menaces. Une fois les risques identifiés et mis en évidence, des mesures de traitement appropriées sont préconisés par l'IAS dans l'optique de les réduire. A l'issu de ce traitement, un risque identifié peut être accepté, refusé, transféré ou réduit (ramené à un niveau acceptable).

Les analyses de risques se font en suivant la méthode EBIOS ou la norme iso 27005. Ainsi, le processus de gestion des risques peut être représenté graphiquement par le schéma suivant :

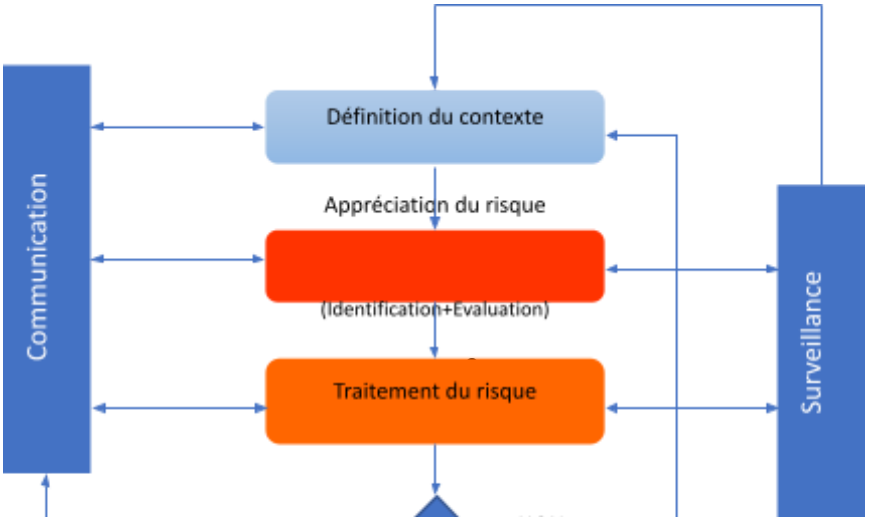


Figure 2 : Processus de gestion des risques de sécurité

II-3 _ Effectuer les revues de conformité des réponses des fournisseurs ou contributeurs internes

Les exigences de sécurité définies par l'IAS sont transmises aux différents fournisseurs afin d'évaluer leur niveau de conformité. En effet, la matrice de conformité qui reprend chaque point de la SSR, permet d'avoir une vue objective sur la conformité des offres des fournisseurs en cas d'appel d'offre pour un projet.

	SPECIFICATIONS DE SECURITE				
	Exigences	C	PC	NC	Commentaires
PLAN D' ECHANGE DOCUMENTAIRE	**Matrice de conformité**				
	MSCVA-1.6-1				
	Matrice de flux				
	MSCVA-1.6-2				
	MSCVA-1.6-3				
	MSCVA-1.6-4				
	Cahier de durcissement				
	MSCVA-2.4-1				
	MSCVA-2.4-2				
	MSCVA-2.4-3				
	Cahier de tests				
	MSCVA-7.1				
	MSCVA-7.2				
CONTROLE DES ACCES LOGIQUES	**Comptes**				
	HR-1.1-1				
	HR-1.1-2				
	HR-1.1-3				
	HR-1.1-4				
	HR-9.2-1				
	HR-3.3-1				
	HR-9.2				

Figure 3 : Extrait de la matrice de conformité v5.9.2 de Bouygues Telecom

Ce tableau permet d'établir en amont de façon précise, sur quoi le fournisseur s'engage à être conforme, partiellement conforme ou non conforme. C'est un document qui sert de référence pendant tout le projet. En cas de non-conformité partielle ou de non-conformité, le fournisseur doit mentionner dans la case commentaire les raisons détaillées de celle-ci.

Pour avoir des informations sur une exigence en particulier, on peut se référer aux spécifications de sécurité réseaux (SSR) qui décline en détails chaque exigence auxquelles doivent se conformer les fournisseurs de Bouygues Telecom (voir extrait sur la page suivante).

3. CONTROLE DES ACCES LOGIQUES

3.1. COMPTES

HR-1.1-1
Si des comptes locaux sont créés sur les matériels et/ou Logiciels du Fournisseur, aucun compte générique ne doit être utilisé.

Plus précisément, chaque individu accédant à des ressources informatiques ou réseaux doit disposer d'un compte qui est :

- Soit un compte nominatif et personnel, utilisé uniquement par cet individu pendant toute la durée de vie du compte ;
- Soit un compte individualisé, attribué à des individus différents pendant la durée de vie du compte, tout en garantissant l'unicité de son attribution.

HR-1.1-2
Si des comptes individualisés locaux sont créés sur les matériels et/ou Logiciels du Fournisseur, ce dernier doit prendre en charge le processus d'individualisation, sans que Bouygues Télécom n'ait connaissance de l'identité réelle de l'individu concerné.

HR-1.1-3
Si des comptes individualisés locaux sont créés sur les matériels et/ou Logiciels du Fournisseur, ce dernier doit mettre en place des moyens non contournables garantissant de pouvoir corréler, sans ambiguïté, les actions (réalisées avec chaque compte individualisé) et les auteurs de ces dernières.

En cas de nécessité (législatif, réglementaire, malveillance, etc.), le Fournisseur doit être en mesure de révéler l'identité réelle de la personne utilisant un compte individualisé à un instant donné ainsi que les actions réalisées.

Figure 4 : Extrait des spécifications de sécurité réseau v5.9.2 de Bouygues Telecom

Après avoir reçu la matrice de conformité complétée par le fournisseur, on réalise ensuite une analyse afin de pouvoir challenger le fournisseur sur les non conformités. Il y a alors un dialogue entre le fournisseur et un IAS afin de discuter ensemble des possibles évolution de cette matrice. Par la suite, on réalise une analyse de risque afin de savoir quelles sont les non-conformités restantes qui sont critiques. On conclut avec un slide sécurité qu'on transmet au chef de projet.

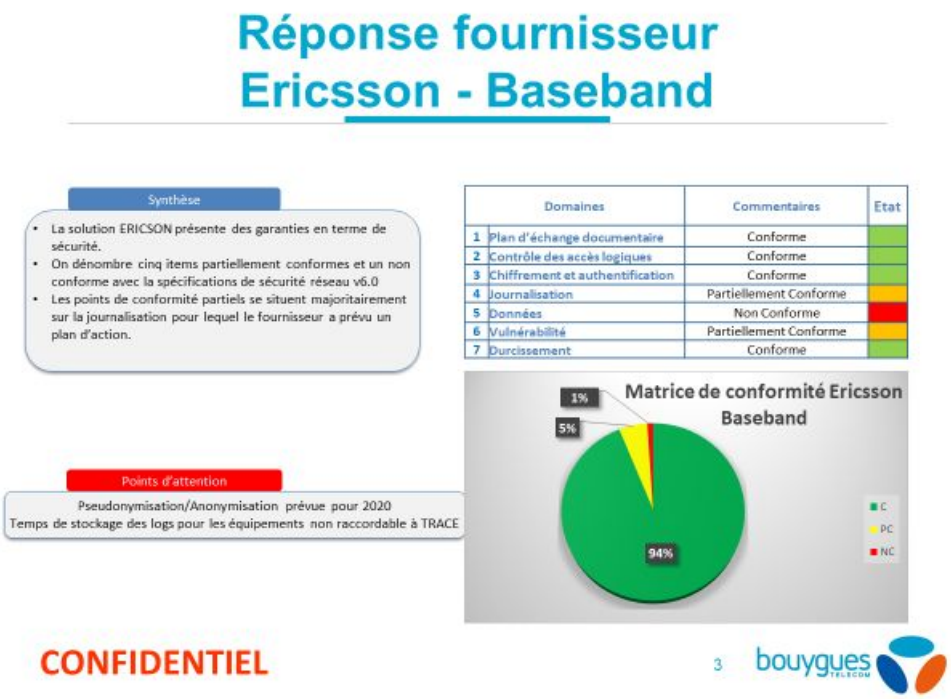


Figure 5 : Extrait d'un slide de sécurité pour le fournisseur Ericsson

II-4 _ Contribution à la matrice de flux global du projet

L'IAS contribue à l'architecture réseau globale d'un projet. En effet, dans l'optique de maintenir le réseau dans un état de conformité optimal, tous les actifs (équipements, applications, ...) doivent être raccordés à de multiples solutions de sécurité réseau (Firewall, SIEM, ...). Pour ce faire, des flux de communications doivent être ouverts entre les actifs qui intègrent le réseau et les différents équipements de sécurité réseau. Ainsi, la matrice de flux globale du projet doit prendre en compte les flux sécurité définissant les adresses IP source et destination, les ports et protocoles supportés.

II-5 _ Rédiger le cahier de test, de raccordement et contribuer au cahier de durcissement.

L'IAS rédige le cahier des tests à effectuer une fois la solution mise en production, afin de s'assurer de sa conformité à la PSR (Politique de Sécurité Réseau). De même, l'IAS a la responsabilité de produire le cahier définissant tous les protocoles et configurations à effectuer pour le raccordement des actifs aux plateformes de sécurité. Ce document est appelé cahier de raccordement (CDR) et est expliqué en détail un peu plus loin dans ce rapport.

Enfin, l'IAS doit contribuer à la rédaction du cahier de durcissement qui reprend obligatoirement les trois éléments suivants :

- Les mesures employées garantissant un niveau de minimalisation, sur les matériels et/ou logiciels du fournisseur, en adéquation avec la matrice de flux,
- Les mesures de sécurité appliquées sur les matériels et/ou logiciel du fournisseur,
- Les ACL et/ou les règles firewall configurées sur les matériels et/ou logiciels du fournisseur, en adéquation avec la matrice de flux.

