Livre blanc

Okta Secure Identity Commitment

Dernière mise à jour : 29/05/2024

Proposer des produits et services d'identité sécurisés de pointe

Promouvoir les bonnes pratiques auprès des clients pour optimiser leur protection

Encourager notre secteur à renforcer la protection contre les attaques ciblant l'identité

Renforcer notre infrastructure d'entreprise

okta

Sommaire

2 Résumé

3 Introduction

5 Proposer des produits et services d'identité sécurisés de pointe

11 Promouvoir les bonnes pratiques auprès des clients pour optimiser leur protection

12 Encourager notre secteur à renforcer la protection contre les attaques ciblant l'identité

13 Renforcer l'infrastructure d'entreprise d'Okta

16 Conclusion

Résumé

L'identité constitue le principal point d'entrée de sécurité en entreprise, tant pour les applications axées collaborateurs que pour celles axées clients. En parallèle, le volume et la complexité des attaques contre les entreprises, des plus petites aux plus grandes, continuent d'augmenter. La détection et la protection contre ces attaques sont cruciales.

Leader indépendant du secteur de l'identité, Okta est en première ligne face aux attaques. Voilà pourquoi nous avons lancé l'initiative « Okta Secure Identity Commitment » pour :

- Proposer des produits et services d'identité sécurisés de pointe
- Promouvoir les bonnes pratiques auprès des clients pour optimiser leur protection
- Encourager notre secteur à renforcer la protection contre les attaques ciblant l'identité
- Renforcer notre infrastructure d'entreprise

Dans le cadre de cette initiative, nous avons déjà lancé ou annoncé un certain nombre de fonctionnalités et mises à niveau importantes au sein de notre infrastructure d'entreprise et de notre gamme de produits. Un récapitulatif de ces mises à jour est proposé ci-après.

Nous sommes conscients qu'il s'agit d'un travail de longue haleine. Dès lors, nous sommes déterminés à nous donner les moyens nécessaires pour anticiper de manière proactive ou réagir rapidement à l'évolution du paysage des cybermenaces.

Introduction

Lorsque nous avons fondé Okta en 2009, nous nous sommes concentrés principalement sur la gestion IT, et plus particulièrement sur l'identité en tant qu'outil permettant de connecter les personnes et les technologies.

Depuis lors, deux grandes tendances ont radicalement changé la perspective sur l'identité et, par extension, la demande en solutions d'identité :

1. **L'identité constitue désormais le principal point d'entrée de sécurité en entreprise**, tant pour les applications axées collaborateurs que pour celles axées clients.
2. **Le volume et la complexité des cyberattaques ne cessent de s'intensifier**. Un large éventail de cybercriminels, dont les groupes spécialisés en ransomware, les acteurs étatiques et les acteurs malveillants internes, développent chaque jour des tactiques, techniques et procédures (TTP) avancées pour contourner les défenses et échapper à la détection.

Ces tendances ont marqué un tournant majeur pour le secteur, mais ont également contraint notre entreprise à se repositionner : axées au départ sur la connectivité entre personnes et technologies, nos solutions sont devenues un point d'entrée critique pour la protection des données essentielles des entreprises.

Cette responsabilité se reflète dans ***notre vision, qui est de permettre à tous d'utiliser n'importe quelle technologie en toute sécurité***.

Okta Secure Identity Commitment

La gestion des identités a évolué pour devenir une infrastructure de sécurité stratégique.

