****

Revue Technologique de l’Entreprise

(Business Technology Review)

**1234 Rue Principale**

**Ville, Code Postal**

www.votresiteweb.com

**8 juillet 2025**

**Revue technologique – [Nom de l’entreprise prospect]**

**Nom de votre entreprise**

**Business Technology Review – (Revue Technologique de l’Entreprise)**

**1**

**Business Technology Review – Profil de l'entreprise**

|  |  |
| --- | --- |
| **Votre nom:** |  |
| **Nom de l'entreprise:** |  |
| **Date:** |  |

Pour bien préparer votre rendez-vous avec Synectra, merci de :

1. Compléter cette auto-évaluation et la retourner à Yohann CAMOIT au moins 48 heures avant votre rendez-vous.
2. En cas de question, contactez directement Yohann. Ces informations seront revues ensemble lors de l’échange.

📌 Une fois complété, ce document nous permettra de préparer notre rendez-vous et de nous concentrer sur vos enjeux les plus importants.

**Examen des technologies d'entreprise – Questionnaire sur vos objectifs**

**Business Technology Review – (Revue Technologique de l’Entreprise)**

**2**

|  |  |
| --- | --- |
| Quels sont les trois objectifs prioritaires de votre entreprise ou de votre service pour ce trimestre ou cette année ? | |
| **1.** |  |
| **2.** |  |
| **3.** |  |

|  |  |
| --- | --- |
| Quels sont vos trois objectifs professionnels pour les 90 prochains jours ? | |
| **1.** |  |
| **2.** |  |
| **3.** |  |

|  |  |
| --- | --- |
| Quelles sont vos 3 principales préoccupations concernant la technologie, le réseau, la sécurité ou le support dans votre entreprise ? | |
| **1.** |  |
| **2.** |  |
| **3.** |  |

|  |  |
| --- | --- |
| Y a-t-il des sujets spécifiques ou des questions que vous souhaitez aborder avec Yohann lors du rendez-vous ? | |
| **1.** |  |
| **2.** |  |
| **3.** |  |

**Business Technology Review – (Revue Technologique de l’Entreprise)**

**3**

Les 3 étapes indispensables pour un système informatique fiable et sécurisé

**Business Technology Review – (Revue Technologique de l’Entreprise)**

**4**

|  |  |  |
| --- | --- | --- |
| **Étape 1 – Consolider les Fondations** | **Étape 2 – Superviser et Anticiper** | **Étape 3 – Assurer la Continuité d’Activité** |
| **Stratégies :**   * Identification exhaustive des ressources critiques (serveurs, équipements, applications). * Évaluation et protection efficace des sauvegardes critiques (locales et cloud). * Renforcement immédiat des fondamentaux de sécurité (EDR, MFA, filtrage mail/web). * Politique rigoureuse de gestion des accès utilisateurs sensibles. * Patch management régulier (OS et applications critiques). * Élimination des équipements obsolètes ou défaillants. * Documentation technique claire et à jour des actifs critiques. * Alignement entre enjeux métiers et exigences IT.   **Tactiques:**   * Audit initial express pour détecter les vulnérabilités critiques (réseau, matériel). * Résolution rapide des problèmes techniques les plus fréquents (STP, VLAN, DHCP, DNS). * Vérification immédiate des systèmes critiques (onduleurs, serveurs). * Entretien structuré avec le dirigeant sur l'historique des incidents majeurs. | **Stratégies :**   * Mise en place d'une supervision proactive continue (RMM, alertes prédictives). * Automatisation des résolutions courantes et répétitives. * Standardisation complète des processus informatiques quotidiens (onboarding/offboarding, support centralisé). * Gestion homogène et sécurisée des accès utilisateurs (Zero Trust). * Suivi rigoureux des performances et disponibilité. * Production régulière de rapports IT clairs et décisionnels pour la direction. * Tableaux de bord simplifiés pour pilotage par les dirigeants et responsables financiers. * Comités de pilotage réguliers pour anticiper les incidents potentiels.   **Tactiques:**   * Déploiement standardisé des agents Datto RMM (Optimal) ou Domotz (Serenity). * Automatisation des alertes critiques via des modèles préconfigurés. * Mise en place d’un portail support centralisé unique. * Processus standard et automatisé pour l'onboarding/offboarding utilisateurs. * Mise à jour mensuelle des rapports simplifiés destinés à la direction. | **Stratégies :**   * Tests réguliers des plans de continuité d’activité (PCA/PRA). * Identification et élimination proactive des points de défaillance uniques (SPOF). * Protection électrique et matérielle adaptée (onduleurs, redondance). * Roadmap stratégique actualisée pour anticiper obsolescence des équipements et logiciels. * Planification anticipée des besoins IT (matériels, licences). * Ajustements réguliers des seuils et procédures pour éviter la récurrence d'incidents connus. * Sensibilisation régulière à la cybersécurité des utilisateurs (module partenaire). * Mise à jour continue des procédures internes (playbooks).   **Tactiques:**   * Validation périodique des scénarios PCA/PRA (tests pratiques). * Surveillance continue des tendances d’utilisation et consommation via RMM pour anticiper les besoins futurs. * Ajustement continu des configurations techniques pour optimiser performance et disponibilité. * Mise en place de sensibilisations régulières à la cybersécurité via partenaire spécialisé. |

