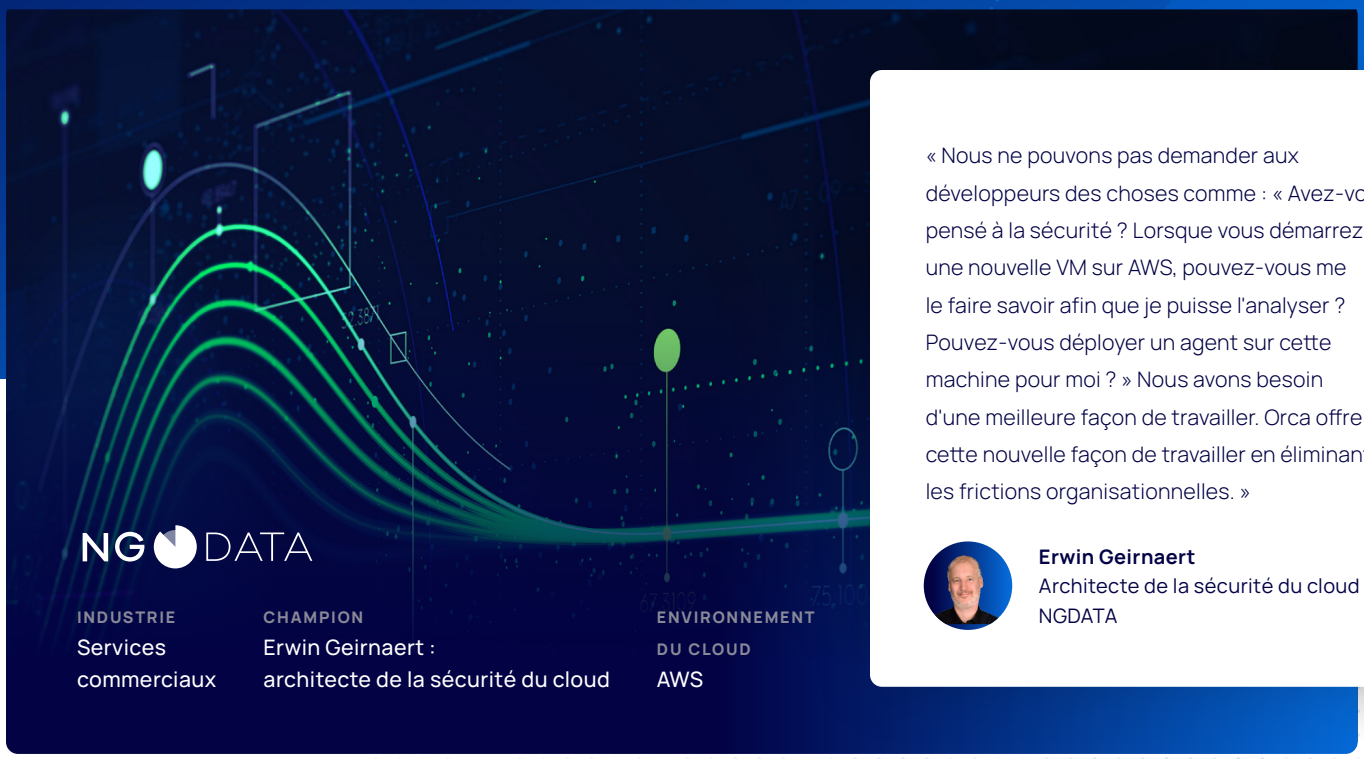
Orca Security fournit à NGDATA un outil unique pour la sécurité, le DevOps et la conformité



NGDATA

INDUSTRIE
Services commerciaux

CHAMPION
Erwin Geirnaert : architecte de la sécurité du cloud

ENVIRONNEMENT DU CLOUD
AWS

« Nous ne pouvons pas demander aux développeurs des choses comme : « Avez-vous pensé à la sécurité ? Lorsque vous démarrez une nouvelle VM sur AWS, pouvez-vous me le faire savoir afin que je puisse l'analyser ? Pouvez-vous déployer un agent sur cette machine pour moi ? » Nous avons besoin d'une meilleure façon de travailler. Orca offre cette nouvelle façon de travailler en éliminant les frictions organisationnelles. »

