Projet : Sécurisez le réseau d'une grande entreprise

Table des matières

Plan-Projet : Sécurisation de l'Architecture Réseau pour une PME

1. Introduction

Ce plan vise à sécuriser l'architecture du système d'information (SI) de l'entreprise **Open Pharma** en identifiant les failles existantes, en répertoriant les équipements nécessaires pour les combler, puis en chiffrant et en planifiant la mise en œuvre. L'objectif est de renforcer la résilience et la sécurité globale du réseau en réduisant les risques de cyberattaques, tout en assurant une continuité des services.

Contexte :

- PME d'environ 11 personnes.
- Budget : 10 000 €, avec l'assistance de l'équipe technique interne pour l'installation.
- Objectif : Renforcer la sécurité du réseau en réutilisant des équipements existants et en achetant des nouveaux équipements.

2. Étape 1 : Identification des Failles de l'Architecture Actuelle

Une analyse approfondie de l'architecture actuelle a révélé plusieurs vulnérabilités et faiblesses qui nécessitent des solutions adaptées. Les failles identifiées incluent :

a. **Manque de pare-feu de nouvelle génération (NGFW)** : La sécurité périmétrique repose sur un pare-feu standard qui n'offre pas une inspection approfondie des flux applicatifs.

b. **Absence de contrôle d'accès réseau (NAC)** : Aucun dispositif ne permet de vérifier les équipements se connectant au réseau interne.

c. **Absence de VPN** : Aucune connexion sécurisée entre différents réseaux via internet.

d. **Absence de segmentation réseau** : Pas de segmentation réseau via VLANs.

e. **Absence de séparation de la couche core et la couche d'accès** : Aucun dispositif ne permet de fournir des services de routage et de sécurité avant de transmettre le trafic à la couche cœur (core) ou à l'extérieur du réseau.

f. **Manque de proxy** : Absence d'intermédiaire entre les utilisateurs et Internet, ni de filtrage pour les requêtes.

g. **L'utilisation de systèmes d'exploitation obsolètes comme Windows Server 2012 R2 et Debian 8 :** peut entraîner plusieurs vulnérabilités et risques de sécurité

3. Étape 2 : Répertorier les Équipements de Sécurisation

Pour sécuriser notre architecture, nous avons identifié les équipements suivants pour combler les failles :

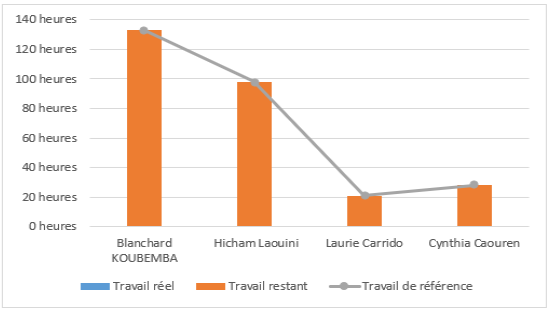
Équipement	Marque et Modèle	Rôle
Pare-feu NGFW (IPS/IDS)	Fortinet FortiGate 60F	Protection avancée contre les menaces, filtrage du trafic réseau, inspection des paquets en profondeur.
Contrôle d'accès réseau (NAC)	Cisco Identity Services Engine (ISE) - Appliance virtuelle pour PME	Empêche les utilisateurs et appareils non autorisés d'accéder au réseau, gestion des politiques de sécurité centralisée.
Passerelle VPN	Perimeter 81 - Plan Essentiel	Création de connexions sécurisées entre différents réseaux via Internet, chiffrement du trafic.
Veeam Backup Essentials	Veeam Data Platform Essentials	Sauvegarde et restauration des données critiques, protection contre les pertes de données et les cyberattaques.
Proxy	Squid Proxy	Intermédiaire entre les utilisateurs et Internet, filtrage des requêtes pour améliorer la sécurité et la performance du réseau.

4. Étape 4 : Chiffrage et Planification de la Sécurisation

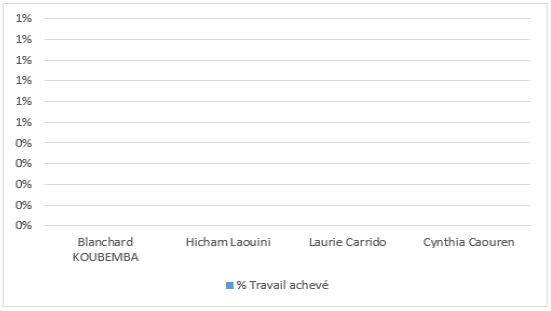
La main d'œuvre sera facturée à hauteur de 1729 euros ce qui correspond à 133 heures de travail pour 13 euros de l'heure.