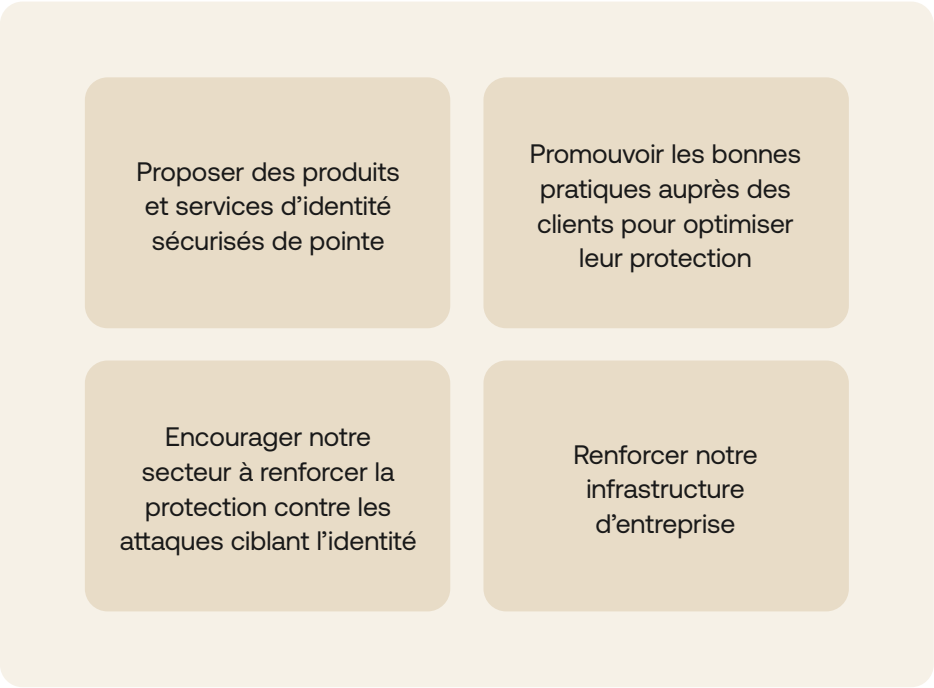
Leader indépendant du secteur de l'identité, Okta est en première ligne de la lutte contre les attaques ciblant l'identité. Nos équipes produits, ingénierie, sécurité et technologies métier apportent constamment des innovations à notre plateforme pour protéger efficacement nos quelque 18 000 clients. Par exemple :

- Okta ThreatInsight ***détecte et bloque plus de 2 milliards de demandes malveillantes*** en l'espace de 30 jours. (D'après un reporting interne effectué entre le 5 décembre 2023 et le 4 janvier 2024)
- Nous avons ***réduit les tentatives de credential stuffing et le trafic des bots malveillants de plus de 90 %*** pour quelques-uns de nos plus gros clients sur une période de 90 jours. (D'après le reporting interne de données anonymisées de clients professionnels entre le 5 octobre 2023 et le 4 janvier 2024)

- Nous contribuons aux bonnes pratiques du secteur : 100 % des collaborateurs d'Okta utilisent ***Okta FastPass avec Device Assurance et Adaptive MFA (AMFA) comme facteurs résistants au phishing***.
  (D'après le reporting interne d'Okta de février 2024)

Nous sommes déterminés à stimuler l'innovation au sein du secteur et à protéger nos clients et leurs ressources les plus sensibles. Voilà pourquoi nous avons lancé l'initiative « Okta Secure Identity Commitment ».

Cet engagement s'articule autour de 4 piliers, détaillés ci-dessous. Le reste du présent document explique comment nous prévoyons de tenir nos engagements.



Proposer des produits et services d'identité sécurisés de pointe

Nous sommes conscients que votre posture de sécurité dépend de nos offres, d'où notre volonté d'optimiser et de prioriser les fonctions de sécurité au sein de nos produits et services d'identité.

De cette manière, nous faisons en sorte que la confiance que nous témoignent les marques les plus réputées soit récompensée par les mesures de protection les plus robustes et innovantes.

Lors de l'événement Oktane 2023, nous avions annoncé une série de fonctionnalités visant à renforcer la sécurité des clients, dont un grand nombre intégrant Okta AI.