Voici une liste des étapes, systèmes et stratégies technologiques à mettre en place. Une fois cette étape franchie, vous pourrez dire que vous avez mis en œuvre un *Plan Technologique Stratégique Synectra*.

Revue Technologique – Nom de l’Entreprise Prospect

Évaluation technologique de votre entreprise

**5**

À côté de chaque élément, cochez « Vrai » ou « Faux », puis attribuez une note de 0 à 5 selon le degré de mise en œuvre ou l’efficacité de ce système pour vous (0 = non en place, 5 = totalement maîtrisé). L’objectif est d’obtenir uniquement des « 5 », mais au minimum un « 4 » dans chaque section.

|  |  |  |
| --- | --- | --- |
| **Étape 1 – Consolider les Fondations : Les 5 pratiques essentielles que vous DEVEZ avoir en place** | | |
| **Article** | **Vrai ou faux ?** | **Note** |
| Vous **tenez à jour l’inventaire** complet de vos serveurs, applications et équipements réseau ; chaque élément critique est clairement identifié. | Vrai/Faux |  |
| Vos sauvegardes (données & emails) sont testées au moins une fois par trimestre : vous **restaurez** un fichier ou une VM pour vérifier la reprise réelle. | Vrai/Faux |  |
| Votre réseau (VLAN, DNS, DHCP, Wi-Fi, liens) a été **audité** récemment ; les coupures ou lenteurs récurrentes ont été corrigées. | Vrai/Faux |  |
| Vos protections de base (antivirus / EDR managé, filtrage mail & web) sont en place et maintenues à jour, et un **MFA** protège au minimum les comptes messagerie, VPN et administrateurs. | Vrai/Faux |  |
| Les mises à jour de sécurité **classées “Critique” par l’éditeur** sont installées dans le mois qui suit leur publication. | Vrai/Faux |  |

**Business Technology Review – (Revue Technologique de l’Entreprise)**

**6**

|  |  |  |
| --- | --- | --- |
| **Étape 2 – Superviser et Anticiper : Les 5 systèmes essentiels que vous DEVEZ avoir en place** | | |
| **Article** | **Vrai ou faux ?** | **Note** |
| Un outil de **supervision 24 / 7** alerte automatiquement avant qu’un incident n’arrête vos équipes. | Vrai/Faux |  |
| Les tâches IT répétitives (ex. redémarrage d’un service, application d’un correctif simple) sont **documentées ou automatisées** pour être réglées sans délai. | Vrai/Faux |  |
| Les arrivées / départs de collaborateurs suivent un **processus standard** ; les accès sont créés ou révoqués au bon moment. | Vrai/Faux |  |
| Toutes les demandes de support passent par des canaux officiels (portail, e-mail support, téléphone) et reçoivent un **numéro de suivi.** | Vrai/Faux |  |
| Vous recevez chaque mois un **tableau de bord clair** (incidents bloquants, disponibilité, alertes cybersécurité) pour décider en toute connaissance. | Vrai/Faux |  |

**Business Technology Review – Prospect Company Name**

**Business Technology Review – Prospect Company Name**

**7**

|  |  |  |
| --- | --- | --- |
| **Étape 3 – Assurer la Continuité d’Activité : Les 5 leviers critiques que vous DEVEZ avoir en place** | | |
| **Article** | **Vrai ou faux ?** | **Note** |
| Un **plan de reprise (PRA/PCA)** a été testé cette année ; vous connaissez le temps maximal d’arrêt accepté (RTO). | Vrai/Faux |  |
| Chaque **point unique de défaillance** (serveur, switch, pare-feu, routeur, lien Internet, onduleur) possède une solution de secours documentée. | Vrai/Faux |  |
| Vous suivez une **feuille de route IT** alignée sur vos objectifs de croissance : remplacement matériel, licences, montée en charge. | Vrai/Faux |  |
| Après un incident bloquant, une **analyse d’incident** est menée pour éviter qu’il ne se reproduise. | Vrai/Faux |  |
| Vos équipes bénéficient d’au moins une session annuelle de **sensibilisation cybersécurité** (incluse ou en module complémentaire). | Vrai/Faux |  |

**Business Technology Review – (Revue Technologique de l’Entreprise)**

**8**