19/04/2024

Lucas DEGRET, François BRASY, Julien LEBRIS, Théodore PALIANI

wILD cODE sCHOOL

EcoSolar Solutions

Dossier Projet

[Contexte 1](#_Toc235184752)

[Historique 1](#_Toc1715855509)

[Installation et processus 1](#_Toc1603457538)

[Enjeux 1](#_Toc1299983899)

[Besoins 1](#_Toc885233327)

[Réseau 2](#_Toc723183464)

[Infrastructure actuelle 2](#_Toc1092665504)

[Conception du réseau proposé 2](#_Toc1527343054)

[Topologie physique 2](#_Toc498749900)

[Topologie logique 2](#_Toc2038278360)

[Composants réseau 2](#_Toc719439516)

[Switches et routeurs 2](#_Toc509888988)

[Points d'accès sans fil 2](#_Toc2113751318)

[Matériel de Datacenter 3](#_Toc586159057)

[Protocoles et services 3](#_Toc183836276)

[DHCP, DNS, SMTP 3](#_Toc2047304469)

[VPN, MPLS, QoS 3](#_Toc117130774)

[Redondance et haute disponibilité 3](#_Toc757776508)

[WAN et LAN 3](#_Toc1322158190)

[Services réseaux et web 3](#_Toc548564088)

[Connectivité 3](#_Toc1239151859)

[Interne (LAN, WLAN) 3](#_Toc1843876908)

[Externe (WAN, Internet) 3](#_Toc122918806)

[Plan d’adressage IP 3](#_Toc1311679665)

[Sécurité réseau 3](#_Toc785072280)

[Firewall, Proxy, Reverse proxy 3](#_Toc97505807)

[Sécurité 3](#_Toc1139054758)

[Analyse des risques 4](#_Toc2105088409)

[EBIOS, Mehari 4](#_Toc33278504)

[Politique de sécurité 4](#_Toc685778923)

[ISO 27000 4](#_Toc1175060951)

[Sécurité physique et logique du Datacenter 4](#_Toc108399299)

[Sécurité des données 4](#_Toc2010632292)

[Cryptographie, PKI et certificats 4](#_Toc1292769276)

[Contrôle d'accès 4](#_Toc53885722)

[LDAP/LDAPS, MFA, Zero trust 4](#_Toc1383847148)

[Protection des endpoints 4](#_Toc330906101)

[Antivirus, EDR 4](#_Toc656966519)

[Sécurité des communications 4](#_Toc89951583)

[SSH, SSL/TLS, DNSSEC 4](#_Toc1747479697)

[Supervision de la sécurité 4](#_Toc981444914)

[SIEM, SOC 4](#_Toc1277233940)

[Plan de réponse aux incidents 5](#_Toc1058921909)

[Détection, réaction et reporting 5](#_Toc173469836)

[Documentation 5](#_Toc1046879079)

[Documentation technique 5](#_Toc1208341667)

[Diagrammes de réseau 5](#_Toc1544477698)

[Spécifications des équipements 5](#_Toc1563224022)

[Manuels d'exploitation 5](#_Toc130063192)

[Procédures opérationnelles 5](#_Toc1883219274)

[Guides d’utilisation 5](#_Toc1242344629)

[Documentation de configuration 5](#_Toc996825622)

[Scripts d'automatisation 5](#_Toc602912458)

[Configurations des équipements 5](#_Toc1694086936)

[Documentation de sauvegarde 5](#_Toc833703483)

[Plans de sauvegarde et restauration 5](#_Toc986742798)

[Documentation de sécurité 5](#_Toc1497651121)

[Politiques de sécurité 6](#_Toc1654718622)

[Plans de réponse aux incidents 6](#_Toc1867179409)

[Sauvegarde 6](#_Toc1089077250)

[Stratégie de sauvegarde 6](#_Toc1071284229)

[Sauvegardes sur site et hors site 6](#_Toc644296094)

[Plan de continuité d’activité (PCA) 6](#_Toc334352102)

[PRA/PCA, Redondance des données 6](#_Toc1292834688)