Erwin Geirnaert
Architecte de la sécurité du cloud
NGDATA

Défis de la sécurité du cloud

- Besoin d'une vue globale en temps réel des actifs AWS pour un patrimoine en constante évolution, de préférence sans utiliser d'agents ;
- Garantie de la protection des actifs des clients et de la propriété intellectuelle de l'entreprise ;
- Besoin d'outils qui s'intègrent au mode de travail des développeurs.

Résultats de la sécurité du cloud

- Obtention d'une vue complète de tous les actifs NGDATA en temps réel ;
- Intégration à Jira pour automatiser le processus de correction des vulnérabilités ;
- Suppression des frictions organisationnelles avec les développeurs pour passer à l'approche DevSecOps.

NGDATA aide les entreprises à générer des expériences client plus personnelles grâce à des informations sur les données

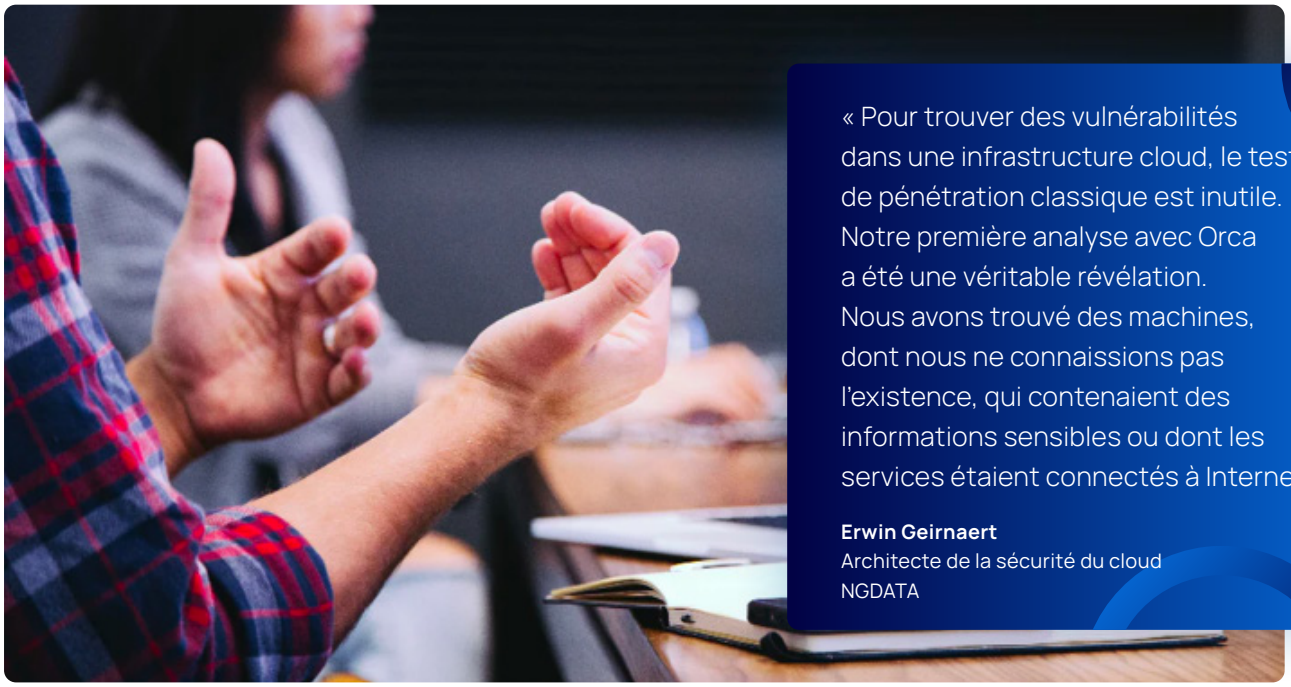
NGDATA aide les marques des secteurs axés sur les données, tels que les services financiers, les télécommunications, les services publics et l'hôtellerie, à créer des expériences client connectées. Leurs services de CDP et de transformation numérique basés sur l'IA placent les personnes au centre de chaque entreprise via l'ADN du client, qui apprend en permanence du comportement pour offrir des expériences convaincantes aux marques du monde entier. NGDATA a son siège à Gand, en Belgique, et possède des bureaux aux États-Unis, en Europe et en Asie-Pacifique.

