Posture de sécurité de l'identité : la checklist indispensable pour se préparer aux attaques

14 questions pour aider votre entreprise à se protéger des cyberattaques axées sur l'identité

Les cybercriminels n'ont que faire de votre pare-feu, ce sont vos identifiants qui l'intéressent. Les acteurs malveillants exploitent les tokens de session pour contourner les MFA faibles via des proxys AiTM et pirater les identités non humaines telles que les comptes de service dormants, dans le but d'infiltrer votre système sans être détectés.

Cette checklist vous permettra de vérifier l'efficacité de votre capacité de défense face au paysage des menaces moderne.

Il convient de noter que cette checklist ne constitue qu'un des composants de votre programme de sécurité global.

Avant l'attaque — Gestion proactive de la posture

Cette section met en avant la nécessité d'éliminer les erreurs de configuration et de réduire la surface d'attaque des identités avant qu'une attaque ne se produise.

1. Validez-vous en permanence le niveau de sécurité des identités humaines et non humaines (comptes de service, clés API, etc.) ?
2. Pouvez-vous appliquer automatiquement le principe du moindre privilège et vérifier que le MFA n'a pas été contourné ?
3. Avez-vous mis en place un processus permettant d'identifier les comptes obsolètes ou partiellement révoqués qui disposent encore d'un accès actif ?
4. Existe-t-il un système destiné à prioriser et à corriger les erreurs de configuration de l'identité et les autorisations excessives afin de réduire l'impact potentiel d'une brèche ?
5. Disposez-vous d'une visibilité suffisante sur les identités pour avoir une vue d'ensemble des entités ayant accès aux différentes ressources et de la manière dont elles s'authentifient, ce qui permet de combler les failles laissées par les outils CSPM et SSPM ?

Identity Security Posture Management

Découvrez et corrigez en permanence les risques liés à l'identité et les erreurs de configuration.

Pendant l'attaque — Détection et réponse continues face aux menaces

Cette section porte sur les fonctionnalités nécessaires pour détecter les menaces et y répondre en temps réel, au moment où elles se produisent.

6. Avez-vous implémenté une authentification résistante au phishing (par exemple Okta FastPass) pour protéger les utilisateurs contre les attaques de phishing ?
7. Surveillez-vous en permanence l'activité des sessions et le comportement des utilisateurs après l'authentification initiale afin de détecter les anomalies et les éventuels déplacements latéraux ?
8. Pouvez-vous automatiser les réponses directes pour circonscrire les incidents, comme la déconnexion universelle des applications et des terminaux, l'application d'un MFA renforcé ou le déclenchement de workflows personnalisés ?
9. Disposez-vous d'une protection contre les bots pilotée par l'IA, capable de détecter et d'atténuer les attaques automatisées sans nécessiter de saisie utilisateur telle qu'un CAPTCHA traditionnel ?
10. Votre système évalue-t-il en permanence les niveaux de risque et le contexte des utilisateurs et des terminaux afin d'évaluer et d'appliquer les politiques de sécurité de façon dynamique tout au long d'une session ?

Identity Threat Protection

Détection et réponse automatisées pour contrer les menaces d'identité en temps réel.

Okta Device Access

Connexion sécurisée au terminal pour renforcer la protection et simplifier l'accès aux ressources.

Okta FastPass

Sécurité Zero Trust grâce à une authentification sans mot de passe et résistante au phishing.

Après l'attaque — Renforcement de la résilience de l'identité

Cette section se concentre sur l'amélioration de la posture de sécurité et de la réponse après un incident.

11. Disposez-vous d'outils d'observation des incidents et d'investigation numérique permettant de mettre au jour le chemin complet des attaques d'identité ?
12. Possédez-vous un système permettant d'optimiser la gestion des incidents grâce à la corrélation des événements d'identité et à une Threat Intelligence partagée entre les outils de sécurité ?
13. Pouvez-vous démontrer votre conformité en associant des contrôles d'identité à des frameworks communs (p. ex. NIST) ?
14. Disposez-vous d'une boucle de rétroaction continue pour analyser les événements de sécurité et optimiser les réponses au fil du temps ?

Okta distingué par le titre de « Overall Leader » dans le rapport KuppingerCole *Leadership Compass for ITDR* 2025.

En savoir plus

Avec Okta

Grâce à une visibilité sur 10 milliards de connexions mondiales et 2 milliards de menaces bloquées chaque mois, Okta est en mesure d'observer les tactiques, techniques et procédures que les autres ne voient pas. En unifiant l'identité, Okta offre une visibilité incomparable sur les signaux et politiques dans vos environnements IT, sécurité et clients, et donne à vos équipes de puissants outils pour détecter et répondre aux menaces en temps réel.

Okta propose un écosystème de sécurité des identités cohérent grâce à une protection des identités orchestrée de bout en bout — avant, pendant et après l'authentification, pour chaque identité (humaine, non humaine et d'IA) et dans tous les environnements.