Livrable 2

Projet : Sécurité et administration

Maxime STOFFEL, Youcef AFANE, Vincent CAUSSE, Romain TOUZÉ et Thaïs VIANES

Sommaire

Table des figures

Préambule

Rappel du contexte

L'entreprise XANADU va changer de locaux. Son directeur souhaite profiter du déménagement pour sécuriser et faire évoluer son système d'information, sachant qu'un nouveau bureau va ouvrir. Ce bureau sera relié à Atlantis par une liaison VPN MPLS opérateur.

Le directeur de XANADU connaît une entreprise qui vient d'être bloquée 3 semaines par un rançongiciel et il n'a pas du tout envie que la sienne vive la même chose. Il souhaite que son système informatique soit stable, fiable, sécurisé et facile à administrer.

Il fait donc appel à CESITECH pour l'aider dans cette démarche. CESITECH demande à votre équipe projet de :

1. Proposer un questionnaire de sécurité à Xanadu pour détecter les vulnérabilités et proposer des mesures correctives basées sur des axes de remédiation.
2. Travailler sur le déploiement du nouveau système informatique de Xanadu, élaborer une cartographie cible du système d'information : vue administration, infrastructure logique et physique.

Cette architecture devra respecter les bonnes pratiques en matière de sécurisation des systèmes d'information, garantir la continuité d'activité, la reprise après incident, ainsi que la traçabilité des événements. Le directeur du groupe souhaite un retour à la normale sous 4 heures pour les services critiques, et 24 heures pour les autres. Vous devez aussi proposer un plan de sauvegarde.

Rappel des attentes du client

Chaque employé doit pouvoir se connecter à distance, soit en tant qu'itinérant (par exemple, les commerciaux), soit en télétravail.

Les besoins en matière de partage de dossiers sont les suivants :

- Un dossier partagé par service, accessible uniquement aux membres du service concerné.
- Un dossier personnel centralisé pour chaque salarié, avec un quota de stockage limité et un accès via le dossier « Mes documents ».
- Le service juridique doit avoir accès aux dossiers des services client et des ressources humaines.

- La direction doit avoir accès aux dossiers de l'ensemble des services.

Dans chaque service, un correspondant informatique sera désigné et devra pouvoir :

- Créer ou modifier les comptes utilisateurs de son service ;
- Gérer les droits d'accès ;
- Intégrer de nouveaux postes de travail au domaine.

Après une première étude, les données gérées ont été classées en trois catégories selon leur criticité :

Données critiques :

- Base de données de l'ERP : contient les informations sur les clients, les contrats, etc.
- Données partagées : documents des services sinistres, juridique et de la direction.

Données importantes :

- Données partagées : documents des services client, conseil et commerce.
- Emails professionnels : correspondances internes et externes importantes.

Données moins critiques :

- Dossiers personnels des employés.

L'entreprise continuera d'utiliser :

- Son ERP, qu'elle ne compte pas changer ;
- Un copieur multifonction (impression, copie, numérisation) et une imprimante couleur ;
- Office 365, incluant la messagerie Outlook.

Le site distant est de Springfield raccordé au site principal via un L3VPN MPLS fourni par l'opérateur télécom, assurant une connectivité privée et une qualité de service garantie (SLA).

Ce que votre équipe connaît de l'infrastructure actuelle de XANADU

L'ERP (type Odoo) repose sur PostgreSQL en backend et suit une architecture en trois tiers :

- Un serveur de base de données PostgreSQL ;

- Un serveur d’applications (contenant les objets métiers, le moteur de workflow, le générateur d’états, etc.) ;
- Un serveur de présentation, qui permet aux utilisateurs de se connecter via n’importe quel navigateur web (Google Chrome, Firefox, etc.).

L'ERP utilise une base de comptes utilisateurs locale, enregistrée dans une table. Parfois, plusieurs utilisateurs partagent un compte générique : par exemple, les utilisateurs du service RH utilisent le login RH:RH.

Volume des données

- Les données bureautiques partagées occupent actuellement 800 Go.
- Les dossiers personnels doivent faire environ 5 Go chacun.
- La base de données de l’ERP fait 10 Go.

Infrastructure

- Un serveur physique contrôleur de domaine, serveur DNS et DHCP sous Windows Server 2019.
- Un NAS bureautique avec des points de partage ouverts à tous, d’une capacité de 2 To.
- Un routeur/box fournissant un accès fibre et un accès internet en NAT.
- Un serveur physique ESXi hébergeant les VM de l’ERP.
- Un copieur connecté au réseau.
- Une imprimante couleur connectée au réseau.

Gestion des données

- Chaque utilisateur a ses dossiers sur son PC, d’environ 5 Go chacun.
- Chaque utilisateur est administrateur de son PC.
- Chacun effectue ses propres sauvegardes avec une clé USB.
- Les utilisateurs utilisent l’interface web de l’ERP en HTTP.
- Les utilisateurs itinérants utilisent leur messagerie Office 365 et Teams. Ils copient, avant de partir, les documents importants sur leur PC. Ils peuvent partager des documents sur leur Microsoft Drive pour communiquer avec leurs collègues, ce qui fait que parfois les documents de l’espace bureautique ne sont pas à jour.
- Les utilisateurs en télétravail n’ont pas accès à l’ERP.

Sauvegardes

Une personne connecte chaque fin de semaine un disque externe au serveur DC, sur lequel un script copie le contenu du NAS. Deux disques externes sont utilisés en alternance, une semaine sur deux.

Un script PowerShell planifié exporte chaque nuit à 23h la base de données de l'ERP vers un partage du NAS.

Un script Windows Backup sauvegarde le serveur DC une fois par semaine, le dimanche, sur le NAS (état du système).

Antivirus

L'antivirus installé sur le serveur DC est celui de Microsoft, configuré avec les paramètres par défaut.

Plusieurs PC utilisent la version gratuite d'un antivirus, avec un paramétrage par défaut laissé à la discrétion de l'utilisateur, qui est administrateur de son poste.

Mises à jour

Elles se font avec un paramétrage par défaut et ne sont pas contrôlées. Des prestataires informatiques les effectuent sur les serveurs lorsqu'ils ont l'occasion de venir pour une mise à jour de l'ERP.

Objectifs du livrable 2

Les objectifs du livrable 2 sont les suivants :

- Proposer la mise en place de la sécurité du réseau comprenant un questionnaire de sécurité, une politique de filtrage, une supervision.

- Proposer des scripts de maintenance pour l'équipe technique de Xanadu.

Questionnaire de Sécurité

En sécurité informatique il est important de vérifier la sécurité de 4 aspects principaux du S.I. : la sécurité physique des équipements, la sécurité logicielle contre les attaques, la formation des collaborateurs et le suivi des échanges et des comportements sur le réseau.

Pour permettre à la société de s'auto évaluer sur le sujet de la sécurité, nous proposons à Xanadu un questionnaire comprenant des questions sur plusieurs aspects de la sécurité. A l'aide de ce questionnaire, l'entreprise pourra s'évaluer sur la majorité des aspects de la sécurité de leur S.I. et ainsi s'améliorer en continue.

Les différents thèmes abordés sont les suivants : la politique de sécurité interne à l'entreprise, la formation des utilisateurs, la sécurisation des postes (accès non autorisés et malwares), la sécurisation du réseau et de ses équipements, la sécurisation des données et la surveillance régulière des flux.

1. Politique de sécurité

Une charte de sécurité est une bonne solution pour mettre en place les bases de la sécurité auprès des collaborateurs.

- Une charte de sécurité a-t-elle été distribuée à tous les collaborateurs ?