Depuis lors, nous nous sommes concentrés sur quelques thèmes clés pour encore améliorer nos produits et services, par exemple :

- Renforcement de l'accès admin aux consoles d'administration des clients
- Renforcement de la sécurité des sessions, des utilisateurs, des applications et des terminaux
- Promotion des bonnes pratiques auprès de notre clientèle

Disponibles depuis peu ou prévus pour la fin mai 2024

Workforce Identity Cloud

- Identity Threat Protection avec Okta AI
- Gouvernance des rôles administrateurs Okta
- MFA obligatoire pour accéder à la console d'administration Okta
- MFA obligatoire pour les actions protégées dans la console d'administration
- Possibilité pour les administrateurs de détecter et de bloquer les demandes émanant de services d'anonymisation
- Liaison IP/ASN avec la console d'administration
- Zone réseau autorisée pour les API
- Liaison de tokens pour les intégrations avec les services d'application M2M
- Prévention du verrouillage de comptes pour les utilisateurs Okta

Fonctionnalités prévues d'ici juillet 2024

Workforce Identity Cloud

- Gestion du niveau de sécurité des identités
- Ajout de nouveaux guides de bonnes pratiques intégrés aux produits
- MFA pour l'accès des applications d'administration propriétaires
- Déploiement d'agent sécurisé pour Active Directory

Customer Identity Cloud

- Amélioration de la fonction Bot Detection pour la récupération de mots de passe
- API de gestion des tokens d'actualisation
- Clés gérées par les clients
- Personnalisation des sessions avec la plateforme d'extensibilité

Fonctionnalités prévues d'ici octobre 2024

Workforce Identity Cloud

- Inscription de FastPass limitée aux terminaux gérés
- Authentification renforcée pour les flux de tenants sensibles
- Okta Privileged Access pour les comptes de service des applications SaaS

Customer Identity Cloud

- Contrôle des sessions simultanées

Customer Identity Cloud

- Fine Grained Authorization
- Fonction Bot Detection de 4e génération avec Okta AI
- Demande d'authentification
- MFA obligatoire pour tous les administrateurs de tableaux de bord
- Extension du mécanisme de déconnexion par voie de retour OIDC à l'aide de déclencheurs
- Liaison ASN pour les sessions d'administration Auth0
- Gestion de sessions et API de gestion des tokens d'actualisation
- Définition de l'inscription progressive à plusieurs facteurs pour les utilisateurs finaux
- Définition de délais d'expiration des sessions au niveau de l'organisation
- Contrôle des accès sécurisés au niveau des tenants

** Veuillez noter que tous les éléments de la roadmap sont sujets à modification. Nous tiendrons les clients informés de l'état des projets précédemment communiqués.*

Disponibles depuis peu

Nous avons récemment lancé plusieurs produits et fonctionnalités destinés à renforcer la sécurité client :

Workforce Identity Cloud

- **Identity Threat Protection avec Okta AI —** Renforcez la résilience des identités post-authentification en évaluant continuellement les risques liés à vos identités. Tirez parti des signaux intégrés des partenaires internes et tiers pour bloquer de façon proactive les menaces émergentes de toute origine post-authentification.
- **Gouvernance des rôles administrateurs Okta —** Éliminez les privilèges permanents pour les rôles administrateurs Okta avec des demandes d'accès ponctuelles, limitées dans le temps pour l'accès individuel et la vérification des accès pour les administrateurs existants.