[Solutions de sauvegarde 6](#_Toc310291932)

[Logiciels et matériel utilisés 6](#_Toc1655110604)

[Tests et validation 6](#_Toc2011608210)

[Fréquence des tests de restauration 6](#_Toc1607894542)

[Stockage sécurisé 6](#_Toc1089848317)

[Solutions de stockage distribué 6](#_Toc150179562)

[Système 6](#_Toc1602274101)

[Infrastructure serveur 7](#_Toc846072127)

[Hyperviseurs, serveurs physiques et virtuels 7](#_Toc1821641107)

[Systèmes d’exploitation 7](#_Toc2000485960)

[Windows Server, Linux 7](#_Toc178731711)

[Services systèmes 7](#_Toc941074452)

[Active Directory, Serveur de fichiers, Serveur de messagerie 7](#_Toc1099833919)

[Gestion des applications métier 7](#_Toc1979310026)

[ERP, CRM 7](#_Toc863162265)

[Automatisation et gestion de configuration 7](#_Toc943684592)

[Scripts, Ansible, etc. 7](#_Toc640662341)

[Supervision 7](#_Toc1304095881)

[Outils et indicateurs de performance 7](#_Toc240120755)

[Virtualisation 7](#_Toc461998826)

[Proxmox, Cluster d'hyperviseur 7](#_Toc202825750)

Cloud Computing 7

[Annexe 8](#_Toc1879647820)

[Tableau 1: Liste du personnel 16](#_Toc164258124)

# Contexte

## Historique

Entreprise fondée, implémentée à Toulouse en 2010 et pionnière spécialisée dans les énergies renouvelables, dédiée au développement et à la fabrication de panneaux solaires à haut rendement. L’entreprise dispose d’un petit Datacenter à Marseille. Elle emploie actuellement une cinquantaine de personne avec une perspective de passer à 80 voire plus.

## Installation et processus

L’ensemble des bureaux, ateliers et entrepôt se trouvent à Toulouse dans un bâtiment plein pied et possède un Datacenter à Marseille.

La production est semi-industrielle :

* Automate non-connecté au SI, conduis par conducteurs de machine et opérateur d’atelier
* Gestion de stock par ERP (Dolibarr), saisie d’information via tablette industriel
* Données et documents lié aux processus et aux produits : Factures, bon de commandes, demandes d’achat, secret industriel … (certains en papier).

## Enjeux

Croissance Exponentielle :

Avec une demande croissante pour ses panneaux solaires haute performance, SolarEco Solutions doit moderniser son infrastructure informatique pour gérer l'augmentation rapide des données et assurer une gestion efficace de la production.

Sécurité des accès :

Les commerciaux de l'entreprise ont besoin d'accéder à l'ERP/CRM de l'entreprise de manière distante pour gérer efficacement leurs activités, accéder aux informations clients, et mettre à jour les données en temps réel. Cela soulève des enjeux spécifiques liés à la sécurité, à la disponibilité, et à la performance de ces accès distants.

Sécurité des Brevets et Données :

La protection des brevets et des données de conception est une priorité cruciale pour assurer la pérennité de la technologie exclusive de SolarEco Solutions. Des mesures de sécurité informatique renforcées sont nécessaires pour garantir la confidentialité et l'intégrité des informations sensibles.

Optimisation de la Chaîne d'Approvisionnement :

Avec l'engagement d'utiliser exclusivement des matériaux français, SolarEco Solutions doit optimiser sa chaîne d'approvisionnement grâce à des solutions informatiques efficaces pour suivre les stocks, les commandes et garantir la traçabilité des matériaux.

Expansion du Datacenter :

Avec l'investissement dans un petit datacenter, SolarEco Solutions doit planifier son expansion pour répondre aux besoins croissants de stockage de données tout en garantissant la sécurité et la disponibilité des informations cruciales.

