Cahier des Charges du Veolia Cyber Hub (VCH) :

**1. Introduction :**

Ce cahier des charges définit les exigences techniques et les bonnes pratiques pour l'installation et la configuration du Veolia Cyber Hub (VCH). L'objectif est de garantir une solution sécurisée, fiable et maintenable, tout en respectant les contraintes spécifiques de l'environnement industriel.

**2. Installation de Docker :**

L'installation de Docker doit être réalisée conformément au guide officiel disponible à l'adresse suivante :

Installation de Docker sur Debian.

**3. Gestion des images Docker :**

Les images disponibles sur le Docker Hub qui seront utilisées dans la solution doivent être sélectionnées avec prudence, selon les règles suivantes :

Images officielles : à privilégier systématiquement.

Images d'éditeurs vérifiés : autorisées si nécessaire.

Autres images : interdites.

Il est recommandé de consulter les documents suivants :

Recommandations de sécurité relatives au déploiement de conteneurs Docker.

Documentation officielle Docker.

**4. Documentation du Projet :**

Une documentation complète est requise pour le projet. Celle-ci doit inclure :

Dossier d’Architecture Technique (DAT) : description de l’architecture du VCH.

Dossier d’Exploitation (DEX) : procédures et bonnes pratiques pour l’exploitation.

Matrice de flux : description des flux réseau entre les composants du VCH et les autres systèmes.

Des exemples de ces documents sont disponibles dans le sous-dossier Documentation du dossier projet.

**5. Service NTP du VCH :**

Le VCH doit intégrer un serveur NTP local permettant la synchronisation des équipements industriels.

**5.1. Synchronisation avec le serveur NTP de Veolia Eau France :**

Le serveur NTP du VCH doit se synchroniser avec le serveur NTP de Veolia Eau France.

Adresses IP des serveurs NTP Veolia Eau France :

10.0.0.42

10.0.1.42

Port d’écoute : 123 (UDP).

**5.2. Synchronisation des équipements industriels :**

Les équipements industriels doivent pouvoir synchroniser leur horloge sur le serveur NTP du VCH.

**5.3. Environnement de test :**

Pour les tests, l’utilisation de deux serveurs NTP publics de votre choix est autorisée.

**6. Gestion des Journaux d’Activité :**

**6.1. Collecte et Relais des Journaux :**

Les équipements doivent envoyer leurs journaux d’activités sur le port 514 du VCH.

Les journaux doivent être relayés au Centre de Sécurité (SOC) de Veolia Eau France en temps réel.

Enclave de Collecte SOC (E-SOC) Veolia Eau France :

Adresses IP : 10.0.0.80, 10.0.1.82

Port d’écoute : 6514 (communication chiffrée vers l’enclave de collecte).

**6.2. Stockage et Visualisation des Journaux :**

Les journaux doivent être stockés avec une rétention de 1 mois ou 196 Go sur le VCH (ces valeurs doivent être personnalisables).

Une interface permettant la visualisation des journaux doit être accessible via le port 8514 du VCH.

L’accès à cette interface doit nécessiter une authentification conforme aux standards de l’ANSSI.

L’interface doit permettre la recherche de journaux par date, nom de machine, typologie d’équipement.

Des graphiques doivent afficher la volumétrie des journaux par typologie d’équipement.

Une vue chronologique doit être disponible pour observer l’évolution des journaux.

Un graphique doit permettre d’identifier les équipements n’ayant pas envoyé de données sur les dernières 24h.

**7. Gestion des Flux Réseau :**

**7.1. Transit des flux WAN/Internet via le VCH :**

Les flux à destination du WAN/Internet depuis les équipements industriels doivent transiter par le VCH.

**7.2. Types de flux supportés :**

Relai de mise à jour Windows (WSUS)

Port d’écoute du VCH : 8530

Destination : serveur WSUS Veolia Eau France (10.0.11.42, Port 8530).

Relai Web (HTTP & HTTPS)

Port d’écoute du VCH : 8080

Destination : serveur Proxy Veolia Eau France (10.0.22.42, Port 8080).

Relai de résolution de noms

Port d’écoute du VCH : 53

Destination : serveur DNS relai Veolia Eau France (10.0.15.42, Port 53).

**7.3. Interfaces de gestion et supervision :**

Interface d’administration du service proxy permettant l’ajout de nouveaux relais.

Interface de visualisation permettant :

La visualisation des trames réseau relayées en temps réel.

La visualisation des clients avec la dernière date et heure d’utilisation des relais configurés.

La visualisation des relais configurés avec le nombre de trames réseau relayées et le nombre de clients associés.

**8. Conformité Industrielle :**

**8.1. Collecte des Informations de Conformité :**

La conformité industrielle repose sur un agent de collecte installé sur les équipements.

Windows : l’agent est disponible dans le sous-dossier Servitude - Conformité du dossier projet.

Linux : un agent de collecte en Shell (Bash) doit être développé.

L’agent doit se baser sur les Recommandations de sécurité de l’ANSSI pour les systèmes GNU/Linux.

Les informations de conformité doivent être transférées vers l’Outil de Conformité Industrielle (OCI) de Veolia Eau France.

OCI Veolia Eau France :

Adresses IP : 10.0.5.42, 10.0.6.42

Port d’écoute : 443

Les informations doivent être envoyées au format JSON vers le VCH.

**8.2. Visualisation de la Conformité :**

Une interface permettant le contrôle de la conformité des postes doit être accessible via le port 8443 du VCH.

L’accès à cette interface doit nécessiter une authentification conforme aux standards de l’ANSSI.

L’interface doit permettre de visualiser les valeurs des paramètres de conformité pour chaque équipement.

Une liste des postes respectant la politique de mots de passe Veolia Eau France doit être disponible.

**9. Sécurité et Contraintes :**

Le VCH est positionné en DMZ sur un site industriel.

Aucun package additionnel ne doit être installé sur les équipements industriels.

L’administration du VCH est sécurisée et effectuée à distance.

Le VCH ne dispose d’aucune connexion Internet.

La solution doit être conçue selon les principes de minimalisme et simplicité.

**10. Conclusion :**

Ce cahier des charges fournit les directives essentielles pour la mise en œuvre du VCH en respectant les exigences de Veolia Eau France. Toute déviation doit être justifiée et validée par l’équipe en charge du projet.