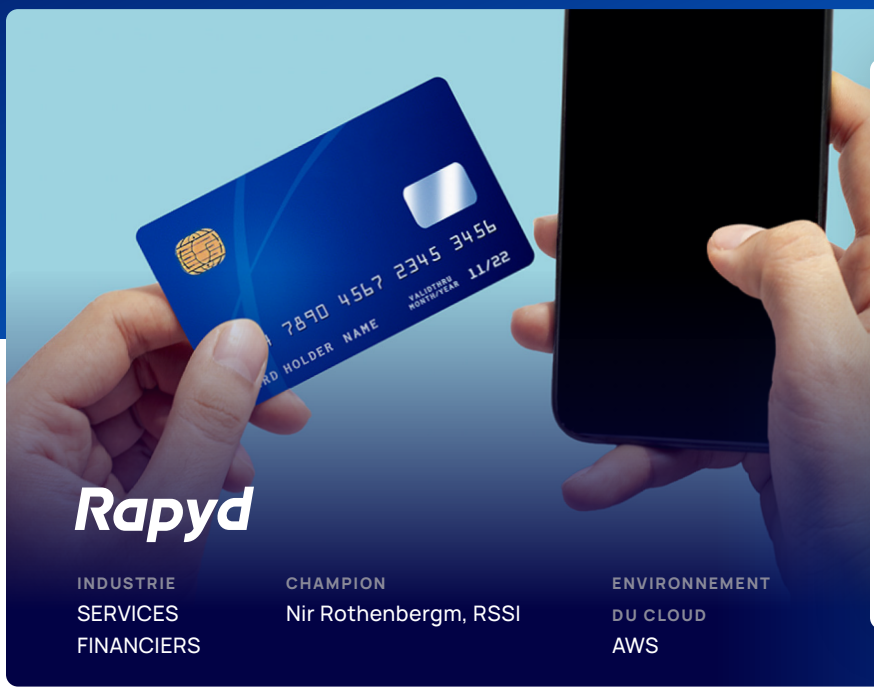
Rapyd utilise la visibilité approfondie du cloud d'Orca Security pour protéger les systèmes de paiement mondiaux



Rapyd

INDUSTRIE
SERVICES FINANCIERS

CHAMPION
Nir Rothenbergm, RSSI

ENVIRONNEMENT DU CLOUD
AWS

« Orca est formidable pour nous aider à travailler avec DevOps. Mon administrateur système peut maintenant montrer et expliquer à DevOps ce que nous avons trouvé. Nous sommes maintenant plus collaboratifs et utiles pour eux. C'est un grand pas vers DevSecOps : les frictions organisationnelles entre DevOps et mon équipe de sécurité ont disparu. »

Nir Rothenberg
RSSI
Rapyd

Défis de la sécurité du cloud

- Bénéficier d'une visibilité contextuelle complète pour exécuter la gestion prioritaire des correctifs ;
- Démontrer la bonne gouvernance et la conformité réglementaire aux auditeurs ;
- Simplification de la sécurité.

Résultats de la sécurité du cloud

- A obtenu une visibilité immédiate et complète de son infrastructure cloud ;
- A intégré Orca à Jira pour automatiser le pipeline CI/CD pour les tâches liées à la sécurité ;
- A créé un environnement collaboratif avec DevOps pour passer à DevSecOps.

Rapyd fait tomber les barrières des paiements universels

Rapyd s'attaque à la fragmentation qui existe dans l'industrie mondiale des paiements. Elle construit la technologie qui supprime les complexités de backend du commerce transfrontalier tout en fournissant une expertise en matière de paiements locaux.

Les entreprises mondiales d'e-commerce, les entreprises technologiques, les marketplaces et les institutions financières utilisent la plate-forme fintech-as-a-service de Rapyd pour intégrer de manière transparente et simple des capacités de fintech et de paiement localisées dans leurs applications. Le Rapyd Global Payments Network permet aux entreprises d'accéder au plus grand réseau de paiement local au monde, qui compte plus de 900 méthodes de paiement préférées localement. Celles-ci incluent les virements bancaires, les portefeuilles électroniques et les espèces dans plus de 100 pays.

Orca simplifie la gestion des correctifs

Chaque système de paiement numérique mondial doit aujourd'hui se concentrer sans relâche sur la sécurité. C'est ce qui anime Nir Rothenberg, le RSSI de Rapyd, qui gère les opérations informatiques et de sécurité. Bien que son entreprise ait mis en place de bonnes pratiques de sécurité, le prouver aux auditeurs a été un défi.