  Remédiation : Mettre en place une charte de sécurité officielle à l'entreprise, la diffuser régulièrement à l'ensemble des employés (penser à la distribuer aux nouveaux employés.

- La charte de sécurité précise-t-elle : que les comptes ne peuvent être partagés, que le mot de passe doit être changé tous les 3 à 6 mois ou que seul une liste d'applications autorisée par l'administration ne peut être utilisées?

  Remédiation : Mettre à jour la charte pour inclure les règles de mots de passe, l'interdiction des comptes partagés et la liste des logiciels autorisés, cela représente les enjeux majeurs de la sécurité des postes.

2. Formation des utilisateurs

La formation des utilisateurs du réseau est un des éléments les plus important dans la sécurisation d'un réseau.

- Les utilisateurs sont-ils formés à ne pas ouvrir de pièces jointes ou liens provenant d'expéditeurs inconnus ?

  Remédiation : Mettre en place une formation annuelle anti-phishing et organiser des tests réguliers de sensibilisation (ex: mails de phishing interne).

- Les utilisateurs ont-ils connaissances des notions de "mot de passe fort" ?

  Remédiation : Fournir une formation simple sur les bonnes pratiques de gestion des mots de passe et imposer des règles techniques via GPO.

3. Sécurisation des accès

La sécurisation des accès aux postes des collaborateurs doit être correctement appréhendée.

- Les comptes de chaque utilisateur sont-ils protégés par un mot de passe répondant aux normes de sécurité ?

  Remédiation : Mettre en place une politique de blocage si un mot de passe initialisé est non conforme à la norme de l'entreprise. (10 caractères minimum, 1 chiffre, 1 majuscule, 1 caractère spécial).

4. Sécurisation des postes utilisateurs

Les postes des utilisateurs représentent des failles, il fait savoir les protéger.

- Un antivirus est-il mis en place sur les postes de tous les utilisateurs ?

  Remédiation : Déployer un antivirus centralisé sur tous les postes et activer les alertes en temps réel. Utiliser les GPO pour bloquer des accès à des types de téléchargements.

- Les utilisateurs mettent ils régulièrement leurs logiciels et systèmes d'exploitation à jours ?

  Remédiation : Les utilisateurs doivent activer les mises à jour automatiques des logiciels . Un mail automatique peut être programmé pour prévenir les

utilisateurs d'une nouvelle version disponible pour un logiciel pour leur permettre de vérifier.

5. Sécurisation des réseaux

Le réseau doit être sécurisé pour filtrer les flux entrants et sortant et dans le réseau en lui-même.

- Un pare-feu existe-t-il pour filtrer le trafic ?

  Remédiation : Installer et configurer un pare-feu professionnel avec des règles restrictives et un filtrage. Ils peuvent être ajouter sous un format physique ou virtualisés sur le routeur.

- Le routeur inclus-t-il une DMZ ?

  Remédiation : Identifier les services accessibles depuis l'extérieur de l'entreprise (clients ou accès web). Une DMZ peut alors être mise en place pour isoler ces services et les isoler du reste du réseau en cas d'attaque malveillante.

- Des Vlan sont-ils en place pour séparer les différents espaces du réseau ?

  Remédiation : Segmenter le réseau en VLAN pour limiter la propagation d'un incident. Le pare feu peut également analyser les échanges entre les VLAN.

6. Sécurisation des équipements

La DMZ représente un excellent rempart entre le SI interne et l'extérieur.

- Une DMZ est-elle en place sur le réseau pour isoler des accès non autorisés ?

  Remédiation : Identifier les services accessibles depuis l'extérieur de l'entreprise (clients ou accès web). Une DMZ peut alors être mise en place pour isoler ces services et les isoler du reste du réseau en cas d'attaque malveillante.

7. Sécurisation des sauvegardes

Les sauvegardes mettent en sécurité les données à un instant T.

- Un plan de sauvegarde est-il mis en place ?

  Remédiation : Un plan de sauvegarde peut être mis en place en prenant en compte la RTO et la RPO garantissant une sécurité optimale des données en cas d'attaque.

- Le plan de sauvegarde répond-il aux attentes 3-2-1 ?

  Remédiation : Le plan de sauvegarde doit prendre en compte une sauvegarde internet (NAS) une sauvegarde externe (NAS externe ou disque dur) et une sauvegarde Cloud.

- Le plan de sauvegarde prend il en compte une sauvegarde immuable ?

  Remédiation : Une sauvegarde immuable peut être mise en place sur le cloud pour conserver les données en lecture seule et bloquer toutes tentatives de corruption.

8. Sécurisation contre les malwares et ransomwares

Les malwares sont le pire ennemi des entreprises, il est donc important de s'en protéger.

- Un VPN est-il utilisé pour les connexions à distance ?

  Remédiation : L'utilisation d'un VPN sécurisé (avec authentification forte) permet de protéger les connexions distantes contre les interceptions et les attaques visant à compromettre le réseau interne.

- Les logiciels antivirus sont-ils configurés pour bloquer les comportements suspects(chiffrement) ?

  Remédiation : Les antivirus modernes doivent être configurés pour détecter le chiffrement massif de fichiers, les accès anormaux et les comportements typiques des ransomwares afin de bloquer l'attaque avant propagation.

9. Sécurisation en cas d'attaque

La sauvegarde régulière des données peut considérablement réduire le temps de remise en route en cas d'attaque.

- Les données sauvegardées ont une durée de sauvegarde de plus de 7jours ?

  Remédiation : Une rétention de sauvegarde d'au moins 7 jours permet de disposer de points de restauration multiples en cas de compromission progressive des données.

- Le RTO maximale est inférieure à 24h ?

  Remédiation : Un RTO inférieur à 24h garantit une reprise d'activité rapide et limite les pertes opérationnelles liées à l'interruption du service.

10. Journalisation et surveillance des logs

Une surveillance du réseau est indispensable pour réagir rapidement en cas d'attaque.

- Une surveillance est-elle mise en place sur le réseau ?

  Remédiation : La mise en place d'une supervision du réseau permet de détecter rapidement les anomalies, les intrusions et les comportements atypiques permettant une réaction rapide.

- Les logs sont-ils accessibles sur les flux dans le réseau ?

  Remédiation : Les journaux doivent être centralisés et accessibles de manière sécurisée pour permettre l'analyse rapide des événements et faciliter les investigations.