## Objectif

L’enjeu majeur est de faire une refonte totale du Service Informatique actuel :

* Moderniser l’infrastructure actuel
* Aménager le Datacenter
* Informatiser l’activité (gestion de prod, gestion commerciale, communication vers l’extérieur)
* Mise en place des bonnes pratiques, démarche de gestion des risques, accès distant

# Réseau

## Infrastructure actuelle

### Infrastructure locale

Le réseau Internet de l’entreprise est relié à un boitier type « box Internet » fourni par le Fournisseur d’Accès Internet (FAI) qui lui attribue une adresse IP publique, un service DNS, internet fibré et d’un service de relais SMTP.

Cette box Internet est raccordée au Pare-feu, Appliance Pfsense, avec pour règle « permit all any any » qui est définie sur l’interface LAN.

Le Pare-feu est relié quant à lui à un switch administrable N2 (VTY non-activé) où dessus n’existe qu’un seul VLAN ou tous les nœuds sont raccordés sur ce switch + 1 point d’accès wifi en WPA2. Un switch similaire se trouve dans l’atelier avec une borne Wifi.

Un réseau IPv4 de classe C (192.1698.1.0/24) y est déployé. Un DHCP avec une étendu pour les 200 premières machines, les 54 dernières sont des fixes pour tous types (imprimantes, serveurs, etc.)

Le système SI est composé :

* D’un hyperviseur Proxmox VE contenant 5 VM :
  + Serveur Windows 2019 Standard : AD, DNS, DHCP
  + Serveur Debian avec l’ERP
  + 1 serveur téléphonie
  + 1 serveur mail
  + 1 serveur Debian 12 avec GLPI installé. Utilisateurs importés depuis l’AD, l’agent GLPI est installé sur Serveur Windows et Linux mais pas sur les postes ni les périphériques type tablette ou smartphone.
* 1 NAS pour le partage de fichier
* 2 bornes Wi-Fi : Bureau et Atelier

L’infrastructure utilise plusieurs types de périphériques :

* Tablette Android
* Smartphones
* Téléphones IP + softphone
* Ordinateur portable et fixe sous Windows intégré au domaine
* Imprimantes

### Infrastructure Datacenter

L'infrastructure du bâtiment est opérationnelle, le DataCenter dispose de 4 baies 19 pouces, il reste à concevoir la partie infrastructure informatique au niveau architecture réseau (switchs, serveurs, routeurs, pare-feu) pour répondre aux besoins des communications externe (nord/sud) et interne (est/ouest).

Chaque baie est équipée de 4 serveurs physiques et d'un switch de type "leaf switches".

On retrouve aussi 3 switchs de type "spine switches", 2 routeurs, 2 pare-feu et 2 liaisons WAN fibrées.

Tout cet ensemble n'est ni brassé ni configuré et donc pas opérationnel.

## Conception du réseau proposé

### Topologie physique local

Nous avons conçu une nouvelle topologie suivant les besoins de l’entreprise.

Multi-WAN

Nous aurons un accès Internet via une connexion fibré dédié à l’entreprise (FTTO) ainsi que d’une clé 4G du même fournisseur. Nous utiliserons la technologie « Multi-WAN » ainsi que de la technologie Actif/Passif. Cette technologie permet une redondance au niveau de l’accès à Internet, si notre connexion tombe en panne la clé 4G prendra la main et nous communiqueras qu’un problème est survenu sur la première connexion.

Cluster de routeur :

Ici, nous aurons deux Pare-feu qui seront raccordés, l’un et l’autre, par les deux accès Internet.

Stack de commutateur N3 :

Les deux Pare-feu précédent seront, quant à eux, reliés à deux commutateurs de niveau 3 qui permettent une distribution entre les Pare-Feu et les switchs de niveau2. Ces derniers permettent une redondance et d’équilibrer les charges d’un trafic Nord-Sud (Intérieur vers extérieur) et d’un trafic Est-Ouest (intérieur vers intérieur) sans passer par le Pare-Feu (s’il n’y a pas besoin). On retrouvera aussi à ce niveau un contrôleur Wi-Fi

Commutateur de Niveau 2 :

Ces commutateurs permettent de relier les utilisateurs finaux sur le réseau. Nous mettrons en place une redondance entre le switch N3 et N2 afin d’éviter toute coupure pour l’utilisateur. Un switch dédié pour éviter une surcharge du réseau (Un switch dédié pour les bureaux, un switch dédié dans la salle serveur pour les serveurs, un switch dédié pour l’atelier).