II-6 _ Réaliser les livrables de sécurité devant être produits

L'IAS doit produire un certain nombre de livrables à chaque étape du processus d'ISP à savoir :

- Annexe de sécurité générique (SSR) et spécifique,
- Matrice de conformité,
- Le slide de sécurité,
- Le cahier de raccordements,
- Le cahier de tests sécurité générique et spécifique,
- Le cahier de durcissement,
- L'analyse de scans de début et de fin,
- L'analyse de risques,
- Le dossier de passation avec la préproduction et l'exploitation.

Le processus d'intégration de la sécurité dans les projets peut être représenté schématiquement par la figure suivante :

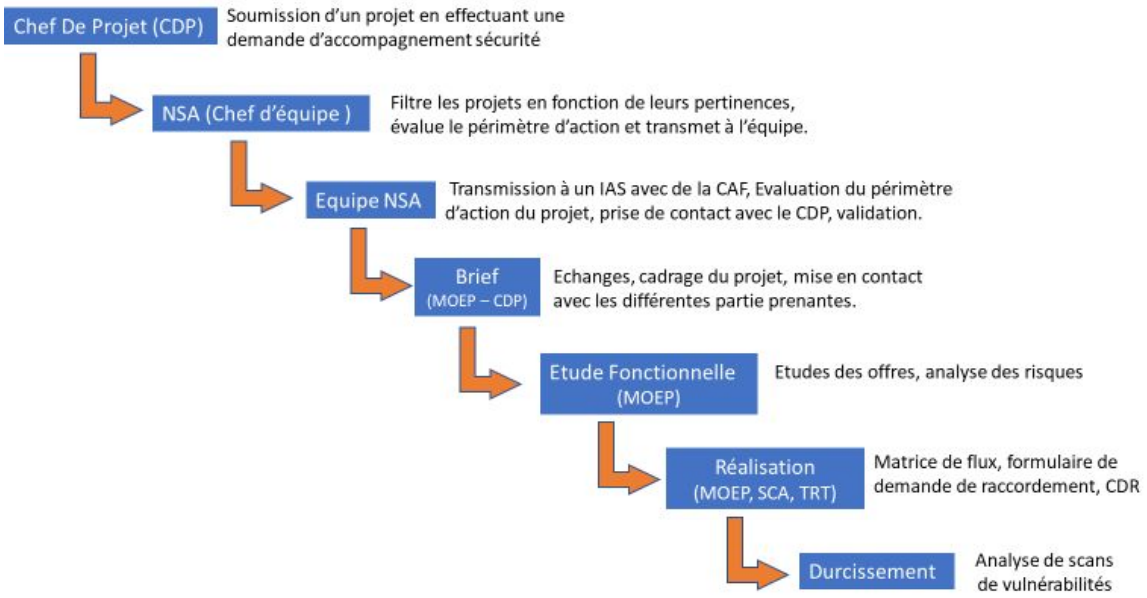


Figure 6 : Schéma représentatif du processus de l'ISP

III _ Raccordement des actifs aux plateformes de sécurité

III-1 _ Objectifs du raccordement

Tous les actifs (équipement ou application) qui rentrent dans le réseau du client doivent être raccordés aux servitudes de sécurité. Ces servitudes permettent de manager l'actif et de le monitorer / surveiller afin de s'assurer qu'il n'introduit pas dans le réseau un risque non maîtrisé et par conséquent que la politique de sécurité réseau (PSR) est respectée.

III-2 _ Les plateformes de sécurité

Les plateformes de sécurité (PFS) sont l'ensemble des infrastructures de sécurité mises en place pour assurer la gestion des accès aux ressources, le monitoring de tous les actifs du réseau (équipements et applications) et la protection contre les logiciels malveillants (vers, virus informatiques, ...). Nous disposons à cet effet des plateformes de sécurité suivantes :

- L'authentification Unifiée (AD),
- Le rebond (Balabit),
- Le coffre-fort de mots de passe (CyberArk),
- Le collecteur de logs (QRadar),
- Le scanneur de vulnérabilités (Nessus),
- La plateforme d'antivirus pour les systèmes Windows (McAfee).

III-3 _ La plateforme d'authentification unifiée

L'Authentification Unifiée (AU) est une infrastructure globale de sécurité qui assure le contrôle des identités et l'application de la GPO (Global POlicy). L'AU est constituée des systèmes Active Directory et d'ACS pour les équipements Cisco. Elle supporte les protocoles suivants : Kerberos (QAS pour les systèmes UNIX/Linux), Tacacs+, Radius, LDAP. Ces protocoles ne sont pas tous utilisés simultanément, mais en fonction des différents cas d'usage :

- Système Windows : le raccordement utilise le protocole Kerberos,
- Système Unix supportant QAS : le Quest Authentication Services, logiciel qui permet de rendre compatible un système Linux à l'Active Directory,
- Autres systèmes d'exploitation (Appliance ou système Unix ne supportant pas l'agent QAS) : les protocoles supportés pour le raccordement à l'AD dans ce cas sont Tacacs+, Radius et LDAP. Ces protocoles sont également utilisés pour raccorder à l'AD toute application installée sur le système d'exploitation.

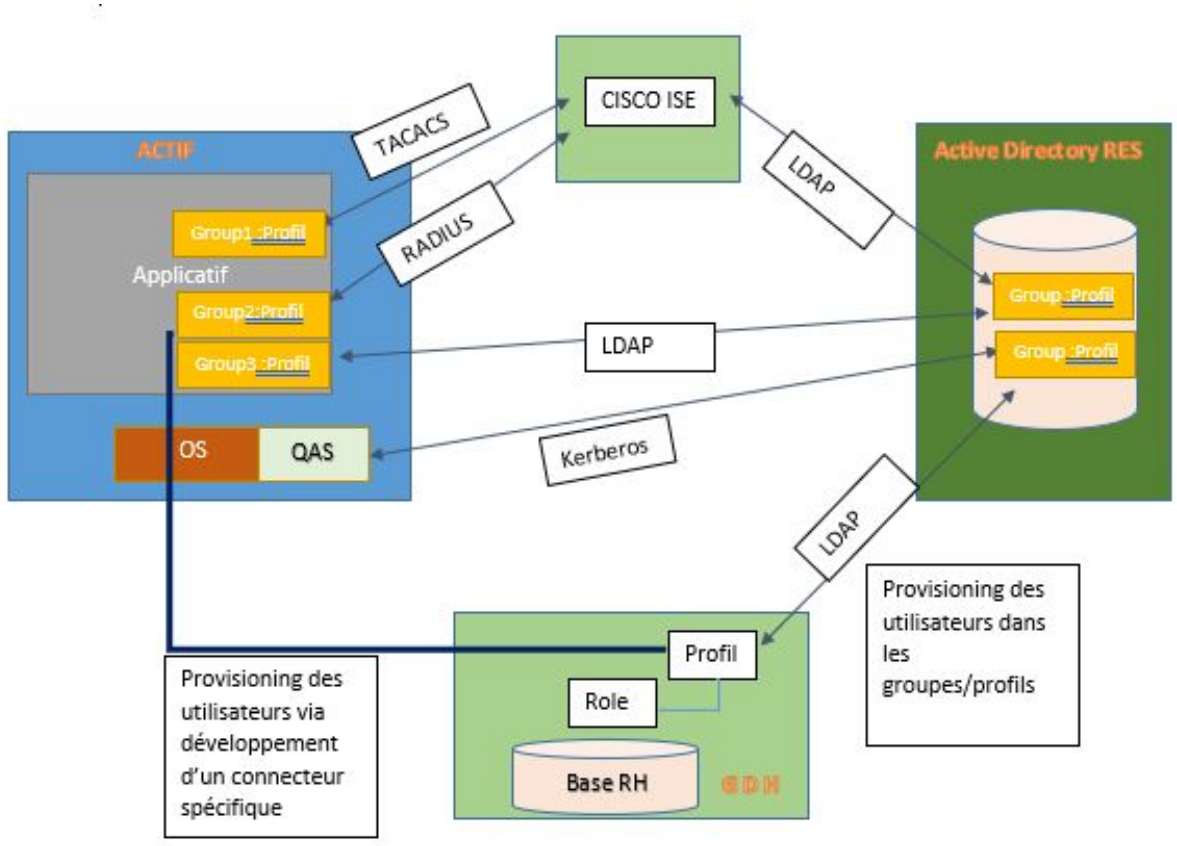


Figure 7 : Principe de raccordement à l'authentification unifiée

III-4 _ La plateforme de rebond

La plateforme de rebond repose sur une infrastructure Balabit. Il s'agit d'une solution de sécurité qui permet de contrôler (qui accède et où) et tracer (enregistrer) les sessions d'administration des équipements du périmètre réseau. Ces sessions peuvent à la fois provenir d'administrateurs externes (TMA, prestataires, ...) et d'administrateurs internes (prestataires ou non) c'est-à-dire situés dans les locaux de l'entreprise. Ainsi, le système rebond sert de passerelle d'accès aux systèmes cibles à la fois pour les accès externes (TMA) et les accès internes (postes bureautiques internes).

La solution rebond permet également de faire des investigations en cas d'incident sécurité par des recherches de mots clés dans les sessions enregistrées.

La plateforme rebond gère plusieurs protocoles d'accès aux équipements cibles à savoir : SSH, SFTP, RDP, HTTP/S, ICA, X11, TELNET, ICA, FTP.

Selon les contraintes techniques des équipements cibles et leur niveau de criticité, nous avons plusieurs modes d'accès :

- Accès via le compte AD réseau.
- Accès via le compte local nominatif ou générique,
- Accès via le compte local avec Credential Store (coffre-fort de mot de passe).

