La société :

TechNova Industries est une PME internationale de +/- 650 employés spécialisée dans le développement de solutions IoT industrielles.

Fondée en 1999, elle a connu une croissance rapide grâce à ses innovations dans les capteurs intelligents, les systèmes de supervision en temps réel et les plateformes cloud industrielles.

L'entreprise a récemment connu une forte croissance, mais son infrastructure informatique n'a pas suivi et présente plusieurs faiblesses identifiées lors d'un audit interne.

Elle possède 8 sites :

3 en France :

- **Paris, le siège social (120 personnes)**
  - Direction générale
  - Datacenter principal
  - Équipes financières & commerciales
- **Lyon (80 personnes)**
  - R&D
  - Développement IoT
  - Laboratoires de prototypage
- **Lille (100 personnes)**
  - Production et assemblage
  - Logistique

2 en Espagne :

- **Barcelone (25 personnes)**
  - Développement firmware IoT
  - Équipe cybersécurité locale
  - Petit cluster virtualisation
- **Séville (75 personnes)**
  - Centre d'assistance multilingue (FR/ES/PT)
  - Petit serveur de fichiers local

1 aux Pays-Bas :

- **Amsterdam (25 salariés)**
  - Plateforme Cloud hybride (Azure + VMware)
  - Infrastructure réseau critique

    - Équipe DevOps & réseaux
    - Fonctionne comme un **site pivot** pour l'Europe du Nord

1 au Maroc

- **Rabat pour la production (180 employés)**
    - Support terrain sur les dispositifs IoT
    - Petit datacenter secondaire (serveur d'inventaire + backup local)

1 aux USA :

- **Austin, Texas (50 employés)**
    - Bureau nord-américain (ventes + intégration IoT)
    - Datacenter local
    - AD Read-Only Domain Controller (RODC)
    - Serveurs d'applications clients
    - Interconnexion VPN IPSec transatlantique

Pays	**Ville**	**Rôle principal**	Activité	**Particularités**	Employés
France	Paris	Siège & Datacenter	Cloud & Bid Data	AD primaire	120
France	Lyon	R&D	IoT industriel	DC secondaire	80
France	Lille	Production	IoT industriel	Aucun DC	100
Espagne	Barcelone	Dev logiciel		Virtualisation locale	25
Espagne	Séville	Support Europe Sud	Développement	Mini-serveur	75
Maroc	Rabat	Support Afrique	Support client	Mini-datacenter	180
USA	Austin (TX)	Hub Amérique du Nord	Support client IoT industriel	RODC + App servers	50
Pays-Bas	Amsterdam	Cloud & Réseau	Cloud & Big Data	Centre DevOps	25

We operate in

8 LOCATIONS

TECHNOVA

Activités principales

🔧 IoT industriel

TechNova conçoit des capteurs destinés aux secteurs :

- De la logistique,
- De l'énergie,
- Du transport,
- De l'agroalimentaire.

Les capteurs sont assemblés sur le site de **Lille**, puis testés et configurés via la plateforme R&D de **Lyon**. Le Développement est assuré par **Séville**

🖥️ Plateforme Cloud & Big Data

Le cœur logiciel repose sur un datacenter hybride situé à :

- Paris (principal)
- Amsterdam (support cloud et réseau)

Notre architecture cloud traite plus de 12 millions d'événements IoT par jour provenant des clients en Europe et en Amérique du Nord