Questionnaire de sécurité	Remédiation
Politique de sécurité	Une charte de sécurité est une bonne solution pour mettre en place les bases de la sécurité auprès des collaborateurs
Une charte de sécurité a-t-elle eté distrubuée à tous les colaborateurs ?	Mettre en place une charte de sécurité officielle à l'entreprise, la diffuserrégulièrement à l'ensemble des employés (pensé à la distribuer aux nouveaux employés.
La charte de sécurité précise elle : que les comptes ne peuvent être partagés, que le mot de passe doit être changé tous les 3 à 6 mois ou que seul une liste d'applications autorisée par l'administration ne peuvent être utilisées?	Mettre à jour la charte pour inclure les règles de mots de passe, l'interdiction des comptes partagés et la liste des logiciels autorisés, cela représente les engeux majeurs de la sécurité des postes.
Formation des utilisateurs	La formation des utilisateur du réseau est un des éléments les plus important dans la sécurisation d'un réseau.
Les utilisateurs sont-ils formés à ne pas ouvrir de pièces jointes ou liens provenant d'expéditeurs inconnus ?	Mettre en place une formation annuelle anti-phishing et organiser des tests réguliers de sensibilisation (ex: mails de phishing interne).
Les utilisateurs ont-ils connaissances des notions de "mot de passe fort" ?	Fournir une formation simple sur les bonnes pratiques de gestion des mots de passe et imposer des règles techniques via GPO.
Sécurisation des accès	La sécurisation des accès aux postes des collaborateurs dois être correctement apréhendée.
Les comptes de chaque utilisateur sont ils protégés par un mot de passe repondant aux normes de sécurité ?	Mettre en place une politique de bloquage si un mot de passe initialisé est non conforme à la norme de l'entreprise. (10 caractères minimum, 1 chiffre, 1 majuscule, 1 caractère spécial).
Sécurisation des postes utilisateurs	Les Postes des utilisateurs représentent des failles, il fait savoir les protéger.
Un antivirus est il mis en place sur les postes de tous les utilisateurs ?	Déployer un antivirus centralisé sur tous les postes et activer les alertes en temps réel. Utiliser les GPO pour bloquer des accès à des types de téléchargements.
Les utilisateurs mettent ils régulièrement leurs logiciels et systèmes d'exploitation à jours ?	Les utilisateurs doivent activer les mises à jours automatiques des logiciels . Un mail automatique peut être programmé pour prévenir les utilisateurs d'une nouvelle version disponible pour un logiciel pour leur permettre de vérifier.
Sécurisation des réseaux	Le réseau doit être sécurisé pour filtrer les flux entrants et sortant et dans le réseau en lui-même.
Un pare-feu existe-t'il pour filtrer le trafic ?	Installer et configurer un pare-feu professionnel avec des règles restrictives et un filtrage. Ils peuvent être ajouter sous un format physique ou virtualisés sur le routeur.
Le routeur inclus t'il une DMZ ?	Identifier les services accessibles depuis l'extérieur de l'entreprise (clients ou accès web). Une DMZ peut alors etre mise en place pour isoler ces services et les isoler du reste du réseau en cas d'attaque malveillante.
Des Vlan sont il en place pour séparer les différents espaces du réseau ?	Segmenter le réseau en VLAN pour limiter la propagation d'un incident. le pare feu peut également analyser les échages entre les VLAN.
Sécurisation des équipements	La DMZ représente un excellent rempars entre le SI interne et l'extérieur.
Une DMZ est elle en place sur le réseau pour isoler des accès non autorisés ?	Mettre en place une DMZ sur un VLAN correctement isolé.
Sécurisation des sauvegardes	Les sauvegardes mettent en sécurité les données à un instant T.
Un plan de sauvegarde est il mis en place ?	Un plan de sauvegarde peut être mis en place en prennent en compte la RTO la RPO garantis une securité optimale des données en cas d'attaque.
Le plan de sauvegarde repond il aux attentes 3-2-1 ?	Le plan de sauvegrde dois prendre en compte une sauvegarde internet (NAS) une sauvegarde externe (NAS externe ou disque dur) et une sauvegarde Cloud.
Le plan de sauvegarde prend il en compte une sauvegarde immuable ?	Une sauvegarde immuable peut etre mise en plce sur le cloud pour concerver les données en lecture seule et bloquer toutes tentatives de corruption.
Sécurisation contre les malwares et ransomwares	Les malware sont le pire énemi des entreprises, il est donc important de s'en protéger.
Un VPN est-il utilisé pour les connexions à distance ?	L'utilisation d'un VPN sécurisé (avec authentification forte) permet de protéger les connexions distantes contre les interceptions et les attaques visant à compromettre le réseau interne.
Les logiciels antivirus sont-ils configurés pour bloquer les comportements suspects(chiffrement) ?	Les antivirus modernes doivent être configurés pour détecter le chiffrement massif de fichiers, les accès anormaux et les comportements typiques des ransomwares afin de bloquer l'attaque avant propagation.
Sécurisation en cas d'attaque	La sauvegarde régulière des données peut considérablement réduire le temps de remise en route en cas d'attaque.
Les données sauvegardées ont une durée de sauvegarde de plus de 7jours ?	Une rétention de sauvegarde d'au moins 7 jours permet de disposer de points de restauration multiples en cas de compromission progressive des données.
Le RTO maximale est infèrieure à 24h ?	Un RTO inférieur à 24h garantit une reprise d'activité rapide et limite les pertes opérationnelles liées à l'interruption du service.
Journalisation et surveillance des logs	Une surveillance du réseau est indispensable pour réagir rapidement en cas d'attaque.
Une surveillance est elle mise en place sur le réseau ?	La mise en place d'une supervision du réseau permet de détecter rapidement les anomalies, les intrusions et les comportements atypiques permettant un réaction rapide.
Les logs sont ils accessibles sur les flux dans le réseau ?	Les journaux doivent être centralisés et accessibles de manière sécurisée pour permettre l'analyse rapide des événements et faciliter les investigations.

Figure 1 - Questionnaire de Sécurité récapitulatif proposé par CESITech

Politique de filtrage

2. Politique de filtrage du pare-feu pfSense Atlantis

Le pare-feu Atlantis constitue le cœur de la sécurisation du réseau principal. Il applique des règles de filtrage par VLAN, permettant de cloisonner les services entre eux, tout en autorisant uniquement les flux strictement nécessaires.

2.1. VLAN Direction (VLAN10)

Le service Direction bénéficie d'un accès complet à l'ensemble du SI :

- Consultation de tous les partages
- Accès aux serveurs métiers
- Accès aux VLAN internes
- Trafic Internet autorisé

Justification :

La Direction a besoin d'une vision globale du SI, notamment pour superviser l'activité, consulter les tableaux de bord ERP, accéder aux services transverses et administrer certains paramètres du système.

2.2. VLAN Ressources Humaines (VLAN20)

Les RH disposent d'un accès restreint mais suffisant pour leurs missions :

- Accès autorisé : DNS, NAS, serveurs métiers (ERP), portail IIS
- Accès interdit : Laboratoire, VLAN Direction, Commercial, Comptabilité, Juridique, etc.
- Accès Internet autorisé (via !RFC1918)

Justification :

- Les RH manipulent des données sensibles → nécessité de cloisonner le service.

- Aucun besoin métier d'accéder aux systèmes du laboratoire ou aux autres services.
- Les flux nécessaires sont exclusivement orientés vers les serveurs du VLAN70.

2.3. VLAN Juridique (VLAN30)

Le service juridique bénéficie d'accès spécifiques :

- Accès autorisé : DNS, serveurs métiers (NAS/AD/ERP), IIS
- Accès interdit : tous les autres VLAN internes (RH, Commercial, BE, LAB, etc.)
- Accès Internet autorisé

Justification :

Le service juridique accède à des dossiers sensibles tels que RH et Client via le NAS. La segmentation permet de réduire l'exposition en cas de compromission et de respecter la confidentialité des échanges.

2.4. VLAN Bureau d'Étude (VLAN40)

Le Bureau d'Étude dispose d'un accès étendu vers les services centraux, ainsi que d'un accès spécifique vers le laboratoire :

- Accès autorisé : DNS, serveurs métiers, portail interne
- Accès au LABO autorisé **via le lien MPLS**, selon le cahier des charges
- Accès interdit : RH, Juridique, Commercial, Comptabilité
- Internet autorisé

Justification :

Le BE échange des données techniques avec le Laboratoire, notamment pour la récupération de fichiers et le traitement des résultats.
Cet accès est également restreint par les ACL sur les partages du NAS pour garantir un mode **lecture seule**.