VUE D'ENSEMBLE DES RESSOURCES

STATISTIQUES DES RESSOURCES
État du travail pour toutes les ressources de travail.



ÉTAT DU TRAVAIL
% du travail accompli par toutes les ressources de travail.



ÉTAT DES RESSOURCES
Travail restant pour toutes les ressources de travail.

Nom	Début	Fin	Travail restant
Blanchard KOUBEMBA	Lun 16/09/24	Mer 23/10/24	133 heures
Hicham Laouini	Lun 16/09/24	Mar 22/10/24	98 heures
Laurie Carrido	Lun 16/09/24	Mar 15/10/24	21 heures
Cynthia Caouren	Lun 16/09/24	Ven 04/10/24	28 heures

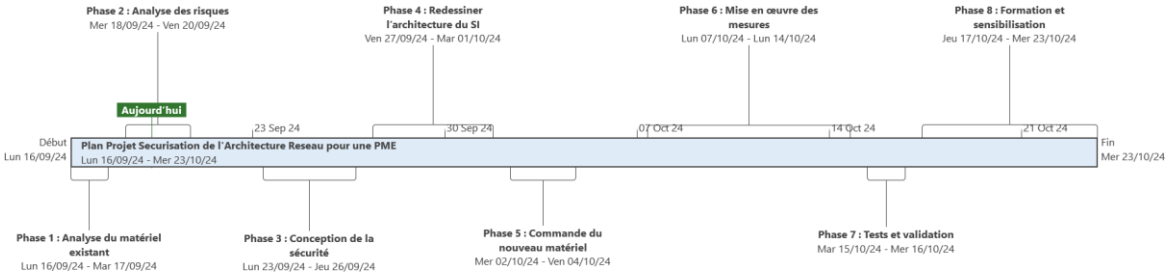
5. Chiffrage des Équipements

Équipement	Quantité	Prix unitaire HT	Total
Fortinet FortiGate 60F	1	1 400,00 €	1 400,00 €
Cisco Identity Services Engine (ISE) - Appliance virtuelle pour PME	1	2 200,00 €	2 200,00 €
Perimeter 81 - Plan Essentiel	1	1 000,00 €	1 000,00 €
Veeam Data Platform Essentials	1	1 500,00 €	1 500,00 €
Squid Proxy	1	1 000,00 €	1 000,00 €
Debian 12	3	- €	- €
Microsoft Windows Server 2019 - licence - 5 licences d'accès client périphériques	6	169,98 €	1 019,88 €
Total			8 119,88 €

Coût total du projet : 9 848,88 €

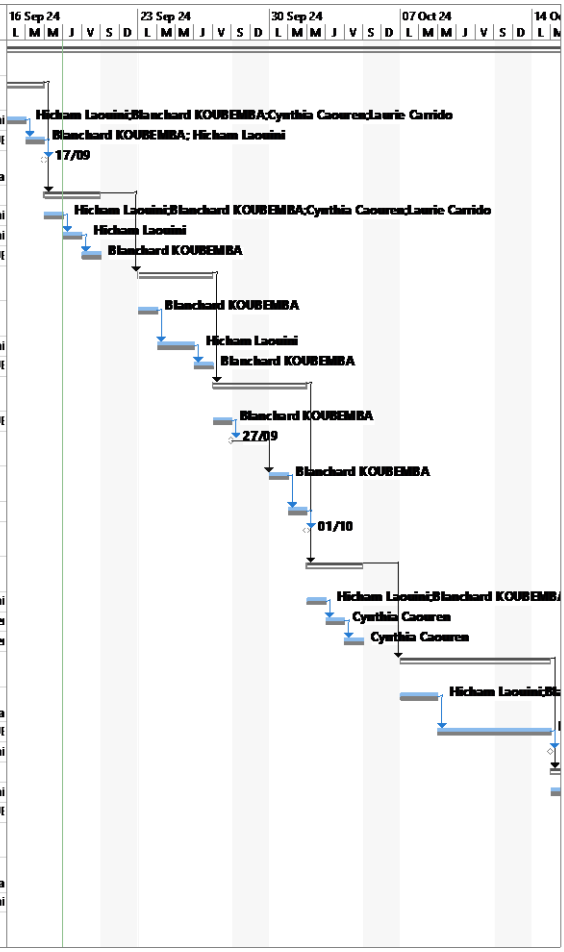
6. Planification du projet de sécurisation