🤝 Support client international

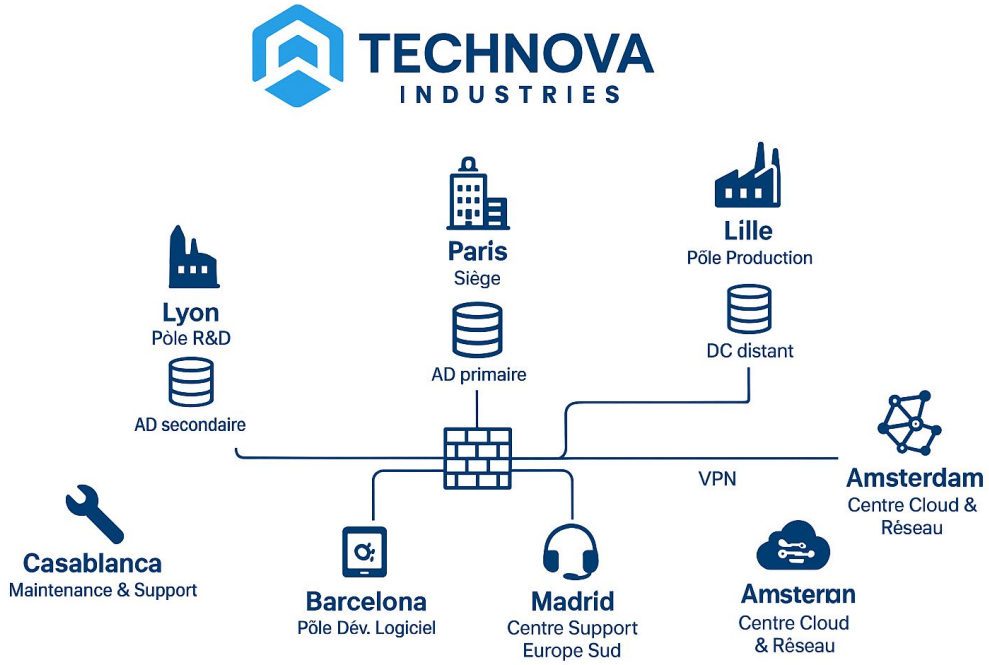
TechNova dispose de trois centres de support :

- **Séville** pour le sud de l'Europe,
- **Austin** pour les États-Unis et le Canada,
- **Rabat** pour l'Afrique francophone.

Les équipes gèrent :

- Les incidents client,
- Le support technique,
- L'intégration des solutions chez les partenaires.

Architecture réseau simplifiée



🔐 Enjeux cybersécurité

TechNova est confrontée à des problématiques réelles qui justifient une étude approfondie :

📌 Sécurité Active Directory

- Domaine unique *technova.corp*
- 3 contrôleurs de domaine : Paris, Lyon, Austin (RODC)
- Problématique : **vieillissement des GPO**, segmentation insuffisante, comptes à privilèges mal ou non gérés

---

📌 Sécurité réseau

- Architecture VPN IPsec pour les sites internationaux
- Firewalls Fortinet, Cisco, Palo Alto, Sophos et Stormshield
- Switchs Cisco, HP,
- Bornes wifi Aruba, forntinet, cisco
- Faible segmentation VLAN dans certains sites (héritage historique)
- Besoin urgent de décommissionner du matériel obsolète et d'uniformiser les systèmes afin de simplifier le réseau

---

📌 Matériel bureautique réseau

- PC et stations de travail obsolète (Windows 7 & 10)
- Téléphonie toujours en cuivre pas intégré au système informatique ce qui engendre des coûts importants
- Ecrans pas adaptés au travail
- Besoin urgent de remettre à plat tous les PC, de rajouter des stations dédiées pour la R&D
- Mise en place du plan 'téléphonie 2030'

📌 GDPR & conformité

L'entreprise gère des données sensibles :

- Positions de véhicules (géolocalisation),
- Mesures environnementales,
- Données d'usines (production),
- Données clients (contact, contrats, tickets).

Les audits ont révélé :

- Manque de chiffrement sur certains flux internes,
- Journaux conservés trop longtemps,
- Absence de registre complet de traitement GDPR.