2.5. VLAN Commercial (VLAN50)

Le réseau Commercial est fortement limité :

- Accès autorisé : DNS, serveurs métiers
- Accès interdit : RH, Juridique, BE, Comptabilité, LABO
- Internet autorisé

Justification :

Les commerciaux n'ont besoin que des informations clients via l'ERP et le NAS. Le cloisonnement empêche toute propagation latérale, notamment depuis des postes potentiellement plus exposés (mobilité, télétravail).

2.6. VLAN Comptabilité (VLAN60)

La Comptabilité dispose de droits proches de ceux des RH :

- Accès autorisé : DNS, serveurs métiers
- Accès interdit : LABO, autres VLAN internes
- Internet autorisé

Justification :

Les besoins se limitent aux applications financières et au ERP. L'isolement est essentiel pour éviter un mouvement latéral vers des données critiques.

2.7. VLAN Serveurs (VLAN70)

Les serveurs nécessitent un accès global :

- Accès total interne
- Accès Internet (mises à jour, antivirus…)

Justification :

Les serveurs doivent communiquer avec l'ensemble des services et pouvoir effectuer des procédures d'administration, de sauvegarde et de synchronisation.

2.8. Interface MPLS (Atlantis)

Le pare-feu Atlantis filtre les flux provenant du site Springfield :

- Autorisation des flux nécessaires : DNS, AD/LDAP, NAS, ERP, IIS
- Accès autorisé au BE
- Accès strictement interdit à tous les autres VLAN
- Blocage des tentatives d'administration du firewall
- Blocage final pour la sécurité

Justification :

- Le LABO ne doit accéder qu'aux ressources métiers centrales.
- Cette segmentation protège Atlantis d'une éventuelle compromission du site distant.
- Les flux autorisés sont conformes aux besoins exprimés lors du cahier des charges.

Ordre	Équipement	Interface	Source	Destination	Protocole	Action	Description
1	pfSense Atlantis	VLAN10_DIRECTION	VLAN10_DIRECTION subnets	Any	Any	Pass	Direction – accès complet à tous les services et VLAN
2	pfSense Atlantis	VLAN20_RH	VLAN20_RH subnets	192.168.1.99	TCP/UDP 53	Pass	RH → DNS (DC)
3	pfSense Atlantis	VLAN20_RH	VLAN20_RH subnets	VLAN70_SERVEURS subnets	Any	Pass	RH → NAS / AD / ERP
4	pfSense Atlantis	VLAN20_RH	VLAN20_RH subnets	192.168.1.162	TCP 80/443	Pass	RH → Web interne IIS DMZ
5	pfSense Atlantis	VLAN20_RH	VLAN20_RH subnets	192.168.1.110	TCP 587	Pass	RH → Serveur Mail (SMTP Submission)
6	pfSense Atlantis	VLAN20_RH	VLAN20_RH subnets	192.168.1.110	TCP 993	Pass	RH → Serveur Mail (IMAPS)
7	pfSense Atlantis	VLAN20_RH	VLAN20_RH subnets	192.168.1.128/27	Any	Block	RH → LAB (interdit)
8	pfSense Atlantis	VLAN20_RH	VLAN20_RH subnets	RFC1918	Any	Block	Blocage RH vers les autres VLAN
9	pfSense Atlantis	VLAN20_RH	VLAN20_RH subnets	!RFC1918	Any	Pass	RH → Internet
10	pfSense Atlantis	VLAN30_JURIDIQUE	VLAN30_JURIDIQUE subnets	192.168.1.99	TCP/UDP 53	Pass	Juridique → DNS
11	pfSense Atlantis	VLAN30_JURIDIQUE	VLAN30_JURIDIQUE subnets	VLAN70_SERVEURS subnets	Any	Pass	Juridique → NAS / AD / ERP
12	pfSense Atlantis	VLAN30_JURIDIQUE	VLAN30_JURIDIQUE subnets	192.168.1.110	TCP 587	Pass	Juridique → Serveur Mail (SMTP Submission)
13	pfSense Atlantis	VLAN30_JURIDIQUE	VLAN30_JURIDIQUE subnets	192.168.1.110	TCP 993	Pass	Juridique → Serveur Mail (IMAPS)
14	pfSense Atlantis	VLAN30_JURIDIQUE	VLAN30_JURIDIQUE subnets	192.168.1.128/27	Any	Block	Juridique → LAB interdit
15	pfSense Atlantis	VLAN30_JURIDIQUE	VLAN30_JURIDIQUE subnets	RFC1918	Any	Block	Juridique → autres VLAN interdit
16	pfSense Atlantis	VLAN30_JURIDIQUE	VLAN30_JURIDIQUE subnets	!RFC1918	Any	Pass	Juridique → Internet
17	pfSense Atlantis	VLAN40_BE	VLAN40_BE subnets	192.168.1.99	TCP/UDP 53	Pass	BE → DNS
18	pfSense Atlantis	VLAN40_BE	VLAN40_BE subnets	VLAN70_SERVEURS subnets	Any	Pass	BE → Serveurs (NAS, AD, ERP)
19	pfSense Atlantis	VLAN40_BE	VLAN40_BE subnets	192.168.1.162	TCP 80/443	Pass	BE → IIS DMZ
20	pfSense Atlantis	VLAN40_BE	VLAN40_BE subnets	192.168.1.128/27	Any	Pass	BE → LAB (autorisé via MPLS)
21	pfSense Atlantis	VLAN40_BE	VLAN40_BE subnets	192.168.1.110	TCP 587	Pass	BE → Serveur Mail (SMTP Submission)
22	pfSense Atlantis	VLAN40_BE	VLAN40_BE subnets	192.168.1.110	TCP 993	Pass	BE → Serveur Mail (IMAPS)
23	pfSense Atlantis	VLAN40_BE	VLAN40_BE subnets	VLAN20_RH subnets	Any	Block	BE → RH interdit
24	pfSense Atlantis	VLAN40_BE	VLAN40_BE subnets	VLAN30_JURIDIQUE subnets	Any	Block	BE → Juridique interdit
25	pfSense Atlantis	VLAN40_BE	VLAN40_BE subnets	RFC1918	Any	Block	BE → autres VLAN internes
26	pfSense Atlantis	VLAN40_BE	VLAN40_BE subnets	!RFC1918	Any	Pass	BE → Internet
27	pfSense Atlantis	VLAN50_COMMERCIAL	VLAN50_COMMERCIAL subnets	192.168.1.99	TCP/UDP 53	Pass	Commercial → DNS
28	pfSense Atlantis	VLAN50_COMMERCIAL	VLAN50_COMMERCIAL subnets	VLAN70_SERVEURS subnets	Any	Pass	Commercial → NAS / AD / ERP
29	pfSense Atlantis	VLAN50_COMMERCIAL	VLAN50_COMMERCIAL subnets	192.168.1.110	TCP 587	Pass	Commercial → Serveur Mail (SMTP Submission)
30	pfSense Atlantis	VLAN50_COMMERCIAL	VLAN50_COMMERCIAL subnets	192.168.1.110	TCP 993	Pass	Commercial → Serveur Mail (IMAPS)
31	pfSense Atlantis	VLAN50_COMMERCIAL	VLAN50_COMMERCIAL subnets	VLAN20_RH subnets	Any	Block	Commercial → RH interdit
32	pfSense Atlantis	VLAN50_COMMERCIAL	VLAN50_COMMERCIAL subnets	VLAN30_JURIDIQUE subnets	Any	Block	Commercial → Juridique interdit
33	pfSense Atlantis	VLAN50_COMMERCIAL	VLAN50_COMMERCIAL subnets	192.168.1.128/27	Any	Block	Commercial → LAB interdit
34	pfSense Atlantis	VLAN50_COMMERCIAL	VLAN50_COMMERCIAL subnets	!RFC1918	Any	Pass	Commercial → Internet
35	pfSense Atlantis	VLAN60_COMPTA	VLAN60_COMPTA subnets	192.168.1.99	TCP/UDP 53	Pass	Compta → DNS
36	pfSense Atlantis	VLAN60_COMPTA	VLAN60_COMPTA subnets	VLAN70_SERVEURS subnets	Any	Pass	Compta → Serveurs
37	pfSense Atlantis	VLAN60_COMPTA	VLAN60_COMPTA subnets	192.168.1.110	TCP 587	Pass	Compta → Serveur Mail (SMTP Submission)
38	pfSense Atlantis	VLAN60_COMPTA	VLAN60_COMPTA subnets	192.168.1.110	TCP 993	Pass	Compta → Serveur Mail (IMAPS)
39	pfSense Atlantis	VLAN60_COMPTA	VLAN60_COMPTA subnets	192.168.1.128/27	Any	Block	Compta → LAB interdit
40	pfSense Atlantis	VLAN60_COMPTA	VLAN60_COMPTA subnets	RFC1918	Any	Block	Compta → autres VLAN
41	pfSense Atlantis	VLAN60_COMPTA	VLAN60_COMPTA subnets	!RFC1918	Any	Pass	Compta → Internet
42	pfSense Atlantis	VLAN70_SERVEURS	VLAN70_SERVEURS subnets	Any	Any	Pass	Serveurs → Accès global
43	pfSense Atlantis	MPLS	VLAN80_LABO subnets	192.168.1.99	TCP/UDP 53	Pass	LAB → DNS AD Atlantis
44	pfSense Atlantis	MPLS	VLAN80_LABO subnets	VLAN70_SERVEURS subnets	Any	Pass	LAB → Serveurs (NAS, AD, ERP)
45	pfSense Atlantis	MPLS	VLAN80_LABO subnets	192.168.1.162	TCP 80/443	Pass	LAB → IIS interne (DMZ)
46	pfSense Atlantis	MPLS	VLAN80_LABO subnets	VLAN40_BE subnets	Any	Pass	LAB → Bureau d'Étude (lecture via NAS/ERP)
47	pfSense Atlantis	MPLS	VLAN80_LABO subnets	RFC1918	Any	Block	LAB → Tous les VLAN Atlantis interdits (RH, Juridique, Compta...)
48	pfSense Atlantis	MPLS	10.10.10.0/30	Any	Any	Pass	Flux techniques MPLS : ping, traceroute, retour des connexions
49	pfSense Atlantis	MPLS	Any	pfSense Atlantis Address	Any	Block	Protection du firewall (pas d'admin via MPLS)
50	pfSense Atlantis	MPLS	Any	Any	Any	Block	Blocage final (sécurité maximale)