### Topologie logique

En attente TOPOLOGIE CISCO THEODORE & JULIEN

## Composants réseau

Voici la liste des composants que nous aurons besoin pour le projet. Nous ne garderons aucun des équipements actuels (switch, pare-feu, routeur) présent dans l’entreprise. Nous préférons partir sur quelque chose de propre et neuf.

### Switches et routeurs

Qui ? Quoi ? Où ? Quand ? Comment ? Pourquoi ? Combien € ?

1 switch administrable de 48 ports de niveau 2 dédié pour les bureaux

2 switch administrable de 16 ports de niveau 2 pour l’atelier et la salle serveur

2 switches administrables de 48 ports de niveau 3 avec possibilité de stack

2 routeurs pour le pare-feu

1 connexion FTTO

Une connexion 4 G

Remarque : La connexion FTTO et 4G viennent du même FAI.

### Points d'accès sans fil

### Dans le cadre de notre projet de mise en place d'un réseau sans fil efficace, nous prévoyons d'installer un contrôleur Wi-Fi administrable de 8 ports avec la fonction Power over Ethernet (PoE). Cette solution permettra une gestion centralisée et simplifiée de notre réseau Wi-Fi, offrant ainsi une meilleure stabilité et une gestion plus efficace des connexions.

### En complément, nous prévoyons d'utiliser trois bornes Wi-Fi supplémentaires. Nous conserverons celles déjà présentes sur place et n'en achèterons qu'une seule de plus, afin de garantir une couverture optimale de tout le bâtiment. Cette approche nous permettra d'éliminer les zones mortes et d'assurer une connectivité fiable dans toutes les zones, tout en optimisant les coûts d'acquisition.

### En résumé, notre solution combinant un contrôleur Wi-Fi administrable de 8 ports en PoE et trois bornes Wi-Fi nous permettra de fournir un réseau sans fil performant et robuste, répondant aux besoins de connectivité de notre infrastructure.

### Matériel de Datacenter

Pour notre projet d'interconnexion au sein du datacenter, nous avons décidé de maintenir en service le matériel existant, tout en optimisant son utilisation pour répondre à nos besoins en interconnexion.

Nous utiliserons donc les commutateurs réseau actuellement en place pour gérer l'interconnexion entre les différents éléments du datacenter. Ces commutateurs seront configurés et optimisés pour assurer des transferts de données rapides et fiables, tout en maintenant la stabilité et la sécurité du réseau.

De même, nous continuerons à utiliser les routeurs existants pour gérer le trafic réseau entrant et sortant, en veillant à ce qu'ils soient correctement configurés pour répondre à nos exigences de performance et de sécurité.

En résumé, notre approche consiste à tirer parti du matériel existant pour assurer une interconnexion efficace au sein du datacenter, en maximisant les ressources disponibles tout en minimisant les coûts associés à l'acquisition de nouveaux équipements.

## Protocoles et services

### DHCP, DNS, SMTP

Pour notre infrastructure réseau, nous avons décidé de mettre en place deux serveurs DHCP distincts qui ne seront pas hébergés sur notre contrôleur de domaine Active Directory (AD). Cette stratégie vise à alléger la charge de travail du contrôleur de domaine en limitant ses responsabilités principales à la gestion du DNS. En évitant de surcharger le contrôleur de domaine avec la fonction DHCP, nous renforçons également la sécurité du réseau en empêchant les utilisateurs du réseau invité d'accéder directement au contrôleur de domaine, réduisant ainsi la surface d'attaque potentielle.

En cas de panne du DHCP principal, nous avons prévu un système de secours pour assurer la continuité du service et garantir que les utilisateurs puissent toujours accéder aux informations essentielles.

Par ailleurs, nous suivons les recommandations de l'ANSSI en déployant deux contrôleurs de domaine AD avec leur propre service DNS pour éviter toute perturbation en cas de panne de l'AD principal.

