okta

Gouvernance totale des identités : 5 étapes pour moderniser votre solution de gouvernance des identités

Face à l'adoption rapide de l'IA et à la prolifération du cloud que nous connaissons aujourd'hui, le périmètre réseau traditionnel disparaît progressivement, faisant de la gouvernance des identités le socle indispensable à un environnement sécurisé. Cette checklist vous fournit une roadmap stratégique pour réaliser un audit de vos capacités de défense et combler le fossé entre la sécurité humaine et non humaine. En se concentrant sur ces grandes étapes, de l'inventaire initial à la gestion automatisée du cycle de vie, les entreprises peuvent prendre les mesures qui s'imposent pour garantir que chaque identité — qu'il s'agisse d'un utilisateur humain, d'une identité non humaine ou d'un agent d'IA — est prise en compte, gouvernée selon le principe du moindre privilège et surveillée en permanence pour déterminer les risques afférents.

Inventaire de toutes les identités

La mise en place dans votre écosystème de sécurité des identités d'une seule source fiable réduit les zones d'ombre créées par la Shadow AI et les comptes de service non gérés.

- ☐ Référencer chaque utilisateur, chaque identité non humaine et chaque agent d'IA
- ☐ Inclure aussi bien les comptes approuvés que les comptes non validés, quel que soit leur type
- ☐ Analyser les plateformes d'agents (AWS Bedrock, Vertex AI, etc.)
- ☐ Identifier l'ensemble des identités (collaborateurs humains et entités non humaines) sur les plateformes cloud, on-premise et SaaS
- ☐ Détecter les comptes orphelins ou inactifs
- ☐ Relier chaque identité aux systèmes et aux données auxquels elle a accès

Identification des propriétaires humains

Le fait de relier chaque entité numérique à une personne responsable permet de garantir l'ancrage des actions automatisées dans un contexte métier transparent.

- ☐ Relier chaque identité (utilisateur humain, identité non humaine ou agent d'IA) à une personne ou équipe responsable
- ☐ Identifier l'objectif commercial de chaque identité
- ☐ S'assurer du transfert de propriété dès lors qu'un collaborateur change de rôle ou quitte l'entreprise
- ☐ Signaler et suspendre les identités sans propriétaire actif validé

okta

Application du principe du moindre privilège

L'adoption d'un modèle sans privilèges permanents permet de s'assurer qu'aucun accès ne perdure et de réduire considérablement l'impact d'éventuelles compromissions d'identifiants.

- ☐ Accorder l'accès uniquement aux ressources strictement nécessaires, et à rien d'autre
- ☐ Utiliser des tokens en flux tendu (JIT) au lieu d'identifiants permanents
- ☐ Éliminer les clés API codées en dur et les identifiants statiques du code ou des pipelines
- ☐ S'assurer que les accès délégués et ceux des sous-agents sont plus restreints que le champ d'application de l'identité sponsor
- ☐ Appliquer la règle de séparation des tâches (SoD) en identifiant et en corrigeant les combinaisons d'accès toxiques

Standardisation de l'évaluation des accès

L'application de standards de certification cohérents à tous les types d'identités permet de s'assurer que les autorisations restent alignées au fil du temps sur les besoins réels de l'entreprise.

- ☐ Appliquer les mêmes standards d'examen et de certification aux comptes de service et aux agents qu'aux collaborateurs
- ☐ Exécuter des campagnes régulières de recertification des utilisateurs et des agents à haut risque
- ☐ Rechercher activement les violations de la règle de séparation des tâches (SoD) ainsi que les éventuelles autorisations conflictuelles pour chaque identité du périmètre
- ☐ Résilier les accès qui ne sont plus justifiés
- ☐ Identifier toute autorisation qui a été étendue hors de son périmètre initial
- ☐ Consigner et limiter dans le temps toute exception, y compris les éventuelles dérogations en matière de séparation des tâches (SoD)

Automatisation de la gestion du cycle de vie des utilisateurs

L'automatisation du cycle de vie des identités, du premier jour jusqu'à l'offboarding, contribue à faire évoluer la sécurité au même rythme que l'entreprise, sans intervention manuelle.

- ☐ Faire passer l'ensemble du provisioning des identités par un processus de demande et de workflow approuvé
- ☐ Déprovisionner automatiquement les identifiants à chaque fois qu'un workflow, une tâche ou un emploi touche à sa fin
- ☐ Configurer l'expiration des identifiants en fonction du rôle ou de la durée de la tâche associés
- ☐ Déclencher la résiliation de l'accès des agents dès lors que le collaborateur sponsor quitte l'entreprise
- ☐ Automatiser la détection des comptes inutilisés ou orphelins pour chaque type d'identité

Optimisation de votre stratégie de gouvernance

Consultez notre eBook sur la gouvernance axée sur la sécurité pour des conseils sur la modernisation de votre posture. Vous y découvrirez comment passer de processus manuels cloisonnés à une résilience automatisée pour chaque utilisateur humain, identité non humaine et agent d'IA de votre écosystème.

Que vous cochiez la plupart des exigences de cette checklist ou que vous commenciez à peine l'inventaire de votre environnement, Okta Identity Governance vous offre le socle stratégique nécessaire à la modernisation de votre posture.

Passer de processus manuels et cloisonnés à un écosystème de sécurité des identités unifié permettra à votre entreprise d'automatiser l'ensemble du cycle de vie de ses utilisateurs humains, identités non humaines et agents d'IA.

Voyez plus loin que les autorisations statiques et adoptez un modèle de résilience continue et automatisée, qui repose sur le principe du moindre privilège et l'accès « en flux tendu », sans ralentir vos activités.

Découvrir Okta Identity Governance

À propos d'Okta
Okta, Inc. – The World's Identity Company™ – protège les identités humaines, machines et d'IA afin que chacun puisse utiliser n'importe quelle technologie en toute sécurité. Nos solutions d'identité client et collaborateur permettent aux entreprises et aux développeurs de protéger leurs agents d'IA, utilisateurs, collaborateurs et partenaires tout en renforçant la sécurité, en améliorant l'efficacité et en stimulant l'innovation. Découvrez pourquoi les plus grandes marques au monde font confiance à Okta pour l'authentification, l'autorisation et bien plus encore sur okta.com/fr.