📌 SOC interne naissant

TechNova dispose d'une petite cellule SOC au sein du site d'Amsterdam :

- Une équipe de 3 analystes
- Outils encore immatures
- Besoin d'un playbook d'investigation unifié
- SIEM basé sur Elastic Stack, mais peu structuré

📌 Sécurité physique

L'entreprise va intégrer un nouveau bâtiment pour la R&D (toujours à Lyon) :

- Nouveaux locaux dédiés à la R&D (voir plans annexe 1, 2 et 3)
- Sécurisation des locaux au niveau physique (caméras, badges d'accès, logs sur ouvertures et fermetures, sécurisation incendie etc…)
- Mesures environnementales,
- Authentification très forte pour les membres des labos de recherche

🔧 Problématiques actuelles à résoudre

- 📌 **Active Directory**
  - Diagnostic des faiblesses de l'Active Directory actuel
  - Fournir un plan de remédiation des faiblesses
  - Refonte des GPO
  - Refonte des Administrateurs trop nombreux
  - Objets obsolètes (comptes inactifs)
  - Mise en place de GPO de durcissement (Windows 10/11, serveurs Windows).
  - Segmentation des rôles administratifs (Tiering Model).
  - Proposition d'un plan de migration vers un environnement moderne (hybride Azure AD possible).
  - Mise en place d'une authentification multi-facteurs

- 📌 **Réseau**
  - Analyse de l'infrastructure réseau existante (topologie, VLAN, routage, segmentation).
  - Production d'une documentation avec schéma réseau existant
  - Refonte de la segmentation réseau (VLAN / ACL / Firewalls)
  - Remplacement des switchs non administrables par des switchs managés (802.1X, VLAN, ACL).
  - Mise en place d'une architecture redondante sur le site principal et les sites le nécessitant
  - Mise à jour ou remplacement des firewalls obsolètes.
  - Refonte du Wi-Fi (WPA3-Enterprise, séparation invités/privés, on-boarding sécurisé).
  - Préconisations pour une migration vers une architecture Zero Trust
  - Proposition d'une nouvelle architecture réseau sécurisée :
    - VLAN de production, R&D, utilisateurs, invités, IoT, serveurs, DMZ, etc.
    - Mise en place d'un firewall de nouvelle génération (NGFW) ou d'une solution UTM.
    - Application de règles de filtrage, plan d'adressage IP et politique de journalisation.
    - Homogénéisation des matériels réseaux (switchs, firewalls, AP..)
    - Fourniture d'un schéma réseau futur

- 📌 **Bureautique**
  - Remise à plat de la partie bureautique dont la future R&D dans les standards actuels
  - Proposition d'une solution 'téléphonie 2030'
  - Proposition d'une solution pour les stations de travails adéquates R&D
  - Faire une proposition pour une sensibilisation cyber pour l'ensemble des sites

- 📌 **Conformité GDPR**
  - Identifier les traitements impliquant des données personnelles.
  - Proposer des mesures techniques pour la conformité GDPR :
    - chiffrement des données,
    - minimisation,
    - rétention,
    - gestion des accès,
    - journalisation et traçabilité,
    - politique de sauvegarde/restauration
  - Production de la documentation nécessaire

- 📌 **Sécurité physique site R&D Lyon 2**
  - Suivant les documents fournis par le client, les sociétés postulantes devront :