En ce qui concerne la sécurité et la confidentialité des communications, nous mettrons en œuvre les protocoles DNSSEC, DNS over TLS (DoT) et DNS over HTTPS (DoH) pour renforcer la protection et la confidentialité des requêtes DNS.

Enfin, nous mettrons en place un serveur de messagerie utilisant le protocole SMTP ou SMTPS pour la gestion des emails, assurant ainsi une communication sécurisée et fiable au sein de notre infrastructure.

### VPN, MPLS, QoS

Pour garantir des connexions sécurisées pour nos utilisateurs distants, nous mettrons en place un agent VPN compatible avec notre pare-feu. Cet agent VPN permettra aux utilisateurs de se connecter de manière sécurisée à notre réseau, tout en bénéficiant des fonctionnalités de protection offertes par le pare-feu. Cela nous permettra de contrôler et de sécuriser efficacement l'accès aux ressources réseau depuis des emplacements distants.

En parallèle, nous utiliserons le protocole MPLS (Multiprotocol Label Switching) pour configurer des chemins dédiés sur notre réseau, sans recourir au processus de routage classique. Cette approche nous permettra de garantir des performances élevées et une qualité de service (QoS) constante pour les applications critiques de l'entreprise, en établissant des circuits virtuels privés entre les différents sites de l'entreprise.

En ce qui concerne la qualité de service (QoS), nous mettrons en place des règles de QoS pour privilégier la bande passante à certains services stratégiques de l'entreprise, tels que l'ERP (Enterprise Resource Planning) et les données partagées. En accordant une priorité à ces services critiques, nous assurerons une utilisation efficace des ressources réseau et une expérience utilisateur optimale pour les applications métier essentielles.

## Redondance et haute disponibilité

### WAN et LAN

**WAN et LAN**: Implémentez des connexions WAN redondantes et un basculement automatique pour maintenir la connectivité en cas de défaillance d'une ligne. Utilisez des protocoles tels que HSRP, VRRP ou GLBP pour la redondance LAN.

### Services réseaux et web

**Sécurité des réseaux et services web**: Déployez des pare-feu en cluster, des équilibreurs de charge et des serveurs web en haute disponibilité avec des configurations de redondance active-passive ou active-active.

## Connectivité

### Interne (LAN, WLAN)

**Interne (LAN, WLAN)**: Configurez des chemins multiples et redondants dans le réseau LAN, avec des liens d'agrégation pour augmenter la bande passante et fournir une redondance. Assurez la disponibilité des points d'accès sans fil par l'utilisation de contrôleurs WLAN en mode cluster.

### Externe (WAN, Internet)

**Externe (WAN, Internet)**: Pour la connectivité externe, envisagez l'utilisation de liaisons MPLS appairées avec des VPN Internet pour une résilience accrue.

## Plan d’adressage IP

## Sécurité réseau

### Firewall, Proxy, Reverse proxy

# Sécurité

## Analyse des risques

### EBIOS, Mehari

## Politique de sécurité

Une politique de sécurité exhaustive a été rédigée et mise en œuvre, s'alignant sur les directives de la norme ISO 27000. Cette politique couvre tous les aspects de la sécurité informatique et des informations chez SolarEco Solutions, y compris les protocoles de gestion des incidents et les procédures de réponse en cas d'urgence.

### ISO 27000

### Sécurité physique et logique du Datacenter

Des mesures de sécurité physiques comprenant le contrôle d'accès par badge et biométrie, ainsi que la surveillance vidéo, ont été renforcées. Sur le plan logique, nous avons déployé des systèmes avancés de détection d'intrusion et de prévention pour protéger l'intégrité du Datacenter.

## Sécurité des données

Nous avons implanté des solutions de cryptographie de pointe, y compris la mise en place d'une infrastructure à clé publique (PKI) et l'émission de certificats numériques, assurant ainsi l'intégrité et la confidentialité des données sensibles.