Figure 2 - Tableau de Filtrage de Atlantis

3. Politique de filtrage du pare-feu pfSense Springfield

3.1. VLAN Labo (VLAN80)

Les règles sont très restrictives :

- Accès autorisé : DNS, serveurs métiers (NAS, ERP, AD), IIS, Bureau d'Étude
- Accès interdit : tous les autres VLAN Atlantis
- Accès Internet autorisé
- Blocage final

Justification :

- Le LABO manipule des données techniques et potentiellement sensibles.
- Les postes sont variés et parfois connectés à des équipements spécialisés → risques accrus.
- L'accès au reste du réseau doit être strictement contrôlé.

3.2. Interface MPLS (Springfield)

Cette interface filtre les flux provenant d'Atlantis :

- Direction → accès complet LABO
- RH → accès LABO autorisé
- BE → accès LABO autorisé
- Tous les autres VLAN → interdits
- Pas d'administration du firewall via MPLS
- Blocage final

Justification :

- Le site Atlantis est la source légitime des accès vers le LABO.
- Les services autorisés correspondent exactement aux besoins métiers (Direction, RH, BE).
- Un cloisonnement fort garantit la sécurité du site distant.

Ordre	Équipement	Interface	Source	Destination	Protocole	Action	Description
1	Springfield	VLAN80_LABO	VLAN80_LABO subnets	192.168.1.99	TCP/UDP 53	Pass	LAB → DNS du DC (Atlantis)
2	pfSense Springfield	VLAN80_LABO	VLAN80_LABO subnets	VLAN70_SERVEURS subnets	Any	Pass	LAB → Serveurs Atlantis (NAS/AD/ERP)
3	Springfield	VLAN80_LABO	VLAN80_LABO subnets	192.168.1.162	TCP 80/443	Pass	LAB → IIS DMZ (site web interne)
4	Springfield	VLAN80_LABO	VLAN80_LABO subnets	192.168.1.48/28 (BE)	Any	Pass	NAS/ERP)
5	pfSense Springfield	VLAN80_LABO	VLAN80_LABO subnets	192.168.1.110	TCP 587	Pass	LABO→ Serveur Mail (SMTP Submission)
6	Springfield	VLAN80_LABO	VLAN80_LABO subnets	192.168.1.110	TCP 993	Pass	LABO→ Serveur Mail (IMAPS)
7	pfSense Springfield	VLAN80_LABO	VLAN80_LABO subnets	RFC1918	Any	Block	LAB → Tout autre réseau privé Atlantis interdit
8	Springfield	VLAN80_LABO	VLAN80_LABO subnets	!RFC1918	Any	Pass	LAB → Internet autorisé
9	Springfield	VLAN80_LABO	VLAN80_LABO subnets	Any	Any	Block	Sécurité : bloque tout le reste
10	Springfield	MPLS	VLAN10_DIRECTION subnets	VLAN80_LABO subnets	Any	Pass	LABO
11	Springfield	MPLS	VLAN20_RH subnets	VLAN80_LABO subnets	Any	Pass	RH Atlantis → accès LABO autorisé
12	pfSense Springfield	MPLS	VLAN40_BE subnets	VLAN80_LABO subnets	Any	Pass	Bureau d'Étude → accès LABO (lecture/lecture seule via ACL)
13	Springfield	MPLS	RFC1918	VLAN80_LABO subnets	Any	Block	interdit
14	pfSense Springfield	MPLS	Any	pfSense Springfield Address	Any	Block	Protection du firewall (aucune admin depuis MPLS)
15	Springfield	MPLS	Any	Any	Block	Blocage final : sécurité Zero-Trust	

Figure 3 - Tableau de filtrage de Springfield

Scripts

Afin de faciliter la maintenance du S.I. et l'adaptabilité en taille (expansion de la société ou arrivée de nouveaux membres du personnel) nous avons mis en place des scripts PowerShell faciles d'utilisation. Ceux-ci sont exécutables par des techniciens même inexpérimentés.

XanaduScripts est un module PowerShell interactif conçu pour simplifier la gestion des utilisateurs Active Directory. Il offre une interface en ligne de commande intuitive avec navigation au clavier pour effectuer les opérations courantes d'administration.

