Sécurité, hébergement et protection des données chez DecisionBrain

Introduction

DecisionBrain est un acteur de référence dans le domaine des logiciels d'aide à la **décision** avancés, s'appuyant sur l'**intelligence artificielle**, l'**optimisation mathématique** (Recherche Opérationnelle) et la **modélisation prédictive** pour répondre aux défis de la planification opérationnelle, de la chaîne d'approvisionnement et la gestion des effectifs à la planification des tournées de véhicules.

La sécurité de l'information est un impératif stratégique chez DecisionBrain et le fondement de la confiance de nos clients. Notre **Système de Management de la Sécurité de l'Information** (SMSI), structuré conformément aux normes **ISO/IEC 27001, 27017 et 27018**, garantit la **Confidentialité**, l'**Intégrité** et la **Disponibilité** (CID) de tous les actifs numériques qui nous sont confiés.

Gouvernance et conformité

Engagement de la direction

La direction de DecisionBrain a établi une politique de sécurité alignée sur les normes ISO/IEC 27001, 27017 et 27018 avec des ressources dédiées à l'amélioration continue du SMSI et des responsabilités en matière de cybersécurité clairement définies. L'objectif principal est de réduire à zéro tout risque majeur (ex. rançongiciels, violations de données).

Conformité réglementaire

En conformité avec le **RGPD**, DecisionBrain applique le principe de Privacy by Design dès les premières étapes du développement. Un délégué à la protection des données (DPO) dédié supervise la gouvernance des données personnelles. Nous maintenons un registre détaillé des activités de traitement et réalisons des Analyses d'Impact relatives à la Protection des Données (AIPD) pour toutes les opérations sensibles.

EUROCERTIFICATIONS ISO/IEC 27001

ISO/IEC 27017

ISO/IEC 27018

Certifications

Standard / Entité	Conformité / Certification
ISO/IEC 27001, 27017, 27018	Cadre méthodologique du SMSI de DecisionBrain
RGPD	Conformité totale ; code de conduite SWIPO appliqué
Scaleway (CSP principal)	ISO 27001, HDS, SecNumCloud (en cours)
DigitalOcean	SOC 2 Type II, SOC 3, CSA STAR Niveau 1
Microsoft Azure	ISO 27001, SOC 1/2/3, HIPAA, FedRAMP, IRAP
AWS	ISO 27001, SOC 1/2/3, PCI-DSS Niveau 1, HIPAA

Infrastructure et hébergement

Architecture Cloud-native et souveraine

Notre plateforme est entièrement **agnostique en matière d'infrastructure**, prenant en charge les déploiements en cloud public, cloud privé ou sur site en mode isolé (on-premise, disconnected cloud, air-gapped). Nous privilégions les fournisseurs basés en Europe, notamment Scaleway, afin de garantir que les données des clients restent soumises au droit européen (RGPD) et ne soient pas exposées à des législations extraterritoriales. La localisation de l'hébergement est définie en collaboration avec chaque client.

Environnements dédiés et non multi-locataires

Chaque client dispose d'un cluster Kubernetes **dédié** et d'un **Cloud Privé Virtuel** (VPC), séparant entièrement les environnements de développement, de recette (UAT) et de production. Le **durcissement** des conteneurs via les images de base BellSoft réduit la surface d'attaque du système d'exploitation.

Sécurité, hébergement et protection des données chez DecisionBrain

Gestion des identités et des accès

La gestion des identités est centralisée via Keycloak, avec prise en charge de l'**OIDC**, **SAML 2.0, SSO** et **LDAP**. L'authentification multifacteur (MFA) est imposée pour tous les accès administratifs et critiques des employés. Les droits d'accès suivent un modèle de Contrôle d'Accès Basé sur les Rôles (RBAC) avec le principe du moindre privilège et sont immédiatement révoqués lors du départ d'un employé.

Protection des données et chiffrement

Au repos

Le chiffrement **AES-256** est disponible pour tous les volumes de stockage et bases de données (PostgreSQL, MongoDB). Nous exploitons le chiffrement **Scaleway Block Storage** (SBS) au niveau de l'infrastructure : transparent pour Kubernetes et permettant le redimensionnement en ligne des volumes sans interruption de service. Les postes de travail des employés sont chiffrés via BitLocker ou FileVault ; les supports amovibles (USB) sont interdits.

En transit

Toutes les communications sont sécurisées avec **HTTPS** et **TLS 1.2/1.3** (certificats Let's Encrypt). L'accès à distance et l'administration des clusters utilisent des tunnels VPN WireGuard ou IPsec.

Sauvegarde et continuité d'activité

Les sauvegardes sont gérées via BackupPC et les API des fournisseurs cloud, selon un processus en trois étapes :

- Snapshots des volumes Kubernetes
- Transfert automatisé vers des buckets S3 isolés
- Archivage immuable via le mode de conformité WORM (Write Once Read Many) de Scaleway

Notre **Plan de Continuité d'Activité** (PCA) utilise Terraform (Infrastructure as Code) pour la reconstruction automatisée des environnements. Le RTO des fonctions critiques est de 24 heures, avec des tests de restauration mensuels. La gestion de crise s'étend de la mobilisation immédiate (0–24h) jusqu'à la restauration complète du service (2–14 jours).

Développement sécurisé (DevSecOps)

La **sécurité** est intégrée tout au long de notre pipeline CI/CD. SonarQube assure l'analyse statique (SAST) ; Trivy et OWASP Dependency Check effectuent des analyses des conteneurs et des bibliothèques à la recherche de CVE. Nos pratiques s'alignent sur l'OWASP Top 10. Des **tests de pénétration** annuels sont réalisés par des tiers certifiés, souvent dans le cadre du processus d'audit de sécurité rigoureux d'IBM. Quatre versions majeures de notre plateforme **DB Gene** sont publiées chaque année, intégrant chacune des bibliothèques et images de base mises à jour.

Supervision et gestion des incidents

L'**observabilité** en temps réel est assurée par Prometheus, Grafana et Loki. Les journaux système et applicatifs sont conservés dans S3 pendant une durée minimale de 90 jours. Les alertes sont gérées via AlertManager et Mattermost. Conformément au RGPD, toute violation de données présentant un risque pour les droits des personnes est signalée à l'autorité de contrôle compétente dans les 72 heures, via des canaux de communication chiffrés et des protocoles d'escalade définis.

Conclusion

DecisionBrain allie excellence technique et rigueur organisationnelle pour protéger les données de ses clients. Grâce à une architecture cloud-native isolée, un alignement sur les normes ISO 27001, 27017 et 27018 et une culture DevSecOps, nous proposons une plateforme décisionnelle performante, souveraine et hautement sécurisée. La transparence et l'auditabilité demeurent la pierre angulaire de notre mission.