- **MFA obligatoire pour accéder à la console d'administration d'Okta —** Empêchez les administrateurs de créer des politiques d'authentification qui n'exigent qu'un seul facteur. Activez d'autres options d'authentification pour éviter l'accès basé sur un seul facteur à la console
- **MFA obligatoire pour les actions protégées dans la console d'administration —** Permet de renforcer le niveau de protection pour les actions critiques dans Okta en exigeant une authentification renforcée des administrateurs qui souhaitent effectuer des actions à fort impact.
- **Possibilité pour les administrateurs de détecter et de bloquer les demandes émanant de services d'anonymisation —** Offre aux administrateurs la possibilité d'autoriser ou de refuser l'accès après évaluation de l'association potentielle d'une adresse IP source à un anonymiseur, dans le but de renforcer le contrôle d'une organisation contre l'accès non autorisé via ce type de sources.
- **Liaison IP/ASN avec la console d'administration —** Pour éviter la prise de contrôle des sessions de ressources (first-party) critiques, Okta révoque automatiquement une session de console d'administration si le numéro ASN (Autonomous System Number) observé pendant une demande web ou d'API diffère du numéro enregistré lors de l'ouverture de la session. En outre, les administrateurs sont en mesure de révoquer automatiquement une session d'administration si l'adresse IP détectée lors de la création de la session change pendant une session active dans les produits Okta suivants : Workflows Admin, Okta Access Requests (Inbox), Okta Privileged Access (OPA), console d'administration Okta.
- **Zone réseau autorisée pour les API —** Empêche les cybercriminels et les malwares de voler des tokens SSWS et de les relire en dehors de la plage d'adresses IP spécifiée pour obtenir un accès non autorisé.
- **Liaison de tokens pour les intégrations avec les services d'application M2M —** Okta a amélioré la sécurité des transactions automatisées en appliquant par défaut la liaison des tokens dans les intégrations M2M à l'aide d'une preuve de possession. De cette façon, seules les applications authentifiées pourront utiliser des tokens pour accéder aux API Okta.
- **Prévention du verrouillage de comptes pour les utilisateurs Okta —** Okta propose une fonctionnalité pour bloquer les tentatives de connexion suspectes à partir de terminaux inconnus. Lorsque la fonctionnalité est activée, elle empêche le verrouillage des comptes des utilisateurs légitimes (y compris des administrateurs) si un autre terminal non connu d'Okta déclenche un verrouillage.

Customer Identity Cloud

- **Fine Grained Authorization —** Offrez aux développeurs la possibilité de définir une logique d'autorisation avec davantage d'options d'évolutivité, de disponibilité et d'audit que les méthodes de contrôle des accès traditionnelles. Disponible pour Workforce Identity Cloud et Customer Identity Cloud.
- **Fonction Bot Detection de 4e génération avec Okta AI —** La nouvelle version de Bot Detection, qui intègre des signaux de risques liés aux tiers et un modèle ML (machine learning) mis à jour, inclura des modèles optimisés, spécialement conçus pour bloquer les inscriptions frauduleuses.
- **Demande d'authentification —** Bloquez l'activité des bots avec une demande d'authentification qui utilise les signaux des terminaux et des navigateurs pour compliquer la tâche des bots par rapport aux CAPTCHA traditionnels.
- **MFA obligatoire pour tous les administrateurs de tableaux de bord —** Auparavant, le MFA restait facultatif pour les administrateurs Auth0. À présent, il est obligatoire pour tous les administrateurs qui utilisent une connexion basée sur un nom d'utilisateur/mot de passe ou une authentification sociale tierce.
- **Extension du mécanisme de déconnexion par voie de retour OIDC à l'aide de déclencheurs —** Permet d'ajouter des événements de type « compte supprimé » et « adresse e-mail modifiée » à la liste existante de déclencheurs de déconnexion (mot de passe modifié, session expirée et autres événements de déconnexion) ; ces déclencheurs se lient à des événements de clôture de session pour demander aux applications de déconnecter les utilisateurs chaque fois qu'une session est invalidée.
- **Liaison ASN pour les sessions d'administration Auth0 —** Okta révoquera automatiquement une session de console d'administration si le numéro ASN (Autonomous System Number) observé pendant une demande web ou d'API diffère du numéro enregistré lors de l'ouverture de la session.
- **Gestion de sessions et API de gestion des tokens d'actualisation —** Offre un accès centralisé à la liste, à la gestion et à la révocation des autorisations utilisateurs dans les applications. Lorsqu'une entreprise soupçonne un détournement de session, la session peut être révoquée de manière préventive pour protéger les clients et l'organisation.
- **Définition de l'inscription progressive à plusieurs facteurs pour les utilisateurs finaux —** À l'aide d'une action post-connexion, l'entreprise peut définir les facteurs secondaires que les utilisateurs finaux doivent adopter dans la configuration MFA. Les clients peuvent ainsi renforcer leur contrôle sur les politiques d'authentification, qui seront ainsi alignées sur leurs objectifs de sécurité.