Parmi les fonctionnalités proposées par les scripts nous retrouvons :

- Gestion des utilisateurs
    - Création
    - Modification
    - Suppression
    - Affichage de la liste complète des utilisateurs
    - Réinitialisation de mot de passe utilisateur
- Gestion du serveur DC
    - Vérifications du DC
    - Vérification de l'AD
    - Vérifications complètes
- Gestion de l'ERP
    - Sauvegarde des bases de données dans l'ERP
    - Vérification de l'ERP
    - Vérifications complètes

1. Gestion des utilisateurs

Le script de gestion des utilisateurs affiche dans un premier temps un menu proposant des options. L'utilisateur peut alors choisir son action : créer un nouvel utilisateur, modifier un compte existant, supprimer un compte ou visualiser le liste complète des utilisateurs. Si le fichier est lancé avec un nom d'action à réaliser alors

le menu ne s'affiche pas et la fonction se déclenche sans nécessiter l'intervention de l'utilisateur. A l'inverse si aucun argument n'est saisi au lancement du script le menu s'affiche et l'utilisateur peux naviguer dans le menu pour sélectionner son option.

```powershell
function Start-UserManagement {
    <#
    .SYNOPSIS
        Point d'entrée principal du script.
    .EXAMPLE
        Start-UserManagement
    #>
    [CmdletBinding(DefaultParameterSetName='Encode')]
    param(
        [ValidateSet("Create", "Update", "Delete", "List")]
        [string]$Action,

        [string]$Nom,
        [string]$Prenom,
        [string]$Group,
        [string]$SamAccountName
    )

    if ($Action) {
        switch ($Action) {
            "Create" { Invoke-CreateUser -Nom $Nom -Prenom $Prenom -Group $Group }
            "Update" { Invoke-UpdateUser }
            "Delete" { Invoke-DeleteUser }
            "List"   { Invoke-ListUsers }
        }
        return
    }

    $continue = $true
    while ($continue) {
        $choice = Show-MainMenu

        switch ($choice) {
            "Créer un utilisateur"    { Invoke-CreateUser }
            "Modifier un utilisateur" { Invoke-UpdateUser }
            "Supprimer un utilisateur"{ Invoke-DeleteUser }
            "Lister les utilisateurs" { Invoke-ListUsers }
            "Réinitialiser le mot de passe utilisateur" { Invoke-ResetUserPassword }
            "Quitter"                 { $continue = $false }
            $null                     { $continue = $false }
        }
    }

    Write-Host "Au revoir !" -ForegroundColor Cyan
}
```

Figure 4 - Script de gestion des comptes utilisateur

En prenant l'exemple de l'ajout d'un compte utilisateur le script demande un nom, un prénom ainsi qu'un groupe pour pouvoir créer l'user au bon endroit dans l'DA.

L'opération peut être annulée à tout moment pas l'administrateur.

```powershell
function Invoke-CreateUser {
    <#
    .SYNOPSIS
        Lance le processus de création d'un utilisateur.
    #>
    [CmdletBinding()]
    param (
        [string]$Nom,
        [string]$Prenom,
        [string]$Group
    )

    if (-not $Nom) {
        $Nom = Read-HostWithEscape "Veuillez spécifier le nom (ESC pour annuler)"
        if (-not $Nom) {
            Write-Host "Opération annulée par l'utilisateur." -ForegroundColor Yellow
            return
        }
    }

    if (-not $Prenom) {
        $Prenom = Read-Host "Veuillez spécifier le prénom (ESC pour annuler)"
        if (-not $Prenom) {
            Write-Host "Opération annulée par l'utilisateur." -ForegroundColor Yellow
            return
        }
    }

    if ($Group -notin $myGroups) {
        $Group = Select-OUGroup
        if (-not $Group -or $Group -eq "Quitter") {
            Write-Host "Opération annulée par l'utilisateur." -ForegroundColor Yellow
            return
        }
    }
```

Figure 5 - Script de saisi des informations d'un nouvel utilisateur dans l'AD

Une fois les valeurs saisies une vérification des informations du nouvel utilisateur doit être faite pas l'administrateur avant que le compte ne soit envoyé dans l'AD.

```powershell
    $SamAccountName = "$($Prenom.ToLower()).$($Nom.ToLower())"
    $DisplayName    = "$Prenom $Nom"
    $UserPrincipalName = "$SamAccountName@$((Get-ADDomain).DNSRoot)"

    Write-Host "`n=== User to create ===" -ForegroundColor Green
    Write-Host "  Display Name : $DisplayName"
    Write-Host "  SamAccountName : $SamAccountName"
    Write-Host "  UPN : $UserPrincipalName"
    Write-Host "  Group : $Group"
    Write-Host ""

    $confirmation = Read-Host "Confirmez-vous la création de cet utilisateur ? (O/N)"
    if ($confirmation -ine 'O') {
        Write-Host "Opération annulée par l'utilisateur." -ForegroundColor Yellow
        return
    }
    New-XanaduUser -Nom $Nom `
        -Prenom $Prenom `
        -Group $Group `
        -Path "OU=Users,OU=Xanadu,$((Get-ADDomain).DistinguishedName)"
}
```

Figure 6 - Script de création d'un nouvel utilisateur dans l'AD

2. Réinitialisation de mot de passe utilisateur

Le mot de passe utilisateur peut également être réinitialisé avec des scripts. Pour cela le nom de l'utilisateur doit être connu et le nouveau mot de passe également. Le nouveau mot de passe est ainsi ajouté au compte utilisateur dans l'AD une fois la fonction terminée.

```powershell
function Invoke-ResetUserPassword {
    <#
    .SYNOPSIS
        Lance le processus de réinitialisation du mot de passe d'un utilisateur.
    #>
    [CmdletBinding()]

    $user = Select-XanaduUser
    if (-not $user) {
        Write-Host "Opération annulée." -ForegroundColor Yellow
        return
    }

    try {
        $newPassword = ConvertTo-SecureString -AsPlainText "Xanadu$(Get-Date -Format 'yyyy')!" -Force

        Get-ADUser -Identity $user.SamAccountName |
            Set-ADAccountPassword -Reset -NewPassword $newPassword -PassThru |
            Set-ADUser -ChangePasswordAtLogon $true

        Write-Host "Mot de passe réinitialisé pour '$($user.DisplayName)'." -ForegroundColor Green
    } catch {
        Write-Host "Erreur lors de la réinitialisation du mot de passe : $_" -ForegroundColor Red
        return
    }
}
```

Figure 7 - Script de réinitialisation d'un mot de passe utilisateur

3. Vérifications du DC et de l'AD

Le script de vérification du DC a pour but une vérification complète des fonctionnalités dont celles de l'AD qui peut également être déclenchée séparément.

```
function Verify-DCIntegrity {
    <#
    .SYNOPSIS
        Point d'entrée principal du script.
    .EXAMPLE
        Verify-DCIntegrity -Mode "All"
        Exécute tous les tests DCDiag.
    .EXAMPLE
        Verify-DCIntegrity -Mode "DC"
        Exécute uniquement les tests liés au contrôleur de domaine.
    .EXAMPLE
        Verify-DCIntegrity -Mode "AD"
        Exécute uniquement les tests liés à Active Directory.
    .PARAMETER Mode
        Spécifie le mode des tests à exécuter. Valeurs possibles : "All", "DC", "AD". Par défaut : "All".
    #>
```

Figure 8 – Commentaires du script de vérification de l'AD et du DC

Lors de l'exécution du script, un grand nombre de test sont réalisés sur l'AD ou le DC.

```
    $ADTests = @(
        "Replications",         # Réplication AD
        "ObjectsReplicated",    # Objets répliqués
        "NCSecDesc",            # Permissions partitions AD
        "KnowsOfRoleHolders",   # Rôles FSMO
        "VerifyReferences",     # Intégrité références AD
        "CrossRefValidation",   # Cross-references
        "CheckSDRefDom",        # Security Descriptors
        "MachineAccount",       # Compte machine AD
        "RidManager",           # Pool RID
        "Intersite",            # Réplication inter-sites
        "KccEvent"              # Topologie réplication
    )
    $DCTests = @(
        "Connectivity",       # Connectivité réseau
        "Advertising",        # Annonces DNS
        "Services",           # Services Windows
        "NetLogons",          # Service Netlogon
        "SysVolCheck",        # Partage SYSVOL
        "FrsEvent",           # Réplication SYSVOL (FRS)
        "DFSREvent",          # Réplication SYSVOL (DFS-R)
        "SystemLog",          # Erreurs système
        "LocatorCheck"        # Localisation DC
    )
```