« Notre activité, ce sont les paiements, nous devons donc être conformes à la norme PCI DSS, et nous le sommes », déclare Rothenberg. « Chaque année, les auditeurs veulent voir que nous avons mis en place un bon processus de correction. Nous corrigeons sans relâche, mais ce n'est jamais à 100 % pour diverses raisons. La documentation pour montrer que nous maîtrisons cela était un vrai problème avant de trouver Orca. »

Rapyd fonctionne pleinement dans le cloud, avec tout sur AWS. Rothenberg voulait un outil intelligent pour fournir une visibilité complète sur les serveurs ayant vraiment besoin d'un correctif. Il a cherché une liste prioritaire avec tout dans son contexte. De nombreux outils peuvent analyser et répertorier ce qui nécessite un correctif, mais sans contexte, la liste est longue et une grande partie n'a pas de sens.

« Les outils AWS natifs manquent d'intelligence. Un analyseur AWS Inspector peut nous donner des résultats, mais ces résultats ne correspondent pas toujours à notre contexte », explique Rothenberg. « Nous obtiendrons une liste de mille correctifs, tous jugés critiques. Mais certains ne peuvent pas être déployés car ils ne correspondent pas à notre distribution, ou ils sont destinés aux serveurs hors ligne où les correctifs n'ont pas d'importance. Si je montre un tel rapport à un auditeur, il pensera que nous ne maîtrisons rien. Imaginons qu'il y a un serveur avec une vulnérabilité critique. Il y a un correctif qui fonctionne sur Ubuntu 18.4, mais nous avons 18.9. Donc, dans ce contexte, nous ne pouvons pas appliquer de correctif. Non seulement cela, mais le serveur n'est pas connecté à Internet, donc ce n'est pas vraiment important de toute façon. Orca nous dit : « Correctif critique, risque moyen. » Je peux montrer cela à un auditeur pour justifier nos actions. »

Rothenberg a évalué divers outils AWS, notamment GuardDuty, Inspector et Detective, ainsi que des outils de sécurité traditionnels basés sur des agents et des scanners de réseau. Il a appris qu'il faut beaucoup de frais généraux pour faire fonctionner ces outils, trop pour se rapprocher de ce qu'Orca livre tout de suite. « Pour les outils basés sur des agents, nous devions créer des serveurs, déployer un agent, écrire et exécuter des scripts, connaître notre environnement et configurer un tableau de bord pour montrer ce que nous voulons voir. Nous devions lui apprendre ce qui est et n'est pas un risque, et faire une grande partie du travail d'analyse nous-mêmes. Et nous devions toujours le peaufiner parce que le risque est dynamique ; ça change. Toutes ces étapes sont automatiques avec Orca. »

Orca identifie une non-conformité aux contrôles CIS et un risque pour les informations personnelles

Rothenberg supervise l'adhésion de Rapyd au Center for Internet Security Controls. Pour cela aussi, il a essayé les outils AWS natifs et les a trouvés insuffisants. « Nous devions découvrir par nous-mêmes ce que signifiaient leurs résultats d'analyse. Mais avec Orca, les résultats de l'analyse sont tous digérés et concentrés. Nous pouvons immédiatement voir la non-conformité au CIS que nous devrions traiter en premier. Lorsque nous avons intégré Orca à Jira, pour attribuer le travail aux DevOps, nous n'avons eu qu'à cliquer sur un bouton. »

Rothenberg affirme que la création de tickets est essentielle pour le suivi des tâches internes. « Connaissant à tout moment les tâches et les risques associés, nous pouvons prioriser ce que nous envoyons au DevOps afin qu'ils ne soient pas submergés. Si nous sommes audités, nous pouvons montrer : « C'est notre pipeline, c'est notre plan de travail. ». Tout est dans Jira et tout a une piste d'audit. »

Le RSI se tourne également vers Orca pour identifier les situations où les données personnelles d'identification sont à risque dans des fichiers qui pourraient ne pas être correctement protégés. « En tant qu'entreprise de paiement, nous sommes très sensibles à l'exposition aux données personnelles d'identification. Si un serveur contient des informations personnelles ou si des clés de chiffrement sont exposées, Orca les détecte immédiatement et nous indique les risques en fonction de cette machine et de l'actif spécifique. Nous sommes en mesure de remédier rapidement à l'incident. »