La figure suivante représente le principe de fonctionnement du rebond :

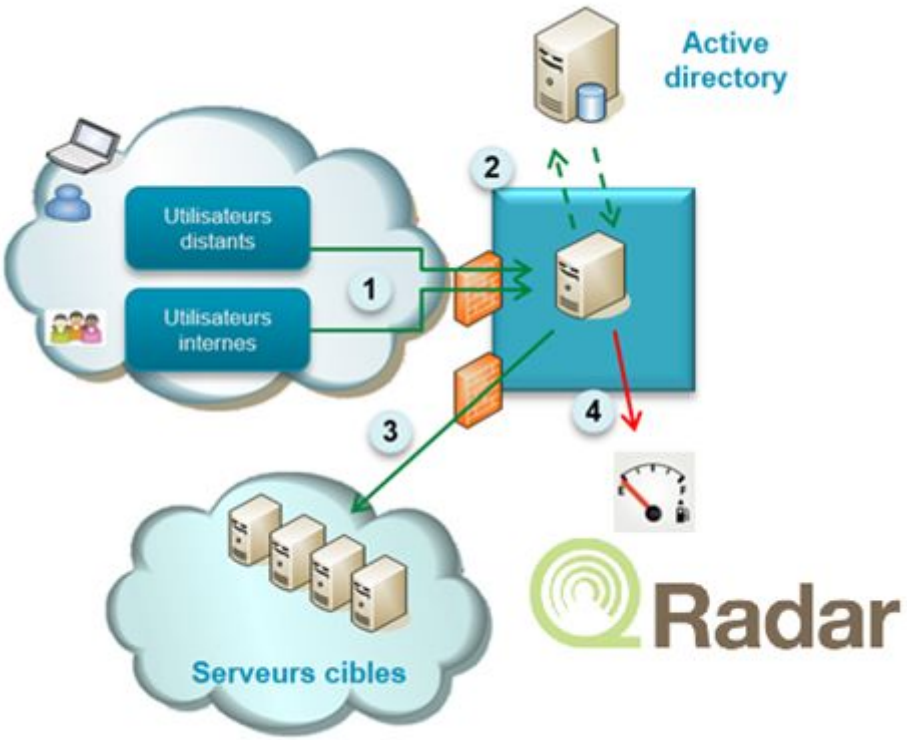


Figure 8 : Schéma du fonctionnement du rebond

1) Connexion de tout utilisateur (interne ou externe) voulant accéder à des serveurs cibles du réseau.
2) Le rebond vérifie que l'utilisateur est bien habilité à accéder aux serveurs cibles en consultant l'annuaire Active Directory.
3) L'utilisateur est connecté aux serveurs s'il possède les droits nécessaires.
4) La session est enregistrée.

III-5 _ Le coffre-fort de mot de passe

Le coffre-fort de mot de passe est basé sur une architecture CyberArk. Il permet de protéger, d'administrer et d'effectuer des changements automatiques des mots de passe d'accès privilégiés. Cette solution crée un point de centralisation pour les entreprises afin d'une part d'optimiser les

mises à jour, et d'autre part d'améliorer la maintenance et de garantir le respect des réglementations. En effet, le coffre-fort de mot de passe permet d'avoir une traçabilité des actions menées par les administrateurs et assure un changement régulier des mots de passe (suivant la périodicité définie). Cette solution offre aussi la possibilité de faciliter l'allocation de ressources aux administrateurs et des sociétés de services externes.

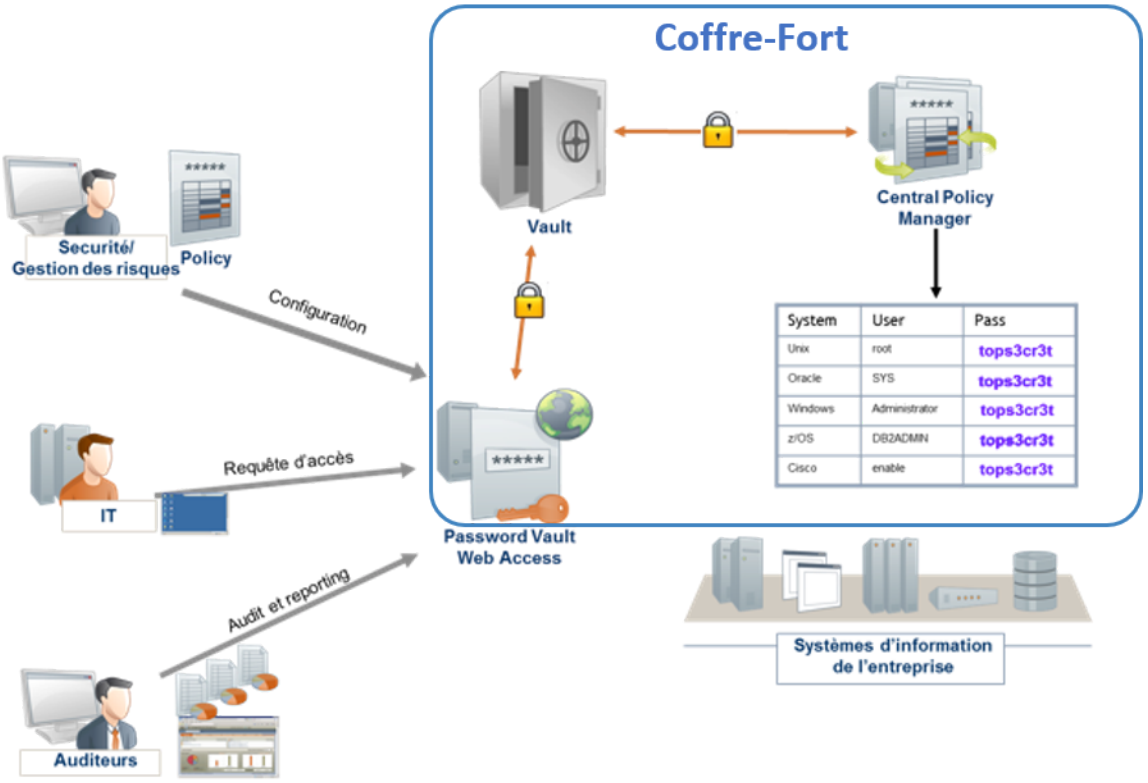


Figure 9 : Architecture de la solution de coffre-fort de mots de passe

Les différents modules dialoguent entre eux par le biais d'un protocole sécurisé :

Le Central Policy Manager (CPM) : service permettant de modifier, vérifier et resynchroniser les mots de passe sur un grand nombre de cibles (OS, équipements réseaux, bases de données, annuaires, ...). changer automatiquement les mots de passe et ainsi transformer la connaissance de ces mots de passe en un droit pouvant être alloué ou révoqué pour les différents utilisateurs. Le CPM offre aussi des fonctions d'auto-découverte permettant d'automatiser le cycle de vie (entrée/sortie) des plateformes gérées par la plateforme CyberArk.

Le Password Vault Web Access : module de présentation offrant l'interface graphique de consultation des informations concernant les mots de passe. Cette interface unique permet également de configurer la solution et d'accéder aux données d'audit et de reporting. Elle est

nationalisable et disponible nativement en Français et Anglais. La nationalisation des interfaces est effectuée en fonction de la langue du navigateur web.

Le Vault : Le Vault est un espace de stockage de données hautement sécurisé intégrant plusieurs couches de sécurité. Les différentes fonctionnalités intégrées dans le coffre-fort sont :

- Chiffrement de session : basé sur un protocole propriétaire de VPN dynamique, chiffré et compressé entre les clients et le serveur Vault,
- Firewall,
- Authentification : support des méthodes standard d'authentification (PKI, RADIUS, SecurID, login et mot de passe),
- Access Control List (ACL) : gestion des droits granulaires sur les coffres contenus au sein de la solution et sur la solution elle-même,
- Dual Control : mécanisme de validation avant utilisation d'un mot de passe,
- Versions : conservation des versions de mots de passe permettant un retour arrière aisé sans mise en œuvre de procédure de restauration de back-up en cas d'erreur de manipulation,
- Audit : toutes les activités sont auditées au sein du Vault. Ces données d'audit ne peuvent pas être supprimées ou modifiées,
- Chiffrement : l'ensemble des données du Vault sont chiffrées.

III-6 _ Le collecteur de logs

Le collecteur de traces est une infrastructure de sécurité qui collecte et stocke des logs produits par les équipements du Réseau. Il est basé sur la technologie « QRadar » développée par IBM.

La plateforme de collecte met en corrélation l'activité des utilisateurs et les données d'évènement. Elle permet ainsi d'identifier et d'alerter rapidement les violations de conformité, de stratégie, des cyber-attaques et des menaces internes. Les logs collectés sont à minima des logs d'authentification pour identifier de manière irréfutable un utilisateur qui accède à un actif.

Une source peut envoyer les logs vers le collecteur selon deux méthodes uniquement : SFTP et Syslog. Ces protocoles ont pour fonction le transport des messages de journalisation générés par un système ou une application vers un serveur/collecteur.