Lors du lancement du script, une option peut être sélectionnée pour se lancer instantanément.

```
    $DCDiagTestsToRun = switch ($Mode) {
        "DC"  { $DCTests }
        "AD"  { $ADTests }
        "All" { $DCTests + $ADTests }
    }
```

Figure 10 – Choix du script de vérification

4. Vérification de l'ERP

Afin de réaliser des vérifications sur la base de données de l'ERP nous avons une troisième commande cmdlet permettant de faire la sauvegarde et de vérifier l'intégrité de notre base de données.

```
109     process {
110         switch ($Mode) {
111             "Save" {
112                 Save-Database
113             }
114             "Verify" {
115                 Verify-LastBackup
116             }
117             "All" {
118                 Save-Database
119                 Verify-LastBackup
120             }
121         }
122     }
```

Figure 11 - Choix du script de vérification sur l'ERP

La sauvegarde de la base de données, via le fichier sqlits, se fait sur notre serveur NAS, avec un dossier qui se doit d'être accessible.

Si un des deux critères n'est pas respecté, on sort de la fonction proprement avant le lancement de tout processus.

```
function Write-Info($msg) {
    Write-Host "[INFO] $msg"
}

function Write-ErrorMsg($msg) {
    Write-Host "[ERROR] $msg" -ForegroundColor Red
}

function Save-Database {
    if (-not (Test-Path $script:DbPath)) {
        Write-ErrorMsg "Base SQLite introuvable : $($script:DbPath)"
        return
    }
    if (-not (Test-Path $script:NasRoot)) {
        Write-ErrorMsg "Dossier NAS inexistant : $($script:NasRoot)"
        return
    }

    $srcObj   = Get-Item $script:DbPath
    $src      = $srcObj.FullName
    $ts       = Get-Date -Format "yyyy-MM-dd_HH-mm"
    $destFile = Join-Path $script:NasRoot "xanadu_$ts.db"

    Write-Info "Copie de '$src' vers '$destFile'..."
    Copy-Item -LiteralPath $src -Destination $destFile -Force
    Write-Info "Sauvegarde terminée."

    # Rotation 30 jours
    Get-ChildItem $script:NasRoot -Filter "xanadu_*.db" |
        Where-Object { $_.LastWriteTime -lt (Get-Date).AddDays(-30) } |
        ForEach-Object {
            Write-Info "Suppression ancienne sauvegarde : $($_.FullName)"
            Remove-Item $_.FullName -Force
        }
}
```

Figure 12 - Scripts de sauvegarde de la base de données de l'ERP sur le NAS

Get-Item récupère l'objet fichier et son chemin complet ("source de vérité").

$ts est un timestamp (année-mois-jour_heure-minute).

Le nom de sauvegarde est construit comme xanadu_YYYY-MM-DD_HH-mm.db → lisible et triable.

Ensuite on applique la politique de rétention en listant tous les fichier xanadu dans le répertoire de backup, et on ne garde que ceux plus récents que 30 jours. On supprime automatiquement les plus anciens, ce qui nous permet de ne pas saturer le NAS sans intervention manuelle.

```
function Verify-LastBackup {
    if (-not (Test-Path $script:NasRoot)) {
        Write-ErrorMsg "Dossier de sauvegarde NAS inexistant : $($script:NasRoot)"
        return
    }

    $last = Get-ChildItem $script:NasRoot -Filter "xanadu_*.db" |
            Sort-Object LastWriteTime -Descending |
            Select-Object -First 1

    if (-not $last) {
        Write-ErrorMsg "Aucune sauvegarde trouvée dans $($script:NasRoot)."
        return
    }

    Write-Info "Dernière sauvegarde : $($last.FullName)"
    Write-Info ("Taille : {0:N0} octets" -f $last.Length)
    Write-Info ("Date   : {0}" -f $last.LastWriteTime)
}
```

Figure 13 - Analyse de la dernière sauvegarde dans le NAS

On recherche la dernière sauvegarde disponible en se basant sur la date de modification.

Si aucune sauvegarde n'est trouvée, message d'erreur explicite. sinon, affichage des métadonnées utiles come le chemin complet, la taille ou la date.

Enfin notre bloc de processus permet de gérer les différents scripts intégrés à la commande pour lancer manuellement la sauvegarde ou la vérification

```
process {
    switch ($Mode) {
        "Save"   { Save-Database }
        "Verify" { Verify-LastBackup }
        "All"    { Save-Database; Verify-LastBackup }
    }
}
```

Figure 14 - Choix des possibilités de script sur la base de données de l'ERP

On appelle les différentes options en paramètre

```
Save-Erp           # équivalent All
Save-Erp -Mode Save
Save-Erp -Mode Verify
```

Figure 15 - Paramètre de lancement d'un mode de vérification sur l'ERP

Supervision

Pour améliorer la sécurité de l'entreprise XANADU, il est important de mettre en place des fonctionnalités de supervision. Cela nous permettra à nous et aux personnels de XANADU en charge de la surveillance de pouvoir voir et analyser les données des différents serveurs, comptes utilisateurs ou autres objets qui compose l'infrastructure mis en place.

1. Tableau des actions de Supervision

Description	Criticité	Source	Action déclenchée	Justification sécurité
Tentative de connexion échouées	Haute	Active Directory (DC)	Alerte mail + blocage du compte	Détection d'attaques par brute force
Connexion Administrateur	Haute	Active Directory (DC)	Alerte mail	Suivi des accès sensibles
Modification de GPO	Haute	Contrôleur de Domaine	Alerte mail	Prévention des modifications non autorisées
Désactivation de l'antivirus	Haute	Antivirus	Alerte mail + isolement automatique	Risque immédiat de compromission
Activité réseau anormale	Moyenne	Routeur	Alerte + capture réseau automatique	Analyse de comportements suspects
Appareil inconnu sur le réseau	Moyenne	Switch	Alerte + blocage automatique	Protection contre les intrusions physiques
Arrêt d'une fonctionnalité système	Haute	Serveur DC	Alerte + Tentative de relance	Prévention d'un arrêt imprévu d'une fonctionnalité
Échec de sauvegarde complète	Haute	Sauvegarde	Tentative de relance de sauvegarde	Protection de l'intégrité des données
Échec de sauvegarde critique	Haute	Sauvegarde	Tentative de relance de sauvegarde	Données hautement sensibles à restaurer
Échec de sauvegarde ERP	Moyenne	Sauvegarde	Tentative de relance de sauvegarde	Continuité de service applicative

Figure 16 - Tableau de Supervision

2. Description des actions de Supervision

Comme vu dans le tableau ci-dessus, nous avons décidé de mettre en place plusieurs mécanismes de surveillance pour suivre les actions suspectes pouvant se produire dans l'infrastructure. En utilisant les différents outils de supervision, nous pouvons mettre en place des alertes, isolement, relance de sauvegarde qui seront dédiés à la sécurité et la maintenance.

