Engineer

La sécurité de vos agents IA

Contrôles d'accès des agents IA : inventaire convenu, constats hiérarchisés, tests d'autorisations et dossier de vérification.

Comprenez à quoi vos agents IA peuvent accéder et encadrez ces accès par des contrôles. Un agent connecté à une messagerie, à des documents ou à une API introduit des autorisations et des scénarios d’échec qui nécessitent un examen. Nous recensons les systèmes convenus, évaluons les risques, mettons en œuvre les contrôles approuvés et testons les actions restreintes. Vous recevez la cartographie des accès, les constats et le dossier de vérification.

Transformez la prestation en résultat

Mettez « La sécurité de vos agents IA » au service d'un résultat pour votre entreprise. Nous pouvons relier le travail technique aux utilisateurs, aux opérations et aux décisions qu'il doit soutenir. Les accès de chaque agent recensés et limités au nécessaire, chaque action consignée hors de sa portée et chaque protection testée plutôt que supposée fiable.

Découvrir nos prestations Contactez-nous →

Examinez les réalisations pertinentes

Consultez les réalisations liées sur cette page pour examiner notre démarche. Interrogez-nous sur les compromis et les conditions qui ont conduit à chaque résultat. 1 000 règles RBAC pour sécuriser Linux — 1,000 règles d'accès écrites pour combler une faille de sécurité

1 000 règles RBAC pour sécuriser Linux Contactez-nous →

Cartographiés : chaque agent et les ressources accessibles

Nous recensons les agents du périmètre convenu, y compris les intégrations approuvées et les autres connexions identifiées avec vos équipes. Pour chacun, la cartographie consigne les identifiants d’accès, les outils et les données accessibles. Vous recevez cette cartographie avec les constats, et la responsabilité de sa mise à jour est convenue lors de la transmission.
Elle décrit l’environnement examiné, avec un périmètre et des lacunes explicitement indiqués.

Verrouillés : le moindre privilège pour chaque agent

Un agent reçoit sa propre identité et le minimum de privilèges nécessaire à sa tâche : des rôles plutôt que des comptes partagés (RBAC), la lecture seule en l'absence d'autorisation d'écriture, des écritures uniquement par des outils spécialisés avec des limites de fréquence et de volume. Les secrets sont séparés par agent et par hôte, jamais collés dans une instruction, et renouvelés sans modification du code. Les textes externes lus par un agent — courriels, pages web ou documents — sont traités comme des données non fiables. Les autorisations des outils et les contrôles de validation font respecter les limites convenues ; un message disant « ignore tes règles » n'autorise aucune action. Les contrôles refusent l'action en cas d'échec : lorsqu'une vérification ne peut pas s'exécuter, l'action est refusée.

Consignés : les actions et leurs bénéficiaires

Chaque appel d'outil est journalisé avec la personne pour laquelle il a agi, ce qui lui a été demandé, ce à quoi il a accédé et ce qui a été renvoyé. Le journal est conservé là où l'agent lui-même ne peut pas le modifier. Les règles d'alerte sont convenues pour le système. Elles peuvent couvrir une rafale de lectures, une utilisation en dehors des horaires prévus ou un accès dépassant le périmètre de données convenu pour l'agent. Lorsqu'un problème survient, ces traces transforment un incident en chronologie plutôt qu'en supposition.

Une cartographie, un verrou et un journal **sont trois affirmations** — tant que personne n'a tenté de les contourner.

Les contrôles convenus sont vérifiés à l'aide de cas représentatifs d'accès, d'utilisation abusive et de reprise avant la transmission.

Un verrou se teste, il ne s'accepte pas sur parole

Nous testons les contrôles d'accès dans le périmètre de la mission et consignons ce qui a été tenté, refusé ou nécessite encore une intervention. Les tests peuvent couvrir les appels d'outils refusés, les limites de débit, l'isolation des identifiants d'accès et les tentatives d'injection d'instructions. Il en résulte un

dossier de vérification examinable et un ensemble de contrôles reproductibles, avec leurs limites indiquées. Le traitement des incidents et le renouvellement des identifiants d'accès font l'objet d'un périmètre distinct lorsqu'une exposition existante doit être contenue.

Les réalisations qui l'étayent

Nous avons effectué ce travail sur des serveurs, des systèmes d'identité et des plateformes. Nous avons écrit 1 000 règles RBAC sur des serveurs Linux et de bases de données, dirigé la gestion des accès sur M365 et l'authentification unique et mené un programme continu d'analyse de sécurité avec 21 audits écrits. Nous avons séparé chaque secret opérationnel par hôte, ajouté une vérification préalable des secrets en une seconde, trouvé trois verrous sur la porte, tous ouverts et prouvé à chaque exécution que le blocage des intrusions fonctionne. Nous avons construit une limitation de débit qui bloque par défaut en cas d'échec et écrit une règle de périmètre après une fuite. La page Comment nous travaillons en sécurité décrit notre propre pratique.

Le déroulement d'une mission

Nous commençons en lecture seule. Nous cartographions les agents du périmètre convenu, leurs identifiants d'accès et les ressources accessibles, puis vous remettons les constats classés par risque, chacun avec sa justification et sa correction. Les corrections sont ensuite apportées dans votre configuration et votre dépôt, soumises à votre validation, avec des contrôles qui échouent lorsque les voies d'accès couvertes dépassent les autorisations convenues. Vous conservez la cartographie, le dossier et les tests — le fichier à remettre à un auditeur ou à un assureur — et les données lues par les agents peuvent être soumises aux mêmes autorisations. Cette prestation s'achète comme le reste de nos travaux, selon les modalités de la page Nos tarifs.

Si des agents détiennent déjà les clés de vos systèmes, dites-nous lesquels.

Audit de sécurité des agents IA dans le périmètre convenu

Cartographiés

Un inventaire convenu des agents, des identifiants d'accès et des accès aux données compris dans le périmètre, conservé avec votre configuration.

Verrouillés

Chaque agent dispose de sa propre identité et du minimum de droits nécessaire ; le texte qu'il lit est traité comme des données, jamais comme des ordres.

Consignés

Chaque action est journalisée en indiquant la personne pour laquelle elle est effectuée, à un endroit que l'agent ne peut pas modifier, avec des alertes en cas d'anomalie.

Parlons de vos agents

Chaque agent que vous exploitez **détient une clé ouvrant un accès** — sachez quelle clé et à quoi elle donne accès.

Nous commençons en lecture seule : une cartographie des agents et des identifiants d'accès dans le périmètre convenu, avec des constats classés par risque.

Demander une cartographie des agents Nos tarifs →

Définissez le périmètre avant de commander les travaux

Présentez le parcours de déploiement, les risques opérationnels et les personnes d'astreinte. Nous pouvons définir un changement avec des vérifications, une procédure de reprise et une responsabilité claire.

Consulter les tarifs Contactez-nous →

Précisez vos besoins avec nous

Dites-nous ce que vous attendez de « La sécurité de vos agents IA », y compris l'échéance et l'équipe qui en assurera la maintenance. Nous pouvons discuter d'une façon concrète d'avancer.

Découvrir nos prestations

welcome@engineer.company +45 50 10 61 84 Copenhague, Danemark

Emportez cette page avec vous

Fiche de contact

Créé avec soin et amour par D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

Droit d'auteur © 2025 – aujourd'hui · Engineer ApS · Tous droits réservés.

Imprimé depuis https://engineer.company/fr/ai-security/