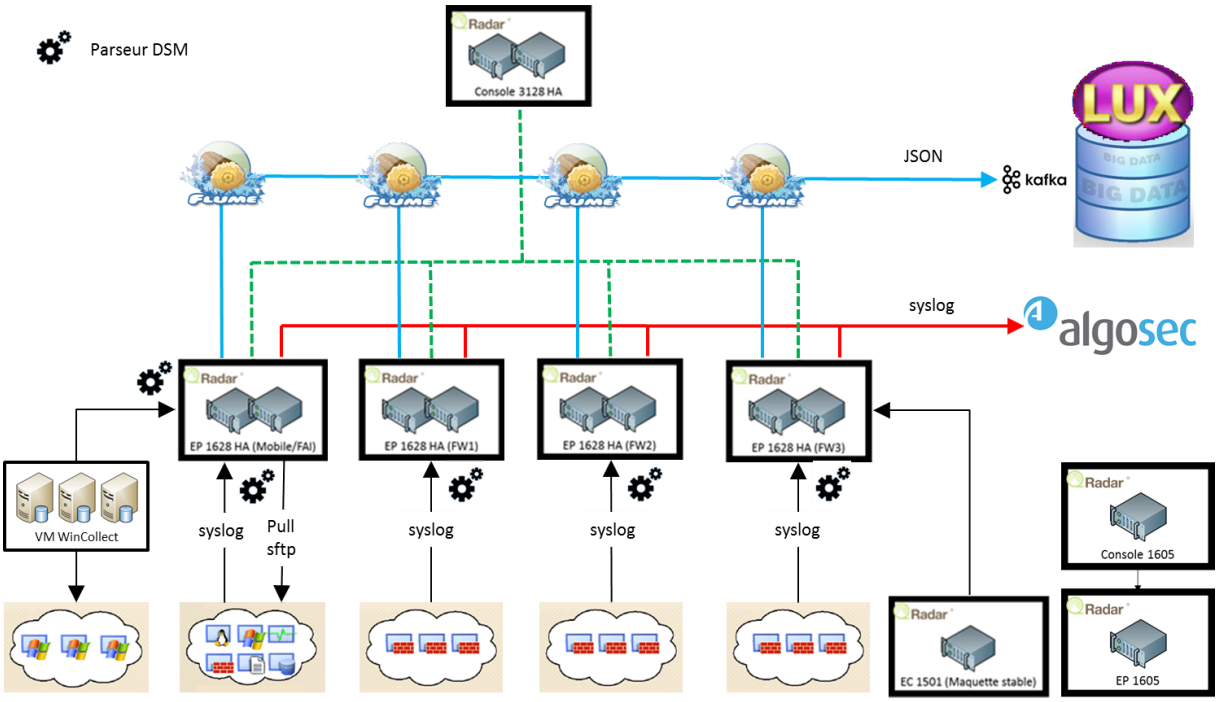


Figure 10 : Architecture du collecteur de logs

III-7 _ Le scanneur de vulnérabilités

Un scanneur de vulnérabilités est un équipement réseau conçu pour identifier les failles d'un système. Le scanneur utilisé chez le client est Nessus. Initialement distribué sous licence GPL (General Public Licence), Nessus est désormais distribué sous licence propriétaire (propriété de la société Tenable Network Security) depuis la version 3, mais reste toujours gratuit pour une utilisation personnelle.

Le scanneur Nessus est basé sur une architecture client-serveur. Il balaye les ports d'un ou plusieurs hôtes à la recherche d'éventuelles failles de sécurité. La figure suivante présente son architecture globale :

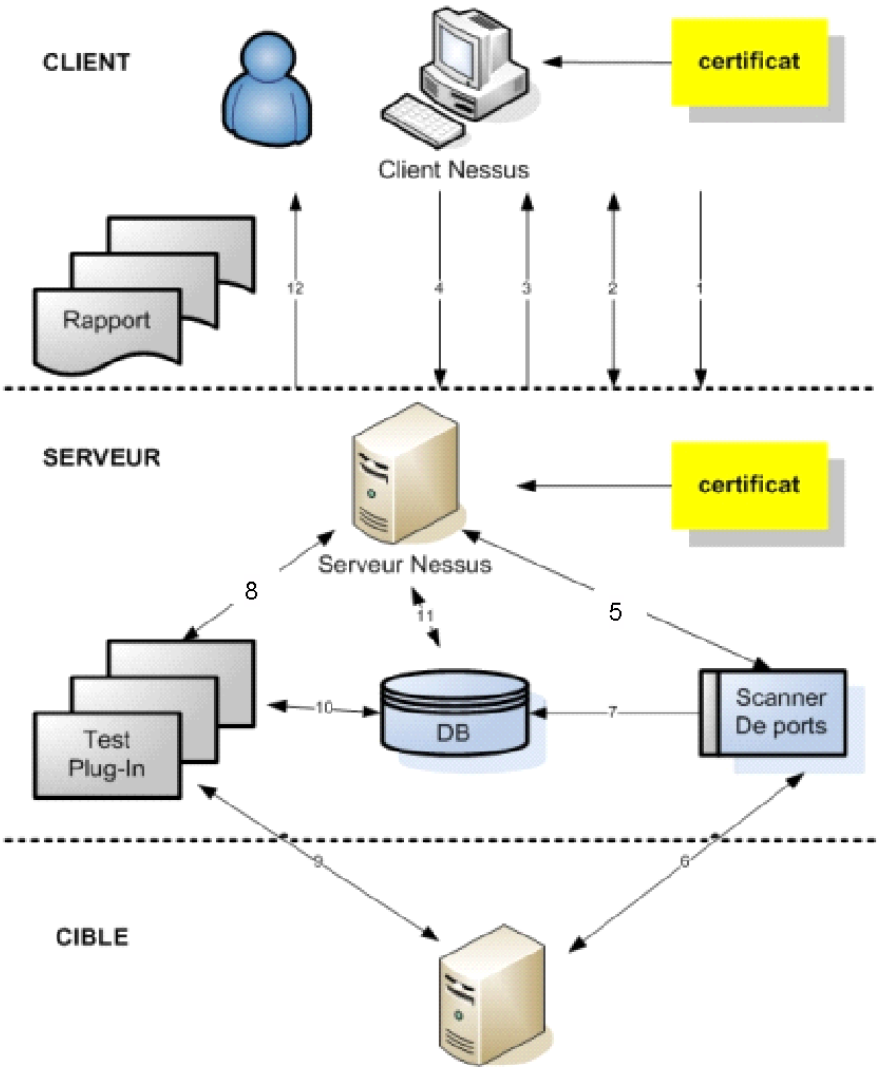


Figure 11 : Schéma de l'architecture globale de Nessus

1) Le client **Nessus** se connecte et s'identifie (à l'aide de son login et de son mot de passe).
2) Le client et le serveur s'échangent leurs certificats afin de crypter les données et que le serveur authentifie le client.
3) Le serveur envoie au client les différents tests et options disponibles.

4) Le client envoie les tests et options choisis au serveur, ainsi que les paramètres de la cible.
5) Le serveur **Nessus** enclenche le scanneur de port disponible (nmap ou autre) pour effectuer un balayage des ports de la cible.
6) La réalisation du scan des ports.
7) Les informations récoltées lors du scan des ports sont enregistrées dans la base de données.
8) Le serveur **Nessus** lance les scripts NASL (plugins) appropriés pour analyser les données recueillies par le scan.
9) Les plugins testent la cible en se basant sur les données de la base de données.
10) Les plugins enregistrent les informations relatives aux tests dans la base de données.

11) Toutes les informations sont envoyées au serveur Nessus lors de l'exécution des tests.
12) Les informations récoltées ainsi que leurs analyses sont mises à la disposition de l'utilisateur sous forme de rapports.

III-8 _ La plateforme d'antivirus

Seuls les systèmes Windows sont raccordés à cette plateforme. Cette plateforme d'Antivirus est un serveur McAfee. Elle permet de suivre de manière globale et centralisée les évènements de sécurité sur les infrastructures. Ainsi, en cas d'événements anormaux, des alarmes sont déclenchées de manière instantanée. La centralisation du service de supervision de l'activité virale permet en plus de faciliter la gestion des mises à jour qui sont capitales pour tout système antivirus.

III-9 _ Récapitulatif des plateformes de sécurité et de leurs fonctions.

En résumé, le tableau suivant nous donne un récapitulatif des différentes plateformes de sécurité et leurs fonctions :

Tableau 1 : Récapitulatif des plateformes de sécurité et leurs fonctions

Plateforme de sécurité	Cas d'usage chez le client	Principaux risques couverts	Principaux services de sécurité
Authentification unifiée	• Raccordement obligatoire pour tous les équipements RES • Services Kerberos, tacacs+ ou radius	• Accès non autorisé aux équipements • Usurpation d'identité • Non imputabilité (comptes nominatifs)	• Authentification déportée (pas de compte local) • Authentification centralisée • Règles de renouvellement et durcissement des mots de passe
Rebond	• Accès obligatoire pour l'administration de tous les équipements réseau • Services ssh, rdp, https, ftp, telnet, sftp, ica	• Accès non autorisé aux équipements • Usurpation d'identité	• Contrôle l'accès des connexions (d'administration) • Authentifie le client, par relais vers l'AU • Trace les connexions et les actions
Coffre-Fort de mots de passe	• Raccordement obligatoire pour tous les actifs du réseau	• Traçabilité des actions des administrateurs de mots de passe • Mise à jour régulière des mots de passe	• Règles de renouvellement et durcissement des mots de passe
Collecteur de logs	• Raccordement aux collecteurs obligatoire pour tous les actifs du réseau • Fonctionne en syslog, sftp (pull et push) ou avec un agent	• Malveillances (diminue le risque, facilite le retour à l'état nominal)	• Collecte et stockage (longue durée) des logs • Alertes de sécurité sur critère d'occurrences ou de scénario • Production d'indicateurs
Scanneur de vulnérabilités	• Raccordement obligatoire pour tous les actifs du réseau	• Vulnérabilités Web • Vulnérabilités OS • Vulnérabilités Protocoles • Ports ouverts non utilisés	• Scan intrusif : découvertes et tentatives d'exploitation des vulnérabilités intrusions sur

		• Services activés non utilisés	les machines scanner et analyser les réactions • Scan non intrusif : découvertes des vulnérabilités d'un système.
Antivirus	• Raccordement obligatoire pour tous les actifs Windows du réseau	• Logiciels malveillants	• Disponibilité et intégrité du SI

III-10 _ Processus de raccordement d'un actif aux plateformes de sécurité

L'ingénieur Accompagnent Sécurité a la responsabilité de conduire le raccordement de chaque actif aux différentes plateformes de sécurité citées précédemment. Dans ce contexte, l'IAS a deux fonctions :

- Dans un premier temps, il produit le cahier de raccordement et s'assure du bon déroulement de son implémentation.
- Dans un second temps, l'IAS vérifie le rapport de tests de sécurité et le rapport de scan Nessus.

