CrowdStrike, Okta & Zscaler : sécurité unifiée, protection intégrale et la cyber-résilience à l'ère de l'IA

Défis

Les adversaires évoluent plus vite que jamais : le temps moyen d'une intrusion observée a atteint son plus bas niveau historique de 48 minutes en 2024, l'intrusion la plus rapide ayant été réalisée en seulement 51 secondes[1]. Parallèlement, 79 % des attaques n'utilisaient aucun malware, mais exploitaient l'usurpation d'identité, l'ingénierie sociale et des erreurs de configuration du cloud pour éviter de se faire détecter[1]. Les stratégies de sécurité traditionnelles, celles qui se contentent d'être réactives, ne peuvent contrer les tactiques en évolution des adversaires modernes. Ces derniers utilisent des méthodes de plus en plus sophistiquées, notamment une automatisation basée sur l'IA et des tactiques furtives, pour s'infiltrer et se déplacer furtivement au sein des environnements. Pour surmonter ces risques, les entreprises doivent s'affranchir de leur traditionnel panel fragmenté d'outils de sécurité cloisonnés, une approche qui accentue la complexité, retarde la prise en charge des incidents et, à terme, affaiblit la sécurité globale.

Vos besoins

Il est temps de réinventer notre approche de la sécurité et d'utiliser la puissance de l'IA pour gagner en rapidité et en évolutivité. Les entreprises ont besoin de plateformes de sécurité sophistiquées qui collaborent de manière homogène pour déployer une protection en profondeur, simple et qui offre de réels gains de productivité.

Solution

Pour faire face à l'évolution des menaces optimisées par l'IA, CrowdStrike, Okta et Zscaler proposent une solution de sécurité transversale et entièrement intégrée. Celle-ci protège efficacement contre les menaces en améliorant la visibilité, en éliminant les zones d'ombre et en accélérant les délais de réponse. Cette approche combinée sécurise et authentifie les identités, permet un contrôle d'accès Zero Trust dynamique et contextuel, protège les terminaux disséminés et tire parti d'un SIEM de nouvelle génération pour détecter et répondre aux menaces en temps réel.

En corrélant les indicateurs de risque provenant de différentes couches (identités, terminaux, le cloud, réseau, etc.), les équipes de sécurité disposent d'une visibilité unifiée sur les mouvements des adversaires, pour ainsi détecter, contenir et neutraliser les menaces avant qu'elles ne causent des dommages. Grâce à une automatisation pilotée par l'IA, au partage bidirectionnel de renseignements de veille sur les menaces et à des actions coordonnées de réponse, la solution conjointe ne se contente pas de détecter les menaces : elle les neutralise avant tout impact majeur.

Les équipes de sécurité peuvent anticiper les tactiques des adversaires, automatiser les actions de lutte contre les menaces et agir au plus vite pour empêcher que les adversaires ne parviennent à leurs fins.

À mesure que les cybermenaces gagnent en rapidité et en sophistication, les entreprises doivent privilégier une défense proactive et optimisée par IA, pour tenir le rythme des adversaires et neutraliser les menaces en amont de leur cible.

Sécurité consolidée : une protection unifiée pour une ère nouvelle

Pour les entreprises qui initient une démarche Zero Trust ou qui élaborent une solution Zero Trust en tirant parti des investissements déjà réalisés, les partenariats solides et la solution intégrée de

1. Rapport sur les menaces mondiales CrowdStrike 2025, https://www.crowdstrike.com/en-us/global-threat-report/

leaders tels que Zscaler, CrowdStrike et Okta jettent les bases d'une solution solution Zero -Trust qui se déploie pour protéger les utilisateurs, les terminaux et les applications.

Cette solution commune offre aux administrateurs une visibilité en temps réel sur le paysage des menaces et sur la posture de sécurité des terminaux et des applications. L'accès aux applications critiques est modulé en fonction de l'utilisateur, du terminal et des politiques d'accès. En cas d'attaque, un processus de réponse est déclenché rapidement sur toutes les cibles. Les défenses sont renforcées par des politiques de prévention qui préviennent le rejeu d'une attaque déjà vécue.

Il en résulte une solution Zero Trust optimale, cloud-native, qui opère de manière dynamique et qui intègre des éléments de contexte. Cette solution aide les équipes de sécurité à garder une longueur d'avance sur des menaces modernes optimisées par l'IA, et à maîtriser les risques. Son déploiement simplifié élimine ainsi la complexité trop souvent associée aux outils conçus et intégrés en interne.