### Cryptographie, PKI et certificats

## Contrôle d'accès

Un système d'authentification renforcé basé sur LDAP/LDAPS a été intégré, complété par la mise en œuvre de l'authentification multi-facteur (MFA) et une approche Zero Trust pour un contrôle d'accès sécurisé aux ressources réseau et systèmes.

### LDAP/LDAPS, MFA, Zero trust

## Protection des endpoints

Des solutions antivirus et de détection et réponse aux endpoints (EDR) ont été installées sur tous les dispositifs connectés au réseau de l'entreprise, fournissant une couche supplémentaire de défense contre les logiciels malveillants et les attaques.

### Antivirus, EDR

## Sécurité des communications

Des protocoles de sécurisation tels que SSH, SSL/TLS et DNSSEC ont été configurés pour sécuriser les communications à travers l'infrastructure réseau, garantissant ainsi que les transferts de données sont chiffrés et protégés contre les écoutes indiscrètes ou les altérations.

### SSH, SSL/TLS, DNSSEC

## Supervision de la sécurité

Un système de gestion des informations et des événements de sécurité (SIEM) a été déployé, en collaboration avec un centre d'opérations de sécurité (SOC), pour une surveillance continue et pour le traitement rapide des alertes de sécurité.

### SIEM, SOC

## Plan de réponse aux incidents

Nous avons développé un plan de réponse aux incidents qui décrit des procédures claires pour la détection, la réaction et le reporting des incidents de sécurité, garantissant une réponse rapide et coordonnée en cas d'incident.

Ces initiatives sécuritaires s'inscrivent dans une démarche globale d'amélioration continue et visent à préparer SolarEco Solutions aux défis de sécurité actuels et futurs, en accord avec son expansion et ses objectifs stratégiques.

### Détection, réaction et reporting

# Documentation

## Documentation technique

### Diagrammes de réseau

### Spécifications des équipements

## Manuels d'exploitation

### Procédures opérationnelles

### Guides d’utilisation

## Documentation de configuration

### Scripts d'automatisation

Lien du Github : [cliquer ici](https://github.com/FrancoisBrasy/AIS2309-P2-Group-2---SolarEcoSolutions-)

### Configurations des équipements

## Documentation de sauvegarde

### Plans de sauvegarde et restauration

### Documentation de sécurité

### Politiques de sécurité

### Plans de réponse aux incidents

# Sauvegarde

## Stratégie de sauvegarde

Dans le cadre de la mise en œuvre de notre stratégie de sauvegarde des données, nous adoptons l'approche recommandée "3-2-1-1-0", en utilisant les méthodes de sauvegarde totale et incrémentielle fournies par Acronis. Cette stratégie implique de maintenir trois copies de toutes les données critiques : la version originale sur le système principal et deux copies supplémentaires. Ces copies sont stockées sur deux types de supports distincts, comme un disque dur interne et un dispositif de stockage externe ou en réseau, afin de protéger contre les défaillances matérielles. De plus, une de ces copies est conservée hors site, assurant la sécurité contre les sinistres locaux. La sauvegarde incrémentielle est effectuée pour minimiser l'utilisation de l'espace de stockage et le temps nécessaire à la sauvegarde, après une sauvegarde totale initiale. Enfin, nous veillons à ce que toutes les sauvegardes soient effectuées sans erreurs (zéro erreur) pour garantir l'intégrité et la récupérabilité des données en cas de besoin. Cette approche rigoureuse assure une protection optimale de nos actifs informationnels essentiels.