Fonctionnalités prévues d'ici juillet 2024

Workforce Identity Cloud

- **Gestion du niveau de sécurité des identités —** Réduisez proactivement votre surface d'attaque liée à l'identité en identifiant et en priorisant les risques tels que les autorisations excessives, les erreurs de configuration, et les failles MFA dans l'infrastructure d'identités, le cloud et les applications SaaS de votre entreprise.
- **Ajout de nouveaux guides de bonnes pratiques intégrés aux produits —** Okta fournira des guides supplémentaires intégrés aux produits pour aider les clients à adhérer aux bonnes pratiques afin de protéger leurs tenants Okta.
- **MFA pour l'accès des applications d'administration propriétaires —** La politique de la console d'administration sera appliquée aux applications d'administration propriétaires pour les certifications des accès Okta, la gestion des droits Okta et l'administration des demandes d'accès Okta. L'accès à ces applications exigera le MFA.
- **Déploiement d'agent sécurisé pour Active Directory —** L'agent AD sera mis à niveau pour tirer parti de l'approche basée sur la preuve de possession OIDC dans les communications avec Okta et ainsi empêcher les parties non autorisées d'accéder aux informations sensibles.

Customer Identity Cloud

- **Amélioration de la fonction Bot Detection pour la récupération de mots de passe —** Offre aux clients la possibilité d'activer la fonction Bot Detection pour les flux de récupération des mots de passe (en plus des flux d'inscription et de connexion, ce qui existe déjà) afin de renforcer la protection contre les tentatives d'usurpation de compte.
- **API de gestion des tokens d'actualisation —** Offre aux développeurs un contrôle à distance du statut d'authentification de leurs utilisateurs grâce à des API de gestion endpoint supplémentaires.
- **Clés gérées par les clients —** Offre aux clients la possibilité de remplacer et de gérer en toute sécurité les clés de chiffrement de premier niveau de leurs tenants, y compris les clés BYOK (Bring Your Own Keys) et CYOK (Control Your Own Keys).
- **Personnalisation des sessions avec la plateforme d'extensibilité —** Définissez des comportements personnalisés basés sur les signaux de risque pour révoquer les sessions suspectes et créez des politiques pour détecter et répondre au piratage en tirant parti de l'API de gestion des sessions avec notre plateforme Actions & Extensibility.

- **Définition de délais d'expiration des sessions au niveau de l'organisation —** Personnalisez l'expiration de sessions à l'aide d'une logique supplémentaire, y compris pour l'organisation.
- **Contrôle des accès sécurisés au niveau des tenants —** Offrez aux clients la possibilité de bloquer du trafic provenant d'adresses IP, de blocs CIDR (Classless Inter-Domain Routing) et de zones géographiques spécifiques pour contrer plus facilement les attaques DDoS en bloquant les demandes en périphérie.

Fonctionnalités prévues d'ici octobre 2024

Workforce Identity Cloud

- **Inscription de FastPass limitée aux terminaux gérés —** Okta offrira aux administrateurs un contrôle accru en leur permettant de configurer des politiques exigeant que les utilisateurs satisfassent une condition préalable avant de les autoriser à inscrire des authentificateurs. Au cours de la première phase, les utilisateurs ne pourront s'inscrire dans Okta Verify FastPass que s'ils possèdent un terminal géré.
- **Authentification renforcée pour les flux de tenants sensibles —** Bénéficiez d'un niveau de protection et de contrôle supplémentaire pour les processus d'authentification utilisateur.
- **Okta Privileged Access pour les comptes de service des applications SaaS —** Accélérez les comptes de service des solutions SaaS et des hyperscalers en tant que ressources protégées dans Okta Privileged Access. Les clients bénéficient de fonctionnalités natives pour gagner en visibilité et gérer le cycle de vie des comptes de service, par exemple la découverte, la gestion, la gouvernance et l'attribution des accès.