La plate-forme logicielle peut être installée sur site ou déployée dans un cloud privé, tandis que tout le travail de développement de produits est effectué dans le cloud. NGDATA a engagé l'architecte de la sécurité du cloud, Erwin Geirnaert de Shift Left Security, pour mettre de l'ordre dans ses environnements cloud, identifier et éliminer systématiquement les vulnérabilités et mettre en œuvre des procédures pour maintenir une bonne posture de sécurité

Orca Security réussit là où les analyses de sécurité classiques échouent

La première tâche de Geirnaert était un test d'intrusion classique pour identifier le plus rapidement possible l'état de l'environnement actuel. L'analyse n'a été que moyennement utile, car il ne s'agissait que d'un instantané dans le temps d'un patrimoine cloud en constante évolution. Mais même avec un scanneur authentifié, s'il ne sait pas quoi analyser, il y a un écart. « Cela ne fonctionne tout simplement pas dans une approche native du cloud », déclare Geirnaert.

Il a ensuite tenté d'obtenir des informations sur les plages d'adresses IP à analyser à partir des journaux Amazon qu'il avait extraits dans un tableau de bord Sumo Logic. Cela a donné des résultats troublants.



« Pour trouver des vulnérabilités dans une infrastructure cloud, le test de pénétration classique est inutile. Notre première analyse avec Orca a été une véritable révélation. Nous avons trouvé des machines, dont nous ne connaissions pas l'existence, qui contenaient des informations sensibles ou dont les services étaient connectés à Internet. »

Erwin Geirnaert
Architecte de la sécurité du cloud
NGDATA

Geirnaert explique comment Orca permet la dynamique DevSecOps. « Un développeur a accès à la console AWS, il peut donc simplement attacher Orca à l'aide d'une stratégie en lecture seule. Il n'a pas besoin de déployer, d'appliquer ou d'installer quoi que ce soit : il configure simplement AWS et fait confiance à la plate-forme Orca pour effectuer l'analyse. Il faut environ cinq minutes pour joindre une stratégie en lecture seule et la faire fonctionner. Et il voit immédiatement les résultats de l'analyse approfondie effectuée par Orca. »

« Avec une vue complète de la conformité, le développeur peut demander : « Ai-je manqué certains paramètres de sécurité dans Amazon qui pourraient avoir un impact sur ma posture de sécurité ? » Il peut immédiatement voir qu'il doit configurer ceci, activer cela, utiliser ceci ou faire cela. Orca met également à jour la conformité. Même sans trouver une vulnérabilité, cela seul nous donne tellement d'informations que nous n'avons pas besoin d'une entreprise de sécurité pour nous dire quoi faire. Orca nous dira ce que nous devons faire et comment le faire », explique Geirnaert.

> « Orca nous permet de donner à différents utilisateurs un accès pour différents rôles. Le RSSI s'intéresse à la conformité. L'ingénieur de sécurité examine les vulnérabilités et les alertes. Le développeur peut découvrir à partir du tableau de bord pourquoi quelque chose pose problème. »
>
> **Erwin Geirnaert**
> Architecte de la sécurité du cloud
> NGDATA

Cela a conduit à rechercher un outil qui pourrait se connecter à l'API AWS et obtenir une vue en temps réel de tous les actifs de NGDATA. Un tel outil devrait révéler les vulnérabilités critiques et déterminer si des informations personnelles ou une propriété intellectuelle étaient en danger. Dans cette quête, Geirnaert a trouvé Orca Security.