L'essentiel sur la solution

Accès adaptatif Zero Trust :

Zscaler applique un accès sur la base du moindre privilège et en fonction de l'identité de l'utilisateur, de la posture du dispositif et du contexte de risque. Zscaler Zero Trust Exchange (ZTE) intègre une protection contre les menaces ciblant les identités avec Okta AI ITP (Identity Threat Protection) et les scores de CrowdStrike Falcon® ZTA, pour déployer des politiques d'accès en temps réel et basées sur les risques.

Gestion automatisée du cycle de vie des identités :

Okta simplifie l'activation et la suppression des comptes et des utilisateurs via le protocole SCIM d'Okta, ce qui permet des mises à jour en temps réel et en fonction des rôles, ainsi qu'une charge de travail moindre.

Détection des menaces liées aux identités et aux terminaux :

CrowdStrike détecte et déjoue les menaces ciblant les utilisateurs et les terminaux en intégrant les alertes émises par Zscaler Deception avec Okta ITP, ce qui permet de traiter chaque menace de manière adaptée. D'autre part, les indicateurs fournis par CrowdStrike constituent des éléments de contexte pertinents qui affinent la détection des menaces.

Authentification en continu et accès basé sur les risques :

Zscaler applique des politiques d'accès dynamiques avec Okta, ce qui déclenche une authentification par paliers, en fonction des comportements anormaux détectés par Zscaler ou CrowdStrike.

Visibilité unifiée sur les risques :

Zscaler Risk360 et le framework Data Fabric importent les logs d'identité depuis Okta et les signaux issus de terminaux depuis CrowdStrike.

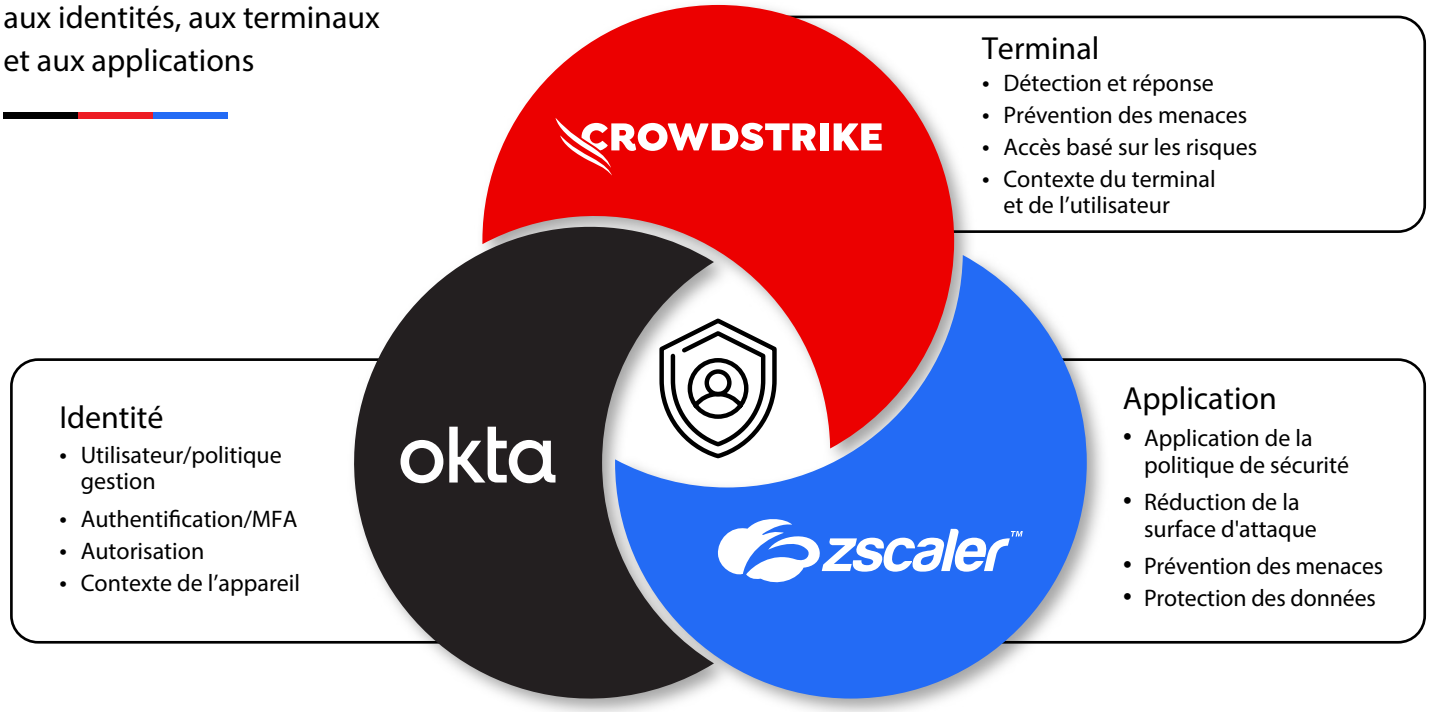
Partage d'informations de veille sur les menaces entre plateformes :

Zscaler partage des données télémétriques pour accélérer la détection et la réponse aux menaces, tandis que CrowdStrike améliore les listes de blocage personnalisées de Zscaler pour concrétiser le principe d'une protection proactive.