1 _ Le cahier de raccordement

Le CDR est un document qui décrit de manière exhaustive le raccordement d'un actif à l'ensemble des plateformes de sécurité. Pour le produire, l'Ingénieur Accompagnement Sécurité recueille toutes les informations sur l'actif à raccorder auprès du chef de projet et du fournisseur. Un formulaire de demande de raccordement (FDR, voir annexe) est transmis à cet effet avec toutes les questions dont les réponses permettront de définir les spécifications de raccordement dans le CDR.

Après production du CDR, une ouverture de flux sécurité est requise afin de permettre la communication entre l'actif à raccorder et les plateformes de sécurité.

De même, il faut s'assurer que l'actif à raccorder est prêt à communiquer avec les plateformes de sécurité. Pour cela, des configurations préalables sont nécessaires. On parle alors de prérequis de raccordement.

2_ Rapport de tests de sécurité et rapport de scans Nessus

Le rapport de tests sécurité est un document qui fait un compte rendu complet du raccordement. Ainsi, il permet d'avoir une vue précise sur le respect des exigences de sécurité à l'issu de la mise en œuvre du cahier de raccordement. Entre autres, nous pourrons donc avoir les précisions sur les éléments suivants :

- Valider le bon fonctionnement du scanneur sur chaque actif,
- Valider la non utilisation des protocoles obsolètes (cf onglet « Protocoles obsolètes »),
- Valider la gestion de l'attribution des profils métiers aux comptes utilisateurs dans GDH/AD,
- Valider que toutes les connexions sont tracées avec la notion d'horaire et d'identification de l'utilisateur,
- Valider que les logs sécurité remontent bien sur TRACE (logs d'authentification et d'actions) et de la possibilité de leur exploitation,
- L'ensemble des services présents doivent être listés dans le cahier de résultats des tests afin de s'assurer qu'aucun service inutile n'est activé,
- Valider les paramètres de robustesses des mots de passe,
- Valider que le changement automatique des mots de passe stockés dans le coffre-fort fonctionne,
- Valider que le certificat utilisé pour les connexions utilisateurs est signé par la PKI du client.

D'autre part, l'Ingénieur Accompagnement Sécurité analyse le rapport du scanneur de vulnérabilité en maquette afin de s'assurer qu'aucune vulnérabilité critique ne passera dans l'environnement de production. De plus, des scans sont effectués sur les actifs raccordés afin de rester dans une logique d'amélioration continue conduisant au durcissement du système.

IV _ Développement d'un outil d'automatisation des CDR

IV-1 _ Problématique

Dans le cadre de notre activité chez NSA, il y a une tâche qui est présente sur tous nos projets : c'est le raccordement aux servitudes de sécurité. Il est formalisé au travers d'un fichier Excel, le cahier de raccordement (CDR), qui regroupe l'ensemble des informations nécessaires pour effectuer le raccordement des actifs aux différentes plateformes de service de sécurité (PFS).

Le problème de ce type de fichiers, c'est qu'ils sont longs à produire et qu'il en faut souvent plusieurs pour un même projet. De plus, les CDR varient souvent d'un projet à l'autre en fonction des différentes spécificités et du contexte, ce qui rend leurs rédactions fastidieuses.

Un outil a donc été mis en place, mais il n'est pas complet car de nouveaux protocoles et de nouvelles plateformes de sécurité se sont ajoutées au fil du temps. De plus, il est obsolète car les informations variables dans le temps telles que les IP des servitudes de sécurité sont disséminées dans un bloc de 50 000 lignes indigestes. Il convient donc de mettre en place un nouvel outil pour répondre aux nouveaux besoins et qui palie aux problématiques déjà existantes.

IV-2 _ Cahier des charges de l'outil d'automatisation des CDR

L'objectif de cet outil est d'améliorer l'efficacité de l'Ingénieur Accompagnement Sécurité au travers du gain de temps, mais également optimiser d'autres éléments de l'activité comme l'échange d'informations entre collaborateurs (exemple : stocker de façon automatique les fichiers générés sur un dossier partagé). Certains de ces éléments ont été définis avant le début du développement, d'autres ont été conçus et proposés à l'issue des réunions bimensuelles, et parfois ils se sont imposés par la force des choses.

La fonction principale de l'outil est de générer des modèles de CDR qui se matérialisent sous la forme d'un fichier Excel avec plusieurs onglets (un onglet par PFS) remplis de façon automatique à partir de différents modèles. Un formulaire permet de collecter les informations nécessaires pour définir les exigences et spécifications techniques des actifs. D'autres idées ont par la suite germé pour donner naissance à des fonctionnalités qui permettent d'automatiser des tâches adjacentes à la génération du CDR telles que :

- La prise en compte de toutes les PFS (notamment Antivirus & Coffre-fort),
- La prise en compte des plateformes SIIV,
- La génération dynamique de l'ensemble des onglets,
- L'importation automatique des spécifications techniques des actifs dans l'outil,
- Le stockage automatique de chaque CDR produit dans un dossier partagé,
- Le contrôle de données,
- La création de matrices pour faciliter la maintenance de l'outil dans le temps et favoriser l'évolutivité des PFS,
- La priorisation des protocoles,

- La prise en compte des demandes TMA (Tierce Maintenance Applicative),
- La création de raccourcis pour faciliter l'accès aux ressources (formulaires, résultats, dossiers partagés).

IV-3 _ Présentation de l'outil d'automatisation des CDR

Un outil qui représente tout un processus :

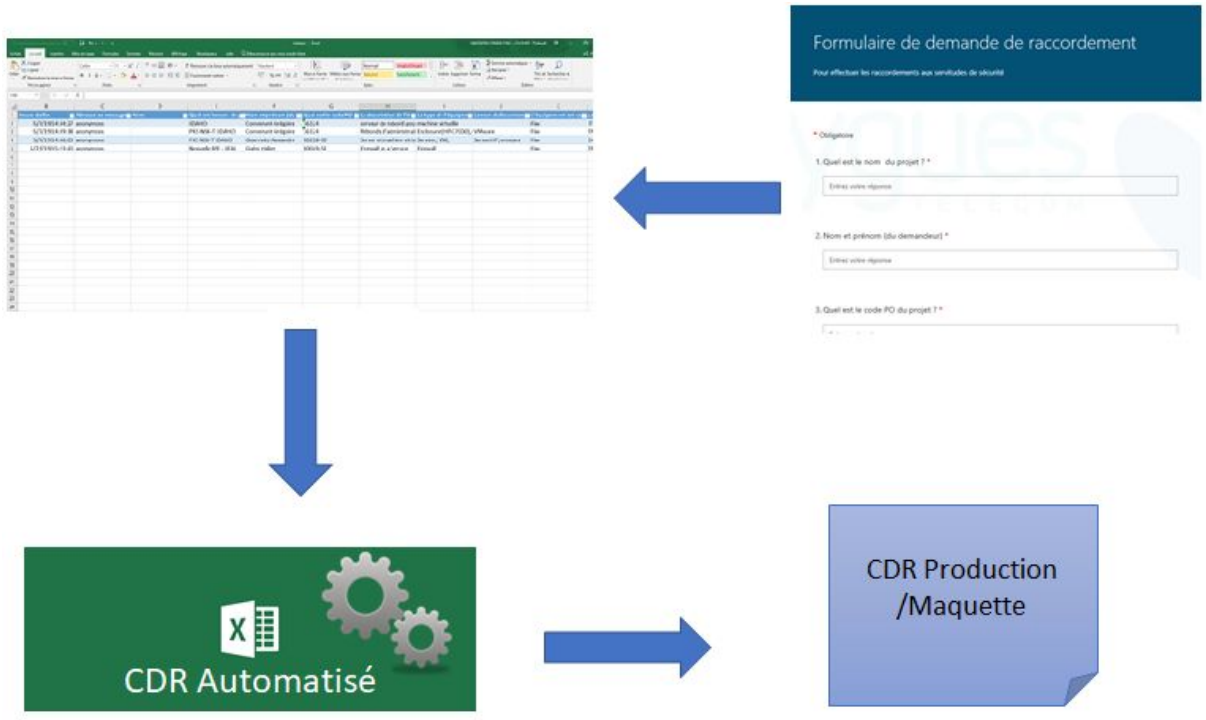


Figure 12 : Schéma du processus de création d'un Cahier De Raccordement (CDR)

Le formulaire de demande de raccordement (voir annexes) a été créé sur Microsoft Forms, qui a pour avantage de stocker les réponses du formulaire dans un tableau Excel de manière séquentielle. C'est les données contenues dans ce tableau que l'on va importer dans l'outil pour lui permettre de générer le CDR approprié.

A l'aide de la fonctionnalité « IMPORT », on récupère les réponses du responsable de l'actif à raccorder.