« Notre première analyse avec Orca a été une véritable révélation. Nous avons trouvé des machines, dont nous ne connaissions pas l'existence, qui contenaient des informations sensibles ou dont les services étaient connectés à Internet. » déclare-t-il. Armé des informations fournies par Orca, il a mis en place des analyses quotidiennes de toutes les adresses IP et machines virtuelles, même si elles ne sont pas connectées à Internet. « Nous avons besoin de bien comprendre ce dont nous disposons pour garantir la protection des actifs des clients, ainsi que de la propriété intellectuelle de NGDATA. »

Orca est un outil transformateur pour DevOps

Les développeurs NGDATA sont répartis dans le monde entier. Geirnaert explique : « Nous ne pouvons pas leur demander : « Avez-vous pensé à la sécurité ? Lorsque vous démarrez une nouvelle VM sur AWS, pouvez-vous me le faire savoir afin que je puisse l'analyser ? Pourriez-vous déployer un agent sur cette machine pour moi ? » Nous avons besoin d'une meilleure façon de travailler. Orca offre cette nouvelle et meilleure façon de travailler en éliminant toute cette friction organisationnelle.

« Je crois fermement à l'approche DevOps, puis au cloud natif et sans serveur, car cela contribuera à augmenter la sécurité sans avoir à former des développeurs à devenir des champions de la sécurité. Nous devons leur fournir des outils qui s'intègrent à la façon dont ils fonctionnent déjà. »

Faciliter la conformité aux réglementations et aux cadres de sécurité

Lorsque Geirnaert a débuté chez NGDATA, il a compilé une liste de meilleures pratiques basée sur le cadre de conformité du Centre pour la sécurité internet pour AWS. Il a utilisé la liste de 100 éléments comme un outil de gestion de projet pour attribuer des tâches. Il n'a plus besoin de cette liste.

« Lorsque nous lançons Orca, elle vérifie dynamiquement les exigences de conformité. Avant Orca, nous écrivions nous-mêmes de telles vérifications dans Sumo Logic. Lorsque nous examinions les événements provenant de la journalisation avec AWS CloudTrail, nous les capturions et les affichions dans les tableaux de bord. Maintenant, nous voyons tout automatiquement et immédiatement dans un seul tableau de bord Orca. »

La conformité au RGPD est facilitée car Orca recherche les données personnelles d'identification sur les serveurs et dans les fichiers. Orca aide à trouver les informations personnelles cachées et les endroits où elles devraient se trouver. En tant que responsable de la sécurité, Geirnaert n'a pas accès aux environnements de production, Orca lui donne donc une visibilité qu'il n'aurait pas en temps normal. En ce qui concerne les données personnelles d'identification, Orca est d'une aide précieuse pour orienter l'application de correctifs ou l'atténuation des problèmes.

Orca simplifie également le processus d'audit. « Nous pouvons facilement filtrer pour afficher où les données personnelles d'identification sont stockées. Comme tout est documenté, nous pouvons facilement montrer les preuves que les auditeurs demandent », déclare Geirnaert.

À propos d'Orca Security

Grâce à sa technologie SideScanning™ unique (brevet en instance), Orca Security assure la sécurité et la conformité à l'échelle du cloud et des charges de travail de services comme AWS, Azure et GCP. Après une intégration instantanée, en lecture seule et sans impact, au fournisseur de services cloud, il détecte les vulnérabilités, les logiciels malveillants, les mauvaises configurations, les risques de mouvement latéral, les risques d'authentification et les données non sécurisées à haut risque, puis hiérarchise les risques en fonction du problème sous-jacent, de son accessibilité et de son rayon d'action, sans déployer d'agents.

orca security

Connectez votre premier compte cloud en quelques minutes et voyez par vous-même : [consultez orca.security](orca.security)

© Copyright Orca Security 2021. Toutes les marques déposées, les marques de service et les noms de commerce référencés dans ce support appartiennent à leurs propriétaires respectifs.