Détection et réponse unifiées aux menaces sur l'ensemble des domaines :

CrowdStrike offre une visibilité complète et des réponses coordonnées et automatisées aux menaces, sur un périmètre large couvrant les terminaux, les identités et les applications. Ceci est possible grâce à des intégrations de CrowdStrike Falcon® Next-Gen SIEM et de CrowdStrike Falcon® Fusion
SOAR avec Okta et Zscaler, pour accélérer la neutralisation des menaces et prévenir les déplacements latéraux.

Évaluations des risques liés aux identités, aux terminaux et aux applications



Partage d'indicateurs et d'informations de veille sur les menaces

Une synergie au service de la cyber-résilience

1. Accès Zero Trust renforcé :
l'accès Zero Trust prévient le déplacement latéral des menaces grâce à des politiques d'accès basées sur l'identité de l'utilisateur, la posture de l'appareil et le contexte temps réel des menaces.

2. Détection et correction automatisées des menaces :
la détection en temps réel et la veille sur les menaces déclenchent des réponses immédiates et coordonnées, avec application des politiques et déconnexion universelle lorsque nécessaire.

3. Visibilité unifiée sur les risques :
Zscaler Risk360 s'intègre avec les logs de CrowdStrike et d'Okta pour fournir des indicateurs contextualisés et des données complètes sur les risques, pour ainsi accélérer les investigations et la remédiation.

4. Enquête et réponse rapides :
L'enquête et la réponse accélérées grâce à l'intégration avec Crowd-Strike Falcon Next-Gen SIEM fournit une visibilité unifiée, une détection optimisée par l'IA et des workflows automatisés pour contenir rapidement les menaces inter-domaines.

5. Gestion efficace des identités :
Le provisionnement basé sur SCIM d'Okta garantit un provisionnement et un déprovisionnement sécurisés et automatisés des utilisateurs, ne permettant que les accès autorisés.

6. Amélioration de l'expérience utilisateur :
L'accès transparent assuré par Okta SSO, MFA et les politiques adaptatives de Zscaler améliore la productivité sans compromettre la sécurité.

Conclusion

CrowdStrike, Okta et Zscaler proposent des solutions de sécurité intégrées qui protègent et simplifient les écosystèmes numériques et contribue à leur évolutivité.

Ensemble, ces trois solutions instituent une approche Zero Trust d'entreprise qui permet des accès basés sur l'identité et renforce la détection des menaces sur tous les domaines. Cette alliance solide entre trois acteurs clés de la cybersécurité améliore de manière proactive la posture de cybersécurité et la résilience à l'ère de l'IA.

À propos de CrowdStrike

CrowdStrike (NASDAQ: CRWD), un leader mondial de la cybersécurité, redéfinit la sécurité moderne avec sa plateforme cloud native et sophistiquée qui protège les instances, les endpoints, le cloud, les identités et les données d'entreprise. Présente dans le cloud et faisant appel à un agent léger, la plateforme Falcon offre un déploiement rapide et évolutif, une protection et des performances de premier rang, un opérationnel simplifié et un time-to-value quasi-immédiat.

À propos d'Okta

Okta, Inc. est un spécialiste mondial de gestion des identités et des accès. Elle sécurise les identités et permet à chacun d'être libre d'utiliser la technologie de son choix de manière sécurisée. Ses solutions permettent aux entreprises et aux développeurs de capitaliser sur une gestion robuste des identités pour favoriser la sécurité et la productivité, tout en protégeant les collaborateurs, l'entreprise et les partenaires. Rendez-vous sur okta.com et découvrez pourquoi les plus grandes enseignes mondiales font confiance à Okta en matière d'authentification, d'autorisation et bien plus.

À propos de Zscaler

Zscaler (NASDAQ: ZS) accélère la transformation digitale de ses clients pour qu'ils gagnent en agilité, productivité, résilience et sécurité. La plateforme Zscaler Zero Trust Exchange™ protège des milliers de clients contre les cyberattaques et les pertes de données en connectant de manière sécurisée les utilisateurs, les dispositifs et les applications, quelle que soit leur localisation. Adossée à plus de 160 data centers dans le monde, Zero Trust Exchange™, basée sur le modèle SASE, constitue la plus vaste plateforme de sécurité cloud in-line au monde.

En savoir plus sur nos solutions à l'adresse okta.com , crowdstrike.com et zscaler.fr |