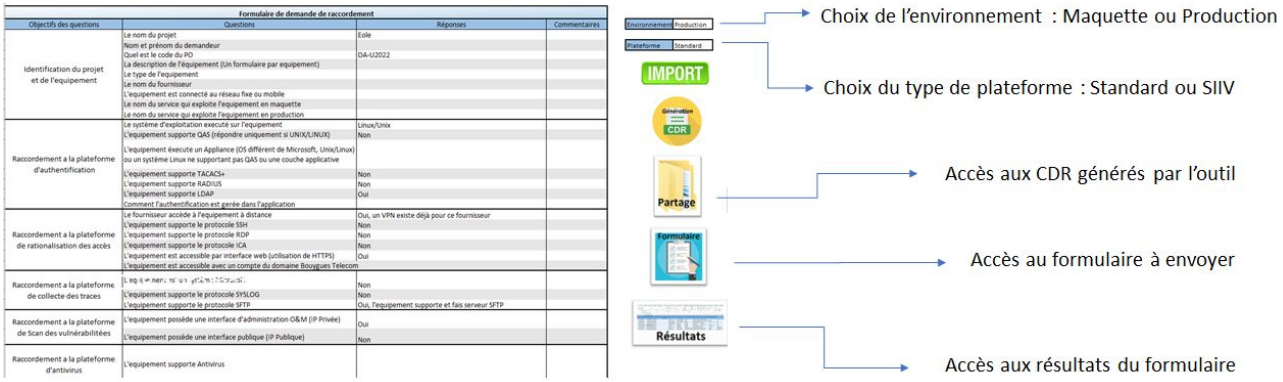


Figure 13 : Capture écran de l'onglet « Formulaire » de l'outil d'automatisation des CDR

Après avoir contrôler la cohérence des réponses, l'IAS va ensuite pouvoir paramétrer l'environnement (Maquette ou Production) et le type de plateforme (Standard ou SIIV) du projet avant de générer le CDR. Des raccourcis permettent également d'avoir un accès rapide aux différentes ressources tels que le formulaire ou le tableau Excel en ligne qui contient les réponses. L'ensemble des entrées à fournir avant de générer le CDR se situant sur un unique onglet, cela présente l'avantage d'avoir une vision globale sur l'ensemble des paramètres.

Après avoir cliqué sur « Génération CDR », un formulaire pré rempli apparait à l'écran.

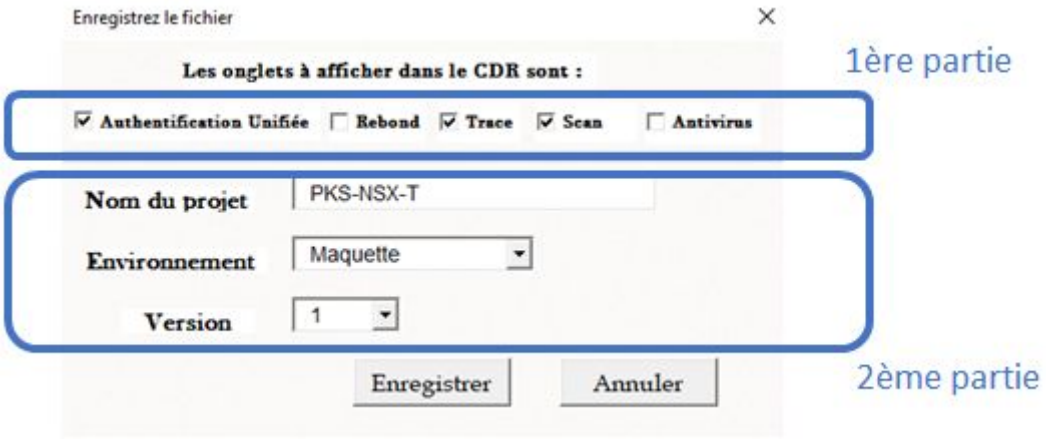


Figure 14 : Capture écran du module de sauvegarde de l'outil d'automatisation des CDR

La 1ère partie définit quels onglets vont être générés (ceux qui sont cochés). A noter qu'une reconnaissance automatique des réponses permet de pré-cocher la première partie.

La 2ème partie est composé de 3 champs qui seront utilisées pour générer le CDR, notamment le titre avec lequel il sera enregistré dans le dossier partagé (le titre sera **NomDuProjet_Environnement_Version**_Date). Ici aussi, les 3 champs (Nom, Environnement et version) sont pré-remplis de manière automatique.

Pour l'utilisateur il s'agit donc seulement de contrôler la pertinence du pré-remplissage du module de sauvegarde.

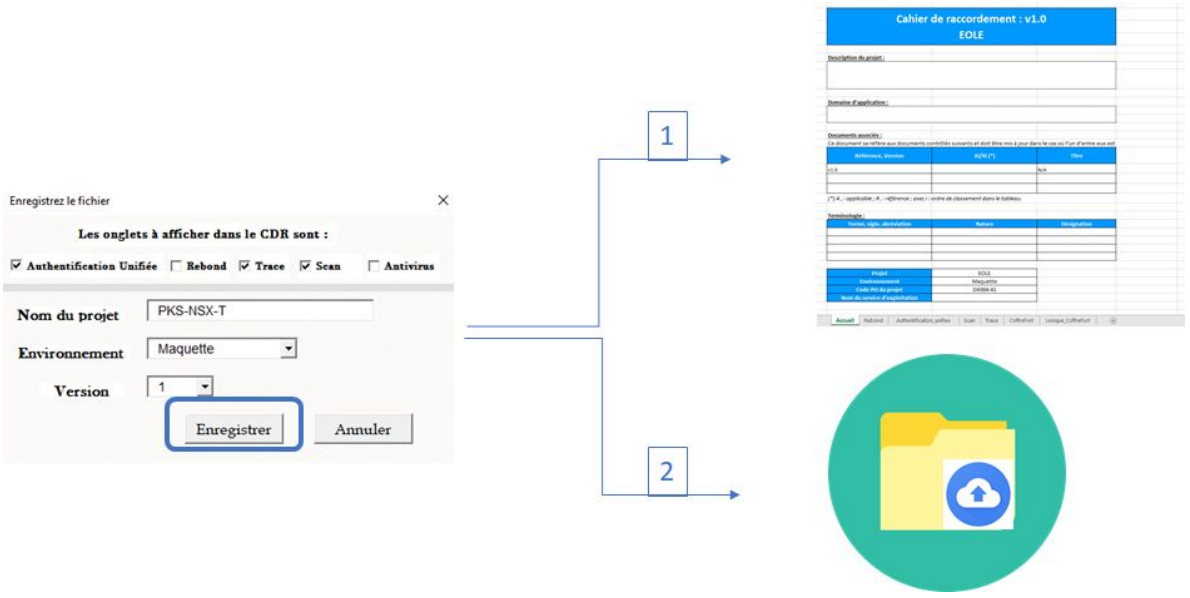
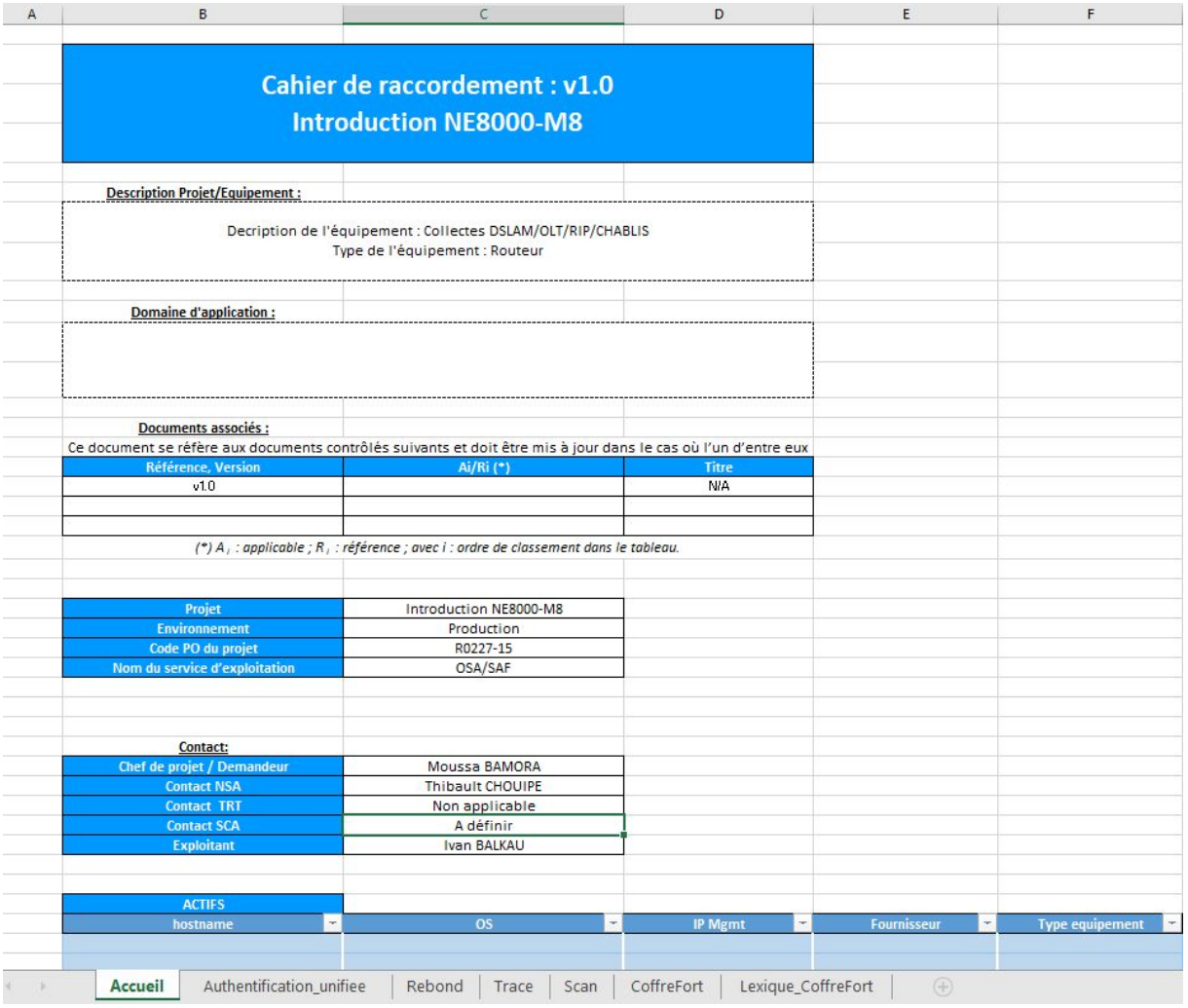


Figure 15 : Schéma du processus de génération d'un Cahier De Raccordement (CDR)

Après avoir enregistré, plusieurs actions sont effectuées durant la génération du CDR :

- Les onglets sélectionner sont générés avec les modèles correspondants aux réponses données en entrée.
- Les onglets confidentiels (exemple : la matrice des données PFS) ou inutiles (exemple : onglet « Formulaire ») sont supprimés.
- Le CDR est enregistré dans un dossier partagé accessible à l'ensemble de l'équipe NSA. Le fichier est converti au format. xslx, c'est-à-dire sans macros (scripts) pour faciliter son utilisation mais également pour des raisons de confidentialité.