Customer Identity Cloud

- **Contrôle des sessions simultanées —** La fonctionnalité de contrôle des sessions simultanées offre à vos tenants la possibilité de contrôler le nombre de terminaux actifs pour les utilisateurs. Que vous l'utilisiez comme signal de risque ou comme plafond pour les identifiants partagés, le contrôle des sessions simultanées vous permet de refuser les nouvelles connexions au-delà des limites définies par votre entreprise.

Promouvoir les bonnes pratiques auprès des clients pour optimiser leur protection

Si elle est mal configurée, l'identité devient un point d'entrée supplémentaire pour les acteurs malveillants ou les collaborateurs internes malintentionnés. Forts d'une expérience de 15 ans et d'une large clientèle de plus de 18 000 entreprises, nous possédons une expertise unique et les compétences spécialisées nécessaires pour aider nos clients à optimiser la configuration de leurs identités.

Pour que nos clients profitent de notre longue expérience, nous renforçons encore nos politiques clients.

Par ailleurs, nous mettons tout en œuvre pour que nos produits soient déployés selon les bonnes pratiques de sécurité d'Okta afin de renforcer directement les défenses des clients contre les brèches liées à l'identité.

Nous nous efforçons de fournir à nos clients et au secteur dans son ensemble des guides de bonnes pratiques et d'autres ressources de formation afin qu'ils puissent rester en phase avec le paysage des menaces :

- **Actions Template Implementation Guides —** Ces guides facilitent l'implémentation des bonnes pratiques en offrant aux clients Customer Identity Cloud un modèle de configuration sécurisé pour commencer leur implémentation.
- **Protecting Administrative Sessions in Okta —** Découvrez les configurations recommandées dans Okta pour protéger les sessions d'administration et l'accès à privilèges, réduire la surface d'attaque, prévenir l'usurpation de compte et limiter l'impact des sessions piratées.
- **Customer Identity Cloud Enhancements to Prevent Account Takeover —** Cet article de blog explique l'importance des nouvelles fonctionnalités pour renforcer la protection contre l'usurpation de compte.
- **Okta Device Access now supports passwordless login and FIDO2 Yubikeys for Desktop MFA —** (WIC) — Après s'être exprimé publiquement en faveur du passwordless pour préparer un futur plus serein et plus sûr, Okta tient ses promesses en l'intégrant dans ses fonctionnalités.
- **Liaison IP ou ASN avec la console d'administration —** (WIC, fonction activée par défaut) — La sécurité par défaut est une bonne pratique du secteur. Nous avons donc choisi de faire de la protection par liaison de l'adresse IP une fonctionnalité par défaut, pour mieux protéger nos clients. En d'autres termes, si un administrateur apparaît subitement dans le système avec une adresse IP différente de celle avec laquelle il s'est connecté au départ, il est automatiquement déconnecté et invité à se reconnecter.

Encourager notre secteur à renforcer la protection contre les attaques ciblant l'identité

Montrer la voie en matière de sécurité de l'identité est un impératif d'Okta. Nous nous sommes fixé pour mission de participer activement à la détection et à la neutralisation des attaques ciblant l'identité dans le cadre de notre secteur. Pour ce faire, nous accélérons le développement de nos capacités et adoptons de nouvelles technologies, telles que l'intelligence artificielle.

Nous jouons également un rôle proactif dans l'élaboration d'une approche sectorielle en matière de sécurité de l'identité. Nous répondons à la complexité croissante et à l'explosion des cybermenaces par des stratégies de prévention, détection et protection de pointe et par des critères de qualité qui sont une référence dans le secteur :