## Plan de continuité d’activité (PCA)

### PRA/PCA, Redondance des données

## Solutions de sauvegarde

### Logiciels et matériel utilisés

## Tests et validation

### Fréquence des tests de restauration

## Stockage sécurisé

### Solutions de stockage distribué

# Système

## Infrastructure serveur

### Hyperviseurs, serveurs physiques et virtuels

## Systèmes d’exploitation

### Windows Server, Linux

## Services systèmes

### Active Directory, Serveur de fichiers, Serveur de messagerie

## Gestion des applications métier

### ERP, CRM

## Automatisation et gestion de configuration

### Scripts, Ansible, etc.

## Supervision

### Outils et indicateurs de performance

## Virtualisation

### Proxmox, Cluster d'hyperviseur

## Cloud Computing

### SaaS/PaaS/IaaS, Environnement hybride

# Conclusion & next step

# Annexe

|  |  |  |  |
| --- | --- | --- | --- |
|  | **NOM** | **PRENOM** | **SERVICE** |
| Directeur général | Wally | Adam | Direction |
| Assistante DG | Herminia | Oliva | Direction |
| Informaticien | Elijah | Blakley | Informatique |
| Stagiaire alternance | Nguvet | Catlett | Informatique |
| Responsable logistique | Penning | Sharilyn | Logistique/approvisionnement |
| Acheteur | Przybyla | Leonardo | Logistique/approvisionnement |
| Agent logistique 1 | Bradwell | Teri | Logistique/approvisionnement |
| Agent logistique 2 | Galasso | Dominique | Logistique/approvisionnement |
| Agent logistique 3 | Waltrip | Antoine | Logistique/approvisionnement |
| Directeur production - DG Adjoint | Phyllis | Biondo | Production |
| Responsable atelier | Davie | Ivan | Atelier |
| Technicien maintenance 1 | Hyatt | Marcy | Atelier |
| Technicien maintenance 2 | Vancleave | Jean | Atelier |
| Responsable production | Twiford | Isabelle | Production |
| Conducteur de machines 1 | Larock | Caroline | Production |
| Conducteur de machines 2 | Demelo | Pierre | Production |
| Conducteur de machines 3 | Gerardo | Lucien | Production |
| Conducteur de machines 4 | Ria | Mathis | Production |
| Opérateur 1 | Bragdon | Elene | Production |
| Opérateur 2 | Bakley | Sandra | Production |
| Opérateur 3 | Rubalcava | Jérémy | Production |
| Opérateur 4 | Schewe | Maye | Production |
| Opérateur 5 | Isenberg | Edmond | Production |
| Opérateur 6 | Vanarsdale | Luc | Production |
| Opérateur 7 | Tokarski | Laurent | Production |
| Opérateur 8 | Plamondon | Elise | Production |
| Opérateur 9 | Shoaf | Marion | Production |
| Opérateur 10 | Garber | Michel | Production |
| Opérateur 11 | Blalock | Cassandra | Production |
| Opérateur 12 | Yarberry | Julie | Production |
| Opérateur 13 | Gutter | Serena | Production |
| Opérateur 14 | Bolden | Damien | Production |
| Opérateur 15 | Chilcott | Baptiste | Production |
| Opérateur 16 | Cosme | Melissa | Production |
| Opérateur 17 | Hae | Patrick | Production |
| Opérateur 18 | Towers | Thibault | Production |
| Responsable R&D | Letts | Valérie | R&D/qualité |
| Technicien R&D 1 | Babb | Violaine | R&D/qualité |
| Technicien R&D 2 | Velva | William | R&D/qualité |
| Directeur commercial | Nguyen | Basile | Service commercial |
| Assistant commercial | Shonda | Philippe | Service commercial |
| Responsable produits | Ben-Talo | Ahmed | Service commercial |
| Commercial 1 | Reverdy | Claude | Service commercial |
| Commercial 2 | Velasco | Lidia | Service commercial |
| Commercial 3 | Persaud | Guy | Service commercial |
| Commercial 4 | Drucilla | Colin | Service commercial |
| Responsable expédition | Fare | Vincent | Expédition |
| Préparateur commande 1 | Otis | Laura | Expédition |
| Préparateur commande 2 | Cushman | Marc | Expédition |
| Directrice Admin. & Fin. | Goosby | Charlotte | Dpt Administratif & Financier |
| Assistant DAF | Valazquez | Leon | Dpt Administratif & Financier |
| Comptable | Fe | Cécile | Dpt Administratif & Financier |
| Employé administratif 1 | Tamar | Mohammed | Dpt Administratif & Financier |
| Employé administratif 2 | Ebner | Sandie | Dpt Administratif & Financier |

Tableau 1: Liste du personnel