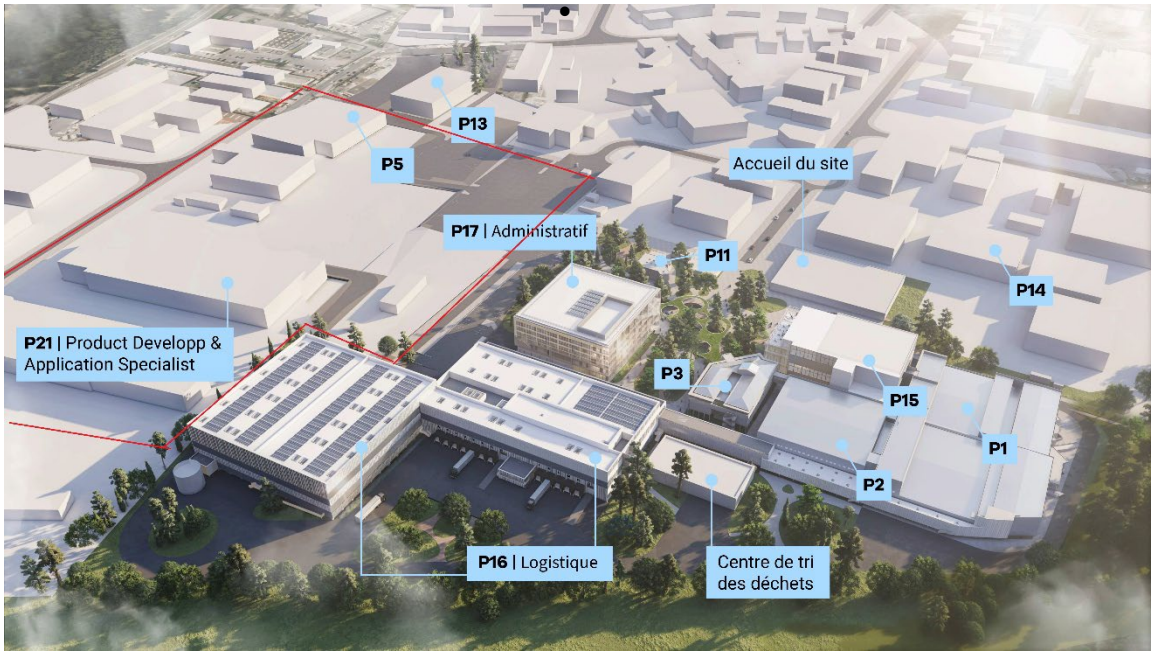
    - Faire une proposition pour la partie sécurité physique des accès aux locaux (badges d'accès, journalisation etc…)
    - Proposer un ensemble de mesures techniques permettant la vidéosurveillance des locaux (intérieurs et extérieurs) avec 2 niveaux d'accès (la partie utilisateurs support R&D et la partie chercheurs R&D)
    - Fournir des solutions adaptées quant au secret des recherches des laboratoires de R&D et à leur stockage numérique
    - ***NB : Le nouveau site sera situé sur un complexe industriel (se reporter à l'annexe 1 – les bâtiments de TechNova sont ceux entourés en rouge – Bâtiments P5 pour l'accueil et les administratifs et P21 pour la R&D)***

- 📌 SOC interne
  - Fournir des propositions d'améliorations du SOC et si besoin de refonde le SOC avec d'autres outils
  - Proposer des conseils sur les bonnes pratiques du SOC
  - Analyser les différents sites et s'appuyer sur cette dernière pour établir besoins en termes de remonté de logs afin de monitorer l'ensemble des sites
  - Fournir une solution type 'puits de logs' et son exploitation avec une équipe réduite
  - Fournir une étude des périmètres à inclure pour les pentests suivants :
    - Réseau
    - Active Directory