- **How to Secure the SaaS Apps of the Future —** Découvrez les exigences essentielles pour sécuriser les applications SaaS modernes contre les attaques post-authentification et renforcer les normes de cybersécurité dans le secteur des technologies en préconisant l'adoption de fonctionnalités de sécurité avancées telles que la preuve de possession, l'évaluation continue des accès et la déconnexion universelle.
- **Leveraging the Okta Identity Security Commitment to Enable Zero Trust —** Découvrez comment les fonctionnalités de sécurité d'Okta facilitent l'implémentation de stratégies Zero Trust optimisées par l'identité en plaçant chacune d'elles dans le contexte d'un principe Zero Trust du NIST Cybersecurity Framework.
- **Bourses d'études pour résoudre la pénurie de compétences dans le secteur des technologies —** Les bourses d'études d'Okta Learning soutiennent le personnel technique sans emploi, y compris les vétérans et les conjoint(e)s de militaires. Elles leur donnent accès au catalogue de formations à la demande d'Okta, à un examen blanc, à un bon de certification Okta et bien plus encore.
- **Okta for Good a alloué 3,1 millions de dollars** dans le cadre de son engagement philanthropique de 50 millions de dollars, y compris deux enveloppes d'un million de dollars sur cinq ans à des partenaires de longue date et à des leaders reconnus pour leur action en faveur de la transformation digitale des ONG.
- **CISA Secure by Design Pledge —** La signature du « CISA Secure by Design Pledge » par Okta, et d'autres sociétés dans le monde, témoigne de l'engagement de notre secteur en faveur de l'adoption sans délai d'une sécurité intégrée dès la conception.

Renforcer l'infrastructure d'entreprise d'Okta

Tous nos collaborateurs, processus et technologies internes doivent respecter les mêmes standards de sécurité que nos produits orientés client, en mettant l'accent sur une approche globale, capitalisant sur nos atouts en matière de sécurité.

Par ailleurs, nous intensifions nos investissements pour renforcer nos systèmes d'entreprise et auxiliaires (attachés à l'environnement de production).

Disponibles depuis peu ou prévus pour la fin mai 2024	Mises à jour prévues d'ici juillet 2024	Mises à jour prévues d'ici octobre 2024
• Extension de la résistance au phishing aux nouveaux collaborateurs • Évaluation de la sécurité interne • Reporting centralisé et normalisé pour la gestion des risques de sécurité • Évaluation de la sécurité des applications SaaS **Fonctionnalités de détection et réponse améliorées, telles que :** • Nouvel outil de gestion de dossiers d'incidents de sécurité • Nouvelle plateforme de threat intelligence • Fonctionnalités supplémentaires de surveillance du Dark Web	• Extension de la résistance au phishing à tous les collaborateurs existants • Protection renforcée des ordinateurs portables • Automatisation de la découverte et du reporting des comptes de service M2M dans les applications SaaS • Protection renforcée des terminaux mobiles	• Fonctionnalités centralisées et uniformisées pour la gestion des vulnérabilités, des ressources et de la posture de sécurité cloud (CSPM) • Outils d'ingestion et d'analyse des journaux améliorés • Analyse améliorée des logiciels open source

** Veuillez noter que tous les éléments de la roadmap sont sujets à modification. Nous tiendrons les clients informés de l'état des projets précédemment communiqués.*

Disponibles depuis peu :

L'infrastructure d'entreprise d'Okta a fait l'objet d'une série de modifications, mises à niveau et améliorations, dont les suivantes :

- **Extension de la résistance au phishing aux nouveaux collaborateurs —** Cela fait longtemps que nous avons déployé Okta FastPass pour offrir un MFA avec résistance au phishing. Cette résistance au phishing a été récemment étendue, via Yubikeys, à tous les nouveaux collaborateurs pour qui l'ensemble du cycle de vie est désormais 100 % passwordless.
- **Évaluation de la sécurité interne —** En partenariat avec un grand cabinet de conseil international, nous avons réalisé une évaluation de sécurité complète de nos produits, infrastructure et systèmes d'entreprise, y compris nos systèmes internes de marketing, de gestion financière, d'administration des ventes, de data warehouse, d'intégration et IaaS.
- **Reporting centralisé et normalisé pour la gestion des risques de sécurité —** Nous avons déployé la solution d'un seul fournisseur pour centraliser la gestion des risques et des problèmes liés à notre programme de gouvernance, de gestion des risques et de la conformité, y compris la gestion des risques liés aux tiers.
- **Évaluation de la sécurité des applications SaaS —** En partenariat avec des experts en sécurité tiers, nous avons réalisé des évaluations de sécurité de nos applications SaaS critiques, dont l'Okta Help Center, ainsi que nos systèmes de gestion financière, de gestion de la relation client (CRM), de gestion du capital humain (HCM), d'administration des ventes, de data warehouse, de marketing, d'intégration et IaaS (Infrastructure-as-a-Service).

