

VOTRE ENVIRONNEMENT EST-IL RÉELLEMENT SÉCURISÉ ?

CHECKLIST POUR LES RESPONSABLES IT & SAP

La sécurité de la plateforme SAP BTP repose sur un modèle de responsabilité partagé entre SAP et ses clients. Les risques sur SAP BTP viennent rarement de la plateforme elle-même : ils viennent surtout de la gouvernance et des paramétrages (droits trop larges, accès externes qui s'éternisent, traçabilité insuffisante, connectivité on-prem trop permissive....). Une configuration négligée peut suffire à créer une exposition majeure. Testons rapidement votre niveau de maîtrise.

1 Gouvernance des privilèges & Architecture SAP BTP

- ☐ 1. Savez-vous qui a des privilèges Admin (Global Account / Subaccounts) ?
- ☐ 2. Avez-vous limité les rôles à privilèges élevés ?
- ☐ 3. L'architecture est-elle conçue pour la sécurité : environnements séparés (Dev/Prod), rôles distincts, frontières claires ?
- ☐ 4. Vos naming conventions sont-elles cohérentes, homogènes et alignées avec les recommandations SAP ?

Un modèle mal structuré est difficile à sécuriser... et encore plus à auditer.

2 Gestion des identités & accès

- ☐ 5. Disposez-vous d'une revue périodique des accès (internes & externes) ?
- ☐ 6. Les utilisateurs externes ont-ils été réduits au strict nécessaire et en lecture seule quand c'est possible ?

La majorité des incidents cloud sont liés à des accès excessifs ou oubliés.

3 Traçabilité, audit & conformité

- ☐ 7. Disposez-vous d'une traçabilité exploitable : SAP Audit Log activé, conservation/archivage, process de consultation ?
- ☐ 8. Pouvez-vous répondre rapidement à : "qui a changé quoi ? quand ?" sur la plateforme et la connectivité ?

Sans logs, il n'y a ni preuve, ni investigation possible en cas d'incident

5 SAP Cloud Connector – Lien critique vers vos back office SAP

- ☐ 9. Votre SAP Cloud Connector est-il sur une version supportée par SAP ?
- ☐ 10. Les alertes du Cloud Connector (SMTP / alerting) sont-elles actives et testées ?
- ☐ 11. Les paramètres de chiffrement (TLS) sont-ils à jour et conformes aux recommandations SAP ?

Un Cloud Connector mal configuré est une porte d'entrée directe vers votre SI interne..

6 Certificats

- ☐ 12. Vos certificats utilisés pour l'administration et les échanges (BTP / Cloud Connector / Backend) sont-ils valides et conformes ?
- ☐ 13. Avez-vous une gestion centralisée et contrôlée des certificats pour éviter les certificats "oubliés" ou mal maîtrisés ?

Les certificats sont souvent "installés une fois"... puis oubliés – jusqu'au jour où une expiration ou une mauvaise configuration ouvre une faille ou bloque l'accès.

7 Sécurité applicative et des protections des données

- ☐ 14. Vos applications BTP permettent-elles l'upload de fichiers et le scan anti-malware est-il activé ?
- ☐ 15. Vos applications utilisent-elles une authentification forte (OAuth / principal propagation / mTLS) ?

Une mauvaise configuration suffit pour transformer votre BTP en point d'entrée vers vos systèmes ou en canal d'exfiltration de données vers l'extérieur.

CE QU'IL FALLAIT RETENIR

SAP BTP est puissant, mais sa maîtrise ne s'improvise pas.

- SAP sécurise l'infrastructure.**
- Vous êtes responsable des accès, des usages et de la configuration.**

La valeur de SAP BTP dépend directement de son niveau de maîtrise.

PROCHAINE ÉTAPE RECOMMANDÉE

Une checklist alerte. Elle ne sécurise pas votre plateforme.

- L'enjeu : passer rapidement à l'action**
 - qualifier votre niveau de maturité
 - sécuriser les points critiques
 - cadrer un premier cas d'usage à valeur

Prochaine étape : un atelier de cadrage SAP BTP pour sécuriser et activer votre plateforme rapidement.

RENCONTREZ UN EXPERT

