Aide-mémoire — Préparation à la sécurité des identités des agents d'IA

Les entreprises se pressent pour déployer des agents d'IA dans leurs systèmes, environnements cloud et applications orientées clients. Mais cet empressement ne s'accompagne pas toujours d'une préparation adéquate. En effet, si **91 % des entreprises** utilisent déjà des agents d'IA, **près de 50 % d'entre elles ne disposent pas d'une supervision formelle,** ce qui pose de nouveaux défis en matière de gouvernance et de contrôle.

Ces identités non humaines offrent autant de nouvelles capacités puissantes qu'elles engendrent de risques. Sans framework d'identité solide, les agents d'IA élargissent la surface d'attaque et créent des failles de sécurité que les contrôles traditionnels ne sont pas conçus pour gérer.

Pour gouverner les agents d'IA en toute sécurité et à grande échelle, les entreprises ont besoin d'un **socle de sécurité axé sur l'identité qui sécurise l'ensemble du cycle de vie des agents, du projet pilote initial à la production.**

Cet aide-mémoire sur la préparation à l'IA rassemble de façon concise des pratiques de sécurité des identités qui vous aident à **préserver la visibilité, exercer un contrôle et vérifier la conformité à grande échelle** dans les écosystèmes d'agents d'IA.

La plupart des entreprises utilisent déjà des agents d'IA, mais près de 50 % d'entre elles ne disposent pas d'une supervision formelle.

Pratiques de sécurité des identités de base pour les écosystèmes d'agents d'IA

Gouverner tous les agents

Établir une visibilité et un contrôle centralisés sur les agents d'IA dans toute l'entreprise

01.

Découvrir et superviser les agents d'IA et les identités non humaines

Découvrez et supervisez en permanence les agents d'IA et les comptes de service associés qui opèrent dans différents environnements. Vous empêcherez ainsi les identités non gérées de fonctionner en dehors du cadre de gouvernance ou des contrôles de surveillance établis.

02.

Établir un registre centralisé des agents

Enregistrez les agents découverts, déterminez leur propriété et définissez leurs autorisations. Un registre centralisé améliore l'attribution de responsabilité, l'auditabilité et la visibilité pour tous les systèmes d'IA.

03.

Centraliser la gouvernance des identités des agents d'IA

Gérez le provisioning, l'authentification, l'autorisation et le déprovisioning via un système d'identité centralisé. Une plateforme unifiée élimine la fragmentation, améliore la cohérence des politiques et favorise l'évolutivité.

04.

Surveiller en permanence l'activité des agents d'IA en temps réel

Surveillez en temps réel l'activité d'authentification, les appels d'API et les modèles comportementaux associés aux agents d'IA. La visibilité en temps réel permet de détecter rapidement les utilisations abusives, les anomalies ou les identifiants compromis.

05.

Consigner et auditer les actions des agents d'IA dans tous les systèmes

Enregistrez et auditez les événements d'authentification, les tentatives d'accès et les actions initiées par des agents. La journalisation avancée prend en charge la résolution des incidents, la validation de la conformité et l'application de la gouvernance.

Sécuriser chaque agent

Déployer des agents d'IA qui agissent de manière sûre, prévisible et conforme à l'intention de l'entreprise

06.

Lier les sessions d'agents à une identité humaine vérifiée

Avant toute action d'agent, établissez une identité humaine vérifiée afin que les actions soient attribuables, responsables et fiables.

07.

Sécuriser les tokens, les identifiants et les secrets dans un coffre-fort dédié

Stockez les tokens, les identifiants et les secrets à longue durée de vie dans un coffre-fort numérique (vault) sécurisé et isolé, plutôt que de les intégrer au code des agents. Émettez des tokens à courte durée de vie à l'exécution afin de réduire l'impact en cas d'incident et de prévenir les fuites.

08.

Appliquer des vérifications d'autorisation et des contrôles « humain dans la boucle »

Autorisez les agents à agir uniquement lorsque cela est permis, avec une approbation humaine requise pour les actions à plus haut risque.

09.

Appliquer un accès sur le principe du moindre privilège aux agents d'IA

Limitez les agents aux ressources et actions autorisées, évaluées au moment de la demande, afin de garantir un comportement limité et prévisible.

Transformez la préparation en action

Votre entreprise est-elle prête à prendre le contrôle de son écosystème d'agents d'IA ? Consultez notre Checklist de conformité de la sécurité des identités de l'IA pour guider vos prochaines étapes.