2.1 Supervision d'authentification

Nous avons prévu plusieurs actions de supervision concernant des problèmes pouvant survenir lors de la connexion des utilisateurs. Par exemple, si l'outil de supervision détecte que, pour un même compte utilisateur, il y a eu 3 tentatives de mots de passes échoués en moins de 1 minute, le compte utilisateur sera bloqué temporairement, le temps d'analyser la situation. On va également recevoir une alerte par mail pour nous communiquer des informations comme le compte utilisé, le poste de travail concernés ainsi que l'heure des tentatives. Avec cet ensemble d'information, on peut dans un premier temps déterminer s'il s'agit d'une attaque par brute force ou simplement d'un utilisateur maladroit. Dans un second temps, on élaborera une stratégie pouvant éviter que ce genre de situation se reproduise en sensibilisant le personnel ou en renforçant la sécurité.

Dans la même volonté, il est important de veiller à ce que le compte administrateur ne soit pas accessible par tout le monde à tout moment. Pour cela, une supervision de ce compte sera mise en place. S'il y a une quelconque tentative de connexion qui semble anormale par rapport au poste de travail, ou à l'horaire de connexion par exemple, le compte administrateur sera automatiquement bloqué. Il faudra attendre l'intervention d'un autre compte administrateur pour le débloquer. De plus, de la même manière que pour la supervision précédente, une alerte par mail est également mise en place. Que cela soit une tentative réussie ou échouée, nous aurons des informations comme l'horaire de l'événement, le compte administrateur ciblé, le poste de travail utilisé ou tout autre indication permettant d'identifier l'auteur de l'événement. Grâce à cela, nous pourrons, comme pour la connexion échouée, établir une stratégie pour identifier la menace et éviter que cela se reproduise.

2.2 Supervision de Sécurité

Pour veiller à une sécurité du réseau, plusieurs autres actions de supervision sont mises en place comme la présence d'alertes sur des modifications non autorisés ou une anomalie sur le réseau. Dans le cas où un utilisateur désactiverait son antivirus, un mail nous sera envoyé pour nous prévenir et nous transmettre les informations descriptives de l'événement. La présence d'un antivirus, la désactivation non autorisée

provoquerait une faille dans l'infrastructure du réseau. Pour éviter cela, le poste de travail sera isolé du réseau pour contrer une attaque globale sur l'entièreté du réseau de l'entreprise.

Certains des GPO mis en place ne devraient pas être modifiés. Afin de vérifier qu'ils restent intacts, une supervision vérifie l'état de modification des GPO définis. Comme pour la plupart des autres actions de supervisions, nous recevrons une alerte mail pour nous prévenir et nous communiquer les principales informations sur changement. Nous estimons que la modification de ces GPO pourrait résulter d'un outrepassement des autorisations accordées à un utilisateur et qu'il est important de prévenir ce genre de cas.

Concernant les possibles anomalies pouvant survenir sur le réseau, il est possible qu'un poste de travail se rajoute sur celui-ci alors qu'il n'est pas prévu. Ne connaissant pas la provenance de ce poste de travail, nous avons décidé d'appliquer un blocage automatique de cet appareil. Ainsi, le temps d'analyser ce nouvel ordinateur, nous évitons une potentiel intrusion physique et renforçons la sécurité du réseau.

Dans le cas où une fonctionnalité du serveur DC tombe en panne, une action de supervision nous alertera de la fonctionnalité avec les informations importantes. De plus, il sera automatiquement exécuté une tentative pour relancer le service tombé en panne. Nous pourrons ainsi analyser cette panne et si elle persiste, trouver un moyen par nous même de relancer le service ou la fonctionnalité qui est tombé en panne.

Au sein du réseau de XANADU, le réseau entre les appareils ainsi que le réseau internet ont besoin d'être stables pour garantir un environnement de travail adéquat à tous les utilisateurs. Pour éviter de perturber ce réseau, nous avons mis en place de la supervision pour détecter un usage anormal du réseau par un utilisateur. De cette manière, nous pouvons détecter ces anomalies et constater des téléchargements anormaux ou la lecture de média trop conséquent.

2.3 Supervision de sauvegarde

En accord avec le plan de sauvegarde décrit dans le livrable précédent, nous devons pouvoir restaurer les données suivant leur criticité et leur importance. Nous avons donc établi que pour chacune des sauvegardes, il faut anticiper le cas où celle-ci ne s'exécute pas correctement. Lors de la sauvegarde complète du dimanche, si une erreur survient, une action de supervision pourra la capter. Dans ce cas, une nouvelle tentative de sauvegarde sera effectuée. L'action de supervision pourra détecter si la sauvegarde échoue 3 fois à la suite et ainsi nous prévenir pour analyser et lancer la réparation. Cela nous permet de protéger l'intégrité des données et d'assurer la restauration des données.

Il y a également la même action appliquée sur la sauvegarde quotidienne et prioritairement sur les données critiques afin de pouvoir plus facilement restaurer ces données dans le temps donné. De la même manière, les sauvegardes de l'ERP sont aussi soumises à une supervision qui nous permet de prévenir la perte de données.

Conclusion :

Cet avancement dans le projet nous permet de prendre en compte de nouveaux aspect techniques et notamment :

- La politique de filtrage à déployer sur les pares-feux. Une description des règles de filtrage mises en place et leurs objectifs.

- 10 scripts commentés d'administration permettant la maintenance quotidienne du système informatique ainsi que son évolutivité au cours du temps.

- Le dispositif de surveillance mis en place sur notre système ainsi que les événements déclencheurs d'alerte. Nous avons distingué les différentes conditions à l'application de la supervision.

- Nous allons également fournis à l'entreprise Xanadu un questionnaire de sécurité permettant d'identifier les vulnérabilités et de mesurer le niveau de sécurité de leur infrastructure, des données et des processus, ainsi que le respect des normes de sécurité.

Glossaire

SI (Système d'Information) : Ensemble organisé de ressources qui permet de collecter, stocker, traiter et distribuer de l'information.

RH(Ressources Humaines) : Services de Xanadu.

BE (Bureau d'Etude) : Services de Xanadu.

VPN (Virtual Private Network) : Réseau privé virtuel reliant des ordinateurs distants.

MPLS (MultiProtocol Label Switching) : Technique de communication sur un réseau.

Rançongiciel : Logiciel bloquant l'accès aux données et demandant une rançon.

ERP (Entreprise Resource Planning) : Logiciel gérant les processus d'une entreprise.

SLA (Service Level Agreement) : Partie d'un contrat entre un prestataire informatique et son client.

DNS (Domain Name System) : Service informatique associant un nom de domaine à une IP.

DHCP (Dynamic Host Configuration Protocol) : Protocole réseau attribuant une IP à une machine.

DC (Domain Controller) : Ordinateur serveur assurant l'authentification de sécurité.

NAS (Network Attached Storage) : Serveur de fichier stockant les données.

ESXI (Elastic Sky X integrated) : Hyperviseur de type 1 déployant des ordinateurs virtuels.

AD (Active Directory) : Fournit services d'identification et d'authentification des membres d'un réseau.

DMZ (Delimitarized Zone) : Sous réseau séparé du local et de l'internet par un pare feu.

VLAN (Virtual Local Area Network) : Réseau local virtuel indépendant.

Firewall : Logiciel permettant d'assurer la sécurité d'un réseau.

GPO (Group Policy Object) : Fonctions de gestions des ordinateurs et des utilisateurs de l'Active Directory.

RTO (Recovery Time Objective) : Durée maximal d'interruption admissible dans une organisation.

IIS (Internet Information Server) : Un serveur Web (HTTP).

ACL (Access Control List) : Une liste des adresses et ports autorisés ou interdits par un pare-feu.