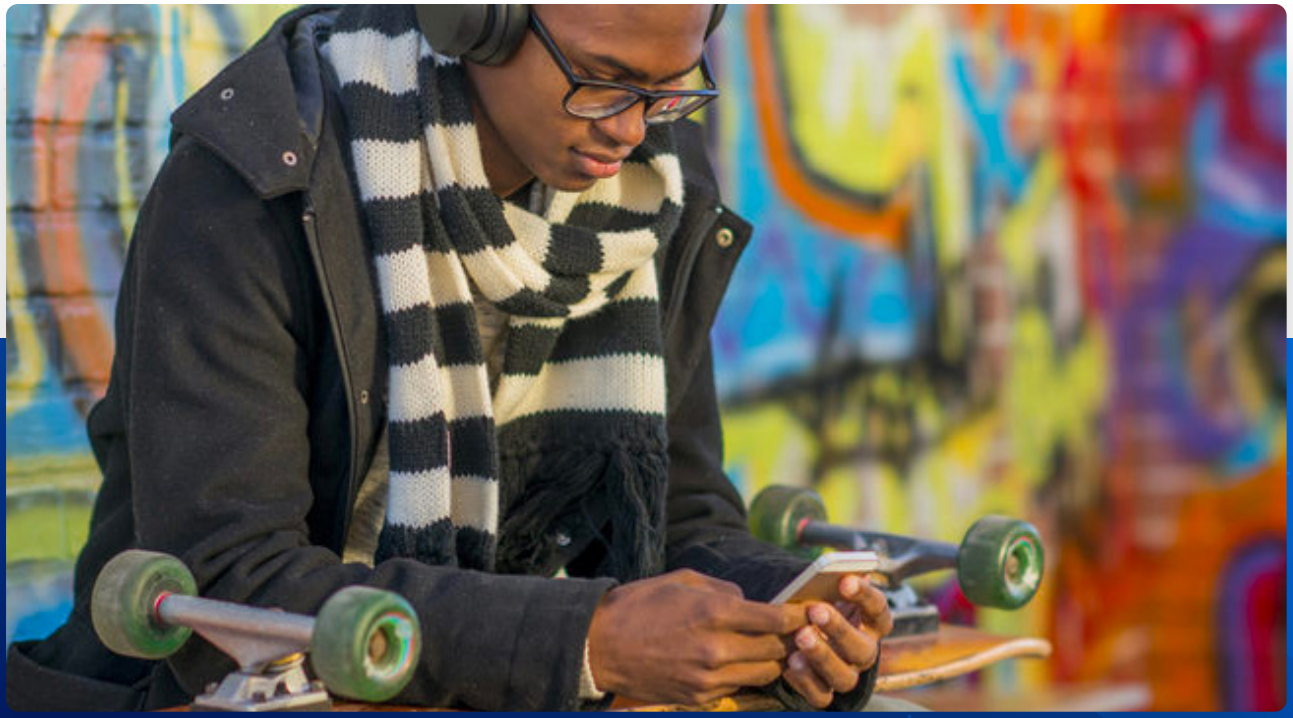
Au cours des années précédentes, Rapyd suivait les vulnérabilités dans les feuilles de calcul Excel. Orca a éliminé ce processus. « Désormais, tout est automatisé et dispose d'un pipeline CI/CD. La prochaine fois que nous serons confrontés à un audit, je pourrai montrer nos rapports Orca et Jira pour montrer les risques que nous suivons et ce que nous faisons pour y remédier », explique Rothenberg. « Avec la façon dont nous surveillons nos actifs aujourd'hui, il devient très simple de démontrer l'application de correctifs et la conformité. »

> « Les analyses d'Orca renvoient un rapport significatif et exploitable qui met tout en contexte. Outre ses conclusions, elle fournit des considérations secondaires pour guider notre processus de gestion des correctifs. »
>
> **Nir Rothenberg**
> Directeur de la sécurité informatique
> Rapyd

La simplicité mène à une meilleure sécurité

Orca a simplifié la vie de l'équipe de sécurité de Rothenberg. « Juste après avoir connecté Orca à notre environnement, elle a immédiatement trouvé beaucoup de choses intéressantes. Sans Orca, nous n'aurions jamais cette visibilité. »

« Orca est formidable pour nous aider à travailler avec DevOps », déclare Rothenberg. « Mon administrateur système peut désormais parler directement à DevOps. Il peut expliquer ce que nous avons trouvé, il peut leur montrer. Cela nous aide à devenir plus professionnels, à mieux voir l'environnement, à mieux le comprendre. Désormais, nous collaborons davantage avec DevOps et nous leur sommes plus utiles. C'est une véritable étape vers DevSecOps. Désormais, nous sommes une machine bien huilée. La friction organisationnelle entre Sécurité et DevOps a disparu. »



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 cloud, elle détecte les vulnérabilités, les logiciels malveillants, les mauvaises configurations, le risque de mouvement latéral, le risque d'authentification et les données à haut risque non sécurisées, puis hiérarchise le risque en fonction du problème sous-jacent, son accessibilité et le rayon d'explosion, tout cela sans déployer d'agents.

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