Fonctionnalités de détection et réponse améliorées, telles que :

- **Nouvel outil de gestion de dossiers d'incidents de sécurité —** Notre nouvel outil est caractérisé par un temps de réponse, une automatisation et une précision améliorés.
- **Nouvelle plateforme de threat intelligence —** Notre nouvelle plateforme permettra d'automatiser et de corréler la threat intelligence afin d'améliorer nos fonctionnalités de détection et réponse aux menaces.
- **Fonctionnalités supplémentaires de surveillance du Dark Web —** Désormais, nous identifions de façon proactive les menaces potentielles en analysant régulièrement le Dark Web pour trouver du contenu lié à Okta.

Mises à jour prévues d'ici juillet 2024 :

- **Extension de la résistance au phishing à tous les collaborateurs existants —** Nous étendrons la résistance au phishing à tous les collaborateurs existants via Yubikeys.
- **Protection renforcée des ordinateurs portables —** L'utilisation des ordinateurs portables Okta sera soumise à des restrictions supplémentaires, en continuant d'appliquer le principe du moindre privilège et une forte granularité dans la définition des rôles.
- **Automatisation de la découverte et du reporting des comptes de service M2M dans les applications SaaS —** Nous allons implémenter un outil destiné à offrir une visibilité complète sur les comptes de service locaux créés dans les applications SaaS, afin d'améliorer la gestion et le renouvellement des secrets utilisés dans le cadre de l'authentification.
- **Protection renforcée des terminaux mobiles —** Nous serons inflexibles quant à la sécurité des terminaux mobiles. Même si le produit Okta Verify offre déjà un excellent niveau de protection (code PIN obligatoire, chiffrement et contrôle des versions du système d'exploitation), nous comptons améliorer notre posture de sécurité globale des terminaux mobiles au moyen de nouvelles restrictions concernant l'accès à privilèges.

Mises à jour prévues d'ici octobre 2024 :

- **Reporting centralisé et normalisé pour la gestion des vulnérabilités, des ressources et de la posture de sécurité cloud (CSPM) —** Nous prévoyons de déployer la solution d'un fournisseur unique pour centraliser toutes les informations liées aux vulnérabilités dans nos environnements de production et d'entreprise.
- **Outils d'ingestion et d'analyse des journaux améliorés —** Nos fonctions de journalisation vont être optimisées pour améliorer la pertinence des alertes. Cela nous permettra d'analyser un incident dans tout l'environnement de logs dans les meilleurs délais.
- **Analyse améliorée de logiciels open source —** Pour améliorer les bonnes pratiques de sécurité, toutes les bibliothèques de sécurité seront analysées afin d'identifier toute attaque contre la chaîne logistique.

Conclusion

Okta est déterminé à jouer un rôle de premier plan dans la lutte contre les attaques prenant l'identité pour cible. C'est la raison pour laquelle nous avons lancé l'initiative « Okta Secure Identity Commitment », articulée au autour de 4 piliers :

- Proposer des produits et services d'identité sécurisés de pointe
- Promouvoir les bonnes pratiques auprès des clients pour optimiser leur protection
- Encourager notre secteur à renforcer la protection contre les attaques ciblant l'identité
- Renforcer notre infrastructure d'entreprise

Il s'agit d'un engagement à long terme et nous continuerons d'évoluer en parallèle avec le paysage technologique et des menaces.