a. Chronologie du projet



b. Le diagramme de GANTT

N°	Mode Tâche	Nom de la tâche	Durée	Début	Fin	Prédé	Noms ressources
1		Plan-Projet : Sécurisation de l'Architecture Réseau pour	28 jours	Lun 16/09/24	Mer 23/10/24		
2		Phase 1 : Analyse du matériel existant	2 jours	Lun 16/09/24	Mar 17/09/24		
3		Inventorier le matériel	1 jour	Lun 16/09/24	Lun 16/09/24		Hicham Laouini
4		Évaluer l'état du matériel	1 jour	Mar 17/09/24	Mar 17/09/24	3	Blanchard KOU
5		Identifier les besoins de mise à jour	0 jour	Mar 17/09/24	Mar 17/09/24	4	Hicham Laouini;Blancha
6		Phase 2 : Analyse des risqu	3 jours	Mer 18/09/24	Ven 20/09/24	2	
7		Identifier les menaces	1 jour	Mer 18/09/24	Mer 18/09/24		Hicham Laouini
8		Évaluer les vulnérabilités	1 jour	Jeu 19/09/24	Jeu 19/09/24	7	Hicham Laouini
9		Analyser l'impact potenti	1 jour	Ven 20/09/24	Ven 20/09/24	8	Blanchard KOU
10		Phase 3 : Conception de la sécurité	4 jours	Lun 23/09/24	Jeu 26/09/24	6	
11		Développer des politiques de sécurité	1 jour	Lun 23/09/24	Lun 23/09/24		Blanchard KOUBEMBA
12		Créer des procédures de	2 jours	Mar 24/09/24	Mer 25/09/24	11	Hicham Laouini
13		Planifier les mesures de s	1 jour	Jeu 26/09/24	Jeu 26/09/24	12	Blanchard KOU
14		Phase 4 : Redessiner l'architecture du SI	3 jours	Ven 27/09/24	Mar 01/10/24	10	
15		Analyser l'architecture ac	1 jour	Ven 27/09/24	Ven 27/09/24		Blanchard KOU
16		Identifier les recommandations de	0 jour	Ven 27/09/24	Ven 27/09/24	15	Blanchard KOUBEMBA
17		Concevoir la nouvelle architecture	1 jour	Lun 30/09/24	Lun 30/09/24	16	Blanchard KOUBEMBA
18		Valider la conception	1 jour	Mar 01/10/24	Mar 01/10/24	17	
19		Mettre en œuvre la nouvelle architecture	0 jour	Mar 01/10/24	Mar 01/10/24	18	
20		Phase 5 : Commande du nouveau matériel	3 jours	Mer 02/10/24	Ven 04/10/24	14	
21		Identifier les fournisseurs	1 jour	Mer 02/10/24	Mer 02/10/24		Hicham Laouini
22		Obtenir des devis	1 jour	Jeu 03/10/24	Jeu 03/10/24	21	Cynthia Caoure
23		Passer les commandes	1 jour	Ven 04/10/24	Ven 04/10/24	22	Cynthia Caoure
24		Phase 6 : Mise en œuvre des mesures	6 jours	Lun 07/10/24	Lun 14/10/24	20	
25		Installer les dispositifs de sécurité	2 jours	Lun 07/10/24	Mar 08/10/24		Hicham Laouini;Blancha
26		Configurer les dispositifs	4 jours	Mer 09/10/24	Lun 14/10/24	25	Blanchard KOU
27		Vérifier l'installation	0 jour	Lun 14/10/24	Lun 14/10/24	26	Hicham Laouini
28		Phase 7 : Tests et validatior	2 jours	Mar 15/10/24	Mer 16/10/24	24	
29		Tester les dispositifs	1 jour	Mar 15/10/24	Mar 15/10/24		Hicham Laouini
30		Valider les résultats	1 jour	Mer 16/10/24	Mer 16/10/24	29	Blanchard KOU
31		Phase 8 : Formation et sensibilisation	5 jours	Jeu 17/10/24	Mer 23/10/24	28	
32		Préparer le matériel de formation	1 jour	Jeu 17/10/24	Jeu 17/10/24		Hicham Laouini;Blancha
33		Former le personnel	3 jours	Ven 18/10/24	Mar 22/10/24	32	Hicham Laouini
34		Sensibiliser aux bonnes pratiques	1 jour	Mer 23/10/24	Mer 23/10/24	33	Blanchard KOUBEMBA



7. Conclusion

Ce plan de sécurisation permettra de combler les failles de l'architecture actuelle et de renforcer la sécurité globale du système d'information. Grâce à l'acquisition de nouveaux équipements et à leur mise en œuvre planifiée, nous réduirons considérablement les risques de cyberattaques et assurerons une protection continue du réseau et des données critiques. Le projet est estimé à 9 848,88 €, avec une mise en œuvre complète d’ici novembre 2024.