Cahier de raccordement : v1.0
Introduction NE8000-M8

Description Projet/Equipement :

Decription de l'équipement : Collectes DSLAM/OLT/RIP/CHABLIS
Type de l'équipement : Routeur

Domaine d'application :

Documents associés :

Ce document se réfère aux documents contrôlés suivants et doit être mis à jour dans le cas où l'un d'entre eux

Référence, Version	Ai/Ri (*)	Titre
v1.0		N/A

(*) A_i : applicable ; R_i : référence ; avec i : ordre de classement dans le tableau.

Projet	Introduction NE8000-M8
Environnement	Production
Code PO du projet	R0227-15
Nom du service d'exploitation	OSA/SAF

Contact:

Chef de projet / Demandeur	Moussa BAMORA
Contact NSA	Thibault CHOUIPE
Contact TRT	Non applicable
Contact SCA	A définir
Exploitant	Ivan BALKAU

ACTIFS				
hostname	OS	IP Mgmt	Fournisseur	Type equipement

Accueil | Authentification_unifiee | Rebond | Trace | Scan | CoffreFort | Lexique_CoffreFort

Figure 16 : Extrait d'un Cahier De Raccordement : onglet « Accueil »

L'onglet Accueil contient de nombreuses informations qui sont utiles tout au long du projet tel que le contexte du projet, les principaux interlocuteurs et l'inventaire des actifs. Ce dernier est complété par l'exploitant afin de permettre aux différents acteurs du projets d'avoir une vision complète sur le type et le nombres d'actifs à raccorder.

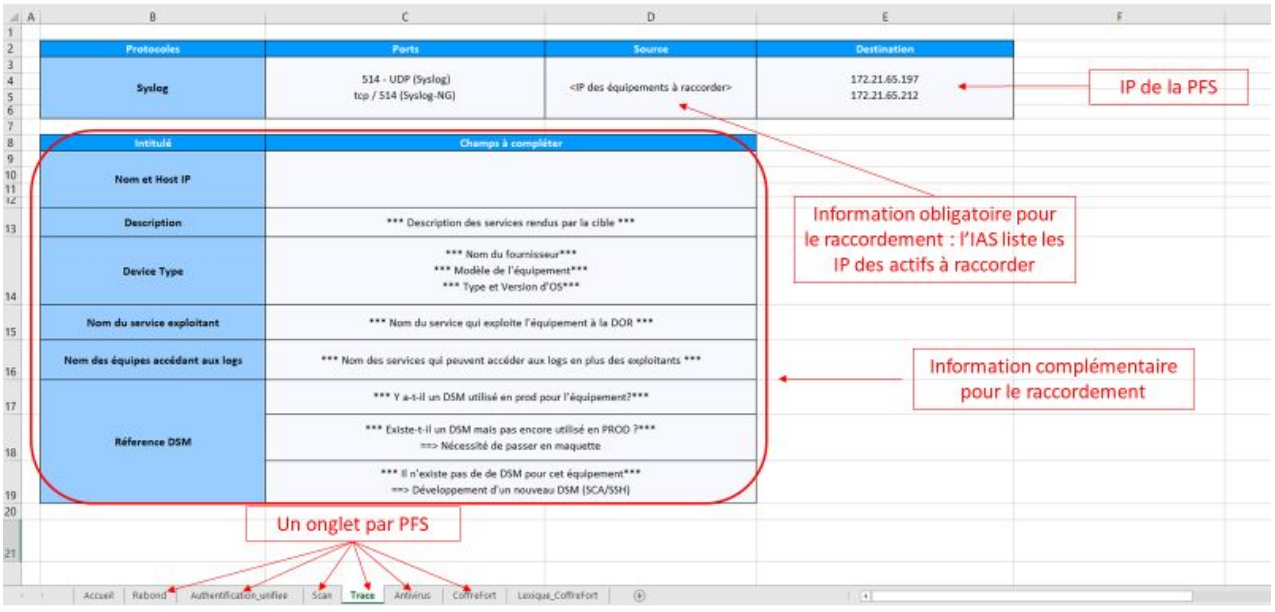


Figure 17 : Extrait d'un Cahier De Raccordement : onglet « Trace »

On constate sur cette capture d'écran que les onglets, ici Trace, sont remplis par des modèles qui permettent à l'IAS de construire son CDR en remplissant seulement deux à trois champs par onglet.

Chaque PFS est représenté par un onglet dans lequel l'Ingénieur Accompagnement Sécurité va devoir renseigner au minimum la liste des IP des actifs à raccorder. Selon le contexte, il peut également renseigner d'autres informations complémentaires.

L'onglet coffre-fort est un peu plus spécifique à renseigner, c'est pourquoi l'onglet « Lexique_Coffrefort » est présent. Il détaille les différents termes techniques utilisé afin de permettre à l'exploitant de comprendre quelles données sont attendues.

Pour répondre à la problématique sur la mise à jour des données qui évoluent dans le temps (comme l'adresse IP d'un serveur), deux matrices ont également été créée (une pour les plateformes standards, l'autre pour les SIIV). On peut donc changer la valeur des IP et des noms de domaine sans avoir à rentrer dans le code informatique. Cela a pour conséquence de permettre à n'importe qui, même quelqu'un qui ne maitrise pas le VBA (Visual Basic For Applications) de pouvoir mettre l'outil à jour.

X

Figure 18 : Extrait de la matrice de données des PFS

III-4 _ Comparaison avec l'ancien outil

Afin d'avoir une vue globale des améliorations apportées par la nouvelle version de l'outil, voici un tableau récapitulatif qui présente les principales différences entre les deux versions :

Tableau 3 : Comparaison de l'ancienne vs la nouvelle version de l'outil

Old Version	New Version
Saisie manuelle des données	Importation automatique à partir du fichier Excel Forms
Non prise en compte des PFS Antivirus & Coffre-fort	Prise en compte des PFS Antivirus & Coffre-fort
Données des PFS (IP, ports, ..) statiques dans le script qui sont aujourd'hui obsolètes	Evolutivité : Création de matrices facilitant la mise à jour des données PFS
Pas de SIIV	Prise en compte des PFS SIIV pour sujets sensibles (LPM)
Pas de priorisation des protocoles	Priorisation des protocoles
Pas de sauvegarde dans les dossiers partagés	Collaboratif : Stockage automatique dans les dossiers partagés
Onglets statiques	Génération/Suppression des onglets en fonction du projet
Un CDR à part pour les demandes TMA	Prise en compte des demandes TMA
Des informations à renseigner sur plusieurs onglets	Un unique onglet regroupe tout les INPUT (évite les erreurs)
NA	Création de raccourcis qui facilite accès au ressources (formulaire en ligne, résultats, dossier partagés, ..)
	Interface conviviale & intuitive
Au niveau technique	
Un bloc de 50 000 lignes de code	Optimisation du code : 7000 lignes de code
1 seul module	Découpage modulaire, un module par PFS
Pas de commentaire et d'indentation	Commentaire + Indentation
Maintenance difficile	Upgrade & maintenance facilitée

IV-5 _ Impact sur l'activité

L'outil permet :

- Un gain de temps très important car il supprime des tâches répétitives et fastidieuses notamment grâce à la génération de modèles qui nécessitent seulement quelques modifications pour être opérationnelles. De plus, un unique formulaire centralise toutes les spécifications techniques des actifs alors qu'avant, il fallait plusieurs échanges entre les différents interlocuteurs pour récolter l'ensemble des informations.
- D'améliorer la qualité des données car toutes les informations sont centralisées sur un unique tableau, ce qui permet de plus facilement détecter les incohérences et diminuer le risque d'erreur.
- De faciliter la collaboration dans l'équipe car les actions sont plus facilement synchronisées (l'ensemble de l'équipe a accès au Excel Forms qui contient toutes les demandes). La sauvegarde automatique dans un dossier partagé permet également d'assurer la continuité car tous les membres de l'équipe ont accès à l'ensemble des CDR.

- De normaliser les CDR : si deux membres de l'équipe génèrent chacun un CDR pour un projet X, ils seront identiques. Cela a de nombreux avantages, notamment lorsqu'un membre de l'équipe est absent.

On constate donc que cet outil à un fort impact sur notre activité. Le gain de temps permet à l'équipe d'augmenter sa capacité au niveau du nombre de projets mais également de pouvoir se concentrer sur d'autres tâches à fortes valeurs ajoutées. De plus, la qualité du service fournie est meilleur et le remplacement d'un membre de l'équipe est facilité grâce au partage automatique des documents et leurs uniformités.