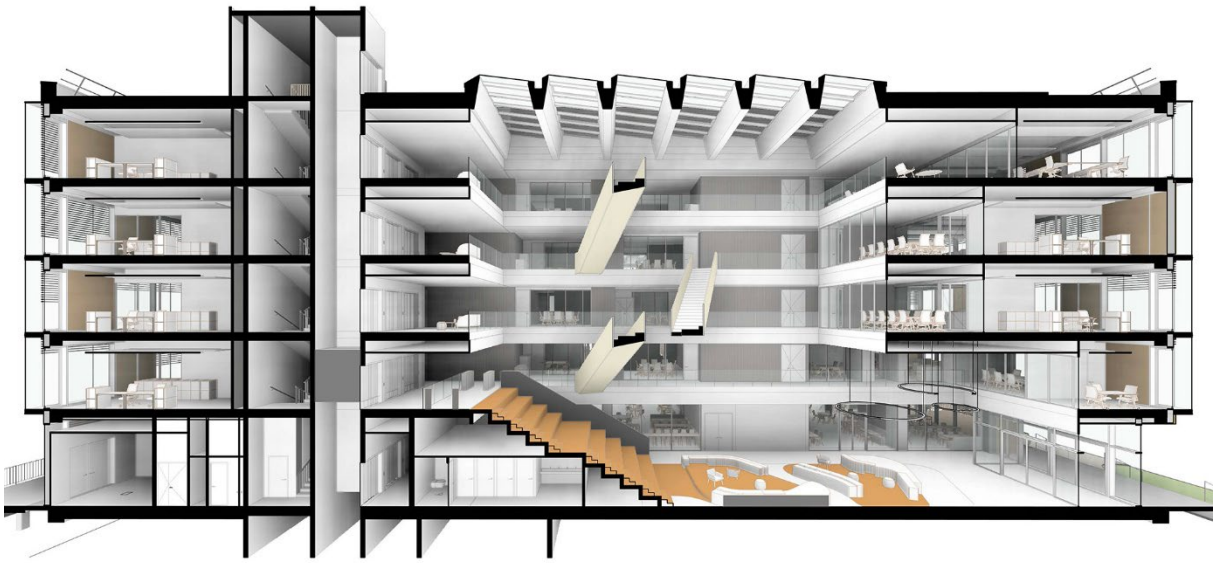
🔧 Production attendue

- Les sociétés souhaitant postuler devront le faire sur l'ensemble des besoins évoqués (cf. problématiques à résoudre)
- Elles devront fournir :
    - Un rapport technique complet (de 10 à 30 pages maximum) sur l'existant à la suite de l'interview du DSI et du RSSI (qui aura lieu le 10/12/2025)
    - Un diagramme réseau avec leur compréhension de l'existant
    - Une analyse détaillée des risques existants
    - Un plan détaillé permettant de comprendre la future topologie réseau proposée (schémas, explications etc…)
    - Le plan d'action pour la remédiation des problématiques Active Directory (GPO, Tiering, sécurisation)
    - Les mesures de mise en conformité pour la partie GDPR
    - Le détail du plan de transition bureautique (Lyon 2, nouveaux matériels et formation cyber)
    - Proposer une solution 'téléphonie 2030'
    - Fournir la meilleure solution pour la sécurisation du site R&D Lyon 2
    - Etablir un cahier des charges pour la mise en place du SOC V2
- Ces éléments devront prendre en compte les aspects suivants :
    - Impact financier du projet (que ce soit et terme de budget **et** de plans d'amortissements/charges pour TechNova)
    - Un planning à rebours de réalisation, site par site et objectif par objectif
    - L'impact sur la production des sites (arrêts de production à prévoir, formations sur les nouveaux outils, etc…)
    - L'impact environnemental de la migration et les avantages avec la future solution globale
    - La partie IA dans les domaines suivants :
        - IA et Cyberdéfense (détection des anomalies sur les logs, risques liés aux attaques assistées par l'IA)
        - Fuite de données liée à l'IA génératives (risques de pertes de données sensibles, risque GDPR)
        - Les axes d'améliorations des outils TechNova (développements, IoT, assistance à la résistance aux outils type ***Flipper***)
- Les sociétés proposeront aussi une solution permettant la réalisation d'un POC reprenant **l'ensemble des composants.** Ce POC devra pouvoir être réalisé en 08:00 maximum
- Elle défendront leur projet lors d'une présentation orale de 20 minutes avec 10 minutes de questions si nécessaire

Annexe 1 – Plan du site R&D Lyon sur le complexe industriel de Lyon-Bron



Annexe 2 – Bâtiments P5 – Accueil & Administratif



Annexe 3 – Bâtiments P21 – R&D – Identiques sur 3 niveaux