Sécurité IA

Déploiement Sécurisé de Dust : Guide Complet RSSI 2026

27 juin 2026 • Mis à jour le 12 juillet 2026 • 22 min de lecture •

7060 mots • 173 vues •

Télécharger le PDF

Déployer une plateforme d'agents IA en entreprise sans maîtriser ses implications de sécurité revient à ouvrir les portes du système d'information à un acteur disposant de larges privilèges d'accès et d'action. Dust, plateforme d'agents IA d'origine française certifiée SOC 2 Type II et forte de plus de 3 000 organisations clientes après sa levée de fonds Series B de 40 millions de dollars en mai 2026, illustre parfaitement ce paradoxe fondamental de l'IA agentique : sa valeur — l'accès profond aux connaissances internes et la capacité d'agir sur les systèmes — est aussi la source de sa dangerosité. Ce guide opérationnel, destiné aux RSSI, architectes sécurité, DSI et AI Champions, cartographie en détail la surface d'attaque d'un déploiement Dust, analyse le modèle de sécurité natif de la plateforme et son partage des responsabilités, recense les vulnérabilités selon les référentiels OWASP LLM Top 10 et OWASP MCP Top 10, documente les trois vulnérabilités publiquement divulguées via le programme HackerOne, et propose une démarche structurée en huit phases, des scénarios de risque détaillés (S1 à S12), une checklist priorisée avec indicateurs de maturité et un modèle en trois niveaux pour monter en maturité par paliers conscients. Trois risques dominent : l'injection de prompt indirecte via des sources empoisonnées, l'autonomie excessive d'agents surprivilégiés, et les fuites par mauvaise configuration — auxquels s'ajoute en 2026 la sécurité du protocole MCP comme nouvelle frontière critique à gouverner rigoureusement. La posture recommandée tient en cinq principes : SSO avec offboarding automatisé via SCIM, cloisonnement des données par Spaces restreints, moindre privilège sur les données, les outils et les comptes de service, validation humaine sur les actions sensibles avec préférence pour le mode lecture seule, et instrumentalisation de l'observabilité couplée à des tests adversariaux réguliers. La sécurité d'un déploiement Dust est avant tout une affaire de configuration et de gouvernance, pas de correctifs à attendre — et elle se construit par paliers de maturité mesurables.