Conclusion

L'intégration de la sécurité dans les projets est un processus itératif et délicat car chaque étape est cruciale. La sécurité n'est pas une fonction distincte et isolée du processus de mise en œuvre des projets. C'est ce principe qui a bien été compris par Bouygues Télécom et l'a amené à se doter d'équipes internes et de consultants en cybersécurité afin d'intégrer la sécurité tout au long de ses projets.

Ce stage a été pour moi une expérience enrichissante car il m'a permis d'être immergé dans le monde du conseil en cybersécurité. J'ai eu la chance de pouvoir toucher à la fois aux aspects techniques, fonctionnels et organisationnels de la cybersécurité. J'ai pu y mettre en pratique de nombreuses notions apprises au cours de l'année académique écoulée. La satisfaction de mon employeur, Davidson Paris, et du client, Bouygues Télécom, est avérée et se matérialise par une proposition d'embauche qui m'a été faite avant même l'issue de ce stage.

Bibliographie

[1] http://www.lefigaro.fr/secteur/high-tech/plus-de-la-moitie-de-la-population-mondiale-a-desormais-acces-a-internet-20190612

[2] https://www.davidson.fr/davidson/histoire/

[3] http://etudiant.aujourdhui.fr/etudiant/info/rapport-de-stage.html

[4] AFNOR NF ISO/IEC 27005 (2018) – *Technique de l'information – Techniques de sécurité – Gestion des risques liées à la sécurité de l'information*

[5] https://www.ibm.com/fr-fr/security/services/managed-security-services/security-operations-centers

[6] Documents internes (Architecture, proce

Annexe

Formulaire de demande de raccordement :

Formulaire de demande de raccordement

v2.0 07/2019

1. Quel est le nom du projet ? *

Entrez votre réponse

2. Nom et prénom (du demandeur) *

Entrez votre réponse

3. Quel est le code PO du projet ? *

Entrez votre réponse

4. La description de l'équipement (service rendu par l'équipement) *

Entrez votre réponse

5. Le type de l'équipement (Routeur, Firewall, Serveur, ...) *

Entrez votre réponse

6. Le nom du fournisseur

Entrez votre réponse

7. L'équipement est connecté au réseau fixe ou mobile ?

- Mobile
- Fixe
- Mobile et Fixe

8. Le nom du service qui exploite l'équipement en maquette

Entrez votre réponse

9. Le nom du service qui exploite l'équipement en production

Entrez votre réponse

10. AU : Le système d'exploitation exécuté sur l'équipement

- Windows
- Unix /Linux
- Autre

11. AU : Si OS Unix / Lunix l'équipement supporte QAS

- Oui
- Non
- Pas applicable

12. AU : L'équipement exécute un Appliance (OS différent de Windows, Unix/ Linux) ou un système Unix/ Linux ne supportant pas QAS ou une Couche Applicative

Entrez votre réponse

19. REBOND : L'équipement supporte le protocole RDP

- Oui
- Non
- Pas applicable

20. REBOND : L'équipement supporte le protocole ICA

- Oui
- Non
- Pas applicable

21. REBOND : L'équipement est accessible par interface web (utilisation de HTTPS)

- Oui
- Non
- Pas applicable

22. REBOND : L'équipement est accessible avec un compte du domaine Bouygues Telecom

- Compte AD RES
- Compte local nominatif ou générique
- Compte Credential Store (coffre fort)
- Autre

23. TRACES : L'équipement est un système Microsoft

- Oui, système microsoft dans le domaine RES
- Oui, hors du domaine RES (quelques serveurs)
- Oui, système microsoft hors du domaine RES (plusieurs serveurs)
- Non

24. TRACES : L'équipement supporte le protocole SYSLOG

- Oui
- Non
- Pas applicable

25. TRACES : L'équipement supporte le protocole SFTP

- Oui, l'equipement supporte et fais serveur SFTP
- Non
- Pas applicable

26. SCANNER : L'équipement possède une interface d'administration O&M (IP Privée)

- Oui
- Non
- Pas applicable

27. SCANNER : L'équipement possède une interface publique (IP Publique)

- Oui
- Non
- Pas applicable

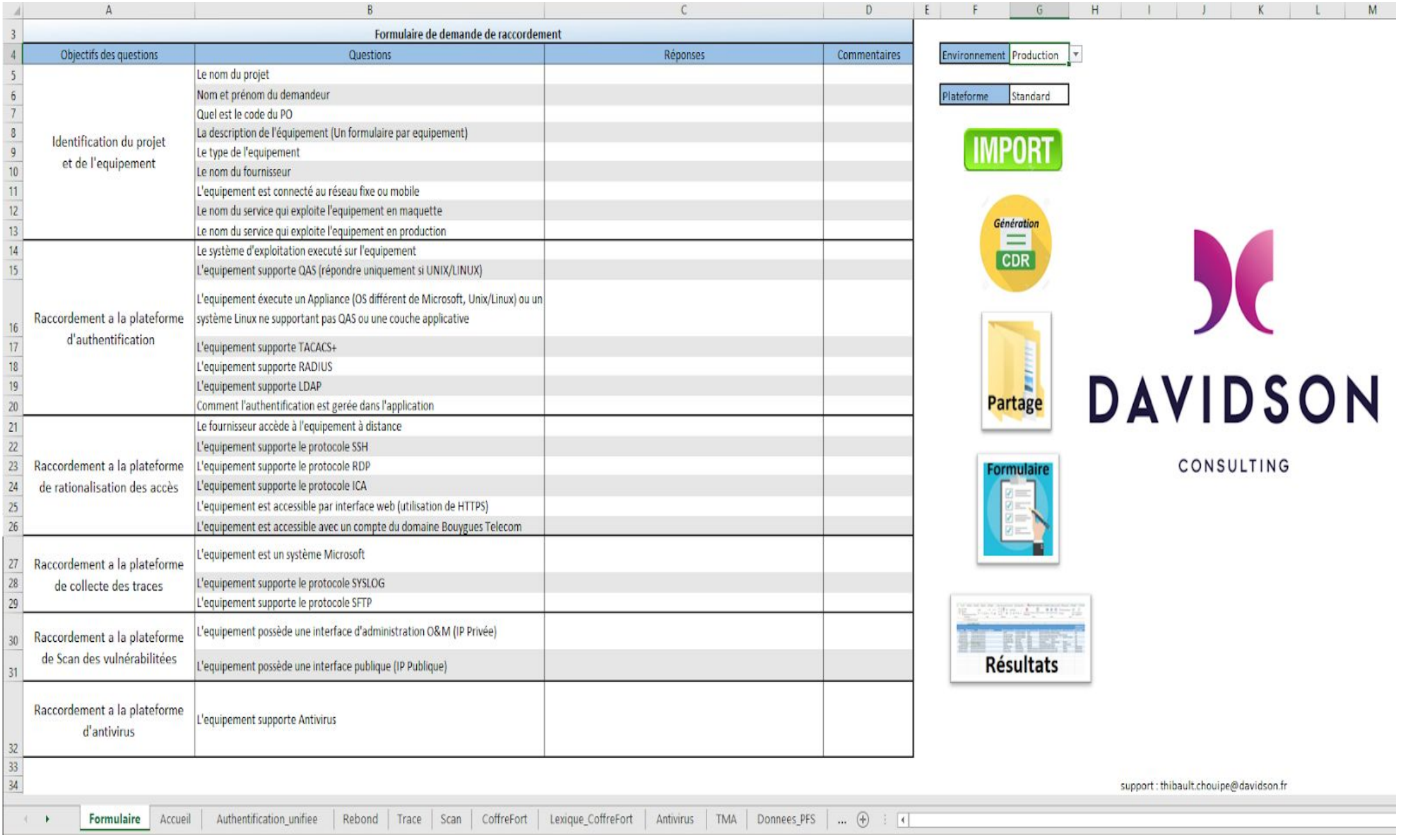
28. Liste des équipements avec "hostname" et @IP

Entrez votre réponse

29. Remarques complémentaires

Entrez votre réponse

Capture d'écran de l'onglet « Formulaire » de l'outil d'automatisation des CDR :



Formulaire de demande de raccordement

Objectifs des questions	Questions	Réponses	Commentaires
Identification du projet et de l'equipement	Le nom du projet		
	Nom et prénom du demandeur		
	Quel est le code du PO		
	La description de l'équipement (Un formulaire par equipement)		
	Le type de l'equipement		
	Le nom du fournisseur		
	L'equipement est connecté au réseau fixe ou mobile		
	Le nom du service qui exploite l'equipement en maquette		
	Le nom du service qui exploite l'equipement en production		
Raccordement a la plateforme d'authentification	Le système d'exploitation executé sur l'equipement		
	L'equipement supporte QAS (répondre uniquement si UNIX/LINUX)		
	L'equipement éxecute un Appliance (OS différent de Microsoft, Unix/Linux) ou un système Linux ne supportant pas QAS ou une couche applicative		
	L'equipement supporte TACACS+		
	L'equipement supporte RADIUS		
	L'equipement supporte LDAP		
	Comment l'authentification est gerée dans l'application		
Raccordement a la plateforme de rationalisation des accès	Le fournisseur accède à l'equipement à distance		
	L'equipement supporte le protocole SSH		
	L'equipement supporte le protocole RDP		
	L'equipement supporte le protocole ICA		
	L'equipement est accessible par interface web (utilisation de HTTPS)		
	L'equipement est accessible avec un compte du domaine Bouygues Telecom		
Raccordement a la plateforme de collecte des traces	L'equipement est un système Microsoft		
	L'equipement supporte le protocole SYSLOG		
	L'equipement supporte le protocole SFTP		
Raccordement a la plateforme de Scan des vulnérabilitées	L'equipement possède une interface d'administration O&M (IP Privée)		
	L'equipement possède une interface publique (IP Publique)		
Raccordement a la plateforme d'antivirus	L'equipement supporte Antivirus		